International Journal of Applied Mathematics

Volume 31 No. 4 2018, 549-585
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
doi: http://dx.doi.org/10.12732/ijam.v31i4.4

CONSTRUCTION OF COMPLEX NESTED IDEAL LATTICES FOR COMPLEX-VALUED CHANNEL QUANTIZATION

C. C. Trinca Watanabe [1 §], J.-C. Belfiore [2],
E. D. De Carvalho [3], J. Vieira Filho [4],
R. Palazzo Jr. [1], R. A. Watanabe [5]

[1] Department of Communications (DECOM)
Campinas State University
Campinas-SP, 13083-852, BRAZIL

[2] Department of Communications and Electronics
Télécom ParisTech
Paris, 75013, FRANCE

[3] Department of Mathematics
São Paulo State University
Ilha Solteira-SP, 15385-000, BRAZIL

[4] Telecommunications Engineering
São Paulo State University
São João da Boa Vista-SP, 13876-750, BRAZIL

[5] Institute of Mathematics, Statistics and
Scientific Computation (IMECC)
Campinas State University
Campinas-SP, 13083-852, BRAZIL

Abstract: In this work we develop a new algebraic methodology which quantizes complex-valued channels in order to realize interference alignment (IA) onto a complex ideal lattice. Also we make use of the minimum mean square error (MMSE) criterion to estimate complex-valued channels contaminated by additive Gaussian noise.

Received: March 14, 2018

[§]Correspondence author

AMS Subject Classification: 03G10, 06B05, 06B10, 11RXX, 13F10, 97N20
Key Words: complex ideal lattices; nested lattices; binary cyclotomic field; principal ideal rings; channel quantization

1. Introduction

In this work we make use of rotated complex lattices constructed through extension fields to develop a new algebraic methodology to perform a complex-valued channel quantization in order to realize interference alignment (IA) [1] onto a complex ideal lattice.

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

$$y_m = \sum_{l=1}^{L} h_{ml} x_l + z_m, \tag{1.1}$$

where $h_{ml} \in \mathbb{C}$ are complex-valued channel coefficients, x_l is a complex lattice point whose message space presents a uniform distribution and z_m is an i.i.d. circularly symmetric complex Gaussian noise. Figure 1 illustrates the corresponding channel model.

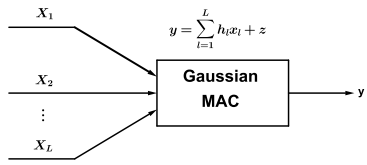

Figure 1: A Gaussian Multiple-Access Channel

Calderbank and Sloane [2] made the important observations that the signal constellation should be regarded as a finite set of points taken from an infinite lattice and the partitioning of the constellation into subsets corresponds to the

partitioning of that lattice into a sublattice and its cosets. We call this general class of coded modulation schemes coset codes.

There is a great number of works based on coset codes and their applications in communications. It is not possible to discuss all of them here, but the references [3] and [4] are great indications for the interested reader.

In the literature we have that $\mathbb{Z}[\xi_{2^r}]$ is the ring of integers of the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$, where ξ_{2^r} denotes the 2^r-th root of unity and $r \geq 3$. Therefore, Giraud et al. [5] show that an algebraic lattice can be associated to this ring of integers $\mathbb{Z}[\xi_{2^r}]$ and this lattice is a scaled version of the $\mathbb{Z}[i]^n$-lattice, where $n = 2^{r-2}$.

In this work we develop a new algebraic methodology which quantizes complex-valued channels in order to realize interference alignment (IA) [1] onto a complex ideal lattice and our channel model is given by equation (1.1). The coding scheme only requires that each relay knows the channel coefficients from each transmitter to itself.

In this new methodology we make use of the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$, where $r \geq 3$, to provide a doubly infinite nested lattice partition chain for any dimension $n = 2^{r-2}$, where $r \geq 3$, in order to quantize complex-valued channels onto these nested lattices. Such complex ideal lattices are described by their corresponding construction A which furnishes us, in this case, nested lattice codes (coset codes). It is very important that the channel gain does not remove the lattice from the initial chain of nested lattices, then we show the existence of periodicity in the corresponding nested lattice partition chains.

After developing such a methodology, we also develop a precoding to ensure onto which lattice a given complex-valued channel must be quantized.

The concept of mean square error has assumed a central role in the theory and practice of estimation since the time of Gauss and Legendre. In particular, minimization of mean square error underlies numerous methods in statistical sciences. In this paper, we make use of the minimum mean square error (MMSE) criterion to estimate complex-valued channels contaminated by additive Gaussian noise.

In the following section we provide a quick preview of the concepts related to coset codes and complex ideal lattices that will figure in the rest of the paper.

2. Preliminaries

Lattices have been very useful in applications in communication theory and, in this work, we use lattices in order to realize interference alignment. In this

section we present basic concepts of the lattice theory.

Definition 1. *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*

$$\Lambda = \{x = \sum_{i=1}^{m} \lambda_i v_i, \text{ where } \lambda_i \in \mathbb{Z}\} \tag{2.1}$$

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 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, and its corresponding $\frac{n}{2}$-dimensional complex lattice is given by $\mathbb{Z}[i]^{\frac{n}{2}}$.

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 $\mathbb{R}^n$ [3].

A sublattice Λ' of Λ is a subset of the points of Λ which is itself an n-dimensional lattice. The sublattice induces a partition Λ/Λ' of Λ into $|\Lambda/\Lambda'|$ cosets of Λ', where $|\Lambda/\Lambda'|$ is the order of the partition.

The coset code $\mathcal{C}(\Lambda/\Lambda'; C)$ is the set of all sequences of signal points that lie within a sequence of cosets of Λ' that could be specified by a sequence of coded bits from C. Some lattices, including the most useful ones, can be generated as lattice codes $\mathcal{C}(\Lambda/\Lambda'; C)$, where C is a binary block code. If C is a convolutional encoder, then $\mathcal{C}(\Lambda/\Lambda'; C)$ is a trellis code [3].

A lattice code $\mathcal{C}(\Lambda/\Lambda'; C)$, where C is a binary block code, is defined as the set of all coset leaders in Λ/Λ', i.e.,

$$\mathcal{C}(\Lambda/\Lambda'; C) = \Lambda \bmod \Lambda' = \{\lambda \bmod \Lambda' \ : \ \lambda \in \Lambda\}. \tag{2.2}$$

Geometrically, $\mathcal{C}(\Lambda/\Lambda'; C)$ is the intersection of the lattice Λ with the fundamental region $\mathcal{R}_{\Lambda'}$ [3], i.e.,

$$\mathcal{C}(\Lambda/\Lambda'; C) = \Lambda \cap \mathcal{R}_{\Lambda'}. \tag{2.3}$$

For this reason, the fundamental region $\mathcal{R}_{\Lambda'}$ is often interpreted as the *shaping region*. Note that there is a bijection between Λ/Λ' and $\mathcal{C}(\Lambda/\Lambda'; C)$; in particular,

$$|\Lambda/\Lambda'| = |\mathcal{C}(\Lambda/\Lambda'; C)|. \tag{2.4}$$

A lattice Λ is said to be *nested* in a lattice Λ' if $\Lambda \subseteq \Lambda'$. We refer to Λ as the coarse lattice and Λ' as the fine lattice. More generally, a sequence of lattices $\Lambda, \Lambda_1, \ldots, \Lambda_P$ is nested if $\Lambda \subseteq \Lambda_1 \subseteq \cdots \subseteq \Lambda_P$. Observe that nested lattices induce nested lattice codes.

In [3] an n-dimensional real lattice Λ is a *mod-2 binary lattice* if and only if it is the set of all integer n-tuples that are congruent modulo 2 to one of the codewords c in a linear binary (n, k) block code C. *Mod-2 binary lattices* are essentially isomorphic to linear binary block codes and this is "*Construction A*" of Leech and Sloane [6].

We call *complex lattice* a $\mathbb{Z}[i]$-lattice

$$\Lambda^c = \{x = \lambda M \ : \ \lambda \in \mathbb{Z}[i]^n\}, \tag{2.5}$$

where M is the *lattice generator matrix* and MM^H is the *Gram matrix*, where H denotes the transpose conjugate.

Complex algebraic lattices can be obtained by using the relative canonical embedding of a number field. Let L be a Galois extension of degree n over $\mathbb{Q}(i)$. We denote by $Gal(L/\mathbb{Q}(i)) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ the Galois group of L over $\mathbb{Q}(i)$ and define the *relative canonical embedding* of L into $\mathbb{C}^n$ as

$$\sigma : L \to \mathbb{C}^n, \text{ where } \sigma(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x)). \tag{2.6}$$

Let O_L be the ring of integers of L. Since $\mathbb{Z}[i]$ is principal, there exists a $\mathbb{Z}[i]$-basis $\mathcal{B}_L = \{w_1, w_2, \ldots, w_n\}$. The generator matrix of the complex algebraic lattice $\Lambda^c(O_L)$ is obtained by applying the relative canonical embedding to the basis of O_L

$$N = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_n(w_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_n(w_n) \end{pmatrix}. \tag{2.7}$$

We now generalize the definition of ideal lattices to the complex case.

Definition 2. *[7] Let $L/\mathbb{Q}(i)$ be a Galois extension of degree n over $\mathbb{Q}(i)$. A complex ideal lattice is a $\mathbb{Z}[i]$-lattice $\Lambda^c = (\mathcal{I}, q)$, where $\mathcal{I}$ is an O_L-ideal and*

$$q : \mathcal{I} \times \mathcal{I} \to \mathbb{Z}[i], \ q(x, y) = Tr_{L/\mathbb{Q}(i)}(x\bar{y}), \ \ \forall \ x, y \in \mathcal{I}, \tag{2.8}$$

where $\bar{}$ denotes the complex conjugation.

When considering complex ideal lattices, the Gram matrix MM^H must be an Hermitian trace form.

Lemma 1. *The matrix N defined, as in (2.7), by embedding the basis $\mathcal{B}_{\mathcal{I}} = \{\nu_1, \nu_2, \ldots, \nu_n\}$ of the ideal $\mathcal{I} \subseteq O_L$*

$$N = \begin{pmatrix} \sigma_1(\nu_1) & \cdots & \sigma_n(\nu_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\nu_n) & \cdots & \sigma_n(\nu_n) \end{pmatrix} \tag{2.9}$$

is the generator matrix of a complex ideal lattice if and only if the complex conjugation commutes with all the other embeddings.

Proof. See [7], page 323. □

If L is a totally complex field containing a totally real field K such that $[L : K] = 2$ (we say that L is a *complex multiplication field-CM field*), then it can be shown that the complex conjugation commutes with all σ_i (see, for example, [8]-Ch. 1).

3. Construction of Complex Nested Lattices from the Binary Cyclotomic Field $\mathbb{Q}(\xi_{2^r})$ in Order to Realize Interference Alignment

In order to realize interference alignment onto a lattice we need to quantize the channel coefficients h_{ml}. Thereby, in this section, we describe a way to find a doubly infinite nested lattice partition chain for any dimension $n = 2^{(r-2)}$, with $r \geq 3$, in order to quantize the channel coefficients. For that, we make use of the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$, with $r \geq 3$, $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}] = \varphi(2^r) = 2^{(r-1)}$, where φ is the Euler function, and $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}(i)] = 2^{(r-2)} = n$. Hence we provide a new algebraic methodology to quantize complex-valued channels.

Such lattices are complex ideal lattices that are described by their corresponding construction A which furnishes us, in this case, nested lattice codes (nested coset codes).

In [9] and [10] we have two examples of channel quantization. For the corresponding quantizations, we make use of the binary cyclotomic fields $\mathbb{Q}(\xi_8)$ and $\mathbb{Q}(\xi_{16})$, respectively. These examples are related to the complex dimensions 2 and 4, respectively.

3.1. Quantization of complex-valued channels onto a lattice

Suppose that our interference channel is complex-valued, specifically $h_{ml} \in \mathbb{C}$. We also suppose that all lattices used by the legitimate user and the interferers are one of a certain lattice partition chain which is extended by periodicity.

In this section we consider n-dimensional complex-valued vectors, where $n = 2^{r-2}$ and $r \geq 3$. Now we show, for a given user, how its codeword can be transformed so that we can perform the channel quantization and, for that, we make use of the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$, where $r \geq 3$.

In fact, consider the following Galois extensions, where $r \geq 3$:

$$\begin{array}{c} \mathbb{Q}(\xi_{2^r}) \\ \Big| \, 2^{(r-2)} \\ \mathbb{Q}(i) \\ \Big| \, 2 \\ \mathbb{Q} \end{array} \tag{3.1}$$

As $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}] = \varphi(2^r) = 2^{(r-1)}$, 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

$$Gal(\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)) = \{\sigma_1 = id : \mathbb{Q}(\xi_{2^r}) \to \mathbb{Q}(\xi_{2^r}), \sigma_2, \sigma_3, \ldots, \sigma_{2^{(r-2)}}\}$$

and

$$Gal(\mathbb{Q}(i)/\mathbb{Q}) = \{\sigma_1 = id : \mathbb{Q}(i) \to \mathbb{Q}(i) \text{ and } \sigma_2 : \mathbb{Q}(i) \to \mathbb{Q}(i), \text{ where } \sigma_2(i) = -i, \text{ respectively}\}. \tag{3.2}$$

By [7] we have that $\mathbb{Q}(\xi_{2^r}) = \mathbb{Q}(\xi_{2^r} + \xi_{2^r}^{-1})\mathbb{Q}(i)$ and $\mathbb{Z}[\xi_{2^r}]$, the ring of integers of $\mathbb{Q}(\xi_{2^r})$, is a free $\mathbb{Z}[i]$-module of rank $2^{(r-2)}$. Besides, the following set

$$\{1, \xi_{2^r}, \xi_{2^r}^2, \ldots, \xi_{2^r}^{(2^{(r-2)}-1)}\} \tag{3.3}$$

is a $\mathbb{Z}[i]$-basis of $\mathbb{Z}[\xi_{2^r}]$.

As $\{1, \xi_{2^r}, \xi_{2^r}^2, \ldots, \xi_{2^r}^{(2^{(r-2)}-1)}\}$ is a $\mathbb{Z}[i]$-basis of $\mathbb{Z}[\xi_{2^r}]$, then the matrix

$$M = \begin{pmatrix} \sigma_1(1) & \sigma_1(\xi_{2^r}) & \sigma_1(\xi_{2^r}^2) & \ldots & \sigma_1(\xi_{2^r}^{(2^{(r-2)}-1)}) \\ \sigma_2(1) & \sigma_2(\xi_{2^r}) & \sigma_2(\xi_{2^r}^2) & \ldots & \sigma_2(\xi_{2^r}^{(2^{(r-2)}-1)}) \\ \sigma_3(1) & \sigma_3(\xi_{2^r}) & \sigma_3(\xi_{2^r}^2) & \ldots & \sigma_3(\xi_{2^r}^{(2^{(r-2)}-1)}) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_{2^{r-2}}(1) & \sigma_{2^{r-2}}(\xi_{2^r}) & \sigma_{2^{r-2}}(\xi_{2^r}^2) & \ldots & \sigma_{2^{r-2}}(\xi_{2^r}^{(2^{(r-2)}-1)}) \end{pmatrix} \tag{3.4}$$

is a generator matrix of the complex algebraic lattice $\sigma(\mathbb{Z}[\xi_{2^r}])$ [7].

Now since $M_0 = \frac{1}{2^{((r-2)/2)}}M$ is a unitary matrix, then $\sigma(\mathbb{Z}[\xi_{2^r}])$ is isomorphic to the $\mathbb{Z}[i]^{2^{(r-2)}}$-lattice [7].

At the receiver, suppose that we apply M_0 to the received vector (1.1) to obtain

$$\bar{y}_m = M_0 y_m = \sum_{l=1}^{L} h_{ml} M_0 x_l + M_0 z_m. \tag{3.5}$$

As z_m is an i.i.d. circularly symmetric complex Gaussian noise and M_0 is a unitary matrix, then the noise in (3.5) is also i.i.d. circularly symmetric complex Gaussian. Now observe the vectors of the form $h_{ml}M_0x_l$, then we can rewrite it as

$$\begin{pmatrix} h_{ml} & 0 & \cdots & 0 \\ 0 & h_{ml} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h_{ml} \end{pmatrix} \cdot M_0 \cdot x_l = H_{ml} \cdot M_0 \cdot x_l. \tag{3.6}$$

The idea we want to develop is to quantize the diagonal matrix H_{ml} by a diagonal matrix whose elements are components of the canonical embedding of the power (positive or negative) of an element of $\mathbb{Z}[\xi_{2^r}]$ with absolute algebraic norm equal to 2.

Observe that $N_{\mathbb{Q}(i)/\mathbb{Q}}(1+i) = (1+i)(1-i) = 2$ and $(1-i)^2 = 2(-i)$. As $-i$ is a unit in $\mathbb{Q}(i)$, then $2\mathbb{Z}[i] = (1-i)^2$ in $\mathbb{Z}[i]$. So 2 is totally ramified in $\mathbb{Q}(i)$.

In [9] and [10] we have

$$N_{\mathbb{Q}(\xi_8)/\mathbb{Q}(i)}(1+\xi_8) = N_{\mathbb{Q}(\xi_{16})/\mathbb{Q}(i)}(1+\xi_{16}) = 1-i. \tag{3.7}$$

Now we can show, by induction over r, that $N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1+\xi_{2^r}) = 1-i$. In fact, consider the following Galois extensions:

$$\begin{array}{c} \mathbb{Q}(\xi_{2^{r+1}}) \\ \Big| 2 \\ \mathbb{Q}(\xi_{2^r}) \\ \Big| 2^{(r-2)} \\ \mathbb{Q}(i) \\ \Big| 2 \\ \mathbb{Q} \end{array} \tag{3.8}$$

Notice that it is easy to verify that $\xi_{2^{r+1}}^2 = \xi_{2^r}$, for all $r \geq 3$. Suppose, by induction, that $N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1+\xi_{2^r}) = 1-i$ and let us prove it for $r+1$. Then

$$N_{\mathbb{Q}(\xi_{2^{r+1}})/\mathbb{Q}(i)}(1+\xi_{2^{r+1}}) = N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(N_{\mathbb{Q}(\xi_{2^{r+1}})/\mathbb{Q}(\xi_{2^r})}(1+\xi_{2^{r+1}}))$$

$$= N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}((1+\xi_{2^{r+1}})(1-\xi_{2^{r+1}})) = N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1-\xi_{2^{r+1}}^2)$$

$$= N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1-\xi_{2^r}) = 1-i. \tag{3.9}$$

Thus 2 is totally ramified in $\mathbb{Q}(\xi_{2^r})$ and $2\mathbb{Z}[\xi_{2^r}] = (2) = \Im^{2^{(r-1)}}$, where $\Im = (1+\xi_{2^r})$.

We have that $\Im$ is the ideal in $\mathbb{Z}[\xi_{2^r}]$ generated by $1+\xi_{2^r}$. Hence the ideal $\Im^k$ is generated by $(1+\xi_{2^r})^k$, for all $k \in \mathbb{Z}$. Observe that, for $k=0$, we have $\Im^0 = \mathbb{Z}[\xi_{2^r}]$.

Now we approximate the matrix H_{ml} with the canonical embedding of the generator $(1+\xi_{2^r})^k$ of $\Im^k$, where $k \in \mathbb{Z}$, and we make use of the following proposition.

Proposition 1. *We have that*

$$\{(1+\xi_{2^r})^k, (1+\xi_{2^r})^k\xi_{2^r}, (1+\xi_{2^r})^k\xi_{2^r}^2, \ldots, (1+\xi_{2^r})^k\xi_{2^r}^{n-1}\}$$

is a $\mathbb{Z}[i]$*-basis of* $(1+\xi_{2^r})^k\mathbb{Z}[\xi_{2^r}]$*, where* $n = 2^{(r-2)}$.

Proof. Let $x \in (1+\xi_{2^r})^k\mathbb{Z}[\xi_{2^r}]$, then $x = (1+\xi_{2^r})^k\alpha$, where $\alpha \in \mathbb{Z}[\xi_{2^r}]$. Thus

$$x = (1+\xi_{2^r})^k(a_0 + a_1\xi_{2^r} + a_2\xi_{2^r}^2 + \ldots + a_{n-1}\xi_{2^r}^{n-1}),$$

where $a_i \in \mathbb{Z}[i]$, $i = 0, 1, \ldots, n-1$, if, and only if,

$$x = a_0(1+\xi_{2^r})^k + a_1(1+\xi_{2^r})^k\xi_{2^r} + a_2(1+\xi_{2^r})^k\xi_{2^r}^2 + \ldots + a_{n-1}(1+\xi_{2^r})^k\xi_{2^r}^{n-1},$$

where $a_i \in \mathbb{Z}[i]$, $i = 0, 1, \ldots, n-1$.

Hence $\{(1+\xi_{2^r})^k, (1+\xi_{2^r})^k\xi_{2^r}, \ldots, (1+\xi_{2^r})^k\xi_{2^r}^{n-1}\}$ generates $(1+\xi_{2^r})^k\mathbb{Z}[\xi_{2^r}]$. We prove now that

$$\{(1+\xi_{2^r})^k, (1+\xi_{2^r})^k\xi_{2^r}, \ldots, (1+\xi_{2^r})^k\xi_{2^r}^{n-1}\}$$

is linearly independent and we use the fact that the set

$$\{1, \xi_{2^r}, \xi_{2^r}^2, \ldots, \xi_{2^r}^{n-1}\}$$

is a $\mathbb{Z}[i]$-basis of $\mathbb{Z}[\xi_{2^r}]$. In fact, let $a_i \in \mathbb{Z}[i]$, with $i = 0, 1, \ldots, n-1$, then

$$a_0(1+\xi_{2^r})^k + a_1(1+\xi_{2^r})^k\xi_{2^r} + \ldots + a_{n-1}(1+\xi_{2^r})^k\xi_{2^r}^{n-1} = 0 \Leftrightarrow$$

$$\Leftrightarrow a_0(1+\xi_{2^r})^k(1+\xi_{2^r})^{-k} + a_1(1+\xi_{2^r})^k(1+\xi_{2^r})^{-k}\xi_{2^r}$$

$$+ \ldots + a_{n-1}(1+\xi_{2^r})^k(1+\xi_{2^r})^{-k}\xi_{2^r}^{n-1} = 0 \Leftrightarrow$$

$$\Leftrightarrow a_0 + a_1\xi_{2^r} + \ldots + a_{n-1}\xi_{2^r}^{n-1} = 0 \Leftrightarrow a_i = 0,\ \forall\ i = 0, 1, \ldots, n-1,$$

so $\{(1+\xi_{2^r})^k, (1+\xi_{2^r})^k\xi_{2^r}, \ldots, (1+\xi_{2^r})^k\xi_{2^r}^{n-1}\}$ is a $\mathbb{Z}[i]$-basis of $(1+\xi_{2^r})^k\mathbb{Z}[\xi_{2^r}]$. □

Then, by Proposition 1, we have that a generator matrix of the complex algebraic lattice $\sigma((1+\xi_{2^r})^k\mathbb{Z}[\xi_{2^r}])$ is given by

$$M_k = \begin{pmatrix} (1+\xi_{2^r})^k & (1+\xi_{2^r})^k\xi_{2^r} & \cdots & (1+\xi_{2^r})^k\xi_{2^r}^{n-1} \\ \sigma_2((1+\xi_{2^r})^k) & \sigma_2((1+\xi_{2^r})^k\xi_{2^r}) & \cdots & \sigma_2((1+\xi_{2^r})^k\xi_{2^r}^{n-1}) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_n((1+\xi_{2^r})^k) & \sigma_n((1+\xi_{2^r})^k\xi_{2^r}) & \cdots & \sigma_n((1+\xi_{2^r})^k\xi_{2^r}^{n-1}) \end{pmatrix}$$

$$= \begin{pmatrix} (1+\xi_{2^r})^k & 0 & \cdots & 0 \\ 0 & \sigma_2((1+\xi_{2^r})^k) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \sigma_n((1+\xi_{2^r})^k) \end{pmatrix} \cdot M. \qquad (3.10)$$

Since $M_0 = \frac{1}{2^{((r-2)/2)}}M$ and M generate the same lattice and by comparing the equations (3.10) and (3.6), then the conclusion is that the matrix H_{ml} can be approximated by

$$M_k' = \begin{pmatrix} (1+\xi_{2^r})^k & 0 & \cdots & 0 \\ 0 & \sigma_2((1+\xi_{2^r})^k) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \sigma_n((1+\xi_{2^r})^k) \end{pmatrix}. \qquad (3.11)$$

Consequently the diagonal matrix H_{ml} is quantized by the diagonal matrix M_k' whose elements are components of the canonical embedding of the power (positive or negative) of an element of $\mathbb{Z}[\xi_{2^r}]$ with absolute algebraic norm equal to 2.

Now, by using the concept of equivalent lattices, observe that

$$M_k'M = \begin{pmatrix} (1+\xi_{2^r})^k & 0 & \cdots & 0 \\ 0 & \sigma_2((1+\xi_{2^r})^k) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \sigma_n((1+\xi_{2^r})^k) \end{pmatrix} \cdot M$$

$$= MM_{(1+\xi_{2^r})^k}, \tag{3.12}$$

where $M_{(1+\xi_{2^r})^k}$ is an $n \times n$ matrix whose entries belong to the ring $\mathbb{Z}[i]$; this means that if $(1+\xi_{2^r})^k$ generates the ideal $(1+\xi_{2^r})^k\mathbb{Z}[\xi_{2^r}]$, then the matrix $M_{(1+\xi_{2^r})^k}$ 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

$$\begin{pmatrix} 1+\xi_{2^r} & 0 & \cdots & 0 \\ 0 & \sigma_2(1+\xi_{2^r}) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \sigma_n(1+\xi_{2^r}) \end{pmatrix} \cdot M = MM_{(1+\xi_{2^r})}, \tag{3.13}$$

then we can see, by induction, that $M'_k M = M(M_{(1+\xi_{2^r})})^k$, for $k \geq 1$; that is, $M_{(1+\xi_{2^r})^k} = (M_{(1+\xi_{2^r})})^k$, for $k \geq 1$.

Now in the following section we present a method that describes for any dimension $n = 2^{r-2}$, with $r \geq 3$, a doubly infinite nested lattice partition chain in order to quantize complex-valued channels onto a lattice, that is, in order to realize interference alignment onto a lattice and, for that, we make use of the Pascal's triangle modulo 2.

3.2. Construction of complex nested ideal lattices from the channel quantization

In [9] and [10] we have that the lattice partition chains related to $r=3$ ($n=2$) and $r=4$ ($n=4$) are given by

$$\cdots \supset (1+i)^{-1}\mathbb{Z}[i]^2 \supset (1+i)^{-1}D_4 \supset \mathbb{Z}[i]^2 \supset D_4 \supset (1+i)\mathbb{Z}[i]^2 \supset$$

$$\supset (1+i)D_4 \supset 2\mathbb{Z}[i]^2 \supset \cdots \tag{3.14}$$

and

$$\cdots \supset ((1+i)\mathbb{Z}[i]^4)^* \supset (\Lambda')^* \supset \Lambda^* \supset D_8^* \supset \mathbb{Z}[i]^4 \supset D_8 \supset \Lambda \supset$$

$$\supset \Lambda' \supset (1+i)\mathbb{Z}[i]^4 \supset \cdots, \tag{3.15}$$

respectively, where $*$ denotes the dual of a lattice.

Here we describe a way to find a doubly infinite nested lattice partition chain for any dimension $n = 2^{r-2}$, where $r \geq 3$. For that, consider the following

Galois extensions:

$$\begin{array}{c} \mathbb{Q}(\xi_{2^r}) \\ \Big| 2 \\ \mathbb{Q}(\xi_{2^{r-1}}) \\ \Big| 2^{(r-3)} \\ \mathbb{Q}(i) \\ \Big| 2 \\ \mathbb{Q} \end{array} \tag{3.16}$$

Let $\Im = (1+\xi_{2^r}) = (1+\xi_{2^r})\mathbb{Z}[\xi_{2^r}]$ and $\mathcal{J} = (1+\xi_{2^{r-1}}) = (1+\xi_{2^{r-1}})\mathbb{Z}[\xi_{2^{r-1}}]$, where $\mathbb{Z}[\xi_{2^r}]$ and $\mathbb{Z}[\xi_{2^{r-1}}]$ are the rings of integers of $\mathbb{Q}(\xi_{2^r})$ and $\mathbb{Q}(\xi_{2^{r-1}})$, respectively. Also, let σ and τ be the canonical embeddings of the ideals in $\mathbb{Q}(\xi_{2^r})$ and $\mathbb{Q}(\xi_{2^{r-1}})$, respectively.

We have $\xi_{2^r}^2 = \xi_{2^{r-1}}$, $\Im^k = ((1+\xi_{2^r})^k) = (1+\xi_{2^r})^k\mathbb{Z}[\xi_{2^r}]$, $\mathcal{J}^k = ((1+\xi_{2^{r-1}})^k) = (1+\xi_{2^{r-1}})^k\mathbb{Z}[\xi_{2^{r-1}}]$, where $k \in \mathbb{Z}$, and, due to the ideal ramification, $\Im^2 = \mathcal{J}$.

The following theorem shows us, for any $r \geq 3$, that the lattice related to the canonical embedding of the ideal $\Im^k$, where $k = 1$, is given by the lattice D_{2n}, where $n = 2^{(r-2)}$.

Theorem 1. *We have, for $k = 1$, that $\sigma(\Im) = D_{2n}$, where $n = 2^{(r-2)}$.*

Proof. See Appendix 1. □

From now on we explain how to obtain, for any $r \geq 3$, the construction A of the lattices related to the canonical embedding of the ideals $\Im^k$, where $k = 1, 2, 3, \ldots, n-1$. For that, we make use of the following proposition:

Proposition 2. *Let $\Lambda = ((1+i)\mathbb{Z}[i]^n + C) \cup (((1+i)\mathbb{Z}[i]^n + C) + c)$, where Λ is an n-dimensional lattice, C is a linear binary block code and c is an n-dimensional binary vector. Then $\Lambda = (1+i)\mathbb{Z}[i]^n + C'$, 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 $c_1, c_2, \ldots, c_l$ and $c_1, c_2, \ldots, c_l, c$ are the rows of the matrices M_C and $M_{C'}$, respectively, that is, the sets

$$\{c_1, c_2, \ldots, c_l\} \text{ and } \{c_1, c_2, \ldots, c_l, c\}$$

are the basis of the linear binary block codes C and C', respectively.

We have to prove that

$$\Lambda = ((1+i)\mathbb{Z}[i]^n + C) \cup (((1+i)\mathbb{Z}[i]^n + C) + c) = (1+i)\mathbb{Z}[i]^n + C'.$$

In fact, if $x \in (1+i)\mathbb{Z}[i]^n + C'$, then

$$x = \lambda + (a_1c_1 + a_2c_2 + \cdots + a_lc_l + a_{l+1}c),$$

where $\lambda \in (1+i)\mathbb{Z}[i]^n$ and $a_i \in \{0,1\}$, for $i = 1, 2, \ldots, l+1$. So if $a_{l+1} = 0$, then $x \in (1+i)\mathbb{Z}[i]^n + C$ and if $a_{l+1} = 1$, then $x \in ((1+i)\mathbb{Z}[i]^n + C) + c$. Hence, either $x \in (1+i)\mathbb{Z}[i]^n + C$ or $x \in ((1+i)\mathbb{Z}[i]^n + C) + c$, that is, $x \in ((1+i)\mathbb{Z}[i]^n + C) \cup (((1+i)\mathbb{Z}[i]^n + C) + c)$. Then we can conclude that

$$((1+i)\mathbb{Z}[i]^n + C') \subset (((1+i)\mathbb{Z}[i]^n + C) \cup (((1+i)\mathbb{Z}[i]^n + C) + c).$$

It is trivial that $((1+i)\mathbb{Z}[i]^n + C) \cup (((1+i)\mathbb{Z}[i]^n + C) + c) \subset ((1+i)\mathbb{Z}[i]^n + C')$, then $\Lambda = ((1+i)\mathbb{Z}[i]^n + C) \cup (((1+i)\mathbb{Z}[i]^n + C) + c) = (1+i)\mathbb{Z}[i]^n + C'$. □

Thereby, for each $k = 1, 2, 3, \ldots, n-1$, we find a binary vector related to each k such that this binary vector is added to the generator matrix of the code related to the construction A of the posterior lattice (we make use of the proposition 2), that is, the lattice related to the position $k+1$. Then, after that, we have the construction A of these lattices.

We denote by c_k such a binary vector with n coordinates related to the position k, where $1 \leq k \leq n-1$.

Let $r \geq 3$ and $n = 2^{r-2}$, we have that $\Im^2 = \mathcal{J}$, $\xi_{2^r}^2 = \xi_{2^{r-1}}$ and, in section 3.1, we have that

$$\{1, \xi_{2^r}, \xi_{2^{r-1}}, \xi_{2^r}\xi_{2^{r-1}}, \xi_{2^{r-1}}^2, \xi_{2^r}\xi_{2^{r-1}}^2, \ldots, \xi_{2^{r-1}}^{2^{r-3}-1}, \xi_{2^r}\xi_{2^{r-1}}^{2^{r-3}-1}\} \tag{3.17}$$

is a $\mathbb{Z}[i]$-basis of $\mathbb{Z}[\xi_{2^r}]$ and the following matrix

$$M = \begin{pmatrix} 1 & \xi_{2^r} & \xi_{2^{r-1}} & \cdots & \xi_{2^{r-1}}^{2^{r-3}-1}\xi_{2^r} \\ 1 & \sigma_2(\xi_{2^r}) & \sigma_2(\xi_{2^{r-1}}) & \cdots & \sigma_2(\xi_{2^{r-1}}^{2^{r-3}-1}\xi_{2^r}) \\ 1 & \sigma_3(\xi_{2^r}) & \sigma_3(\xi_{2^{r-1}}) & \cdots & \sigma_3(\xi_{2^{r-1}}^{2^{r-3}-1}\xi_{2^r}) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_n(\xi_{2^r}) & \sigma_n(\xi_{2^{r-1}}) & \cdots & \sigma_n(\xi_{2^{r-1}}^{2^{r-3}-1}\xi_{2^r}) \end{pmatrix} \tag{3.18}$$

generates the complex algebraic lattice $\sigma(\mathbb{Z}[\xi_{2^r}])$.

First we find the binary vectors related to the positions k, where k is odd. In fact, let $k = 2\alpha+1$, where $0 \leq \alpha \leq (2^{r-3}-1)$. Since $\Im = \Im^2 \cup (\Im^2 + (1+\xi_{2^r}))$, we have

$$\Im^k = \Im^{k-1}\Im = \Im^{k+1} \cup (\Im^{k+1} + (1+\xi_{2^{r-1}})^\alpha (1+\xi_{2^r})). \tag{3.19}$$

Then the lattice related to the canonical embedding of the ideal $\Im^k$, where $k = 2\alpha + 1$, can be expressed, via an isomorphism, by

$$\sigma(\Im^k) = \sigma(\Im^{k+1}) \cup (\sigma(\Im^{k+1}) + \sigma((1+\xi_{2^{r-1}})^\alpha (1+\xi_{2^r}))). \tag{3.20}$$

As we want to provide the construction A of the lattices related to each k, then we must have the element $\sigma((1+\xi_{2^{r-1}})^\alpha(1+\xi_{2^r}))$ modulo $2 \equiv 1+i$.

By using the fact that $H_{ml}M = M(M_{(1+\xi_{2^r})})^k$, since the matrices M and M_0 provide the same lattice, the $\mathbb{Z}[i]^n$-lattice, and the fact that $(M_{(1+\xi_{2^r})})^k$ is a generator matrix of the lattice related to the canonical embedding of the ideal $(1+\xi_{2^r})^k\mathbb{Z}[\xi_{2^r}]$ whose position in the nested lattice partition chain compared to the $\mathbb{Z}[i]^n$-lattice is equal to k, we have that

$$\sigma((1+\xi_{2^{r-1}})^\alpha(1+\xi_{2^r})) \equiv M \cdot c_k \text{ (modulo } (1+i) \equiv 2) \tag{3.21}$$

and, thus, $\sigma(\Im^k) = \sigma(\Im^{k+1}) \cup (\sigma(\Im^{k+1}) + c_k)$.

In [11] observe that the row α from the Pascal's triangle modulo 2 indicates the coefficients of $(1+\xi_{2^{r-1}})^\alpha$ modulo 2 (coefficients equal to 0 or 1).

We can see that the elements $1, \xi_{2^{r-1}}, \xi_{2^{r-1}}^2, \ldots, \xi_{2^{r-1}}^{2^{r-3}-1}$ are located at the odd positions of the basis (3.17) and the elements

$$\xi_{2^r}, \xi_{2^r}\xi_{2^{r-1}}, \ldots, \xi_{2^r}\xi_{2^{r-1}}^{2^{r-3}-1}$$

are located at the even positions of the basis (3.17) and are posterior to the elements $1, \xi_{2^{r-1}}, \xi_{2^{r-1}}^2, \ldots, \xi_{2^{r-1}}^{2^{r-3}-1}$, respectively.

Hence, 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 (3.17) and the fact that, for all $k = 2\alpha + 1$, where $0 \leq \alpha \leq (2^{r-3}-1)$, we have $(1+\xi_{2^{r-1}})^\alpha(1+\xi_{2^r})$, we can conclude that each coefficient of the row α filled by zeros must be repeated twice and, after that, this new vector has n coefficients (coordinates).

Then, with this construction, we can find, for any $r \geq 3$, all the binary vectors c_k with n coordinates related to the positions $k = 2\alpha + 1$, where $0 \leq \alpha \leq (2^{r-3}-1)$.

Besides, through the procedure of such a construction and basic properties given in [11], we can show, for any $r \geq 3$ ($n = 2^{r-2}$) and $k = 2\alpha + 1$, where $0 \leq \alpha \leq (2^{r-3} - 1)$, that the binary vector c_k related to the position $k = 2\alpha + 1$ is simply the row $k = 2\alpha + 1$ from the Pascal's triangle modulo 2 filled by zeros to obtain n coefficients modulo 2.

Now, without loss of generality, we find the binary vectors related to the positions k, where k is even. In fact, let $k = 2\alpha$, where $1 \leq \alpha \leq (2^{r-3} - 1)$. Since $\Im = \Im^2 \cup (\Im^2 + (1 + \xi_{2^r}))$, we have

$$\sigma(\Im^k) = \sigma(\Im^{k+1}) \cup (\sigma(\Im^{k+1}) + \sigma((1 + \xi_{2^{r-1}})^\alpha)). \tag{3.22}$$

As we want to provide the construction A of the lattices related to each k, then we must have the element $\sigma((1 + \xi_{2^{r-1}})^\alpha)$ modulo $2 \equiv 1 + i$.

Since $H_{ml}M = M(M_{(1+\xi_{2^r})})^k$ and $(M_{(1+\xi_{2^r})})^k$ is a generator matrix of the lattice related to the canonical embedding of the ideal $(1 + \xi_{2^r})^k\mathbb{Z}[\xi_{2^r}]$ whose position in the nested lattice partition chain compared to the $\mathbb{Z}[i]^n$-lattice is equal to k, we have that

$$\sigma((1 + \xi_{2^{r-1}})^\alpha) \equiv M \cdot c_k \text{ (modulo } (1 + i) \equiv 2) \tag{3.23}$$

and, consequently, $\sigma(\Im^k) = \sigma(\Im^{k+1}) \cup (\sigma(\Im^{k+1}) + c_k)$.

The row α from the Pascal's triangle modulo 2 indicates the coefficients of $(1 + \xi_{2^{r-1}})^\alpha$ modulo 2 (coefficients equal to 0 or 1).

We can see that the elements $1, \xi_{2^{r-1}}, \xi_{2^{r-1}}^2, \ldots, \xi_{2^{r-1}}^{2^{r-3}-1}$ are located at the odd positions of the basis (3.17) and the elements

$$\xi_{2^r}, \xi_{2^r}\xi_{2^{r-1}}, \ldots, \xi_{2^r}\xi_{2^{r-1}}^{2^{r-3}-1}$$

are located at the even positions of the basis (3.17) and are posterior to the elements $1, \xi_{2^{r-1}}, \xi_{2^{r-1}}^2, \ldots, \xi_{2^{r-1}}^{2^{r-3}-1}$, respectively.

Then, 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 (3.17) and the fact that, for all $k = 2\alpha$, where $1 \leq \alpha \leq (2^{r-3} - 1)$, we have $(1+\xi_{2^{r-1}})^\alpha$, we can conclude that the coefficients of the row α filled by zeros are put at the odd positions, with the same order, and the even positions are equal to zero. After that, this new vector has n coefficients (coordinates).

Thereby, with this construction, we can find, for any $r \geq 3$, all the binary vectors c_k with n coordinates related to the positions $k = 2\alpha$, where $1 \leq \alpha \leq (2^{r-3} - 1)$.

Besides, through the procedure of such a construction and basic properties given in [11], we can show, for any $r \geq 3$ ($n = 2^{r-2}$) and $k = 2\alpha$, where

$1 \leq \alpha \leq (2^{r-3} - 1)$, that the binary vector c_k related to the position $k = 2\alpha$ is simply the row $k = 2\alpha$ from the Pascal's triangle modulo 2 filled by zeros to obtain n coefficients modulo 2.

As we have seen, the binary vector c_k is found through the constructions above for the cases where k is either odd or even and, in both cases, the binary vector c_k is the row k from the Pascal's triangle modulo 2 filled by zeros to obtain n coefficients modulo 2; that is, for $k = 1, \ldots, n-1$, the binary vector c_k is the row k from the Pascal's triangle modulo 2 filled by zeros to obtain n coefficients modulo 2.

Then, for obtaining the construction A of the lattice related to the canonical embedding of the ideal $\Im^k$, where $k = 1, 2, \ldots, n-1$, we have

$$\sigma(\Im^k) = \sigma(\Im^{k-1}\Im) = \sigma(\Im^{k+1}) \cup (\sigma(\Im^{k+1}) + c_k) =$$

$$= ((1+i)\mathbb{Z}[i]^n + C_{k+1}) \cup (((1+i)\mathbb{Z}[i]^n + C_{k+1}) + c_k), \tag{3.24}$$

where $\sigma(\Im^{k+1}) = (1+i)\mathbb{Z}[i]^n + C_{k+1}$ is the complex code formula (Construction A) for the lattice related to the canonical embedding of the ideal $\Im^{k+1}$.

Therefore, by using Proposition 2, we can conclude that $\sigma(\Im^k) = (1+i)\mathbb{Z}[i]^n + C_k$, 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}.

Let $M_{(1+\xi_{2^r})}$ represent a generator matrix of the lattice related to the position $k = 1$ calculated by using (3.13). Hence the following theorem gives us the extension by periodicity of the nested lattice partition chain for the positive positions, that is, $k \geq 0$.

Theorem 2. *For $k = n\beta + j$, where $\beta \in \mathbb{N}$ and $0 \leq j \leq n-1$, we have that $M_{(1+\xi_{2^r})^{(n\beta+j)}} = (M_{(1+\xi_{2^r})})^{k=(n\beta+j)}$ is a generator matrix of the lattice $(1+i)^\beta \Lambda_j$ 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. See Appendix 2. □

Consequently, by Theorem 2, we can conclude that the periodicity of the nested lattice partition chain for the positive positions is equal to $k = n$ because $\sigma(\Im^n) = (1+i)\mathbb{Z}[i]^n$, that is, $\sigma(\Im^n)$ is a scaled version of the $\mathbb{Z}[i]^n$-lattice. Therefore, we can obtain the construction A of the lattices related to the canonical embedding of the ideals $\Im^k$, where $k = 1, 2, \ldots, n-1$, that is, we can find

the construction A of these lattices by starting the calculations from the last position ($k = n - 1$) to the first ($k = 1$) by using Proposition 2.

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 $\mathbb{Z}[i]^n = D_{2n} \cup (D_{2n} + (1, 0, 0, \ldots, 0))$, where $\Lambda_1 = D_{2n} = \mathbb{Z}[i]^n + C_1$. Thereby, by using Proposition 2, we have $\mathbb{Z}[i]^n = (1 + i)\mathbb{Z}[i]^n + C_0$, 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. Then we obtain the construction A of the lattice related to the canonical embedding of the ideal when $k = 0$, that is, we obtain the construction A of the $\mathbb{Z}[i]^n$-lattice.

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 3. *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. See Appendix 3. □

Now the following theorem gives us the extension by periodicity of the nested lattice partition chain for the negative positions, that is, $k \leq -1$.

Theorem 3. *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 $k \in \mathbb{N}^*$. Then we have

$$\langle \overrightarrow{x}, \overrightarrow{y} \rangle = Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(x \cdot y),$$

where $x \in \Im^k$ and $y \in \Im^{-k}$. So $x = (1 + \xi_{2^r})^k x_0$, where $x_0 \in \mathbb{Z}[\xi_{2^r}]$, and $y = (1 + \xi_{2^r})^{-k} y_0$, where $y_0 \in \mathbb{Z}[\xi_{2^r}]$.

It is easy to see that

$$Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(x \cdot y) = \sum_{i=1}^{n} \sigma_i(x \cdot y) = \sum_{i=1}^{n} \sigma_i(x)\sigma_i(y)$$

$$= \sum_{i=1}^{n} \sigma_i(x_0)\sigma_i(y_0) = Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(x_0 \cdot y_0).$$

We have that $Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(x_0 \cdot y_0) \in \mathbb{Z} \subset \mathbb{Z}[i]$, then

$$\langle \overrightarrow{x}, \overrightarrow{y} \rangle = Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(x \cdot y) \in \mathbb{Z}[i].$$

Thus, $\sigma(\Im^{-k}) \subset \sigma(\Im^k)^*$, for all $k \in \mathbb{N}^*$. We also have that

$$Vol[\sigma(\Im^k)^*] = \frac{1}{Vol[\sigma(\Im^k)]} = Vol[\sigma(\Im^{-k})].$$

So the index $|\sigma(\Im^k)^*/\sigma(\Im^{-k})|$ is equal to 1 and, then, $\sigma(\Im^{-k}) = \sigma(\Im^k)^*$. □

By using Theorems 2 and 3 we can conclude that we have n ($k = 0, 1, 2, \ldots, n-1$) different lattices in the doubly infinite nested lattice partition chain.

Hence, in this section, we have constructed a doubly infinite nested lattice partition chain related to any dimension $n = 2^{r-2}$, where $r \geq 3$, in order to realize interference alignment onto a lattice. Then, for the complex case, we have a generalization to obtain a doubly infinite nested lattice partition chain in order to quantize complex channel coefficients in order to realize interference alignment onto a lattice.

Besides, consequently, we have constructed nested lattice codes (nested coset codes) with $(1+i)\mathbb{Z}[i]^n$ being the corresponding sublattice.

4. Precoder

In Section 3 we show that complex-valued channels can be quantized onto a lattice. Therefore, precoding is essential to ensure onto which lattice a given complex-valued channel coefficient must be quantized. Hence, in this section, we provide the details of such a precoding which is related to the dimension $n = 2^{r-2}$, where $r \geq 3$.

Observe that $\xi_{2^r}^n = i \in \mathbb{Z}[i]$, where $n = 2^{r-2}$. A generator of an ideal of a ring of integers multiplied by a unit of this ring of integers also generates such an ideal. Thus we must analyse all the possible generators and, for each case, utilize a precoding for that the respective channel approximations be aligned onto one of the n different lattices related to the doubly infinite nested lattice partition chain constructed in Section 3.2. As generators, note that $(1 + \xi_{2^r})^n = (1 + i) \in \mathbb{Z}[i]$.

In Section 3.2 we have n different lattices related to the doubly infinite nested lattice partition chain, the other lattices are equivalent to one of these n

different lattices. Observe that these n different lattices are the lattices related to the positions $0, 1, 2, 3, \ldots, n-1$ of the doubly infinite nested lattice partition chain.

Remember that the position of the lattices in the doubly infinite nested lattice partition chain is related to the power of the principal ideal $(1+\xi_{2^r})\mathbb{Z}[\xi_{2^r}] = \Im$, that is, let $(1+\xi_{2^r})^k$ and by computing k modulo n, we have that $k \in \{0, 1, 2, 3, \ldots, n-1\}$ and the ideal $(1+\xi_{2^r})^k\mathbb{Z}[\xi_{2^r}] = \Im^k$ furnishes us, by using the Galois embedding, the lattice related to the position k of the doubly infinite nested lattice partition chain.

We have that all the possible generators are $(\xi_{2^r})^{k'}(1+\xi_{2^r})^k\lambda$ [12], where $\lambda \in \mathbb{Z}[i]$ and $k, k' \in \mathbb{Z}$. Then we have to analyse the product $(\xi_{2^r})^{k'}(1+\xi_{2^r})^k$, since $\lambda \neq 1$ removes the element $(\xi_{2^r})^{k'}(1+\xi_{2^r})^k$ from the origin. Therefore, all the possible generators of the ideals are the elements $(\xi_{2^r})^{k'}(1+\xi_{2^r})^k$, where $k, k' \in \mathbb{Z}$.

We also have that k and k', for the dimension $n = 2^{r-2}$ $(r \geq 3)$, each of them has n possibilities of values, since $\xi_{2^r}^n = i \in \mathbb{Z}[i]$ and $k \in \{0, 1, 2, 3, \ldots, n-1\}$. So, by analysing the element $(\xi_{2^r})^{k'}(1+\xi_{2^r})^k$, we have a total of n^2 possibilities of values for it.

Now as it is not possible to discuss all the cases for k and k' in order to precode the complex-valued channel coefficients h_{ml}, then we explain the process to realize the precoding in each case, i.e., for each case, we ensure that the complex-valued channel coefficient belongs to a corresponding lattice (one of the n different lattices). For that, we observe the form of the generator in each case.

For the case $k \equiv 0$ modulo n and $k' \equiv 0$ modulo n, we have no precoding because h_{ml} is approximated by an element that belongs in $\mathbb{Z}[i]$.

For the other cases we fix a particular one, then h_{ml} is approximated by $(\xi_{2^r})^{k'}(1+\xi_{2^r})^k$, that is,

$$h_{ml} \to (\xi_{2^r})^{k'}(1+\xi_{2^r})^k, \tag{4.1}$$

for some fixed k and k'.

Thereby, for each i such that $1 \leq i \leq n$, the element $(\xi_{2^r})^{k'}(1+\xi_{2^r})^k$ must be multiplied by a constant ζ_i such that $(\xi_{2^r})^{k'}(1+\xi_{2^r})^k \cdot \zeta_i = \sigma_i((\xi_{2^r})^{k'}(1+\xi_{2^r})^k)$ (for $i = 1$, we have $\zeta_i = 1$). We need this kind of multiplication to ensure the

precoding which is given as it follows:

$$\begin{pmatrix} h_{ml} & 0 & 0 & 0 & \cdots & 0 \\ 0 & h_{ml}\cdot\zeta_2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & h_{ml}\cdot\zeta_3 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & h_{ml}\cdot\zeta_n \end{pmatrix} \rightarrow$$

$$\rightarrow \begin{pmatrix} \sigma_1((\xi_{2^r})^{k'}(\mu)^k) & 0 & 0 & \cdots & 0 \\ 0 & \sigma_2((\xi_{2^r})^{k'}(\mu)^k) & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \sigma_n((\xi_{2^r})^{k'}(\mu)^k) \end{pmatrix} \sim M'_k, \quad (4.2)$$

where $\mu = 1 + \xi_{2^r}$.

Consequently, we ensure onto which lattice a given complex-valued channel coefficient must be quantized.

Now we need to argue how we can find, given an arbitrary $h_{ml} \in \mathbb{C}$, the appropriate k and k', that is, given an arbitrary $h_{ml} \in \mathbb{C}$, we find k and k' such that $h_{ml} \rightarrow (\xi_{2^r})^{k'}(1+\xi_{2^r})^k$. Hence, after finding the appropriate integers k and k', we compute them modulo n and then we use one of the n^2 possible cases in order to realize the complex-valued channel quantization for dimension n.

So let $h_{ml} \in \mathbb{C}$. From the new algebraic methodology described in Section 3 in order to realize interference alignment onto a lattice, it is natural the approximation $\parallel h_{ml} \parallel \rightarrow \parallel 1 + \xi_{2^r} \parallel^k$, where $k \in \mathbb{Z}$. Consequently, to find the appropriate k, we have $\frac{log\|h_{ml}\|}{log\|1+\xi_{2^r}\|} \rightarrow k \in \mathbb{Z}$, that is, we choose k as being the closest integer value to the value $\frac{log\|h_{ml}\|}{log\|1+\xi_{2^r}\|}$.

Now, after finding k, finally we can find k' by using the argument function. In fact, we have that $h_{ml} \rightarrow (\xi_{2^r})^{k'}(1+\xi_{2^r})^k$ (note that we already know k), then, to find k', we have $\frac{arg(h_{ml})-narg(1+\xi_{2^r})}{\pi/2^{r-1}} \rightarrow k' \in \mathbb{Z}$, that is, we choose k' as being the closest integer value to the value $\frac{arg(h_{ml})-narg(1+\xi_{2^r})}{\pi/2^{r-1}}$.

Then, by knowing k and k', we can realize for dimension n the corresponding complex-valued channel quantization described in Section 3.1 by using the process of precoding for dimension n described in this section.

5. Minimum Mean Square Error Criterion for the Complex-Valued Channel Quantization

In Section 3.1 we introduce a new algebraic methodology to quantize complex-valued channel coefficients. The purpose of this section is to minimize the mean square error related to the quantization of this work, consequently, it provides us the best estimation for such a quantization.

In Section 3.1, for fixed m and l, we have that the matrix H_{ml} is quantized by M'_k, where Section 3.2 guarantees that $k \in \{0, 1, \ldots, n-1\}$.

In this section we have $l = 1, 2, \ldots, L$, then for the sake of simplicity we denote M'_k by M'_{k_l} and $M_{(1+\xi_{2^r})^k}$ by $M_{(1+\xi_{2^r})^{k_l}}$, where $k_l \in \{0, 1, \ldots, n-1\}$.

The following theorem furnishes us the computation of the corresponding mean square error.

Theorem 4. *The $n \times n$ matrix $B = \frac{1}{\eta} \sum_{l=1}^{L} h_{ml}(M_0 M_{(1+\xi_{2^r})^{k_l}} M_0^H)$ minimizes the mean square error $E[\overrightarrow{v}_m^H \overrightarrow{v}_m]$, where*

$$\eta = (\|h\|^2 + \frac{1}{\rho}), \quad h = (h_{m1}, h_{m2}, \ldots, h_{mL}),$$

ρ is the signal-to-noise ratio (SNR),

$$\overrightarrow{v}_m = \sum_{l=1}^{L} \left(h_{ml} \left(M_0^H B M_0 \right) - M_{(1+\xi_{2^r})^{k_l}} \right) \overrightarrow{v_l} + M_0^H B \overrightarrow{z}_m, \tag{5.1}$$

$\overrightarrow{v}_l \in \mathbb{Z}[i]^n$ and $M'_{k_l} M_0 = M_0 M_{(1+\xi_{2^r})^{k_l}}$, for $l = 1, \ldots, L$, with $M_{(1+\xi_{2^r})^{k_l}} \in \mathbb{M}_n(\mathbb{Z}[i])$ and H denotes the transpose conjugate of a matrix, where $\mathbb{M}_n(\mathbb{Z}[i])$ denotes the set of the $n \times n$ matrices with integer complex entries. The equality $M'_{k_l} M_0 = M_0 M_{(1+\xi_{2^r})^{k_l}}$ means that the matrices M'_{k_l} and $M_{(1+\xi_{2^r})^{k_l}}$ generate the same lattice. In addition, the mean square error is given by

$$P_s \frac{1}{\eta} (\eta \sum_{l=1}^{L} Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(((1+\xi_{2^r})^{k_l})^2)$$

$$- \sum_{l,j=1}^{L} h_{ml} h_{mj} Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}((1+\xi_{2^r})^{k_l}(1+\xi_{2^r})^{k_j})), \tag{5.2}$$

where P_s is the signal power.

Proof. See Appendix 4. □

Equation (5.2) is an expression of the mean square error and, by minimizing such an equation, the minimum solution of the mean square error is obtained.

Thereby, for finding the corresponding minimum solution, we have to minimize the following expression:

$$\eta \sum_{l=1}^{L} Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(((1+\xi_{2^r})^{k_l})^2)$$

$$- \sum_{l,j=1}^{L} h_{ml} h_{mj} Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}((1+\xi_{2^r})^{k_l}(1+\xi_{2^r})^{k_j}). \tag{5.3}$$

Equation (5.3) is a quadratic form whose variables are

$$a_{l0}, a_{l1}, \ldots, a_{l(n-1)} \in \mathbb{Z}[i],$$

where $l = 1, \ldots, L$, and

$$(1+\xi_{2^r})^{k_l} = a_{l0} + a_{l1}\xi_{2^r} + a_{l2}\xi_{2^r}^2 + \cdots + a_{l(n-1)}\xi_{2^r}^{n-1}. \tag{5.4}$$

We can associate the quadratic form (5.3) to the following functional

$$F(a) = \eta \sum_{l=1}^{L} Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(((1+\xi_{2^r})^{k_l})^2)$$

$$- \sum_{l,j=1}^{L} h_{ml} h_{mj} Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}((1+\xi_{2^r})^{k_l}(1+\xi_{2^r})^{k_j}) = a^t Q a, \tag{5.5}$$

where $a = (a_{10}, a_{11}, \ldots, a_{1(n-1)}, \ldots, a_{L0}, a_{L1}, \ldots, a_{L(n-1)}) \in \mathbb{Z}[i]^{Ln}$ and Q is the corresponding $Ln \times Ln$ symmetric matrix.

Since Q is a complex symmetric square matrix, we apply the Takagi decomposition of the matrix $Q = VDV^t$, where D is a real nonnegative diagonal matrix and V is unitary.

The goal is to find $a \in (\mathbb{Z}[i]^{Ln} - \{0\})$ such that a is the vector which minimizes $F(a)$. Hence

$$\min_{a \in (\mathbb{Z}[i]^{Ln} - \{0\})} F(a) = \min_{a \in (\mathbb{Z}[i]^{Ln} - \{0\})} a^t Q a$$

$$= \min_{a\in(\mathbb{Z}[i]^{Ln}-\{0\})} a^t V D V^t a = \min_{b\in\Lambda'} b^t D b, \tag{5.6}$$

where $b = V^t a$ and Λ' is the corresponding lattice.

Thereby, given complex-valued channels h_{ml}, where $l = 1, 2, \ldots, L$, we find $a \in \mathbb{Z}[i]^{Ln}$ which gives us the best estimation for the respective equations in (5.4), therefore, we obtain the best estimation for the corresponding quantizations $M'_{k_l} \sim (M_{(1+\xi_{2^r})})^{k_l}$. Notice that by applying the stipulated value for the complex-valued channels h_{ml}, where $l = 1, 2, \ldots, L$, we have the value of η by conditioning a value for ρ and, through Section 4, we can find the value of the corresponding powers k_l, where $l = 1, 2, \ldots, L$.

As we perform the complex-valued channel quantization described in Section 3.1, the corresponding codewords x_l, where $l = 1, 2, \ldots, L$, are transformed in lattice points which belong to one of the n lattices constructed in Section 3.2. By using the minimum mean square error criterion, the corresponding estimation for $h_{ml}x_l$ is a point of the lattice related to the power k_l which is associated to a coset of this lattice with $(1+i)\mathbb{Z}[i]^n$ being the corresponding sublattice and, consequently, we have an efficient decoder for such a complex-valued channel quantization and the corresponding achievable computation rate at each node is maximized.

5.1. Minimum mean square error criterion for the two-complex dimensional quantization

In [9], for the two-complex dimensional case and $L = 2$, we have the corresponding complex-valued channel quantization and the construction of complex nested ideal lattices from such a channel quantization.

By (5.5) the functional related to such a minimization is given by

$$F(a) = \eta \sum_{l=1}^{2} Tr_{\mathbb{Q}(\xi_8)/\mathbb{Q}(i)}(((1+\xi_8)^{k_l})^2)$$

$$- \sum_{l,j=1}^{2} h_{ml}h_{mj} Tr_{\mathbb{Q}(\xi_8)/\mathbb{Q}(i)}((1+\xi_8)^{k_l}(1+\xi_8)^{k_j}) = a^t Q a, \tag{5.7}$$

where $a \in \mathbb{Z}[i]^4$, $\eta = (\|h\|^2 + \frac{1}{\rho})$, $h = (h_{m1}, h_{m2})$, ρ is the signal-to-noise ratio (SNR) and Q is the corresponding 4×4 symmetric complex matrix.

Since Q is a complex symmetric square matrix, we apply the Takagi decomposition of the matrix $Q = VDV^t$, where D is a real nonnegative diagonal matrix and V is unitary.

The goal is to find $a \in (\mathbb{Z}[i]^4 - \{0\})$ such that a is the vector which minimizes $F(a)$. Hence

$$\min_{a\in(\mathbb{Z}[i]^4-\{0\})} F(a) = \min_{a\in(\mathbb{Z}[i]^4-\{0\})} a^t Q a$$
$$= \min_{a\in(\mathbb{Z}[i]^4-\{0\})} a^t V D V^t a = \min_{b\in\Lambda'} b^t D b, \tag{5.8}$$

where $b = V^t a$ and Λ' is the corresponding lattice.

Following the theoretical construction developed in Section 5, for the two-complex dimensional case and $L = 2$, the input elements h_{m1}, h_{m2} of the functional (5.7) are uniformly distributed random numbers. Also we randomly generate the values of the SNR ρ for each computational experiment i, where $i = 1, 2, \ldots, 10$. Thereby we compute the values of η in the second column of Table **??**. Therefrom the functional (5.7) and its respective quadratic form is obtained. The minimum of the equation (5.8) corresponds to a $b \in \Lambda'$ such that b is the closest lattice point to the origin.

For each computational experiment i, we find the vector $a \in (\mathbb{Z}[i]^4 - \{0\})$ which gives us the best estimation for the respective equations in (5.4). In (5.4) we have

$$\begin{cases} (1+\xi_8)^{k_1} = a_{10} + a_{11}\xi_8 & \text{(a)} \\ (1+\xi_8)^{k_2} = a_{20} + a_{21}\xi_8 & \text{(b)} \end{cases}, \tag{5.9}$$

where (a) and (b) correspond, respectively, to the best estimation of the quantizations M'_{k_1} and M'_{k_2}. Each k_l, where $l = 1, 2$, is computed by taking the closest integer of the following value

$$\frac{\log \|h_{ml}\|}{\log \|1+\xi_8\|} \tag{5.10}$$

and, after that, we compute such an integer value mod 2 to obtain k_l. In Figure 2 each lattice is represented by either $\Lambda_0 = \mathbb{Z}[i]^2$ (blue dots) or $\Lambda_1 = D_4$ (red crosses).

The corresponding estimations for $h_{m1}x_1$ and $h_{m2}x_2$ are represented in Table **??** by the vectors $P1_i$ and $P2_i$, respectively, for the computational experiments $i = 1, \ldots, 10$. These estimations are points of the lattices related to the powers k_1 and k_2, respectively, and are associated to a coset of such lattices with $(1+i)\mathbb{Z}[i]^2$ being the corresponding sublattice. Consequently, we have an efficient decoder for such a two-complex dimensional channel quantization and the corresponding achievable computation rate at each node is maximized.

In Figure 2, for the sake of ilustration, 5 computational experiments from Table **??** ($i = 4, 6, 7, 8, 10$) are used for the representation of the corresponding estimations (for the other ones such a representation is analogous). The

points $P1_i$ (continous) and $P2_i$ (dashed) are estimations for $h_{m1}x_1$ and $h_{m2}x_2$, respectively.

From the computational experiments, we observe that we obtain a two-dimensional hyperplane by taking the values of h_{m1} and h_{m2} such that $||h_{m1}|| = ||h_{m2}|| = 1$. We can generate such a two-dimensional hyperplane through the projection of the last complex coordinate.

i-th	η	k_1	k_2	$P1_i$ (Cont.)	$P2_i$ (Dashed)	Color
1	3.4781	1	1	(0, 22+26i)	(0, 7+35i)	-
2	4.5525	0	0	(0, -72-72i)	(0, -90-90i)	-
3	336.0012	0	0	(0, -18-98i)	(0, -18-162i)	-
4	2.5855	0	1	(0, -4-2i)	(0, -2-4i)	Blue
5	300.7523	1	0	(0, -12-16i)	(0, -3-13i)	-
6	3.6555	1	0	(0, 2-18i)	(0, 3-22i)	Magenta
7	2.5852	1	0	(0, 20+4i)	(0, 6+8i)	Red
8	3.1153	0	0	(0, -12-16i)	(0, -3-13i)	Black
9	2.7803	0	0	(0, -50-66i)	(0, -25-70i)	-
10	2.9633	1	0	(0, -4i)	(0, 2-3i)	Green

Table 1: Data from the Computational Experiments

6. Conclusion

This work presents a new algebraic methodology to quantize complex-valued channels in order to realize interference alignment (IA) [1] onto a complex ideal lattice. Such a methodology makes use of the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$, where $r \geq 3$, to provide a doubly infinite nested lattice partition chain for any dimension $n = 2^{r-2}$, where $r \geq 3$, in order to quantize complex-valued channels onto these nested lattices.

We prove the existence of periodicity in the corresponding nested lattice partition chains to guarantee that the channel gain does not remove the lattice from the initial chain of nested complex ideal lattices.

Precoding is essential to ensure onto which lattice a given complex-valued channel must be quantized. Therefore Section 4 provides us such a precoder.

In this work we minimize the mean square error related to the corresponding quantization to providing us the best estimation for such a quantization. Consequently, we obtain an efficient decoder. In Section 5.1 we exemplify this new

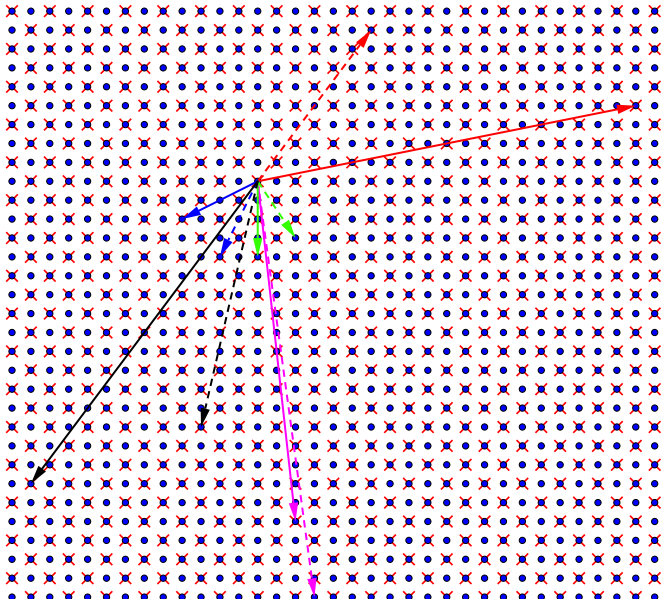

Figure 2: Representation of the Vectors $P1_i$ and $P2_i$ from Table I. Note that $\Lambda_1 = D_4 \subseteq \Lambda_0 = \mathbb{Z}[i]^2$.

algebraic methodology through the two-complex dimensional channel quantization and show all the corresponding computational experiments.

The proposed algebraic methodology is original and can be approached to applications such as compute-and-forward [13] and homomorphic encryption schemes.

7. Appendix 1: The lattice related to the canonical embedding of the ideal $\Im^k$, where $k = 1$, is given by the lattice D_{2n}, where $n = 2^{(r-2)}$

We have $\mathbb{Z}[i]^n/\sigma(\Im)/D_n^2$ and

$$\mathbb{Z}[i]^n = D_n^2 \cup (D_n \oplus (D_n + (1,0,0,\ldots,0)))\cup$$

$$\cup((D_n + (1,0,0,\ldots,0)) \oplus D_n) \cup ((D_n + (1,0,0,\ldots,0))\oplus$$

$$\oplus(D_n + (1,0,0,\ldots,0))) = D_n^2 \cup (D_n^2 + (0,1,0,0,\ldots,0))\cup$$

$$\cup(D_n^2 + (1,0,0,\ldots,0)) \cup (D_n^2 + (1,1,0,0,\ldots,0)).$$

Then $\sigma(\Im)$ 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 $\Im = \Im^2 \cup (\Im^2 + (1+\xi_{2^r}))$, then $\sigma(\Im) = \sigma(\Im^2) \cup \sigma(\Im^2 + (1+\xi_{2^r})) = D_n^2 \cup \sigma(\Im^2 + (1+\xi_{2^r}))$ and we can conclude that $\sigma(\Im^2 + (1+\xi_{2^r}))$ 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 $\sigma(\Im^2 + (1+\xi_{2^r})) = \sigma(\Im^2) + \sigma(1+\xi_{2^r}) = D_n^2 + \sigma(1+\xi_{2^r})$, where

$$\sigma(1+\xi_{2^r}) = (1+\xi_{2^r}, \sigma_2(1+\xi_{2^r}), \ldots, \sigma_n(1+\xi_{2^r})) =$$

$$= (1+\xi_{2^r}, 1+\sigma_2(\xi_{2^r}), \ldots, 1+\sigma_n(\xi_{2^r})),$$

where, in section 3.1, we have that $\{id = \sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_n\}$ is the Galois group of the field extension $\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)$ and id is the identity map.

Also, in section 3.1, we have that a $\mathbb{Z}[i]$-basis of $\mathbb{Z}[\xi_{2^r}]$ is given by

$$\{1, \xi_{2^r}, \xi_{2^r}^2, \xi_{2^r}^3, \ldots, \xi_{2^r}^{n-1}\} =$$

$$= \{1, \xi_{2^r}, \xi_{2^{r-1}}, \xi_{2^{r-1}}\xi_{2^r}, \xi_{2^{r-1}}^2, \ldots, \xi_{2^{r-1}}^{2^{r-3}-1}, \xi_{2^{r-1}}^{2^{r-3}-1}\xi_{2^r}\}$$

and the following matrix

$$M = \begin{pmatrix} 1 & \xi_{2^r} & \xi_{2^{r-1}} & \cdots & \xi_{2^{r-1}}^{2^{r-3}-1}\xi_{2^r} \\ 1 & \sigma_2(\xi_{2^r}) & \sigma_2(\xi_{2^{r-1}}) & \cdots & \sigma_2(\xi_{2^{r-1}}^{2^{r-3}-1}\xi_{2^r}) \\ 1 & \sigma_3(\xi_{2^r}) & \sigma_3(\xi_{2^{r-1}}) & \cdots & \sigma_3(\xi_{2^{r-1}}^{2^{r-3}-1}\xi_{2^r}) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_n(\xi_{2^r}) & \sigma_n(\xi_{2^{r-1}}) & \cdots & \sigma_n(\xi_{2^{r-1}}^{2^{r-3}-1}\xi_{2^r}) \end{pmatrix}$$

generates the complex algebraic lattice $\sigma(\mathbb{Z}[\xi_{2^r}])$.

Thus, we have

$$\sigma(1+\xi_{2^r}) = M \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 1+\xi_{2^r} \\ 1+\sigma_2(\xi_{2^r}) \\ 1+\sigma_3(\xi_{2^r}) \\ 1+\sigma_4(\xi_{2^r}) \\ 1+\sigma_5(\xi_{2^r}) \\ \vdots \\ 1+\sigma_n(\xi_{2^r}) \end{pmatrix}.$$

Then we can conclude that

$$\sigma(\Im^2 + (1 + \xi_{2^r})) = D_n^2 + (1, 1, 0, 0, \ldots, 0) =$$

$$= (D_n + (1, 0, 0, \ldots, 0)) \oplus (D_n + (1, 0, 0, \ldots, 0))$$

and

$$\sigma(\Im) = D_n^2 \cup ((D_n + (1, 0, 0, \ldots, 0)) \oplus (D_n + (1, 0, 0, \ldots, 0))) = D_{2n}.$$

Therefore, 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 $k = 1$.

8. Appendix 2: Extension by periodicity of the nested lattice partition chain for the positive positions, that is, $k \geq 0$

In section 3.2, we have the lattices Λ_j, where $0 \leq j \leq n-1$ and Λ_j is the lattice related to the position j. Also we have that $M_{(1+\xi_{2^r})^j} = (M_{(1+\xi_{2^r})})^j$ is a generator matrix of the lattice Λ_j and we know that the matrices $(M_{(1+\xi_{2^r})})^n$ and $(1+i)I_{n\times n}$ are equivalent matrices, where $I_{n\times n}$ is the $n \times n$ identity matrix.

Then, for $k = n$, the matrix $(M_{(1+\xi_{2^r})})^n$ generates the lattice $(1+i)\mathbb{Z}[i]^n$; for $k = n+j$, we have $M_{(1+\xi_{2^r})^{(n+j)}} = (M_{(1+\xi_{2^r})})^{(n+j)} = ((M_{(1+\xi_{2^r})})^n)(M_{(1+\xi_{2^r})})^j = (1+i)(M_{(1+\xi_{2^r})})^j$ as being a generator matrix of the lattice $(1+i)\Lambda_j$ and, for $k = 2n+j$, we have $M_{(1+\xi_{2^r})^{(2n+j)}} = (M_{(1+\xi_{2^r})})^{(2n+j)} = ((M_{(1+\xi_{2^r})})^{2n})(M_{(1+\xi_{2^r})})^j = (1+i)^2(M_{(1+\xi_{2^r})})^j = 2(M_{(1+\xi_{2^r})})^j$ as being a generator matrix of the lattice $2\Lambda_j$, since the matrices $(M_{(1+\xi_{2^r})})^n$ and $(1+i)I_{n\times n}$ are equivalent.

Then we suppose, by hypothesis of induction, that $(M_{(1+\xi_{2^r})})^{n\beta+j}$, where $\beta \in \mathbb{N}$ and $0 \leq j \leq n-1$, is a generator matrix of the lattice $(1+i)^\beta \Lambda_j$.

We show, for $k = n(\beta+1)+j$, that the lattice $(1+i)^{\beta+1}\Lambda_j$ has a generator matrix as being the matrix $(M_{(1+\xi_{2^r})})^{(n(\beta+1)+j)}$. In fact, $(M_{(1+\xi_{2^r})})^{n(\beta+1)+j} = ((M_{(1+\xi_{2^r})})^n)((M_{(1+\xi_{2^r})})^{(n\beta+j)})$, by using the hypothesis of induction and the fact that $(1+i)I_{n\times n}$ and $(M_{(1+\xi_{2^r})})^n$ are equivalent matrices, we have $(M_{(1+\xi_{2^r})})^{n(\beta+1)+j}$ as a generator matrix of the lattice $(1+i)^{\beta+1}\Lambda_j$.

Hence, we show, for $k = n\beta + j$, where $\beta \in \mathbb{N}$ and $0 \leq j \leq n-1$, that the matrix $(M_{(1+\xi_{2^r})})^{n\beta+j}$ is a generator matrix of the lattice $(1+i)^\beta \Lambda_j$.

Therefore, if β is even, we have $\beta = 2\epsilon$, where $\epsilon \in \mathbb{N}$, and $(1+i)^\beta \Lambda_j = 2^{\beta/2}\Lambda_j$, for $\beta \neq 0$; for $\beta = 0$, we have the lattice Λ_j. Now if β is odd, we have $\beta = 2\epsilon + 1$, where $\epsilon \in \mathbb{N}$, and $(1+i)^\beta \Lambda_j = 2^{(\beta-1)/2}(1+i)\Lambda_j$.

9. Appendix 3: 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 $d_k \geq 2$

We have that C_0 is the universal code $\mathbb{F}_2^n = \{0,1\}^n$ 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 [11] 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 to obtain n coefficients, that is, are the rows from M_{C_0} by removing the first one (row 0 of the Pascal's triangle).

We 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 rows of the matrix M_{C_1} are given by the rows 1,2 of the Pascal's triangle modulo 2 filled by zeros to obtain 2 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 $r = 4$ ($n = 4$ 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.

In [11] we have the following basic properties of the Pascal's triangle modulo 2:

1) Row $2^\vartheta - 1$ consists of 2^ϑ ones: 111...111 (2^ϑ 1's);

2) Row 2^ϑ consists of two ones separated by $2^\vartheta - 1$ zeros: 100...001 (($2^\vartheta - 1$) 0's);

3) More generally, row $2^\vartheta + u$, where $0 \leq u < 2^\vartheta$, consists of two copies of the row u separated by $(2^\vartheta - 1 - u)$ 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 $r = \vartheta + 3$ and then $\vartheta = 2$. By Property 2) we have that the row 4 consists of two 1's separated by 3 zeros and, by 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 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 three properties, we prove it by induction. Let $r \geq 3$, $r = \vartheta + 3$, $k = 1, 2, 3, \ldots, n-1 = 2^{r-2} - 1$ and the rows $2^\vartheta + u$, where $0 \leq u \leq 2^\vartheta - 1$, which consist of two copies of the row u separated by $2^\vartheta - 1 - u$ zeros. Suppose that the rows $1, 2, 3, \ldots, 2^\vartheta, 2^\vartheta + 1, \ldots, 2^{\vartheta+1} - 1$ have an even

number of 1's and, at least, two 1's.

Now we show, by induction, that this is valid for $r+1 = \vartheta+4 = (\vartheta+1)+3$. So, for $r+1$, we have Property 3) given by the rows $2^{\vartheta+1}+u$, where $0 \leq u \leq 2^{\vartheta+1}-1$, which consist of two copies of the row u separated by $2^{\vartheta+1}-1-u$ zeros and we have the rows $1, 2, 3, \ldots, 2^{\vartheta+1}-1, 2^{\vartheta+1}, 2^{\vartheta+1}+1, \ldots, 2^{\vartheta+2}-1$ that generate the code C_1 related to $r+1$.

However, by hypothesis of induction, we have that the rows $1, 2, 3, \ldots, 2^{\vartheta}, 2^{\vartheta}+1, \ldots, 2^{\vartheta+1}-1$ have an even number of 1's and, at least, two 1's and since the rows $2^{\vartheta+1}+u$, where $0 \leq u \leq 2^{\vartheta+1}-1$, consist of two copies of the row u separated by $2^{\vartheta+1}-1-u$ zeros, it follows that the rows $1, 2, 3, \ldots, 2^{\vartheta+1}-1, 2^{\vartheta+1}, 2^{\vartheta+1}+1, \ldots, 2^{\vartheta+2}-1$ have an even number of 1's and, at least, two 1's (row $2^{\vartheta+1}$).

Then we prove, by induction, that d_k is even and $d_k \geq 2$.

10. Appendix 4: Providing an expression for the corresponding mean square error

From equation (1.1), we have

$$B\overrightarrow{y}_m = \sum_{l=1}^{L} B(h_{ml}I)\overrightarrow{x}_l + B\overrightarrow{z}_m =$$

$$= \sum_{l=1}^{L} M'_{k_l}\overrightarrow{x}_l + \sum_{l=1}^{L}(B(h_{ml}I) - M'_{k_l})\overrightarrow{x}_l + B\overrightarrow{z}_m,$$

where $M'_{k_l}\overrightarrow{x}_l = M'_{k_l}(M_0\overrightarrow{v}_l) = M_0(M_{(1+\xi_{2^r})^{k_l}}\overrightarrow{v}_l)$, with $M_{(1+\xi_{2^r})^{k_l}} \in \mathbb{M}_n(\mathbb{Z}[i])$. Hence

$$\sum_{l=1}^{L} M'_{k_l}\overrightarrow{x}_l = \sum_{l=1}^{L} M_0(M_{(1+\xi_{2^r})^{k_l}}\overrightarrow{v}_l) = M_0\sum_{l=1}^{L}(M_{(1+\xi_{2^r})^{k_l}}\overrightarrow{v}_l).$$

We also have that

$$\sum_{l=1}^{L}(B(h_{ml}I) - M'_{k_l})\overrightarrow{x}_l = \sum_{l=1}^{L}((M_0M_0^H)h_{ml}B - M'_{k_l})\overrightarrow{x}_l =$$

$$= \sum_{l=1}^{L}((M_0M_0^H)h_{ml}B)\overrightarrow{x}_l - \sum_{l=1}^{L} M'_{k_l}\overrightarrow{x}_l =$$

$$= \sum_{l=1}^{L} (M_0 M_0^H) h_{ml} B (M_0 M_0^H) \overrightarrow{x}_l - \sum_{l=1}^{L} M_0 (M_{(1+\xi_{2^r})^{k_l}} \overrightarrow{v}_l) =$$

$$= \sum_{l=1}^{L} (M_0 M_0^H) h_{ml} B M_0 \overrightarrow{v}_l - \sum_{l=1}^{L} M_0 (M_{(1+\xi_{2^r})^{k_l}} \overrightarrow{v}_l) =$$

$$= M_0 \left(\sum_{l=1}^{L} (M_0^H h_{ml} B M_0) \overrightarrow{v}_l \right) - M_0 \sum_{l=1}^{L} M_{(1+\xi_{2^r})^{k_l}} \overrightarrow{v}_l =$$

$$= M_0 \sum_{l=1}^{L} (h_{ml} (M_0^H B M_0) - M_{(1+\xi_{2^r})^{k_l}}) \overrightarrow{v}_l$$

and $B\overrightarrow{z}_m = M_0 (M_0^H B \overrightarrow{z}_m)$.

Then we conclude that

$$\overrightarrow{y}'_m = M_0^H B \overrightarrow{y}_m = \sum_{l=1}^{L} M_{(1+\xi_{2^r})^{k_l}} \overrightarrow{v}_l +$$

$$+ \sum_{l=1}^{L} (h_{ml} (M_0^H B M_0) - M_{(1+\xi_{2^r})^{k_l}}) \overrightarrow{v}_l + M_0^H B \overrightarrow{z}_m,$$

where $\overrightarrow{v}_m = \sum_{l=1}^{L} (h_{ml} (M_0^H B M_0) - M_{(1+\xi_{2^r})^{k_l}}) \overrightarrow{v}_l + M_0^H B \overrightarrow{z}_m$ is the noise term ($\overrightarrow{v}_m$ is an $n \times 1$ column vector). Thus the mean square error is given by

$$E[\overrightarrow{v}_m^H \overrightarrow{v}_m] = Tr(E[\overrightarrow{v}_m^H \overrightarrow{v}_m]) =$$

$$= E[Tr(\overrightarrow{v}_m^H \overrightarrow{v}_m)] = E[Tr(\overrightarrow{v}_m \overrightarrow{v}_m^H)] = Tr(E[\overrightarrow{v}_m \overrightarrow{v}_m^H]) \text{ and}$$

$$Tr(E[\overrightarrow{v}_m \overrightarrow{v}_m^H]) =$$

$$= Tr(E[(\sum_{l=1}^{L} (h_{ml} (M_0^H B M_0) - M_{(1+\xi_{2^r})^{k_l}}) \overrightarrow{v}_l + M_0^H B \overrightarrow{z}_m) \cdot$$

$$\cdot(\sum_{l=1}^{L}(h_{ml}(M_0^H B M_0) - M_{(1+\xi_{2^r})^{k_l}})\overrightarrow{v}_l + M_0^H B \overrightarrow{z}_m)^H]).$$

Since the variables $\overrightarrow{v}_l$ and $\overrightarrow{z}_m$ are uncorrelated, for $l = 1, \ldots, L$, we have

$$E[\overrightarrow{v}_m \overrightarrow{v}_m^H] = \sum_{l=1}^{L}(h_{ml}(M_0^H B M_0) - M_{(1+\xi_{2^r})^{k_l}}) \cdot E[\overrightarrow{v}_l \overrightarrow{v}_l^H] \cdot$$

$$\cdot(h_{ml}(M_0^H B^H M_0) - M_{(1+\xi_{2^r})^{k_l}}^H) +$$

$$+ M_0^H B E[\overrightarrow{z}_m \overrightarrow{z}_m^H] B^H M_0.$$

Hence

$$E[\overrightarrow{v}_m^H \overrightarrow{v}_m] = Tr(\sum_{l=1}^{L}(h_{ml}(M_0^H B M_0) - M_{(1+\xi_{2^r})^{k_l}}) \cdot E[\overrightarrow{v}_l \overrightarrow{v}_l^H] \cdot$$

$$\cdot(h_{ml}(M_0^H B^H M_0) - M_{(1+\xi_{2^r})^{k_l}}^H) +$$

$$+ M_0^H B E[\overrightarrow{z}_m \overrightarrow{z}_m^H] B^H M_0).$$

Let $E[\overrightarrow{v}_l \overrightarrow{v}_l^H] = P_s$, for all $l = 1, \ldots, L$, and $E[\overrightarrow{z}_m \overrightarrow{z}_m^H] = \sigma_N^2$, where P_s is the signal power, σ_N^2 is the noise variance and $\rho = \frac{P_s}{\sigma_N^2}$ is the signal-to-noise ratio (SNR). Then

$$E[\overrightarrow{v}_m^H \overrightarrow{v}_m] = P_s Tr(\sum_{l=1}^{L}(h_{ml}(M_0^H B M_0) - M_{(1+\xi_{2^r})^{k_l}}) \cdot$$

$$\cdot(h_{ml}(M_0^H B^H M_0) - M_{(1+\xi_{2^r})^{k_l}}^H) + \frac{1}{\rho} M_0^H B B^H M_0) =$$

$$= P_s Tr(\sum_{l=1}^{L} h_{ml}^2 (M_0^H B B^H M_0) -$$

$$-\sum_{l=1}^{L} h_{ml}[(M_0^H B M_0) M^H_{(1+\xi_{2^r})^{k_l}} + M_{(1+\xi_{2^r})^{k_l}} (M_0^H B^H M_0)] +$$

$$+\sum_{l=1}^{L} M_{(1+\xi_{2^r})^{k_l}} M^H_{(1+\xi_{2^r})^{k_l}} + \frac{1}{\rho} M_0^H B B^H M_0).$$

Thereby we have

$$E[\overrightarrow{v}^H_m \overrightarrow{v}_m] = P_s Tr((\|h\|^2 + \frac{1}{\rho}) M_0^H B B^H M_0 -$$

$$-\sum_{l=1}^{L} h_{ml} (M_0^H B M_0) M^H_{(1+\xi_{2^r})^{k_l}} - \sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}} (M_0^H B^H M_0) +$$

$$+\sum_{l=1}^{L} M_{(1+\xi_{2^r})^{k_l}} M^H_{(1+\xi_{2^r})^{k_l}}),$$

where $h = (h_{m1}, h_{m2}, \ldots, h_{mL})$.

Let $F = M_0^H B M_0$ ($F^H = M_0^H B^H M_0$) and $\eta = (\|h\|^2 + \frac{1}{\rho})$. Then

$$E[\overrightarrow{v}^H_m \overrightarrow{v}_m] = P_s \eta Tr(F \cdot F^H - \frac{1}{\eta} F \sum_{l=1}^{L} h_{ml} M^H_{(1+\xi_{2^r})^{k_l}} -$$

$$-\frac{1}{\eta} F^H \sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}} + \frac{1}{\eta} \sum_{l=1}^{L} M_{(1+\xi_{2^r})^{k_l}} M^H_{(1+\xi_{2^r})^{k_l}}) =$$

$$= P_s \eta Tr((F - \frac{1}{\eta} \sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}})(F - \frac{1}{\eta} \sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}})^H +$$

$$+\frac{1}{\eta} \sum_{l=1}^{L} M_{(1+\xi_{2^r})^{k_l}} M^H_{(1+\xi_{2^r})^{k_l}} -$$

$$-\frac{1}{\eta^2}(\sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}})(\sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}})^H).$$

Observe that $F = \frac{1}{\eta}\sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}}$ minimizes $E[\overrightarrow{v}_m^H \overrightarrow{v}_m]$. Since $F = M_0^H B M_0$, it follows that

$$BM_0 = \frac{1}{\eta} M_0 \sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}} \Leftrightarrow$$

$$\Leftrightarrow B = \frac{1}{\eta} M_0 (\sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}}) M_0^H =$$

$$= \frac{1}{\eta} \sum_{l=1}^{L} h_{ml} (M_0 M_{(1+\xi_{2^r})^{k_l}} M_0^H).$$

Hence $B = \frac{1}{\eta}\sum_{l=1}^{L} h_{ml}(M_0 M_{(1+\xi_{2^r})^{k_l}} M_0^H)$ minimizes $E[\overrightarrow{v}_m^H \overrightarrow{v}_m]$ and the mean square error is given by

$$P_s Tr(\sum_{l=1}^{L} M_{(1+\xi_{2^r})^{k_l}} M_{(1+\xi_{2^r})^{k_l}}^H -$$

$$-\frac{1}{\eta}(\sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}})(\sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}})^H) =$$

$$= P_s(\sum_{l=1}^{L} Tr(M_{(1+\xi_{2^r})^{k_l}} M_{(1+\xi_{2^r})^{k_l}}^H) - \frac{1}{\eta} \parallel \sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}} \parallel_F^2) =$$

$$= P_s(\sum_{l=1}^{L} \parallel M_{(1+\xi_{2^r})^{k_l}} \parallel_F^2 - \frac{1}{\eta} \parallel \sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}} \parallel_F^2),$$

with $\parallel A \parallel_F = \sqrt{Tr(AA^t)}$, where A is an $m \times n$ complex matrix. The norm $\parallel \cdot \parallel_F$ is called *Frobenius norm.*

Since

$$\parallel M_{(1+\xi_{2^r})^{k_l}} \parallel_F^2 = Tr(M_{(1+\xi_{2^r})^{k_l}} M_{(1+\xi_{2^r})^{k_l}}^H) =$$

$$= Tr(M_{(1+\xi_{2^r})^{k_l}} M^H_{(1+\xi_{2^r})^{k_l}} M_0^H M_0) =$$

$$= Tr(M_0 M_{(1+\xi_{2^r})^{k_l}} M^H_{(1+\xi_{2^r})^{k_l}} M_0^H) =$$

$$= \sum_{i=1}^{n} \sigma_i((1+\xi_{2^r})^{k_l})^2 = \sum_{i=1}^{n} \sigma_i(((1+\xi_{2^r})^{k_l})^2) =$$

$$= Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(((1+\xi_{2^r})^{k_l})^2) \text{ and}$$

$$\| \sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}} \|_F^2 = Tr((\sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}})(\sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}})^H) =$$

$$= Tr(M_0(\sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}})(\sum_{l=1}^{L} h_{ml} M_{(1+\xi_{2^r})^{k_l}})^H M_0^H) =$$

$$= Tr((\sum_{l=1}^{L} h_{ml} M_0 M_{(1+\xi_{2^r})^{k_l}})(\sum_{l=1}^{L} h_{ml} M^H_{(1+\xi_{2^r})^{k_l}} M_0^H)) =$$

$$= \sum_{l,j=1}^{L} h_{ml} h_{mj} Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}((1+\xi_{2^r})^{k_l}(1+\xi_{2^r})^{k_j}),$$

the mean square error is given by

$$P_s(\sum_{l=1}^{L} Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(((1+\xi_{2^r})^{k_l})^2) -$$

$$-\frac{1}{\eta} \sum_{l,j=1}^{L} h_{ml} h_{mj} Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}((1+\xi_{2^r})^{k_l}(1+\xi_{2^r})^{k_j})) =$$

$$= P_s \frac{1}{\eta}(\eta \sum_{l=1}^{L} Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(((1+\xi_{2^r})^{k_l})^2) -$$

$$- \sum_{l,j=1}^{L} h_{ml} h_{mj} Tr_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}((1+\xi_{2^r})^{k_l}(1+\xi_{2^r})^{k_j})).$$

Acknowledgment

This work has been supported by the following Brazilian Agencies: FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) under grants No. 2013/03976-9 and 2013/25977-7, CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) under grant No. 6562-10-8 and CNPq (Conselho Nacional de Desenvolvimento Cientfico e Tecnolgico) under grant No. 303059/2010-9.

References

[1] J. Tang and S. Lambotharan, Interference alignment techniques for MIMO multi-cell interfering broadcast channels, *IEEE Trans. on Communications*, **61** (2013), 164-175.

[2] A.R. Calderbank and N.J.A. Sloane, New trellis codes based on lattices and cosets, *IEEE Trans. on Information Theory*, **33** (1987), 177-195.

[3] G.D. Forney, Coset Codes - Part I: Introduction and geometrical classification, *IEEE Transactions on Information Theory*, **34**, No 5 (1998), 1123-1151.

[4] R. Zamir, Lattices are everywhere, In: *Proc. 4th Annual Workshop on Information Theory and its Applications (ITA)* (2009).

[5] X. Giraud, E. Boutillon and J-C. Belfiore, Algebraic tools to build modulation schemes for fading channels, *IEEE Transactions on Information Theory*, **43**, No 3 (1997), 938-952.

[6] J. Leech and N.J.A. Sloane, Sphere packings and error correcting codes, *Canadian J. of Mathematics*, **23** (1971), 718-745.

[7] E. Bayer-Fluckiger, F. Oggier and E. Viterbo, Algebraic lattice constellations: bounds on performance, *IEEE Trans. on Information Theory*, **52**, No 1 (2006), 319-327.

[8] S. Lang, *Complex Multiplication*, Springer-Verlag, New York (1983).

[9] C.C. Trinca, J.-C. Belfiore, E.D. de Carvalho and J. Vieira Filho, Coding for the Gaussian interference channel, In: *XXXI Simposio Brasileiro de Telecomunicaes (SBrT)* (2013).

[10] C.C. Trinca, J.-C. Belfiore, E.D. de Carvalho and J. Vieira Filho, Construction of nested 4-dimensional complex lattices in order to realize interference alignment onto a lattice, In: *6th Internat. Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC 2015)* (2015).

[11] B.R. Hodgson, On some number sequences related to the parity of binomial coefficients, *Université Laval, Québec G1K 7P4, Canada*, **30**, No 1 (1990), 35-47.

[12] K. Conrad, Dirichlet's unit theorem, Retrieved from: *http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/unittheorem.pdf.*

[13] B. Nazer and M. Gastpar, Compute-and-forward: Harnessing interference through structured codes, *IEEE Trans. on Information Theory*, **57**, No 10 (2011), 6463-6486.