Trends in Computational and Applied Mathematics, **23**, N. 1 (2022), 33-50
Sociedade Brasileira de Matemática Aplicada e Computacional
Online version ISSN 2676-0029
www.scielo.br/tcam
doi: 10.5540/tcam.2022.023.01.00033

Construction of Complex Lattice Codes via Cyclotomic Fields

E. D. DE CARVALHO[1*], A. A. ANDRADE[2], T. SHAH[3] and C. C. TRINCA[4]

Received on April 20, 2021 / Accepted on June 18, 2021

ABSTRACT. Through algebraic number theory and Construction A we extend an algebraic procedure which generates nested complex lattice codes from the polynomial ring $\mathbb{F}_2[x]/(x^n-1)$, where $\mathbb{F}_2=\{0,1\}$, by using ideals from the generalized polynomial ring $\frac{\mathbb{F}_2[x,\frac{1}{2}\mathbb{Z}_0]}{((x^{\frac{1}{2}})^{2n}-1)}$ through the ring of integers $\mathscr{O}_{\mathbb{L}}$ of the cyclotomic field $\mathbb{L}=\mathbb{Q}(\zeta_{2^s})$, where ζ_{2^s} is a 2^s-th root of the unit, with $s>2$.

Keywords: complex lattice codes, binary cyclotomic fields, monoid Rings.

1 INTRODUCTION

Several works [5], [6], [3], [10], [8] over lattice theory have been dedicated to *Construction A* and lattice set partitioning via coset codes. The advantage of these algebraic approaches is that it is possible to unify different coding problems related to algebraic block codes and Euclidean space codes.

Construction A has been introduced by Conway and Sloane [3] where the authors establish an algebraic correspondence between lattices from $\mathbb{R}^n$ or $\mathbb{C}^n$ and linear codes over finite fields $\mathbb{F}_p$. Codes obtained by Construction A are denominated *lattice codes*.

In this work we have interest in scaled versions of the $\mathbb{Z}[i]^n$-lattice, i.e., complex lattices isomorphic to the lattice $\phi^k\mathbb{Z}[i]^n$, for some Gaussian integer ϕ and some positive integer k. Such n-dimensional complex lattices are the simplest lattices obtained in $\mathbb{C}^n$. Since we consider the

*Corresponding author: Edson Donizete de Carvalho – E-mail: edson.donizete@unesp.br
[1]State University of São Paulo, Department of Mathematics, FEIS, Av. Brasil Sul, 56, Centro, 15385-000, Ilha Solteira, SP, Brazil – E-mail: edson.donizete@unesp.br https://orcid.org/0000-0003-1016-7632
[2]State University of São Paulo, Department of Mathematics, IBILCE, R. Cristóvão Colombo, 2265, Jardim Nazareth, 15054-000, São José do Rio Preto, SP, Brazil – E-mail: antonio.andrade@unesp.br https://orcid.org/0000-0001-6452-2236
[3]University of Quaid-i-Azam, Department of Mathematics, Quaid-i-Azam University Islamabad, 45320, Islamabad, Paquistan – E-mail: stariqshah@gmail.com https://orcid.org/0000-0002-6587-1638
[4]Federal University of Tocantins, Department of Bioprocess and Biotechnology Engineering,UFT, Chácara 69-72 Rua Badejós, Lote 7 s/n, Jardim Sevilha, 77404-970, Gurupi, TO, Brazil – E-mail: cibtrinca@yahoo.com.br https://orcid.org/0000-0003-2857-7410

$\mathbb{Z}[i]^n$-lattice generated by the canonical basis, it is simple to characterize the corresponding fundamental region.

From a chain of nested binary cyclic codes given by equation (1.1)

$$\mathscr{C}_{n-1} \subset \mathscr{C}_{n-2} \subset \ldots \mathscr{C}_1 \subset \mathscr{C}_0 \tag{1.1}$$

and a chain of nested complex lattices given by equation (1.2)

$$(1+i)^{n-1}\mathbb{Z}[i]^n \subset (1+i)^{n-2}\mathbb{Z}[i]^n \subset \ldots \subset (1+i)\mathbb{Z}[i]^n \subset \mathbb{Z}[i]^n, \tag{1.2}$$

Forney in [5] proposes a practical way to encoding lattices via Construction A, therefore each binary cyclic code $\mathscr{C}_k$ can be seen as the set of all n-tuples reduced by the residue system of the complex lattice $(1+i)^k\mathbb{Z}[i]^n$ modulo $(1+i)$.

By using this algebraic approach, Forney [5] shows how binary codes, lattice codes and trellis codes can be constructed as coset codes. These cosets are formed by the sequences of signal points of the outputs of binary encoders. As a consequence of the identification of the complex coset codes $(1+i)^k\mathbb{Z}[i]^n/(1+i)\mathbb{Z}[i]^n$ with the binary codes $\mathscr{C}_k$, respectively, we can see the algebraic block codes $\mathscr{C}_k$ [5] as principal ideals of the factor ring $\mathbb{F}_2[x]/(x^n-1)$ of the Euclidean domain $\mathbb{F}_2[x]$, where $\mathbb{F}_2$ denotes the binary field.

On the other hand, Andrade and Palazzo [4] propose a new method to construct cyclic, BCH, alternant, Goppa and Srivastava codes. In this new algebraic approach the authors obtain cyclic codes from principal ideals of the factor ring $\mathbb{F}_p[x]/(x^n-1)$ of the polynomial ring $\mathbb{F}_p[x]$, where $\mathbb{F}_p$ denotes the finite field, while Shah et al. [1] use a monoid ring instead of a polynomial ring and also obtain cyclic, BCH, alternant, Goppa and Srivastava codes.

The main goal of this work is to extend the procedure of constructing complex lattice codes on $\mathbb{C}^n$ via the polynomial ring $\mathbb{F}_2[x]/(x^n-1)$ to the monoid ring $\frac{\mathbb{F}_2[x,\frac{1}{2}\mathbb{Z}_0]}{((x^{\frac{1}{2}})^{2n}-1)}$ [1]. If we continue the discussion of lattice codes from an algebraic and geometric point of view, the following question appears in this context:

Is it possible to obtain a similar algebraic/geometric procedure to obtain a correspondence between binary algebraic block codes obtained from monoid rings and binary lattice codes?

The goal of this paper is to develop fundamental tolls from the theory of algebraic lattices and linear codes over the polynomial ring $\mathbb{F}_2[x]/(x^n-1)$ and the monoid ring $\frac{\mathbb{F}_2[x,\frac{1}{2}\mathbb{Z}_0]}{((x^{\frac{1}{2}})^{2n}-1)}$ to answer this question. Algebraic number theory provides an effective mean to construct scaled versions of the $\mathbb{Z}[i]^n$-lattice obtained via totally complex number fields [12], [2] and [11]. These scaled versions of the $\mathbb{Z}[i]^n$-lattice are given by algebraic lattices obtained via the canonical embeddings applied on ideals from a ring of a totally complex number field.

By using concepts from the ramification index of the prime ideal $\mathscr{I} = (1-\zeta_{2^s})$ on the Galois extension $\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(i)$ of degree $n = 2^{s-2}$, we establish a general correspondence between the sequence of the ideals $\mathscr{I}^k = (1-\zeta_{2^s})^k\mathbb{Z}[\zeta_{2^s}]$, where $k \in \{0,1,\cdots,n-1\}$, and the sequence of

the nested lattices Λ_k which are a scaled version of the $\mathbb{Z}[i]^n$-lattice and are obtained through the relative embedding of the ideals $\mathscr{I}^k$ in $\mathbb{C}^n$, where $\mathbb{Z}[\zeta_{2^s}]$ is the algebraic ring of integer of the number field $\mathbb{Q}(\zeta_{2^s})$ and ζ_{2^s} is a 2^s-th root of unity.

Consequently, this leads us two similar algebraic procedures. In the first one we identify the sets of all n-tuples reduced by the residue system of the nested complex lattices Λ_k modulo $(1+i)$ with complex lattice codes proposed by Forney [5] as ideals from the factor ring $\mathbb{F}_2[x]/(x^n-1)$. In the second one we rewrite the ζ_{2^s}-th root of unity and, consequently, we also identify the sets of all n-tuples reduced by the residue system of the nested complex lattices Λ_k modulo $(1+i)$ with complex lattice codes proposed by Forney [5] as ideals from the monoid ring $\frac{\mathbb{F}_2[x,\frac{1}{2}\mathbb{Z}_0]}{((x^{\frac{1}{2}})^{2n}-1)}$ [1].

2 GENERALIZED POLYNOMIALS AND CYCLIC CODES

Let $(S,*)$ and $(\mathscr{R},+,\cdot)$ be a commutative semigroup and an associative, commutative and unitary ring, respectively. The set $\mathscr{T}$ is given by all finite nonzero functions f from S to $\mathscr{R}$, where $\mathscr{R}$ is a ring with respect to the addition and multiplication operations which are defined as: $(f+g)(s)=f(s)+g(s)$ and $(f\cdot g)(s)=\sum\limits_{t*u=s} f(t)g(u)$, where the symbol $\sum\limits_{t*u=s}$ indicates that the sum is taken over all the pairs (t,u) of elements from S such that $t*u=s$. Whenever s cannot be written on the form $t*u$, with $t,u\in S$, then it is settled that $(f\cdot g)(s)=0$.

If S is monoid, then $\mathscr{T}$ is called *monoid ring*. This ring $\mathscr{T}$ is represented by $\mathscr{R}[S]$ whenever S is a multiplicative semigroup and the elements of $\mathscr{T}$ are written either as $\sum\limits_{s\in S} f(s)s$ or as $\sum\limits_{i=1}^{n} f(s_i)s_i$. The representation of $\mathscr{T}$ is given by $\mathscr{R}[x;S]$ whenever S is an additive semigroup. A nonzero element f of $\mathscr{R}[x;S]$ is uniquely represented in the canonical form $\sum\limits_{i=1}^{n} f(s_i)x^{s_i}=\sum\limits_{i=1}^{n} f_i x^{s_i}$, where $f_i\neq 0$ and $s_i\neq s_j$, for $i\neq j$, and is called *generalized polynomial*.

The concepts of degree and order are not generally defined in a semigroup ring. Though, if S is a totally ordered semigroup, then the degree and the order of an element of the monoid ring $\mathscr{R}[x;S]$ can be defined. If $f=\sum\limits_{i=1}^{n} f_i x^{s_i}$ is the canonical form of the nonzero element $f\in\mathscr{R}[x;S]$, where $s_1<s_2<\cdots<s_n$, then s_n is called the degree of f and we denote it by $\deg(f)=s_n$. Analogously, the order of f is defined and denoted by $ord(f)=s_1$. Now, if $\mathscr{R}$ is an integral domain, then, for $f,g\in\mathscr{R}[x;S]$, it follows that $\deg(fg)=\deg(f)+\deg(g)$ and $ord(fg)=ord(f)+ord(g)$. By [1], for a commutative ring B with identity, $\mathfrak{R}=\frac{B[x,\frac{1}{2}\mathbb{Z}_0]}{((x^{\frac{1}{2}})^n-1)}$ is a finite ring.

A linear code $\mathscr{C}$ of length n over B is a submodule in the space of all n-tuples of B^n and $\mathscr{C}$ is a cyclic code, if $v=(v_0,v_{\frac{1}{2}},v_1,\cdots,v_{\frac{n-1}{2}})\in\mathscr{C}$, every cyclic shift $v^{(1)}=(v_{\frac{n-1}{2}},v_0,v_{\frac{1}{2}},\cdots,v_{n-2})\in\mathscr{C}$, where $v_{\frac{i}{2}}\in B$, for $i=0,1,\cdots,n-1$.

Theorem 2.1. *[1] A subset $\mathscr{C}$ of $\mathfrak{R}=\frac{B[x,\frac{1}{2}\mathbb{Z}_0]}{((x^{\frac{1}{2}})^n-1)}$ is a cyclic code if and only if $\mathscr{C}$ is an ideal of $\mathfrak{R}$.*

If $f(x^{\frac{1}{2}}) \in B[x, \frac{1}{2}\mathbb{Z}_0]$ is a monic pseudo polynomial of degree n, then $\Re = \frac{B[x,\frac{1}{2}\mathbb{Z}_0]}{(f(x^{\frac{1}{2}}))}$ is the set of residue classes of pseudo polynomials in $B[x, \frac{1}{2}\mathbb{Z}_0]$ module the ideal $(f(x^{\frac{1}{2}}))$ and a class can be represented as $\overline{a}(x^{\frac{1}{2}}) = \overline{a}_0 + \overline{a}_{\frac{1}{2}} x^{\frac{1}{2}} + \overline{a}_1 x + \cdots + \overline{a}_{\frac{n-1}{2}} (x^{\frac{1}{2}})^{\frac{n-1}{2}}$.

Let $B = \mathbb{F}_2[x]$, where $\mathbb{F}_2$ is the binary field.

Proposition 2.2. *The binary polynomial $x^n - 1$ is factored over the ring $\mathbb{F}_2[x]$ as the product of n monomials of the form $(x-1)$, i.e.,*

$$x^n - 1 = (x-1)^n.$$

Proof. Over the polynomial ring $\mathbb{F}_2[x]$, it follows that $x^n - 1 = (x-1)^n$. In fact, from Newton's binomial theorem for $(x-1)^n$, it follows that

$$(x-1)^n = x^n + \binom{n}{1} x^{n-1}(-1) + \cdots + \binom{n}{n} (-1)^n. \tag{2.1}$$

Since $n = 2^s$ and the coefficients are in $\mathbb{F}_2$, then it follows that $x^n - 1 = (x-1)^n$ (observe that $-1 \equiv 1$ *mod* 2). Therefore the polynomial $x^n - 1$ can be written as

$$x^n - 1 = \underbrace{(x-1).....(x-1)}_{n\ times}. \tag{2.2}$$

□

From Equation (2.2), it follows that the binary polynomial $x^n - 1$ has 2^n divisors in $\mathbb{F}_2[x]$. Thenceforth there are 2^n cyclic codes generated by the binary polynomials which divide the polynomial $x^n - 1$ in the polynomial ring $\mathbb{F}_2[x]$. Let $\mathbb{F}_2[x, \frac{1}{2}\mathbb{Z}_0]$, where $\mathbb{F}_2$ is the binary field, then we have the following result.

Proposition 2.3. *The generalized polynomial $((x^{\frac{1}{2}})^{2n} - 1)$ is factored in the generalized polynomial ring $\mathbb{F}_2[x, \frac{1}{2}\mathbb{Z}_0]$ as the product of $2n$ generalized monomials of the form $(x^{\frac{1}{2}} - 1)$, i.e.,*

$$(x^{\frac{1}{2}})^{2n} - 1 = ((x^{\frac{1}{2}}) - 1)^{2n}.$$

Proof. Analogously to the proof of Proposition 2.2, it follows that

$$(x^{\frac{1}{2}})^{2n} - 1 = \underbrace{((x^{\frac{1}{2}}) - 1).....((x^{\frac{1}{2}}) - 1)}_{2n\ times}, \tag{2.3}$$

which proves the result. □

It is provided from Equation (2.3) that the generalized polynomial $(x^{\frac{1}{2}})^{2n} - 1$ has 2^{2n} divisors in $\mathbb{F}_2[x, \frac{1}{2}\mathbb{Z}_0]$. Then there are 2^{2n} cyclic codes generated by the generalized polynomials which divide the generalized polynomial $(x^{\frac{1}{2}})^{2n} - 1$ in the generalized polynomial ring $\mathbb{F}_2[x, \frac{1}{2}\mathbb{Z}_0]$.

3 RESULTS FROM ALGEBRAIC NUMBER THEORY

Let $\mathbb{F}$ and $\mathbb{L}$ be fields such that $\mathbb{F} \subseteq \mathbb{L}$. We say that $\mathbb{L}$ is a finite extension of $\mathbb{F}$ if the dimension of $\mathbb{L}$ as a vector space over $\mathbb{F}$ is finite and we denote it by $\mathbb{L}/\mathbb{F}$.

The Galois group $Gal(\mathbb{L}/\mathbb{F})$ associated with the finite extension $\mathbb{L}/\mathbb{F}$ is defined as the set of all automorphisms σ of $\mathbb{L}$ that fix every element of $\mathbb{F}$. The order of the Galois group satisfies $o(Gal(\mathbb{L}/\mathbb{F})) \leq [\mathbb{L} : \mathbb{F}]$. The extension field is said to be Galois if the equality holds and it is called Abelian (cyclic) if the Galois group is Abelian (cyclic). We say that $\mathbb{L}$ is an algebraic number field if $\mathbb{F} = \mathbb{Q}$, that is, if $\mathbb{L}$ is a finite extension of $\mathbb{Q}$.

If $\mathbb{L}$ is an algebraic number field, an element $w \in \mathbb{L}$ is called an algebraic integer if there is a monic polynomial $p(x) \in \mathbb{Z}[x]$ such that $p(w) = 0$. The set

$$\mathscr{O}_{\mathbb{L}} = \{w \in \mathbb{L} \mid w \text{ is an algebraic integer}\} \tag{3.1}$$

is called ring of integers of $\mathbb{L}$. It can be shown that $\mathscr{O}_{\mathbb{L}}$ as a $\mathbb{Z}$ - module has a basis $\{w_0, \ldots, w_{n-1}\}$ over $\mathbb{Z}$ called integral basis, that is, every element $w \in \mathscr{O}_{\mathbb{L}}$ can be uniquely written as $w = \sum_{i=1}^{n} a_i w_i$, where $a_i \in \mathbb{Z}$, for all $i = 1, 2, \cdots, n$.

Example 3.1. *Let $\mathbb{L}$ a cyclotomic field given by $\mathbb{L} = \mathbb{Q}(\zeta_{2^s})$, with $s \geq 2$, where ζ_{2^s} is a primitive 2^s-th root of unity. Furthermore:*

1. *This extension field is a Galois extension with*

$$Gal(\mathbb{L}/\mathbb{Q}) = \{\sigma_j : \sigma_j(\zeta_m) = \zeta_m^j, \text{ where } gcd(m, j) = 1\}$$

which is a cyclic multiplicative group of order $2^{s-1} = \varphi(2^s) = \#\{0 \leq m < 2^s \mid gcd(m, 2^s) = 1,\ m \in \mathbb{Z}\}$. The function φ is called Euler function;

2. *We denote the ring of integers of $\mathbb{L}$ by $\mathscr{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_{2^s}]$ and its integral basis is given by $\{1, \zeta_{2^s}, \zeta_{2^s}^2, \ldots, \zeta_{2^s}^{\varphi(2^s)-1}\} = \{1, \zeta_{2^s}, \zeta_{2^s}^2, \ldots, \zeta_{2^s}^{2^{s-1}-1}\}$.*

Let $\mathbb{Q}(\zeta_{2^{s-1}})$ and $\mathbb{Q}(\zeta_{2^s})$ denoted by $\mathbb{L}_{s-1}$ and $\mathbb{L}_s$, respectively. Consequently we have $\mathbb{L}_s = \mathbb{L}_{s-1}(\zeta_{2^s})$. Thenceforward we obtain the following tower of finite extension fields

$$\mathbb{L}_s/\mathbb{L}_{s-1}/\cdots/\mathbb{L}_3/\mathbb{L}_2,$$

where $[\mathbb{L} = \mathbb{L}_s : \mathbb{L}_{s-1}] = [\mathbb{L}_{s-1} : \mathbb{L}_{s-2}] = \cdots = [\mathbb{L}_3 : \mathbb{L}_2] = 2$ and $\mathbb{L}_2 = \mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$. Also the minimal polynomial $\mu_{\zeta_{2^s}}(x)$ of ζ_{2^s} over $\mathbb{Z}[i]$ has degree $\frac{\varphi(2^s)}{2} = \frac{2^{s-1}}{2} = 2^{s-2}$ and it is given by

$$\mu_{\zeta_{2^s}}(x) = \prod_{i=0}^{2^{s-2}-1} (x - \zeta_{2^s}^i). \tag{3.2}$$

From there the 2^{s-2} distinct $\mathbb{Q}(i)$-homomorphisms are denoted by σ_i, where $i \in \{0, \ldots, 2^{s-2}-1\}$, and $\sigma_i(\zeta_{2^s}) = \zeta_{2^s}^i$, for all $i \in \{0, \ldots, 2^{s-2}-1\}$.

If $\mathbb{L}$ is an algebraic number field of degree n, then the trace and the norm of an element $w \in \mathbb{L}$ are defined as the numbers $Tr_{\mathbb{L}/\mathbb{Q}}(w) = \sum_{i=0}^{n-1} \sigma_i(w)$ and $N_{\mathbb{L}/\mathbb{Q}}(w) = \prod_{i=0}^{n-1} \sigma_i(w)$, respectively. Furthermore:

1. If $\mathbb{L}/\mathbb{K}/\mathbb{Q}$ is a tower of finite extension fields, then, for each $w \in \mathbb{L}$, it follows that

$$N_{\mathbb{L}/\mathbb{Q}}(w) = N_{\mathbb{K}/\mathbb{Q}}(N_{\mathbb{L}/\mathbb{K}}(w)); \tag{3.3}$$

2. If $x, y \in \mathbb{L}$, then

$$N_{\mathbb{L}/\mathbb{Q}}(xy) = N_{\mathbb{L}/\mathbb{Q}}(x)N_{\mathbb{L}/\mathbb{Q}}(y). \tag{3.4}$$

Let $\{w_0, w_1, \cdots, w_{N-1}\}$ be an integral basis of $\mathscr{O}_{\mathbb{L}}$ and let $\Im$ be an ideal of $\mathscr{O}_{\mathbb{L}}$. The *norm* of $\Im$ is defined by $\mathscr{N}_{\mathbb{L}/\mathbb{Q}}(\Im) = |\mathscr{O}_{\mathbb{L}}/\Im|$, i.e., it is the cardinality of the quotient ring $\mathscr{O}_{\mathbb{L}}/\Im$. If ζ_{2^s} is a 2^s-th root of unity, then $\zeta_{2^s}^2 = \zeta_{2^{s-1}}$ or, equivalently,

$$\zeta_{2^s} = \zeta_{2^{s-1}}^{\frac{1}{2}}. \tag{3.5}$$

Lemma 3.1. *If $s \geq 3$, then $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(\zeta_{2^{s-1}})}(1-\zeta_{2^s}) = 1-\zeta_{2^{s-1}}$.*

Proof. The finite extension field $\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(\zeta_{2^{s-1}})$ has degree 2. Consequently, we can see $\mathbb{Q}(\zeta_{2^s})$ as a field extension of the field $\mathbb{Q}(\zeta_{2^{s-1}})$ whose minimal polynomial is given by $m(x) = x^2 - \zeta_{2^{s-1}}$ and the Galois group is given by $G(\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(\zeta_{2^{s-1}}) = \{id, \sigma_1\}$, where $id(\zeta_{2^s}) = \zeta_{2^s}$ and $\sigma_1(\zeta_{2^s}) = -\zeta_{2^s}$. Therefore, $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(\zeta_{2^{s-1}})}(1-\zeta_{2^s}) = (1-\zeta_{2^s})(1+\zeta_{2^s}) = 1-\zeta_{2^s}^2 = 1-\zeta_{2^{s-1}}$. □

Proposition 3.2. *If $s \geq 3$, then $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(i)}(1-\zeta_{2^s}) = 1-i$.*

Proof. If $s = 3$, then $N_{\mathbb{Q}(\zeta_{2^3})/\mathbb{Q}(i)}(1-\zeta_{2^3}) = N_{\mathbb{Q}(\zeta_{2^3})/\mathbb{Q}(\zeta_{2^2})}(1-\zeta_{2^3})$. By Lemma 3.1, we have that $N_{\mathbb{Q}(\zeta_{2^3})/\mathbb{Q}(\zeta_{2^2})}(1-\zeta_{2^3}) = 1-\zeta_{2^2} = 1-i$. Now we consider an induction over $s-1$, that is, suppose that $N_{\mathbb{Q}(\zeta_{2^{s-1}})/\mathbb{Q}(i)}(1-\zeta_{2^{s-1}}) = 1-i$. By using the fact that the property of relative norm on finite extensions is transitive, we have

$$N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(i)}(1-\zeta_{2^s}) = N_{\mathbb{Q}(\zeta_{2^{s-1}})/\mathbb{Q}(i)}(N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(\zeta_{2^{s-1}})}(1-\zeta_{2^s})).$$

By Lemma 3.1, it follows that $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(\zeta_{2^{s-1}})}(1-\zeta_{2^s}) = 1-\zeta_{2^{s-1}}$. Thus, by using induction over $s-1$, we have that $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(i)}(1-\zeta_{2^s}) = 1-i$. □

Remark 3.3. *Since $[\mathbb{Q}(\zeta_{2^s}) : \mathbb{Q}(i)] = n$, from Proposition 3.2, it follows that $(1-i)\mathbb{Z}[\zeta_{2^s}]$ is completely factored as a power of prime ideal in $\mathbb{Z}[\zeta_{2^s}]$ of the form $(1-i)\mathbb{Z}[\zeta_{2^s}] = (1-\zeta_{2^{s-1}})^n\mathbb{Z}[\zeta_{2^s}]$, where $n = \frac{\varphi(2^s)}{2} = \frac{2^{s-1}}{2} = 2^{s-2}$.*

4 COMPLEX LATTICES AND LATTICE CODES

If Λ is an n-dimensional complex lattice with basis $\{u_1, u_2, \ldots, u_m\}$, then its *generator matrix* is given by

$$M = \begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ u_{21} & u_{22} & \cdots & u_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{m1} & u_{m2} & \cdots & u_{mn} \end{pmatrix},$$

where $u_i = (u_{i1}, u_{i2}, \ldots, u_{in})$, for $i = 1, 2, \ldots, m$.

The matrix $G = MM^T$ is called *Gram matrix* of the complex lattice Λ, where M^T denotes the transpose of M. We can also define $\Lambda = \{x = \lambda M \mid \lambda \in \mathbb{Z}[i]^m\}$. The *determinant of the lattice* Λ is defined as the determinant of the matrix G, that is, $Det(\Lambda) = Det(G)$.

The fundamental parallelepiped of Λ is the set $\mathscr{P}_0$ formed by all points in $\mathbb{C}^n$ which are convex combinations of vectors of the basis, that is, $\mathscr{P}_0 = \{x = \sum_{i=1}^m \alpha_i u_i \mid \alpha_i \geq 0 \text{ and } \sum_{i=1}^m \alpha_i = 1\}$.

A subset $\Lambda' \subset \Lambda$ is called *sublattice* if Λ' itself is a lattice, i.e, Λ' is an additive subgroup of Λ. The sublattice Λ' can also be characterized as $\Lambda' = \{x = \lambda BM \mid \lambda \in \mathbb{Z}[i]^m\}$, where M is the generator matrix associated with the lattice Λ and B is a scaling matrix with integral entries.

The sublattice Λ' induces a partition of Λ into classes which is called *quotient lattice* and it is denoted by Λ/Λ'. The cardinality of Λ/Λ' is given by

$$|\Lambda/\Lambda'| = \frac{volume(\mathscr{P}'_0)}{volume(\mathscr{P}_0)} = |det(B)|, \tag{4.1}$$

where $volume(\mathscr{P}'_0)$ and $volume(\mathscr{P}_0)$ denote the volume of the fundamental parallelepiped $\mathscr{P}'_0$ (associated with the sublattice Λ') and the volume of the fundamental parallelepiped $\mathscr{P}_0$ (associated with the lattice Λ), respectively.

4.1 Complex ideal lattices from $\mathbb{Q}(\zeta_{2^s})$

In Section 4.2 we build, for each n, a chain of nested complex lattices which are isomorphic to scaled versions of the lattice $\mathbb{Z}[i]^n$. For that we make use of ideal lattices which are obtained from ideals of the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta_{2^s})$.

Let $\mathbb{L} = \mathbb{Q}(\zeta_{2^s})$ be a finite extension field over $\mathbb{Q}(i)$ with degree $n = 2^{s-2}$, where $s \geq 3$. From an ideal $\Im \subseteq \mathscr{O}_\mathbb{L} = \mathbb{Z}[\zeta_{2^s}]$ (ring of integers of the number field $\mathbb{L}$), we can obtain a complex algebraic lattice Λ by using the relative complex embedding of $\mathbb{L}$ into $\mathbb{C}^n$ which is defined as it follows:

$$\sigma : \mathbb{L} \Rightarrow \mathbb{C}^n, \text{ with } \sigma(x) = (\sigma_0(x), \ldots, \sigma_{n-1}(x)), \tag{4.2}$$

where $\sigma_i \in Gal(\mathbb{L}/\mathbb{Q}(i))$, for all $i \in \{0, 1, \ldots, n-1\}$.

Remark 4.1. *Note that the lattice Λ in $\mathbb{C}^n$ is obtained through the relative complex embedding* (4.2) *applied to the ideal $\Im$. Besides the application* (4.2) *establishes an isomorphism between $\mathscr{O}_\mathbb{L}$ and the $\mathbb{Z}[i]^n$-lattice.*

Let $\{1, \zeta_{2^s}, \ldots, \zeta_{2^s}^{n-1}\}$ be a $\mathbb{Z}[i]$-basis of the ring of integers $\mathbb{Z}[\zeta_{2^s}]$, then a generator matrix M of the complex lattice $\mathbb{Z}[i]^n$ is given by

$$M = \begin{pmatrix} \sigma_0(1) & \cdots & \sigma_{n-1}(1) \\ \vdots & \ddots & \vdots \\ \sigma_0(\zeta_{2^s}^{n-1}) & \cdots & \sigma_{n-1}(\zeta_{2^s}^{n-1}) \end{pmatrix}. \tag{4.3}$$

Proposition 4.2. *[7] The matrix M obtained from Equation (4.3) is a generator matrix of the complex ideal lattice $\mathbb{Z}[i]^n$ if, and only if, the complex conjugation commutes with all σ_i, for all $i \in \{0, 1, \cdots, n-1\}$.*

The field $\mathbb{Q}(\zeta_{2^s})$, where $s \geq 3$, is a *CM* field, i.e., $\mathbb{Q}(\zeta_{2^s})$ is a totally imaginary quadratic extension of $\mathbb{K} = \mathbb{Q}(\theta)$, where $\theta = \zeta_{2^s} + \zeta_{2^s}^{-1}$.

Proposition 4.3. *[7] A complex ideal lattice $\Lambda = (\Im, b)$ is a $\mathbb{Z}[i]$-lattice, where $\Im$ is a $\mathbb{Z}[\zeta_{2^s}]$-ideal, b is a bilinear form given by $b(x,y) = T_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(i)}(x\overline{y})$, for all $x, y \in \Im$, and $\overline{a} = \overline{a_1 + a_2 i} = a_1 - a_2 i$ denotes the complex conjugation in $\mathbb{Z}[i]$.*

The matrix

$$G = M\overline{M}^t = \begin{pmatrix} \sum_{i=0}^{n-1} \sigma_i(1)\overline{\sigma_i(1)} & \cdots & \sum_{i=0}^{n-1} \sigma_i(1)\overline{\sigma_i(\zeta_{2^s}^{n-1})} \\ \vdots & \ddots & \vdots \\ \sum_{i=0}^{n-1} \sigma_i(\zeta_{2^s}^{n-1})\overline{\sigma_i(1)} & \cdots & \sum_{i=0}^{n-1} \sigma_i(\zeta_{2^s}^{n-1})\overline{\sigma_i(\zeta_{2^s}^{n-1})} \end{pmatrix} \tag{4.4}$$

is called Gram matrix of the ideal lattice $\mathbb{Z}[i]^n$.

Next proposition provides us complex ideal lattices related to principal ideals.

Proposition 4.4. *[7] Let $\Im = \alpha\mathbb{Z}[\zeta_{2^s}]$ be a principal ideal of $\mathbb{Z}[\zeta_{2^s}]$. Then $\Lambda = (\Im, b)$ is a complex ideal lattice over $\mathbb{Z}[i]$, where b is a bilinear form given by $b(x,y) = cT_{\mathbb{Z}[\zeta_{2^s}]/\mathbb{Q}(i)}(x\overline{y})$, for all $x, y \in \Im$, and c is a normalized factor.*

Observe that $T_{\mathbb{Z}[\zeta_{2^s}]/\mathbb{Q}(i)}(\alpha w_j \overline{\alpha}\overline{w_j})_{j=0}^{n-1}$ can be written as the product of matrices given by $MU\overline{U}^t\overline{M}^t$, where M is the matrix related to the relative embedding defined in (4.3) and $U = dig(\sigma_0(\alpha), \ldots, \sigma_{n-1}(\alpha))$.

4.2 Scaled versions of the $\mathbb{Z}[i]^n$-lattice from $\mathbb{Q}(\zeta_{2^s})$

Trinca et al. in [11] show that complex ideal lattices obtained from the complex relative embedding (4.2) of ideals from $\mathbb{Z}[\zeta_{2^s}]$ are isomorphic to a scaled version of the $\mathbb{Z}[i]^n$-lattice. In this section we show that the complex ideal lattices Λ_k obtained through the ideals $\Im^k$, where $k \in \{0, \ldots, n-1\}$, from $\mathbb{Z}[\zeta_{2^s}]$ are isomorphic to $(1-i)^k\mathbb{Z}[i]^n$ and are a scaled version of $\mathbb{Z}[i]^n$, that is, $det(\Lambda_k) = 2^k$ since the Gram matrix of $(1-i)^k\mathbb{Z}[i]^n$ is $2^k Id$.

By Proposition 3.2, since $\alpha = 1-\zeta_{2^s}$, we have $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}}(1-\zeta_{2^s}) = 2$. For each $k \in \{0,1,\ldots,n-1\}$, we have the element $\alpha = (1-\zeta_{2^s})^k$, then the Gram matrix G_k associated with complex ideal lattice Λ_k is $G_k = M_k\overline{M_k}^t$, where M_k is the generator matrix associated with Λ_k which is given by

$$M_k = \begin{pmatrix} \alpha & \alpha\zeta_{2^s} & \cdots & \alpha\zeta_{2^s}^{n-1} \\ \sigma_2(\alpha) & \sigma_2(\alpha\zeta_{2^s}) & \cdots & \sigma_2(\alpha\zeta_{2^s}^{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha) & \sigma_n(\alpha\zeta_{2^s}) & \cdots & \sigma_n(\alpha\zeta_{2^s}^{n-1}) \end{pmatrix}.$$

The matrix M_k can also be written as $M.U^k\overline{M}^t\overline{U^k}^t$, where M denotes the generator matrix of the complex lattice $\Lambda \cong \mathbb{Z}[i]^n$ and $U^k = dig(\sigma_0((1-\zeta_{2^s})^k),\ldots,\sigma_{n-1}((1-\zeta_{2^s})^k)$.

Proposition 4.5. *Each complex ideal lattice Λ_k associated with the ideal $(1-\zeta_{2^s})^k\mathbb{Z}[\zeta_{2^s}]$ is a scaled version of the $\mathbb{Z}[i]^n$-lattice, i.e., Λ_k is isomorphic to a binary complex lattice $(1-i)^k\mathbb{Z}[i]^n$, for $k \in \{0,\ldots,n-1\}$.*

Proof. Let $\alpha = 1-\zeta_{2^s}$ and let $\{\alpha, \alpha\zeta_{2^s},\ldots,\alpha\zeta_{2^s}^{n-1}\}$ be a $\mathbb{Z}[i]$-basis of the complex ideal lattice Λ_k. Now consider the Gram matrix G_k associated with Λ_k. Therefore we have

$$M_k\overline{M_k^t} = \begin{pmatrix} \sum_{i=0}^{n-1}\sigma_i(\alpha)\overline{\sigma_i(\alpha)} & \cdots & \sum_{i=1}^{n}\sigma_i(\alpha)\overline{\sigma_i(\alpha\zeta_{2^s}^{n-1})} \\ \vdots & \ddots & \vdots \\ \sum_{i=0}^{n-1}\sigma_i(\alpha)\overline{\sigma_i(\alpha)} & \cdots & \sum_{i=1}^{n}\sigma_i(\alpha)\overline{\sigma_i(\alpha\zeta_{2^s}^{n-1})} \end{pmatrix}, \tag{4.5}$$

where M_k is the generator matrix of the complex ideal lattice Λ_k.

It follows that the Gram matrix G_k can be written as

$$G_k = M_k\overline{M_k}^t = \sum_{i=0}^{n-1}\sigma_i(\alpha^k)M\sum_{i=0}^{N-1}\overline{\sigma_i(\alpha^k)}\overline{M}^t = \sigma_i(\alpha^k)\overline{\sigma_i(\alpha^k)}M\overline{M}^t, \tag{4.6}$$

where M is the generator matrix of the lattice $\Lambda \cong \mathbb{Z}[i]^n$. Consequently, by using the property of the relative norm, we have $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(i)}(\alpha^k) = (1-i)^k$ and $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(i)}(\overline{\alpha^k}) = (1-i)^k$. Then, we obtain

$$G_k = M_k\overline{M_k}^t = (1-i)^k\overline{(1-i)}^kM\overline{M}^t. \tag{4.7}$$

Thenceforward we know that M denotes the generator matrix of the complex ideal lattice $\Lambda \cong \mathbb{Z}[i]^n$. Then we can conclude from equation (4.7) that $M_k = (1-i)^kM$ represents a generator matrix of the complex ideal lattice $\Lambda_k = (1-i)^k\mathbb{Z}[i]^n$. □

Notice that the Gram matrix G_k given by equation (4.7) can be written as $G_k = 2^kId$, where Id denotes the identity matrix of order n. Therefore we conclude that all complex ideal lattices Λ_k, where $k \in \{0,\ldots,n-1\}$, are a scaled version of the $\mathbb{Z}[i]^n$-lattice.

Remark 4.6. *Notice that the complex homomorphisms in* (4.2) *and Propositions 4.3 and 4.5 establish a isomorphism between the ideal $\Im^k = (1-\zeta_{2^{s-1}})^k\mathbb{Z}[\zeta_{2^s}]$ and the complex ideal lattice*

$\Lambda_k \cong (1-i)^k\mathbb{Z}[i]^n$, *that is,* $\sigma(\mathbb{Z}[\zeta_{2^s}]) = \Lambda = \mathbb{Z}[i]^n$ *and* $\sigma(\Im^k) = \Lambda_k,\ \forall\, k \in \{1,\ldots,n-1\}$. *In this case we obtain a correspondence between the chain of ideals given by equation* (4.8)

$$\Im^{n-1} \subset \Im^{n-2} \subset \cdots \subset \Im \subset \mathbb{Z}[\zeta_{2^s}], \tag{4.8}$$

where $\Im^k = (1-\zeta_{2^{s-1}})^k\mathbb{Z}[\zeta_{2^s}]$, *and the chain of complex ideal lattices given by equation* (4.9)

$$\Lambda_{n-1} \subset \Lambda_{n-2} \subset \cdots \subset \Lambda_2 \subset \Lambda_1 \subset \Lambda = \mathbb{Z}[i]^n, \tag{4.9}$$

where $\Lambda_k \cong (1-i)^k\mathbb{Z}[i]^n$, *for all* $k \in \{1,\ldots,n-1\}$.

5 LATTICE CODES OBTAINED IN $\mathbb{C}^N$ FROM THE POLYNOMIAL RING $\mathbb{F}_2[X]/(1-X^n)$ AND THE GENERALIZED POLYNOMIAL RING $\frac{\mathbb{F}_2[X,\frac{1}{2}\mathbb{Z}_0]}{((1-X^{\frac{1}{2}})^{2n})}$

In this section we propose an algebraic / geometrical procedure to the construction of lattice codes in $\mathbb{C}^n$ via cyclic codes characterized by ideals generated by binary polynomials $(1-x)^k$ from the polynomial ring $\mathbb{F}_2[x]/(1-x^n)$ in $\mathbb{C}^n$ and via cyclic codes characterized by ideals generated by generalized polynomials $(1-x^{\frac{1}{2}})^k$ from the generalized polynomial ring $\frac{\mathbb{F}_2[x,\frac{1}{2}\mathbb{Z}_0]}{((1-x^{\frac{1}{2}})^{2n})}$ in $\mathbb{C}^n$. For that, we make use of algebraic tools from the algebraic number theory.

5.1 Binary cyclic codes from quotient rings

This section is started by describing an algebraic procedure which establishes an isomorphism between the binary cyclic codes $\mathscr{C}_k$ characterized by the ideals generated by the polynomials $(1-x)^k$ from the polynomial ring $\mathbb{F}_2[x]/(1-x^n)$ which are described by the following chain of ideals in (5.1)

$$(1-x)^{n-1} \subset (1-x)^{n-2} \subset \cdots \subset (1-x) \subset \mathbb{F}_2[x]/(1-x^n) \tag{5.1}$$

and the quotients of lattices of the form $\Lambda_k/(1-i)\Lambda_k$, where Λ_k denotes the lattice of the chain described in 4.9 of the Remark 4.6 and it is the complex ideal lattice $(1-i)^k\mathbb{Z}[i]$.

For that we use a result from group theory which is very important for the development of the algebraic procedure that we propose in this section. If G_2 is a subgroup of a group G_1, then the group G_1 can be written as it follows

$$G_1 = G_2 + [G_1/G_2]\,, \tag{5.2}$$

where $[G_1/G_2]$ denotes the quotient group of G_1 by G_2.

As $1+i$ is equal to $1-i$ due to the product of invertible elements from $\mathbb{Z}[i]$, then, for convenience, we identify the nested complex ideal lattices Λ_k's module $1-i$ by binary lattice codes proposed by Forney [5] which are characterized by an ideal of the ring $\mathbb{F}_2[x]/(1-x^n)$. Consequently such binary lattice codes are also characterized by an ideal of the ring $\frac{\mathbb{F}_2[x,\frac{1}{2}\mathbb{Z}_0]}{((x^{\frac{1}{2}})^{2n}-1)}$.

Proposition 5.1. *The complex lattice $\Lambda = \mathbb{Z}[i]^n$ can be written as $\Lambda = (1-i)\Lambda + \mathscr{C}_0$, where $\mathscr{C}_0 = (n,n)$ is the universal binary linear code which is characterized by the polynomial ring $\mathbb{F}_2[x]/(1-x^n)$.*

Proof. From Remark 3.3 it follows that the ideal $(1-i)\mathbb{Z}[\zeta_{2^s}]$ from the ring $\mathbb{Z}[\zeta_{2^s}]$ is a subgroup of $\mathbb{Z}[\zeta_{2^s}]$. From equation 5.2, we have

$$\mathbb{Z}[\zeta_{2^s}] = (1-i)\mathbb{Z}[\zeta_{2^s}] + [\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]]\,. \tag{5.3}$$

From Remark 4.6 and making use of the complex homomorphism 4.2 over the rings $\mathbb{Z}[\zeta_{2^s}]$ and $(1-i)\mathbb{Z}[\zeta_{2^s}]$, then it follows equation 5.4:

$$\Lambda = (1-i)\Lambda + [\Lambda/(1-i)\Lambda]\,, \tag{5.4}$$

where $\Lambda = \mathbb{Z}[i]^n$.

Now we show that the quotient lattice $[\Lambda/(1-i)\Lambda]$ is isomorphic to the universal binary linear code $\mathscr{C}_0$ which is characterized by the polynomial ring $\mathbb{F}_2[x]/(1-x^n)$. Equations 5.3 and 5.4 are equal due to the complex isomorphism σ in (4.2). Therefore we use equation 5.3 to establish an isomorphism between $[\Lambda/(1-i)\Lambda]$ and the polynomial ring $\mathbb{F}_2[x]/(1-x^n)$. For that, let $v = a_0 + a_1\zeta_{2^s} + \cdots + a_{n-1}\zeta_{2^s}^{n-1} \in \mathbb{Z}[\zeta_{2^s}]$. Since $a_k \in \mathbb{Z}[i]$, with $k = 0,1,\ldots,n-1$, then we can write each term a_k as $a_k = (1+i)b_k + c_k$, where $b_k, c_k \in \mathbb{Z}[i]$ and $N_{\mathbb{Q}(i)/\mathbb{Q}}(c_k) \leq 1$. Consequently $c_k = 0, \pm 1, \pm i$. Thenceforth,

$$v = ((1-i)b_0 + c_0) + ((1-i)b_1 + c_1)\zeta_{2^s} + \cdots + ((1-i)b_{n-1} + c_{n-1})\zeta_{2^s}^{n-1} =$$

$$= [(1-i)b_0 + (1-i)b_1\zeta_{2^s} + \cdots + (1-i)b_{n-1}\zeta_{2^s}^{n-1}] + [c_0 + c_1\zeta_{2^s} + \cdots +$$

$$+ c_{n-1}\zeta_{2^s}^{n-1}] = (1-i)(b_0 + b_1\zeta_{2^s} + \cdots + b_{n-1}\zeta_{2^s}^{n-1}) + (c_0 + c_1\zeta_{2^s} + \cdots + c_{n-1}\zeta_{2^s}^{n-1}).$$

By denoting $w = (1-i)(b_0 + b_1\zeta_{2^s} + \cdots + b_{n-1}\zeta_{2^s}^{n-1})$ and considering u as it follows

$$u = c_0 + c_1\zeta_{2^s} + \cdots + c_{n-1}\zeta_{2^s}^{n-1}, \tag{5.5}$$

then $w \in (1-i)\mathbb{Z}[\zeta_{2^s}]$ and $u \in [\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]]$.

Now we show that $[[\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]] \cong \mathscr{C}_0$, that is,

$$v - w = u \cong r_0 + r_1 x + \cdots + r_{n-1}x^{n-1} \in \mathbb{F}_2[x]/(1-x^n).$$

Since $\mathbb{Z}[i]/(1-i)\mathbb{Z}[i]$ is isomorphic to the binary field $\mathbb{F}_2 = \{0,1\}$, then in $\mathbb{Z}[i]$ we have the following congruences

$$(1-i) \;\equiv\; 0\, mod\,(1-i),\; \pm i \;\equiv\; 1\, mod\,(1-i) \text{ and } \pm 1 \;\equiv\; 1\, mod\,(1-i). \tag{5.6}$$

Consequently, consider

$$\varepsilon : [\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]] \to \mathbb{F}_2[x]/(1-x^n), \tag{5.7}$$

where $\varepsilon(u) = \varepsilon(c_0 + c_1\zeta_{2^s} + \cdots + c_{n-1}\zeta_{2^s}^{n-1}) = \sum_{k=0}^{n-1}(c_k \, mod\,(1-i))x^k = r_0 + r_1x + \cdots + r_{n-1}x^{n-1} \in \mathbb{F}_2[x]/(1-x^n)$, with $c_k \, mod\,(1-i) = r_k \in \mathbb{F}_2$. The application ε is an isomorphism. In fact, let $u = \sum_{k=0}^{n-1} c_k\zeta_{2^s}^k$ and $u' = \sum_{k=0}^{n-1} c'_k\zeta_{2^s}^k$ elements from $\mathbb{Z}[\zeta_{2^s}]$, then $\varepsilon(u+u') = \varepsilon([\sum_{k=0}^{n-1} c_k\zeta_{2^s}^k] + [\sum_{k=0}^{n-1} c'_k\zeta_{2^s}^k]) = \varepsilon(\sum_{k=0}^{n-1}(c_k+c'_k)\zeta_{2^s}^k) = \sum_{k=0}^{n-1}((c_k+c'_k) \; mod\; (1-i))\zeta_{2^s}^k = \sum_{k=0}^{n-1}(c_k \; mod\; (1-i))\zeta_{2^s}^k + \sum_{k=0}^{n-1}(c'_k \; mod\; (1-i))\zeta_{2^s}^k = \varepsilon(\sum_{k=0}^{n-1} c_k\zeta_{2^s}^k)) + \varepsilon(\sum_{k=0}^{n-1} c'_k\zeta_{2^s}^k)$. Besides, analogously, since $c_k \, mod\,(1-i) = r_k \in \mathbb{F}_2$, we have that ε preserves the corresponding multiplication of the rings. Thenceforward ε is an homomorphism between $[\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]]$ and $\mathbb{F}_2[x]/(1-x^n)$.

Let $\sum_{k=0}^{n-1} c_k\zeta_{2^s}^k$ and $\sum_{k=0}^{n-1} c'_k\zeta_{2^s}^k \in [\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]]$ such that

$$\varepsilon(\sum_{k=0}^{n-1} c_k\zeta_{2^s}^k) = \varepsilon(\sum_{k=0}^{n-1} c'_k\zeta_{2^s}^k).$$

If $\varepsilon(\sum_{k=0}^{n-1} c_k\zeta_{2^s}^k) = r_0 + r_1x + \cdots + r_{n-1}x^{n-1}$ and $\varepsilon(\sum_{k=0}^{n-1} c'_k\zeta_{2^s}^k) = r'_0 + r'_1x + \cdots + r'_{n-1}x^{n-1}$, then $r_k = r'_k$, for all $k \in \{0,\ldots,n-1\}$. Therefore $c_k = c'_k \; mod\; (1-i)$, for all $k \in \{0,\ldots,n-1\}$, that is, $c_k = c'_k$ in $\mathbb{Z}[i]/(1-i)\mathbb{Z}[i]$. Consequently ε is injective.

Now if $r_0 + r_1x + \cdots + r_{n-1}x^{n-1} \in \mathbb{F}_2[x]/(1-x^n)$, then there exists $c_0 + c_1\zeta_{2^s} + \cdots + c_{n-1}\zeta_{2^s}^{n-1} \in \mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]$ such that $\varepsilon(c_0 + c_1\zeta_{2^s} + \cdots + c_{n-1}\zeta_{2^s}^{n-1}) = r_0 + r_1x + \cdots + r_{n-1}x^{n-1}$. In fact, if $r_i = 0 \in \mathbb{F}_2$, then we have a corresponding $c_i = 0 \; mod\; (1-i) \in \mathbb{Z}[i]$ and, if $r_i = 1 \in \mathbb{F}_2$, then we also have a corresponding $c_i = 1 \; mod\; (1-i) \in \mathbb{Z}[i]$. Note that -1 and $\pm i \in \mathbb{Z}[i]$ are equal to 1 modulo $(1-i)$. Therefore ε establishes an isomorphism between $[\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]]$ and $\mathbb{F}_2[x]/(1-x^n)$. □

Proposition 5.2. *The lattice $\Lambda_k = (1-i)^k\mathbb{Z}[i]^n$, where $k = 0,1,\ldots,n-1$, can be written as $\Lambda_k = (1-i)\Lambda_k + \mathscr{C}_k$, where $\mathscr{C}_k$ is the linear binary code characterized by the ideal $(1-x)^k\mathbb{F}_2[x]/(1-x^n)$ from the polynomial ring $\mathbb{F}_2[x]/(1-x^n)$.*

Proof. Analogously to the proof of the Proposition 5.1, it follows that the ideal $\Im^k$ from the ring $\mathbb{Z}[\zeta_{2^s}]$ can be written as

$$\Im^k = (1-i)\Im^k + \left[\Im^k/(1-i)\Im^k\right]. \tag{5.8}$$

From Remark (4.6), by applying the complex homomorphism σ from 4.2 on the rings $\Im^k$ and $(1-i)\Im^k$, we have

$$\Lambda_k = (1-i)\Lambda_k + [\Lambda_k/(1-i)\Lambda_k]. \tag{5.9}$$

Now we show that the quotient lattice $[\Lambda_k/(1-i)\Lambda_k]$ is isomorphic to the linear binary code $\mathscr{C}_k$ which is characterized by the ideal $(1-x)^k\mathbb{F}_2[x]/(1-x^n)$ from the polynomial ring $\mathbb{F}_2[x]/(1-x^n)$. Equations (5.8) and (5.9) are equal due to the complex isomorphism σ from

(4.2). Therefore we use equation (5.8) to establish an isomorphism between $[\Lambda_k/(1-i)\Lambda_k]$ and the ideal $(1-x)^k\mathbb{F}_2[x]/(1-x^n)$ from the polynomial ring $\mathbb{F}_2[x]/(1-x^n)$. For that, let $v=(1-\zeta_{2^s})^k(a_0+a_1\zeta_{2^s}+\cdots+a_{n-1}\zeta_{2^s}^{n-1})\in\Im^k=(1-\zeta_{2^s})^k\mathbb{Z}[\zeta_{2^s}]$.

Since $a_k\in\mathbb{Z}[i]$, where $k=0,1,\ldots,n-1$, it follows that each term a_k can be written as $a_k=(1-i)b_k+c_k$, where $b_k,c_k\in\mathbb{Z}[i]$ and $N_{\mathbb{Q}(i)/\mathbb{Q}}(c_k)\leq 1$. Consequently $c_k=0,\pm1,\pm i$ and

$$v=(1-\zeta_{2^s})^k[((1-i)b_0+c_0)+((1-i)b_1+c_1)\zeta_{2^s}+\cdots+((1-i)b_{n-1}+$$

$$+c_{n-1})\zeta_{2^s}^{n-1}]=(1-\zeta_{2^s})^k[(1-i)b_0+(1-i)b_1\zeta_{2^s}+\cdots+(1-i)b_{n-1}\zeta_{2^s}^{n-1}]+$$

$$+(1-\zeta_{2^s})^k[c_0+c_1\zeta_{2^s}+\cdots+c_{n-1}\zeta_{2^s}^{n-1}]=$$

$$=(1-\zeta_{2^s})^k(1-i)(b_0+b_1\zeta_{2^s}+\cdots+b_{n-1}\zeta_{2^s}^{n-1})+$$

$$+(1-\zeta_{2^s})^k(c_0+c_1\zeta_{2^s}+\cdots+c_{n-1}\zeta_{2^s}^{n-1}).$$

By denoting $w=(1-\zeta_{2^s})^k(1-i)(b_0+b_1\zeta_{2^s}+\cdots+b_{n-1}\zeta_{2^s}^{n-1})$ and considering u as it follows

$$u=(1-\zeta_{2^s})^k(c_0+c_1\zeta_{2^s}+\cdots+c_{n-1}\zeta_{2^s}^{n-1}), \tag{5.10}$$

then $w\in(1-i)\Im^k$ and $u\in\left[\Im^k/(1-i)\Im^k\right]$.

Now we show that $\left[\Im^k/(1-i)\Im^k\right]\simeq\mathscr{C}_k$, that is,

$$v-w=u\simeq(1-x^k)(r_0+r_1x+\cdots+r_{n-1}x^{n-1})\in(1-x)^k\mathbb{F}_2[x]/(1-x^n).$$

For that, consider the map

$$\varepsilon_k:\left[\Im^k/(1-i)\Im^k\right]\to(1-x)^k\mathbb{F}_2[x]/(1-x^n) \tag{5.11}$$

given by $\varepsilon_k(u)=\varepsilon_k((1-\zeta_{2^s})^k(c_0+c_1\zeta_{2^s}+\cdots+c_{n-1}\zeta_{2^s}^{n-1}))=(1-x)^k\sum_{k=0}^{n-1}(c_k\,mod\,(1-i))x^k=(1-x)^k(r_0+r_1x+\cdots+r_{n-1}x^{n-1})\in(1-x)^k\mathbb{F}_2[x]/(1-x^n)$, where $c_k\,mod\,(1-i)=r_k\in\mathbb{F}_2$.

Let $u=(1-\zeta_{2^s})^k\sum_{k=0}^{n-1}c_k\zeta_{2^s}^k$ and $u'=(1-\zeta_{2^s})^k\sum_{k=0}^{n-1}c'_k\zeta_{2^s}^k$ elements from $\left[\Im^k/(1-i)\Im^k\right]$, then $\varepsilon_k(u+u')=\varepsilon([(1-\zeta_{2^s})^k\sum_{k=0}^{n-1}c_k\zeta_{2^s}^k]+[(1-\zeta_{2^s})^k\sum_{k=0}^{n-1}c'_k\zeta_{2^s}^k)])=\varepsilon_k((1-\zeta_{2^s})^k\sum_{k=0}^{n-1}(c_k+c'_k)\zeta_{2^s}^k)=(1-x)^k\sum_{k=0}^{n-1}((c_k+c'_k)\,mod\,(1-i))\zeta_{2^s}^k=(1-x)^k\sum_{k=0}^{n-1}(c_k\,mod\,(1-i))\zeta_{2^s}^k+(1-x)^k\sum_{k=0}^{n-1}(c'_k\,mod\,(1-i))\zeta_{2^s}^k=\varepsilon_k((1-\zeta_{2^s})^k\sum_{k=0}^{n-1}c_k\zeta_{2^s}^k))+\varepsilon_k((1-\zeta_{2^s})^k\sum_{k=0}^{n-1}c'_k(\zeta_{2^s}^k))$. Besides, analogously, since $c_k\,mod\,(1-i)=r_k\in\mathbb{F}_2$, we have that ε_k preserves the corresponding multiplication of the rings. Thenceforward ε_k is an homomorphism between $\left[\Im^k/(1-i)\Im^k\right]$ and $(1-x)^k\mathbb{F}_2[x]/(1-x^n)$.

Now let $(1-\zeta_{2^s})^k\sum_{k=0}^{n-1}c_k\zeta_{2^s}^k$ and $(1-\zeta_{2^s})^k\sum_{k=0}^{n-1}c'_k\zeta_{2^s}^k\in\left[\Im^k/(1-i)\Im^k\right]$ such that

$$\varepsilon_k((1-\zeta_{2^s})^k\sum_{k=0}^{n-1}c_k\zeta_{2^s}^k)=\varepsilon_k((1-\zeta_{2^s})^k\sum_{k=0}^{n-1}c'_k\zeta_{2^s}^k).$$

If $\varepsilon_k((1-\zeta_{2^s})^k\sum_{k=0}^{n-1}c_k\zeta_{2^s}^k)=(1-x)^k(r_0+r_1x+\cdots+r_{n-1}x^{n-1})$ and $\varepsilon_k((1-\zeta_{2^s})^k\sum_{k=0}^{n-1}c'_k\zeta_{2^s}^k)=(1-x)^k(r'_0+r'_1x+\cdots+r'_{n-1}x^{n-1})$, then $r_k=r'_k$, for all $k\in\{0,\ldots,n-1\}$. Therefore $c_k=c'_k \ mod\ (1-i)$, for all $k\in\{0,\ldots,n-1\}$, that is, $c_k=c'_k$ in $\mathbb{Z}[i]/(1-i)\mathbb{Z}[i]$. Consequently ε_k is injective.

Now if $(1-x)^k(r_0+r_1x+\cdots+r_{n-1}x^{n-1})\in(1-x)^k\mathbb{F}_2[x]/(1-x^n)$, then there exists $(1-\zeta_{2^s})^k(c_0+c_1\zeta_{2^s}+\cdots+c_{n-1}\zeta_{2^s}^{n-1})\in[\Im^k/(1-i)\Im^k]$ such that $\varepsilon_k((1-\zeta_{2^s})^k(c_0+c_1\zeta_{2^s}+\cdots+c_{n-1}\zeta_{2^s}^{n-1}))=(1-x)^k(r_0+r_1x+\cdots+r_{n-1}x^{n-1})$. If fact, if $r_i=0\in\mathbb{F}_2$, then we have a corresponding $c_i=0 \ mod\ (1-i)\in\mathbb{Z}[i]$ and, if $r_i=1\in\mathbb{F}_2$, then we also have a corresponding $c_i=1 \ mod\ (1-i)\in\mathbb{Z}[i]$. Note that -1 and $\pm i\in\mathbb{Z}[i]$ are equal to 1 modulo $(1-i)$. Therefore ε_k establishes an isomorphism between the code $\mathscr{C}_k$ and the quotient ring $\left[\Im^k/(1-i)\Im^k\right]$. □

Now we establish an isomorphism between the binary cyclic codes $\mathscr{C}'_k$, where $k=0,1,\ldots,n-1$, which are characterized, respectively, by the ideals $(1-x^{\frac{1}{2}})^k$ from the generalized polynomial ring $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$ and the quotient lattices $\Lambda_k/(1-i)\Lambda_k$, where Λ_k is the complex lattice from the chain of nested complex lattices which is given in (4.9).

Next we have the corresponding chain of the ideals $(1-x^{\frac{1}{2}})^k$ from the generalized polynomial ring $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$:

$$(1-x^{\frac{1}{2}})^{n-1}\subset(1-x^{\frac{1}{2}})^{n-2}\subset\cdots\subset(1-x^{\frac{1}{2}})\subset\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}. \tag{5.12}$$

Therefore we make use of the following remark to stablish such an isomorphism.

Remark 5.3. *By considering the change of variable $y=x^{\frac{1}{2}}$, then*

(i) *there exists an identification between the elements of $\mathbb{F}_2[y]/(1-y)^n$ and $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$. In fact, if $u=a_0+a_1y+\cdots+a_{n-1}y^{n-1}\in\mathbb{F}_2[y]/(1-y)^{2n}$, then the corresponding identification can be given by $h(a_0+a_1y+\cdots+a_{n-1}y^{n-1})=a'_0+a'_{\frac{1}{2}}x^{\frac{1}{2}}+\cdots+a_{\frac{n-1}{2}}(x^{\frac{1}{2}})^{n-1}\in\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$, where $a_k=a'_{\frac{k}{2}}\in\mathbb{F}_2$, for all $k\in\{0,1,\ldots,n-1\}$.*

(ii) *there is an identification between the ideals $(1-y)^k\mathbb{F}_2[y]/(1-y)^n$ from the polynomial ring $\mathbb{F}_2[y]/(1-y)^n$ and the ideals $(1-x^{\frac{1}{2}})^k\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$ from the generalized polynomial ring $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$. In fact, if $u=(1-y)^k(a_0+a_1y+\cdots+a_{n-1}y^{n-1})\in(1-y)^k\mathbb{F}_2[y]/(1-y)^n$, then the corresponding identification can be given by $h((1-y)^k(a_0+a_1y+\cdots+a_{n-1}y^{n-1}))=(1-x^{\frac{1}{2}})^k(a'_0+a'_{\frac{1}{2}}x^{\frac{1}{2}}+\cdots+a_{\frac{n-1}{2}}(x^{\frac{1}{2}})^{n-1})\in\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$, where $a_k=a'_{\frac{k}{2}}\in\mathbb{F}_2$, for all $k\in\{0,1,\ldots,n-1\}$.*

Proposition 5.4. *The complex lattice $\Lambda=\mathbb{Z}[i]^n$ can be written as $\Lambda=(1-i)\Lambda+\mathscr{C}'_0$, where $\mathscr{C}'_0=(n,n)$ is the universal binary code characterized by the generalized polynomial ring $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$.*

Proof. This proof is analogous to the proof of the Proposition 5.1, then we make use of the equations (5.3) and (5.4). Consequently it is necessary to show that the corresponding quotient lattice $[\Lambda/(1-i)\Lambda]$ is isomorphic to the code $\mathscr{C}_0'$ which is characterized by the generalized polynomial ring $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$.

Since equations (5.3) and (5.4) are equal due to the complex isomorphism σ from (4.2), then we consider equation (5.3) to establish an isomorphism between $[\Lambda/(1-i)\Lambda]$ and the generalized polynomial ring $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$.

Note that $\mathbb{Z}[\zeta_{2^s}] = (1-\zeta_{2^s})^n\mathbb{Z}[\zeta_{2^s}] + [\mathbb{Z}[\zeta_{2^s}]/(1-\zeta_{2^s})^n\mathbb{Z}[\zeta_{2^s}]]$. From Proposition 5.1, equation (5.5), each element $u \in [\mathbb{Z}[\zeta_{2^s}]/(1-\zeta_{2^s})^n\mathbb{Z}[\zeta_{2^s}]]$ is written as

$$u = c_0 + c_1\zeta_{2^s} + \cdots + c_{n-1}\zeta_{2^s}^{n-1}, \tag{5.13}$$

where $c_k \in \mathbb{Z}[i]$ and $N_{\mathbb{Q}(i)/\mathbb{Q}}(c_k) \leq 1$. Consequently $c_k = 0, \pm 1, \pm i$. Now we show that $[[\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]] \simeq \mathscr{C}_0'$, where $\mathscr{C}_0' = (n,n)$ is the universal binary code characterized by the generalized polynomial ring $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$. By using the polynomial ring over the binary field $\mathbb{F}_2$ described as $\mathbb{F}_2[y]/(1-y^n)$ through Remark 5.3, item (i), from Proposition 5.1, it follows that the map

$$\varepsilon : [\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]] \to \mathbb{F}_2[y]/(1-y^n) \tag{5.14}$$

which is given by $\varepsilon(u) = \varepsilon(c_0 + c_1\zeta_{2^s} + \cdots + c_{n-1}\zeta_{2^s}^{n-1}) = \sum_{k=0}^{n-1}(c_k \, mod\,(1-i))x^k = r_0 + r_1x + \cdots + r_{n-1}x^{n-1} \in \mathbb{F}_2[y]/(1-y^n)$, where $c_k \, mod\,(1-i) = r_k \in \mathbb{F}_2$, is an isomorphism between $[\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]]$ and $\mathbb{F}_2[y]/(1-y^n)$. Now, from equation (3.5), the 2^s-th root of unity can be written as $\zeta_{2^s} = \zeta_{2^{s-1}}^{\frac{1}{2}}$, thenceforth, each element $u = c_0 + c_1\zeta_{2^s} + \cdots + c_{n-1}\zeta_{2^s}^{n-1} \in [\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]]$ can be written as $u = d_0 + d_{\frac{1}{2}}\zeta_{2^{s-1}}^{\frac{1}{2}} + \cdots + d_{\frac{n-1}{2}}(\zeta_{2^{s-1}}^{\frac{1}{2}})^{n-1}$ and, consequently, $c_k = d_{k/2}$, for all $k = 0,\ldots,n-1$. Also by considering the change of variable $y = x^{\frac{1}{2}}$ from Remark 5.3, it follows that the isomorphism ε from (5.14) can be written as

$$\varepsilon' : [\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]] \to \mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}, \tag{5.15}$$

where $\varepsilon'(u) = \varepsilon(d_0 + d_{\frac{1}{2}}\zeta_{2^{s-1}}^{\frac{1}{2}} + \cdots + d_{\frac{n-1}{2}}(\zeta_{2^{s-1}}^{\frac{1}{2}})^{n-1}) = \sum_{k=0}^{n-1}(d_{k/2} \, mod\,(1-i))(x^{\frac{1}{2}})^k = t_0 + t_{\frac{1}{2}}(x^{\frac{1}{2}}) + \cdots + t_{\frac{n-1}{2}}(x^{\frac{1}{2}})^{n-1} \in \mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^n$, with $c_k \, mod\,(1-i) = t_{\frac{k}{2}} \in \mathbb{F}_2$ and $c_k = d_{k/2}$, for all $k = 0,1,\ldots,n-1$. Thenceforward $[[\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]]$ and $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$ are isomorphic, then the proof is concluded. □

Proposition 5.5. *The lattice $\Lambda_k = (1-i)^k\mathbb{Z}[i]^n$ which is a scaled version of the $\mathbb{Z}[i]^n$-lattice can be written as $\Lambda_k = (1-i)\Lambda_k + \mathscr{C}_k'$, where $\mathscr{C}_k'$ is the code characterized by the ideal $(1-x^{\frac{1}{2}})^k\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^n$ from the generalized polynomial ring $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$.*

Proof. It is necessary to show that the quotient lattice $[\Lambda_k/(1-i)\Lambda_k]$ is isomorphic to the code $\mathscr{C}_k'$ characterized by the ideal $(1-x^{\frac{1}{2}})^k\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$ from the generalized polynomial ring $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$.

Since equations (5.8) and (5.9) are equal due to the complex isomorphism σ from 4.2, then we consider equation (5.8) to establish an isomorphism between $[\Lambda_k/(1-i)\Lambda_k]$ and the ideal $(1-x^{\frac{1}{2}})^k\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$ from the generalized polynomial ring $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$. For that, let $v=(1-\zeta_{2^s})^k(a_0+a_1\zeta_{2^s}+\cdots+a_{n-1}\zeta_{2^s}^{n-1})\in\Im^k=(1-\zeta_{2^s})^k\mathbb{Z}[\zeta_{2^s}]$.

Since $a_k\in\mathbb{Z}[i]$, where $k=0,1,\ldots,n-1$, then each term a_k is given by $a_k=(1-i)b_k+c_k$, where $b_k,c_k\in\mathbb{Z}[i]$ and $N_{\mathbb{Q}(i)/\mathbb{Q}}(c_k)\leq 1$. Consequently $c_k=0,\pm1,\pm i$ and

$$v=(1-\zeta_{2^s})^k[((1-i)b_0+c_0)+((1-i)b_1+c_1)\zeta_{2^s}+\cdots+((1-i)b_{n-1}+$$

$$+c_{n-1})\zeta_{2^s}^{n-1}]=(1-\zeta_{2^s})^k[(1-i)b_0+(1-i)b_1\zeta_{2^s}+\cdots+(1-i)b_{n-1}\zeta_{2^s}^{n-1}]+$$

$$+(1-\zeta_{2^s})^k[c_0+c_1\zeta_{2^s}+\cdots+c_{n-1}\zeta_{2^s}^{n-1}]=$$

$$=(1-\zeta_{2^s})^k(1-i)(b_0+b_1\zeta_{2^s}+\cdots+b_{n-1}\zeta_{2^s}^{n-1})+$$

$$+(1-\zeta_{2^s})^k(c_0+c_1\zeta_{2^s}+\cdots+c_{n-1}\zeta_{2^s}^{n-1}).$$

By denoting $w=(1-\zeta_{2^s})^k(1-i)(b_0+b_1\zeta_{2^s}+\cdots+b_{n-1}\zeta_{2^s}^{n-1})$ and considering u as it follows

$$u=(1-\zeta_{2^s})^k(c_0+c_1\zeta_{2^s}+\cdots+c_{n-1}\zeta_{2^s}^{n-1}), \tag{5.16}$$

then $w\in(1-i)\Im^k$ and $u\in\left[\Im^k/(1-i)\Im^k\right]$.

Now we show that $\left[\Im^k/(1-i)\Im^k\right]\simeq\mathscr{C}'_k$, that is,

$$v-w=u\simeq(1-x^{\frac{1}{2}})^k(t_0+t_{\frac{1}{2}}(x^{\frac{1}{2}})+\cdots+t_{\frac{n-1}{2}}(x^{\frac{1}{2}})^{n-1})\in(1-x^{\frac{1}{2}})^k\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}.$$

By using the polynomial ring over the binary field $\mathbb{F}_2$ described as $\mathbb{F}_2[y]/(1-y^n)$ through Remark 5.3, item (i), from Proposition 5.1, it follows that the map

$$\varepsilon'_k:\left[\Im^k/(1-i)\Im^k\right]\to(1-y)^k\mathbb{F}_2[y]/(1-y^n) \tag{5.17}$$

which is given by $\varepsilon'_k(u)=\varepsilon'_k((1-\zeta_{2^s})^k(c_0+c_1\zeta_{2^s}+\cdots+c_{n-1}\zeta_{2^s}^{n-1}))=(1-y)^k\sum_{k=0}^{n-1}(c_k\,mod\,(1-i))y^k=(1-y)^k(r_0+r_1y+\cdots+r_{n-1}y^{n-1})\in(1-y)^k\mathbb{F}_2[y]/(1-y^n)$ establishes an isomorphism between $\left[\Im^k/(1-i)\Im^k\right]$ and the ideal $(1-y)^k\mathbb{F}_2[y]/(1-y^n)$, where $c_k\,mod\,(1-i)=r_k\in\mathbb{F}_2$, for all $k\in\{0,1,\ldots,n-1\}$.

Now, from equation (3.5), the 2^s-th root of unity can be written as $\zeta_{2^s}=\zeta_{2^{s-1}}^{\frac{1}{2}}$, thenceforth, each element $u=(1-\zeta_{2^s})^k(c_0+c_1\zeta_{2^s}+\cdots+c_{n-1}\zeta_{2^s}^{n-1})\in\left[(1-\zeta_{2^s})^k\mathbb{Z}[\zeta_{2^s}]/(1-i)(1-\zeta_{2^s})^k\mathbb{Z}[\zeta_{2^s}]\right]$ can be written as $u=(1-\zeta_{2^{s-1}}^{\frac{1}{2}})^k(d_0+d_{\frac{1}{2}}\zeta_{2^{s-1}}^{\frac{1}{2}}+\cdots+d_{\frac{n-1}{2}}(\zeta_{2^{s-1}}^{\frac{1}{2}})^{n-1})$ and, consequently, $c_k=$

$d_{k/2}$, for all $k = 0, 1, \ldots, n-1$. Also by considering the change of variable $y = x^{\frac{1}{2}}$ from Remark 5.3, it follows that the isomorphism ε'_k can be written as

$$\varepsilon'_k : \left[(1-\zeta_{2^s})^k\mathbb{Z}[\zeta_{2^s}]/(1-i)(1-\zeta_{2^s})^k\mathbb{Z}[\zeta_{2^s}]\right] \rightarrow$$

$$\rightarrow (1-x^{\frac{1}{2}})^k\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}, \tag{5.18}$$

where $\varepsilon'_k(u) = \varepsilon((1-\zeta_{2^{s-1}}^{\frac{1}{2}})^k(d_0 + d_{\frac{1}{2}}\zeta_{2^{s-1}}^{\frac{1}{2}} + \cdots + d_{\frac{n-1}{2}}(\zeta_{2^{s-1}}^{\frac{1}{2}})^{n-1})) = (1-x^{\frac{1}{2}})^k\sum_{k=0}^{n-1}(d_{k/2}\,mod\,(1-i))(x^{\frac{1}{2}})^k = (1-x^{\frac{1}{2}})^k(t_0 + t_{\frac{1}{2}}(x^{\frac{1}{2}}) + \cdots + t_{\frac{n-1}{2}}(x^{\frac{1}{2}})^{n-1}) \in (1-x^{\frac{1}{2}})^k\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$, with $d_{k/2}\,mod\,(1-i) = t_{k/2} \in \mathbb{F}_2$. Thenceforward $\left[(1-\zeta_{2^s})^k\mathbb{Z}[\zeta_{2^s}]/(1-i)(1-\zeta_{2^s})^k\mathbb{Z}[\zeta_{2^s}]\right]$ and $(1-x^{\frac{1}{2}})^k\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$ are isomorphic, then the proof is concluded. □

Observe that the complex lattice codes $\mathscr{C}_k$ and $\mathscr{C}'_k$, where $k = 0, 1, \ldots, n-1$, which are characterized, respectively, by the ideals $(1-x)^k\mathbb{F}_2[x]/(1-x^n)$ from the polynomial ring $\mathbb{F}_2[x]/(1-x^n)$ and by the ideals $(1-x^{\frac{1}{2}})^k\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$ from the generalized polynomial ring $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$, are nested codes. Therefore, these codes can be applied to quantize complex-valued channels [11] in order to realize interference alignment [9]. Besides, since these codes are constructed by using ideals from the rings $\mathbb{F}_2[x]/(1-x^n)$ and $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^{2n}$, respectively, then it is obtained the multiplication structure [8] which can be applied to nonlinear distributed computing over a wireless network.

Acknowledgements

This work has been supported by the following Brazilian Agencies: CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) under grant No. 6562-10-8 and FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) under grant No. 2013/25977-7.

REFERENCES

[1] T.S. Amanullah & A.A. de Andrade. A Decoding Procedure which Improves Code Rate and Error Corrections. *Journal of Advanced Research in Applied Mathematics*, **4**(4) (2012), 37–50.

[2] J. Boutros & E. Viterbo. Signal space diversity: a power-and bandwidth-efficient diversity technique for the Rayleigh fading channel. *IEEE Transactions on Information Theory*, **44**(4) (1998), 1453–1467.

[3] J.H. Conway & N.J.A. Sloane. "Sphere Packings, Lattices and Groups". Springer-Verlag, New York (1988).

[4] A.A. de Andrade & R.P. Junior. Linear codes over finite rings. *Tendências em Matemática Aplicada e Computacional (TEMA)*, **6**(2) (2005), 207–217.

[5] G.D. Forney. Coset Codes - Part I: Introduction and Geometrical Classification. *IEEE Transactions on Information Theory*, **34**(5) (1988), 1123–1151.

[6] G.D. Forney. Coset Codes - Part II: binary lattices and related codes. *IEEE Transactions on Information Theory*, **34**(5) (1988), 1152–1187.

[7] F. Oggier. "Algebraic methods for channel coding". Ph.D. thesis, École Polytechnique Fédérale de Lausanne, Lausanne (2005). PhD Thesis.

[8] F. Oggier & J.C. Belfiore. Enabling multiplication in lattice codes via Construction A. In "2013 IEEE Information Theory Workshop (ITW)", volume 1. IEEE (2013), p. 1–5.

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

[10] C.C. Trinca. "A contribuition to the study of channel coding in wireless communication systems". Ph.D. thesis, Universidade Estadual Paulista (UNESP), Ilha Solteira, SP (2013). PhD Thesis.

[11] C.C. Trinca, J.C. Belfiore, E.D. de Carvalho, J. Vieira Filho, R. Palazzo Jr. & R.A. Watanabe. Construction of Complex Nested Ideal Lattices for Complex-Valued Channel Quantization. *International Journal of Applied Mathematics*, **31**(4) (2018), 549–585.

[12] E.B. X. Giraud & J.C. Belfiore. Algebraic tools to build modulation schemes for fading channels. *IEEE Transactions on Information Theory*, **43**(3) (1997), 938–952.

CC BY