Complex Lattices Codes via Binary Fields

Edson D. Carvalho, Antônio A. Andrade e Cibele C. Trinca

FEIS-UNESP / IBILCE-UNESP/UFT
edson.donizete@unesp.br / antonio.andrade@unesp.br/cibtrinca@yahoo.com.br

Encontro de Códigos, Reticulados e Informação (ENCORI)
IMECC-UNICAMP
15/06 a 16/06/2023

Sumário

1. Introduction
   - Coset Codes and Construction A
2. Main Objective of this work
3. Generalized polynomials
4. Binary Cyclotomic Fields
5. Binary ciclyc codes $\mathcal{C}_{n-k}$ from quotient rings
6. Binary cyclic codes $\mathcal{C}_k$ from monoid rings
7. ACKNOWLEDEGEMENT

Sumário

1. Introduction
   - Coset Codes and Construction A
2. Main Objective of this work
3. Generalized polynomials
4. Binary Cyclotomic Fields
5. Binary ciclyc codes $\mathcal{C}_{n-k}$ from quotient rings
6. Binary cyclic codes $\mathcal{C}_k$ from monoid rings
7. ACKNOWLEDEGEMENT

Coset Codes and Construction A

- Several works [J. H. Conway and N. J. A. Sloane; *Sphere Packings, Lattices and Groups*, New York: Springer-Verlag, 1988.] [G. D. Forney; *Coset Codes - Part I: Introduction and Geometrical Classification*, IEEE Trans. Inform. Theory, 34, 1123–1151, 1988.] over lattices theory have dedicated to *Construction A* and the lattice sets partitioning via coset codes.
- The advantage of these algebraic approach is that it makes possible to unified different kind of coding problems related to algebraic block codes and Euclidean space codes. The lattices obtained by Construction A are denominated by *lattice codes*.

- From a nested binary cyclic code, a chain of embedded cyclic codes given by Equation (1)

$$\mathcal{C}_{n-1} \subset \mathcal{C}_{n-2} \subset \ldots \mathcal{C}_1 \subset \mathcal{C}_0, \tag{1}$$

and a chain of nested binary complex lattices given by Equation (2)

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

- Forney showed how binary codes, lattice codes and trellis codes can be constructed as coset codes.
- These cosets are sequences of signals points of the outputs of binary encoders. As consequence of the identification of complex binary coset lattices $(1+i)^k\mathbb{Z}[i]^n/(1+i)\mathbb{Z}[i]^n$ by binary code $\mathcal{C}_k$, we can be see the algebraic block codes $\mathcal{C}_k$ as the principal ideals in the factor ring $\mathbb{F}_2[x]/(x^n-1)$ of polynomial Euclidean domain $\mathbb{F}_2[x]$, where $\mathbb{F}_2$ denotes the binary field.

Sumário

1. Introduction
   - Coset Codes and Construction A
2. Main Objective of this work
3. Generalized polynomials
4. Binary Cyclotomic Fields
5. Binary ciclyc codes $\mathcal{C}_{n-k}$ from quotient rings
6. Binary cyclic codes $\mathcal{C}_k$ from monoid rings
7. ACKNOWLEDEGEMENT

Main objective of this work

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

Sumário

1. Introduction
   - Coset Codes and Construction A
2. Main Objective of this work
3. Generalized polynomials
4. Binary Cyclotomic Fields
5. Binary ciclyc codes $\mathcal{C}_{n-k}$ from quotient rings
6. Binary cyclic codes $\mathcal{C}_k$ from monoid rings
7. ACKNOWLEDEGEMENT

Generalized polynomials

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 $\mathcal{R}[x;S]$ can be defined. If $f = \sum_{i=1}^{n} f_i x^{s_i}$ is the canonical form of the nonzero element $f \in \mathcal{R}[x;S]$, 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 $\mathcal{R}$ is an integral domain, then, for $f, g \in \mathcal{R}[x;S]$, it follows that $\deg(fg) = \deg(f) + \deg(g)$ and $ord(fg) = ord(f) + ord(g)$. For a commutative ring B with identity, $\Re = \frac{B[x, \frac{1}{2}\mathbb{Z}_0]}{((x^{\frac{1}{2}})^n - 1)}$ is a finite ring.

Cycle Codes

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

Cyclic Codes

[Tariq Shah, Amanullah, Antonio Aparecido de Andrade; *A Decoding Procedure which Improves Code Rate and Error Corrections*, Journal of Advanced Research in Applied Mathematics, 4(4), 37-50, 2012.]

Theorem

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

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 $\overline{a}(x^{\frac{1}{2}}) = \overline{a}_0 + \overline{a}_{\frac{1}{2}}x^{\frac{1}{2}} + \overline{a}_1 x + \cdots + \overline{a}_{\frac{n-1}{2}}(x^{\frac{1}{2}})^{n-1}$.

Sumário

1. Introduction
   - Coset Codes and Construction A
2. Main Objective of this work
3. Generalized polynomials
4. Binary Cyclotomic Fields
5. Binary ciclyc codes $\mathcal{C}_{n-k}$ from quotient rings
6. Binary cyclic codes $\mathcal{C}_k$ from monoid rings
7. ACKNOWLEDEGEMENT

Binary Cyclotomic Fields

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

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

   is 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 the Euler function.

2. We denote the integers rings of $\mathbb{L}$ by $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_{2^s}]$ and its integral basis by $\{1, \zeta_{2^s}, \zeta_{2^s}^2, \cdots, \zeta_{2^s}^{\varphi(2^s)-1}\} = \{1, \zeta_{2^s}, \zeta_{2^s}^2, \cdots, \zeta_{2^s}^{2^s-1}\}$.

Binary Cyclotomic Fields

Using concepts of the ramification index of prime ideal $\mathcal{I} = (1 - \zeta_{2^s})$ on Galois extension $\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}$ of degree $n = 2^{s-2}$. We will established a general correspondence between a sequence of ideals of kind $\mathcal{I}^k = (1 - \zeta_{2^s})^k \mathbb{Z}[\zeta_{2^s}]$ (for $k \in \{0, 1, \cdots, n-1\}$) and a sequence of nested lattices Λ_k that we showed are scaled version of $\mathbb{Z}[i]^n$-lattices (obtained by the relative embedding of the ideals $\mathcal{I}^k$ in $\mathbb{C}^n$), where $\mathbb{Z}[\zeta_{2^s}]$ is the algebraic integer of number field $\mathbb{Q}(\zeta_{2^s})$ and ζ_{2^s} is a 2^s-th root of unity.

Proposition

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

Scaled version of $\mathbb{Z}[i]^n$-lattices from $\mathbb{Q}(\zeta_{2^s})$

We showed the ideal lattices Λ_k obtained by ideals in $\mathbb{Z}[\zeta_{2^s}]$ listed by $\Im^k$ for $k \in \{0, \ldots, n-1\}$ are also isomorphic to $(1-i)^k\mathbb{Z}[i]^n$, and are a scaled version of $\mathbb{Z}[i]^n$, is that, $det(\Lambda_k) = 2^k$, since the Gram matrix of $(1-i)^k\mathbb{Z}[i]^n$ is $2^k Id$.

For each $k \in \{0, 1, \ldots, n-1\}$, we chosen the element $\alpha = (1-\zeta_{2^s})^k$, then we can be written the generating matrices G_k associated to ideal lattices Λ_k as $G_k = M_k\overline{M_k}^t$, where M_k is the Gram matrix associated to Λ_k given by

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

Scaled version of $\mathbb{Z}[i]^n$-lattices from $\mathbb{Q}(\zeta_{2^s})$

We establish a isomorphism between ideas $\Im^k = (1-\zeta_{2^{s-1}})^k\mathbb{Z}[\zeta_{2^s}]$ and complex lattices $\Lambda_k \simeq (1-i)^k\mathbb{Z}[i]^n$, that is, $\sigma(\mathbb{Z}[\zeta_{2^s}]) = \Lambda$ and $\sigma(\Im^k) = \Lambda_k,\ \ \forall k \in \{1,\ ldots, n-1\}$. In this case, we obtain a correspondence between ideals in the chain of ideals given by Equation 3 and embedded complex lattices given by Equation 4.

$$\Im^{n-1} \subset \Im^{n-2} \subset \ldots \subset \Im \subset \mathbb{Z}[\zeta_{2^s}], \tag{3}$$

where $\Im^k = (1-\zeta_{2^{s-1}})^k\mathbb{Z}[\zeta_{2^s}]$.

$$\Lambda_{n-1} \subset \Lambda_{n-2} \subset \ldots \subset \Lambda_2 \subset \Lambda_1 \subset \Lambda, \tag{4}$$

onde $\Lambda_k \simeq (1-i)^k\mathbb{Z}[i]^n$ para todo $k \in \{1,\ldots,n-1\}$.

Sumário

1. Introduction
   - Coset Codes and Construction A
2. Main Objective of this work
3. Generalized polynomials
4. Binary Cyclotomic Fields
5. Binary ciclyc codes $\mathcal{C}_{n-k}$ from quotient rings
6. Binary cyclic codes $\mathcal{C}_k$ from monoid rings
7. ACKNOWLEDEGEMENT

Binary ciclyc codes $\mathcal{C}_{n-k}$ from quotient rings

Proposition

The lattice Λ given by a scaled version of the lattice $\mathbb{Z}[i]^n$, up to isomorphism, is written as $\Lambda = (1-i)\Lambda + \mathcal{C}_0$, where $\mathcal{C}_0 = (n, n)$ is code characterized by the polynomials ring $\mathbb{F}_2[x]/(1-x^n)$.

Part of the proof

It follows that the ideal $(1-i)\mathbb{Z}[\zeta_{2^s}]$ in the ring $\mathbb{Z}[\zeta_{2^s}]$ is a subgroup of $\mathbb{Z}[\zeta_{2^s}]$. It follows that
$\mathbb{Z}[\zeta_{2^s}] = (1-i)\mathbb{Z}[\zeta_{2^s}] + [\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]]$.
We making use of the complex homomorphism in the rings $\mathbb{Z}[\zeta_{2^s}]$ and $(1-i)\mathbb{Z}[\zeta_{2^s}]$, up to isomomorphism, it follows the
$\Lambda = (1-i)\Lambda + [\Lambda/(1-i)\Lambda]$.
For this, 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 $k = 0, 1, \ldots, n-1$, it follows that we can rewritten each term a_k in the form $a_k = (1+i)b_k + c_k$, where $b_k, c_k \in \mathbb{Z}[i]$ and $N_{\mathbb{Q}(i)/\mathbb{Q}}(c_k) \leq 1$.

Part of the proof

Thus, $c_i = 0, \pm 1, \pm i$. Then

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

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

Denoting $w = (1-i)(b_0 + b_1\zeta_{2^s} + \cdots + b_{n-1}\zeta_{2^s}^{n-1}$ and considering u given by the Equation

$$u = c_0 + c_1\zeta_{2^s} + \cdots + c_{n-1}\zeta_{2^s}^{n-1}, \tag{5}$$

Thus, $w \in (1-i)\mathbb{Z}[\zeta_{2^s}]$ and $u \in [\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]]$. Now, we need to show that $[[\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]] \simeq \mathcal{C}_0$, that is,

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

Part of the proof

- Since $\mathbb{Z}[i]/(1-i)\mathbb{Z}[i]$ is isomorph to the binary field $\mathbb{F}_2 = \{0,1\}$, it follows that in $\mathbb{Z}[i]$ we have the congruency vale a congruência dada pela equação (6)

$$(1-i) \equiv \ 0 \, mod \, (1-i), \ \pm i \equiv \ 1 \, mod \, (1-i), \ \pm 1 \equiv \ 1 \, mod \, (1-i). \tag{6}$$

- Thus, we can consider

$$\epsilon : [\mathbb{Z}[\zeta_{2^s}]/(1-i)\mathbb{Z}[\zeta_{2^s}]] \to \mathbb{F}_2[x]/(1-x^n), \tag{7}$$

given by $\epsilon(u) = \epsilon(c_0 + c_1\zeta_{2^s} + \cdots + c_{n-1}\zeta_{2^s}^{n-1}) =$
$\sum_{k=0}^{n} c_k \, mod \, (1-i)x^k = r_0 + r_1 x + \cdots + r_{n-1}x^{n-1} \in \mathbb{F}_2[x]/(1-x^n)$,
where $c_k \, mod \, (1-i) = r_k \in \mathbb{F}_2$.

Proposition

The lattice Λ_k, a scaled version of the lattice $(1-i)^k\mathbb{Z}[i]^n$, up to isomorphism, is written as $\Lambda_k = (1-i)\Lambda_k + \mathcal{C}_k$, where $\mathcal{C}_k$ is a code characterized by the ideal $(1-i)^k\mathbb{F}_2[x]/(1-x^n)$ in the polynomial ring $\mathbb{F}_2[x]/(1-x^n)$.

Sumário

1. Introduction
   - Coset Codes and Construction A
2. Main Objective of this work
3. Generalized polynomials
4. Binary Cyclotomic Fields
5. Binary ciclyc codes $\mathcal{C}_{n-k}$ from quotient rings
6. Binary cyclic codes $\mathcal{C}_k$ from monoid rings
7. ACKNOWLEDEGEMENT

Observação

We have $\zeta_{2^s} = \zeta_{2^{s-1}}^{1/2}$ and also considering the change of the variable $y = x^{\frac{1}{2}}$, then

(i) there exists an identification between the elements of $\mathbb{F}_2[y]/(1-y)^n$ and $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^n$. In fact, if $u = a_0 + a_1 y + \cdots + a_{n-1} y^{n-1} \in \mathbb{F}_2[y]/(1-y)^n$, then is sufficient to take the identification given by $h(a_0 + a_1 y + \cdots + a_{n-1} y^{n-1}) = a'_0 + a'_{\frac{1}{2}} x^{\frac{1}{2}} + \cdots + a_{\frac{n-1}{2}} (x^{\frac{1}{2}})^{n-1} \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^n$, onde os indices $a_k = a'_{\frac{k}{2}} \in \mathbb{F}_2$ para todo $k \in \{0, 1, \ldots, n-1\}$.

(ii) there is an identification between ideals $(1-y)^k\mathbb{F}_2[y]/(1-y)^n$ of the polynomial ring $\mathbb{F}_2[y]/(1-y)^n$ and the ideals $(1-x^{\frac{1}{2}})^k\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^n$ in the generalized polynomial ring $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^n$. 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 it is sufficent to take the identification given by $h((1-y)^k)(a_0+a_1y+\cdots+a_{n-1}y^{n-1}))=(1-x^{\frac{1}{2}})^k(a'_0+a'_{\frac{1}{2}}x^{\frac{1}{2}}+\cdots+a_{\frac{n-1}{2}}(x^{\frac{1}{2}})^{n-1})\in\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]/(1-x^{\frac{1}{2}})^n$, where $a_k=a'_{\frac{k}{2}}\in\mathbb{F}_2$, for all $k\in\{0,1,\ldots,n-1\}$..

Proposition

The lattice Λ given by an scaled version of the lattice $\mathbb{Z}[i]^n$, up to isomorphism, is written in the form $\Lambda = (1-i)\Lambda + \mathcal{C}'_0$, where $\mathcal{C}'_0 = (n, n)$ is the code characterized by the generalized polynomial ring $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_0]/(1 - x^{\frac{1}{2}})^n$.

Proposition

The lattice Λ_k given by a scaled version of the lattice $(1-i)^k\mathbb{Z}[i]^n$, up to isomorphism, is givne by $\Lambda_k = (1-i)\Lambda_k + \mathcal{C}'_k$, where $\mathcal{C}_k$ is the code characterized by the ideal $(1-i)^k\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_0]/(1 - x^{\frac{1}{2}})^n$ in the generalized polynomial ring $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_0]/(1 - x^{\frac{1}{2}})^n$.

Sumário

1. Introduction
   - Coset Codes and Construction A
2. Main Objective of this work
3. Generalized polynomials
4. Binary Cyclotomic Fields
5. Binary ciclyc codes $\mathcal{C}_{n-k}$ from quotient rings
6. Binary cyclic codes $\mathcal{C}_k$ from monoid rings
7. ACKNOWLEDEGEMENT

ACKNOWLEDEGEMENT

The authors would to like to thank the comite of Encori and Departament of Mathematics of UNESP/Ilha Solteira