Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 151–156*

Lattices codes from the ring $\mathbb{F}_3[x; \frac{1}{3}\mathbb{Z}_0]$ [1]

Edson Donizete de Carvalho edson@mat.feis.unesp.br
Department of Mathematics - São Paulo State University, Ilha Solteira - Brazil
Antônio Aparecido de Andrade andrade@ibilce.unesp.br
Department of Mathematics - São Paulo State University, S. J. Rio Preto - Brazil
Tariq Shah stariqshah@gmail.com
Department of Mathematics - Quaid-i-Azam University, Islamabad - Pakistan

Abstract. In this paper, firstly, we present a construction of lattice codes from cyclic codes over the finite field $\mathbb{F}_3$ via the ring of algebraic integers $\mathcal{O}_L$ of the cyclotomic field $\mathbb{L} = \mathbb{Q}(\zeta_{3^s})$. Secondly, making use of the ring $\mathcal{O}_L$, we present a construction of lattice codes via cyclic codes obtained through the monoid ring $\mathbb{F}_3[x; \frac{1}{3}\mathbb{Z}_0]$.

1 Introduction

Lattices codes has been introduced in [3], as a consequence of the relative embedding of linear codes over the finite field $\mathbb{F}_p$ into $\mathbb{R}^n$.

The main objective of this work is to extend the procedure to construction of lattices codes from linear codes obtained from the semi-group rings [2] and [1]. For the purpose, we developed an algebraic method based on the algebraic numbers theory. First, we considered the family of the cyclotomic number fields $\mathbb{L} = \mathbb{Q}(\zeta_{3^s})$ of degree $n = 3^{s-1}$ over $\mathbb{Q}(\zeta_3)$. In the next, we established a correspondence between the sequence of ideals of kind $\Im^r = (1 - \zeta_{3^s})^r \mathcal{O}_L$ (for $r \in \{0, 1, \cdots, m\}$) and the sequence of nested lattices $\Lambda(\Im^r)$ obtained as relative embedding of the ideal $\Im^r = (1 - \zeta_{3^s})^r \mathcal{O}_L$ in $\mathbb{C}^n$, where $\mathcal{O}_L$ is the ring of algebraic integers of $\mathbb{L}$.

In particular for $i = 0$, we obtain the complex lattice $\Lambda(\mathcal{O}_L)$, which is isomorphic to $\mathcal{A}_2^n$-lattice. Finally, as a consequence of this correspondence, we also established a correspondence between lattice codes C_r obtained from these nested lattices $\Lambda(\Im^r)$ and the cyclic codes over finite quotient polynomial ring and finite quotient monoid ring [1].

2 Linear cyclic codes through monoid rings

A linear code $\mathcal{C}$ of length n over a commutative ring B with identity is a B-submodule in the space of all n-tuples of B^n, and a linear code $\mathcal{C}$ over

[1]This research is partially supported by grant 2013/25977-7, São Paulo Research Foundation (FAPESP)

B is a cyclic code, if $v = (v_0, v_1, \cdots, v_{n-1}) \in \mathcal{C}$, every cyclic shift $v_1^{(1)} = (v_{n-1}, v_1, \cdots, v_{n-2}) \in \mathcal{C}$, where $v_i \in B$ for $0 \leq i \leq n-1$. By [1] for a commutative ring B with identity, $\Re = \frac{B[x, \frac{1}{3}\mathbb{Z}_0]}{((x^{\frac{1}{3}})^{3n}-1)}$ is a finite ring.

A linear code $\mathcal{C}$ of length $3n$ over B is a submodule in the space of all $3n$-tuples of B^{3n} and $\mathcal{C}$ is a cyclic code, if $v = (v_0, v_{\frac{1}{3}}, v_{\frac{2}{3}}, v_1, \cdots, v_{\frac{3n-1}{3}}) \in \mathcal{C}$, every cyclic shift $v^{(1)} = (v_{\frac{3n-1}{2}}, v_0, v_{\frac{1}{3}}, \cdots, v_{n-1}) \in \mathcal{C}$, where $v_i \in B$ for $i = 0, 1, \cdots, \frac{3n-1}{3}$.

Theorem 1. *[1] A subset $\mathcal{C}$ of $\Re = \frac{B[x, \frac{1}{3}\mathbb{Z}_0]}{((x^{\frac{1}{3}})^{3n}-1)}$ is a cyclic code if and only if $\mathcal{C}$ is an ideal of $\Re$.*

If $f(x^{\frac{1}{3}}) \in B[x, \frac{1}{3}\mathbb{Z}_0]$ is a monic pseudo polynomial of degree n, then $\Re = \frac{B[x, \frac{1}{3}\mathbb{Z}_0]}{(f(x^{\frac{1}{3}}))}$ is the set of residue classes of pseudo polynomials in $B[x, \frac{1}{3}\mathbb{Z}_0]$ module the ideal $(f(x^{\frac{1}{3}}))$ and a class can be represented as $\overline{a}(x^{\frac{1}{3}}) = \overline{a}_0 + \overline{a}_{\frac{1}{3}} x^{\frac{1}{3}} + \overline{a}_{\frac{2}{3}} x^{\frac{2}{3}} + \overline{a}_1 x + \cdots + \overline{a}_{\frac{3n-1}{3}} x^{\frac{3n-1}{3}}$. A principal ideal of $\Re$ consists of all multiples of a fixed pseudo polynomial $(g(x^{\frac{1}{3}}))$ by elements of $\Re$, where $(g(x^{\frac{1}{3}}))$ is called a generator pseudo polynomial of the ideal.

3 Nested lattices from complex lattices $\mathcal{A}_2^n$

We call a sequence of lattices $\Lambda_1, \cdots, \Lambda_m$ to be a nested lattices on lattice Λ if $\Lambda \subseteq \Lambda_1 \subseteq \cdots \subseteq \Lambda_m$. In this case, we propose an arithmetic construction procedure of a sequence of nested lattices $\Lambda, \Lambda_1, \cdots, \Lambda_{m-1}$ on the complex lattice Λ_m, where $\Lambda_m \simeq \mathcal{A}_2^n$, where $\mathcal{A}_2$ is a hexagonal lattices.

For it, we consider the cyclotomic number field $\mathbb{L} = \mathbb{Q}(\zeta_{3^s})$ of degree $n = 3^{s-1}$ over the number field $\mathbb{Q}(\zeta_3)$, where ζ_{3^s} is 3^s-th root of unity. Trinca *et.al* [4] showed to complex lattices $\Lambda(\mathbb{Z}[\zeta_{3^s}])$ obtained via Minkowisk embedding of the ring of algebraic integers $\mathbb{Z}[\zeta_{3^s}]$ is isomorphic to the $\mathcal{A}_2^n$, that also is isomorphic to $\mathbb{Z}[\zeta_3]^n$, where $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}[\zeta_{3^s}]$ are rings of algebraic integers associated to $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_{3^s})$, respectively.

In the following, we will find prime ideals as a prime triplet $(p; \mathcal{P}; \Im_i)$ on Galois extension $\mathbb{L}/\mathbb{F}$, i.e, $p, \mathcal{P}$ and $\Im$ are prime ideals in the ring of algebraic integers $\mathbb{Z}$, $\mathbb{Z}[\zeta_3]$ and $\mathcal{O}_L$, respectively.

It is very easy to check the relative norm $N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}$ applied over $(1-\zeta_3)$ is 3. Therefore, $(1-\zeta_3^2)$ is a prime ideal in the ring of algebraic integers $\mathbb{Z}[\zeta_3]$.

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

Proof. First notices, for each $s > 1$, it follows that $\zeta_{3^s}^3 = \zeta_{3^{s-1}}$ and the finite extension field $\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_{3^{s-1}})$ has degree 3. Consequently, we can see $\mathbb{Q}(\zeta_{3^s})$ as a field extension of the field $\mathbb{Q}(\zeta_{3^{s-1}})$ with the minimal polynomial associate given by $m(x) = x^3 - \zeta_{3^{s-1}}$ and this polynomial can be factorized as $m(x) = (x - \zeta_{3^s})(x - \zeta_{3^s}\zeta_{3^{s-1}})(x - \zeta_{3^s}\zeta_{3^{s-1}}^2)$ and the Galois group is given by $G(\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_{3^{s-1}}) = \{id, \sigma_1, \sigma_2\}$, where $\sigma_1(\zeta_{3^s}) = \zeta_{3^s}, \sigma_2(\zeta_{3^s}) = \zeta_{3^{s-1}}\zeta_{3^s}$ and $\sigma_3(\zeta_{3^s}) = \zeta_{3^{s-1}}\zeta_{3^s}$. Therefore, it follows that $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_{3^{s-1}})}(1 - \zeta_{3^s}) = (1 - \zeta_{3^s})(1 - \zeta_{3^s}\zeta_{3^s})(1 - \zeta_{3^s}\zeta_{3^s}^2) = (1 - \zeta_{3^s}^3) = 1 - \zeta_{3^{s-1}}$. □

Proposition 1. *If $s > 0$, then the ideal $\Im = (1 - \zeta_{3^s})\mathcal{O}_L$ is a prime ideal in the ring $\mathcal{O}_L$.*

Proof. For $s = 1$, it is easy to check $N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(1 - \zeta_3) = 3$. Now, we consider an induction over $s - 1$, that is, that $N_{\mathbb{Q}(\zeta_{3^{s-1}})/\mathbb{Q}}(1 - \zeta_{3^{s-1}}) = 3$. We can also show $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}}(1 - \zeta_{3^s}) = N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}}(1 - \zeta_{3^{s-1}}) = 3$. As consequence of the property of relative norm on extension of finite extension is transitive, we obtain

$$N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}}(1 - \zeta_{3^s}) = N_{\mathbb{Q}(\zeta_{3^{s-1}})/\mathbb{Q}}(N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(3^{s-1})}(1 - \zeta_{3^s})).$$

Thus, for consequence of induction over $s-1$, we obtain $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}}(1-\zeta_{3^s}) = 3$. By Lemma 1, it follows that $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}}(1 - \zeta_{3^s}) = 1 - \zeta_{3^{s-1}}$. Furthermore, $\Im = (1 - \zeta_{3^s})\mathcal{O}_L$ is prime ideal in the ring $\mathcal{O}_L$. □

Let $u = 1 - \zeta_{3^s}$, for each ideal $\Im^r = u^r\mathcal{O}_L$, we consider the correspondent n dimensional complex ideal obtained via the canonical homomorphism.

Lemma 2. [5] *If Λ' is a sublattice of Λ of order $|\Lambda/\Lambda'|$, then $V(\Lambda') = |\Lambda/\Lambda'|V(\Lambda)$.*

Remark 2. *We can be consider all ideals listed as a sequence of ideals written as $\Im^r = (u^r)\mathcal{O}_L$. Thus, we have $\{u^r, u^r\zeta_{3^s}, \cdots, u^r\zeta_{3^s}^{n-1}\}$ is a $\mathbb{Z}[\zeta_3]$-basis of the correspondent complex ideal lattice $\Lambda(\Im^r)$, because $\{1, \zeta_{3^s}, \cdots, \zeta_{3^s}^{n-1}\}$ is a $\mathbb{Z}[\zeta_3]$-basis of the complex lattices $\Lambda(\mathcal{O}_L)$. Then,*

$$M_r = \begin{pmatrix} u^r & u^r\zeta_{3^s} & \cdots & u^r\zeta_{3^s}^{n-1} \\ \sigma_2(u^r) & \sigma_2(u^r\zeta_{3^s}) & \cdots & \sigma_2(u^r\zeta_{3^s}^{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(u^r) & \sigma_n(u^r\zeta_{3^s}) & \cdots & \sigma_n(u^r\zeta_{3^s}^{n-1}) \end{pmatrix}$$

is the generator matrix of complex ideal lattice $\Lambda(\Im^r)$.

Proposition 2. *The complex ideal lattice $\Lambda(\Im^r)$ is a sublattice of the complex lattice $\Lambda(\mathcal{O}_L)$, whose index of the lattice $\Lambda(\mathcal{O}_L)$ by the sublattice $\Lambda(\Im^r)$ is given by $[\Lambda(\mathcal{O}_L) : \Lambda(\Im^r)] = 3^r$.*

Proof. Notices the fact $\Lambda(\Im^r)$ is a sublattice of the complex lattice $\Lambda(\mathcal{O}_L)$ is directly consequence of Remark 2. When we compute the index of the complex ideal lattices $\Lambda(\Im^r)$ by the complex lattices $\Lambda(\mathcal{O}_L)$, we obtain $\mid \Lambda(\mathcal{O}_L) : \Lambda(\Im^r) \mid = \dfrac{vol(\Lambda(\Im^r))}{vol(\Lambda(\mathcal{O}_L))}$.

Now, we consider the real lattices $\Lambda(\Im^r)$ and $\Lambda(\mathcal{O}_L)$ obtained from complex lattices given by $\Lambda(\Im^r)$ and $\Lambda(\mathcal{O}_L)$, respectively. Thus, $3^r = N_{\mathbb{Q}(\zeta_{3^s}):\mathbb{Q}}(\Im^r) = \mid \mathcal{O}_L : \Im^r \mid = \dfrac{vol(\Lambda(\Im^r))}{vol(\Lambda(\mathcal{O}_L))}$. Therefore, $\mid \Lambda(\mathcal{O}_L) : \Lambda(\Im^r) \mid = 3^r$. □

Consequently, we obtain a sequence of complex sublattices on complex lattices $\Lambda(\mathcal{O}_L) \simeq \mathbb{Z}[\zeta_3]^n$ given by Equation (1)

$$\cdots \subset \Lambda(\Im^r) \subset \Lambda(\Im^{r-1}) \subset \cdots \Lambda(\Im^2) \subset \Lambda(\Im) \subset \Lambda(\mathcal{O}_L). \tag{1}$$

4 Families of lattices codes though polynomial ring and monoid ring

The main objective in this section is to established one correspondence between sublattices $\Lambda(\Im^r)$ belong to to the complex lattices $\Lambda(\mathcal{O}_L)$ and to the cyclic codes over $\mathbb{F}_3$. For it, we first consider the following remark.

Remark 3. *Let $\Im^r = (1-\zeta)^r \mathcal{O}_L$ be an ideal in $\mathcal{O}_L$ and its correspondent complex ideal lattice $\Lambda(\Im^r)$. Since, $(1-\zeta_3)\Lambda(\Im^r)$ is a sublattice of $\Lambda(\Im^r)$, it follows that we can express $\Lambda(\Im^r)$ as $\Lambda(\Im^r) = (1-\zeta_3)\Lambda(\Im^s) + C_r$, where C_r is coset representative $[\Lambda(\Im^s)/(1-\zeta_3)\Lambda(\Im^r)]$ [5].*

Theorem 4. *The each complex ideal lattice C_r of Remark 3 corresponding to the cyclic code generated by $(1-x)^r$, where $0 < r = n-k \leq n$ and r is the dimension of the cyclic code over $\mathbb{F}_3$.*

Proof. We rewrite ζ_{3^s} as ζ. Let $\Im^r = (1+\zeta)^r \mathcal{O}_L$ be an ideal in $\mathcal{O}_L$ and its correspondent complex lattice $\Lambda(\Im^r)$ in $\mathbb{R}^{2n}$. If $u_r \in \Lambda(\Im^r)$, then we can written u_r as $u_r = (1-\zeta)^r(a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1})$, where $a_k \in \mathbb{Z}[\zeta_3]$, with $k = 0, 1, \cdots, n-1$. Since $\mathbb{Z}[\zeta_3]/(1-\zeta_3)\mathbb{Z}[\zeta_3]$ is isomorphic to $\mathbb{F}_3 = \{0, 1, -1\}$, it follows that we can be written a_k as $a_k = (1-\zeta_3)b_k + c_k$, where $b_k \in \mathbb{Z}[\zeta_3]$ and $c_k = 0, 1, \zeta_3$ or ζ_3^2. Therefore, $u_s = (1-\zeta)^r[((1-\zeta_3)b_0 + c_0) + ((1-\zeta_3)b_1 + c_1)\zeta + \cdots + ((1+\zeta_3)b_{n-1} + c_{n-1})\zeta^{n-1}] = (1+\zeta)^r[(1+\zeta_3)b_0 + (1+\zeta_3)b_1\zeta + \cdots + (1+\zeta_3)b_{n-1}\zeta^{n-1}] + +(1-\zeta)^r[c_0 + c_1\zeta + \cdots + c_{n-1}\zeta^{n-1}] = (1-\zeta)^r(1+i)(b_0 + b_1\zeta + \cdots + b_{n-1}\zeta^{n-1}) + (1-\zeta)^r(c_0 + c_1\zeta + \cdots + c_{n-1}\zeta^{n-1}) = (1-\zeta_3)(1+\zeta)^r(b_0 + b_1\zeta + \cdots + b_{n-1}\zeta^{n-1}) + (1-\zeta)^r(c_0 + c_1\zeta + \cdots + c_{n-1}\zeta^{n-1})$. Let $w_r = (1-\zeta_3)(1-\zeta)^r(b_0 + b_1\zeta + \cdots + b_{n-1}\zeta^{n-1})$. We have $w_r \in (1-\zeta_3)\Im^r \subset \Im^r$. Let $u_r - w_r = c$. Thus, $u_r = w_r + (1-\zeta)^r(c_0 + c_1\zeta + \cdots + c_{n-1}\zeta^{n-1})$, where $c_k \in \{0, 1, \zeta_3, \zeta_3^2\}$. We also have $\zeta^n = \zeta_3^3 \equiv 1$ (modulo $(1-\zeta_3)$), so $\zeta^n = 1$ over the field

$\mathbb{F}_3 = \{0, 1, -1\}$. If $x = \zeta$, then $x^n = 1$ over $\mathbb{F}_3$, and therefore, $u_r(x) - w_r(x) = (1-x)^r(\overline{c}_0 + \overline{c}_1 x + \cdots + \overline{c}_{n-1}x^{n-1})$ (modulo $x^n - 1$). So we can conclude that $[u_r(x) - w_r(x)] = \{(1-x)^r(\overline{c}_0 + \overline{c}_1 x + \cdots + c_{n-1}x^{n-1})$ (modulo $x^n - 1$); $c_k \in \mathbb{F}_3\} = (1-x)^r)$, which corresponds to the ideal in $\frac{\mathbb{F}_3[x]}{(x^N-1)}$ generated by $(1-x)^r$, where $0 < r \leq n$. Then C_s is isomorphic to ideal $(1-x)^r$ in $\frac{\mathbb{F}_3[x]}{(x^n-1)} \simeq \mathbb{F}_3^n$. For our proposed we denote by ϕ this isomorphism. Consequently, it is immediately to see and verified $\phi^{-1}(C_r) \subseteq \mathbb{Z}[\zeta_3]^n$ and it is a sublattices in $\mathbb{Z}[\zeta_3]^n$. Therefore, C_r is a parity check cyclic code, which has dimension $n-1$. However, we have $u_r \in \Im^r = (1-\zeta)^r$ an arbitrary element and, after the quotient, we have the identification with the ideal in $\frac{\mathbb{F}_3[x]}{(x^n-1)}$ generated by $(1-x)^r$. Then, C_r is a cyclic code over $\mathbb{F}_3$ with generator polynomial $(1-x)^r$, which has dimension $n-r$. □

4.1 Lattices codes though monoid rings

For our convenience, we denote $B = \mathbb{F}_3$. Consequently, we have $B[x] = B[x, \mathbb{Z}_0] \subset B[x, \frac{1}{3}\mathbb{Z}_0]$. For it, initially we shown there is a closed relation between polynomial belong to finite polynomial ring $\frac{\mathbb{F}_3[x]}{(x^N-1)}$ and generalized polynomial belongs to the finite factor monoid ring $B[x, \frac{1}{3}\mathbb{Z}_0]/((x^{\frac{1}{3}})^{3n} - 1)$. We established this relations via primitive elements belong to the tower of cyclotomic fields $\mathbb{Q}(\zeta_{3^s})$.

Proposition 3. *There is an isomorphism between the residue classes of the generalized polynomials belongs to the finite monoid ring $B[x, \frac{1}{3}\mathbb{Z}_0]/((x^{\frac{1}{3}})^{3n}-1)$ and the residue classes of polynomials belongs to finite polynomial ring $B[x]/(x^{3n} - 1)$.*

Proof. Notice each element (the residue classes of the pseudo polynomial) of $B[x, \frac{1}{3}\mathbb{Z}_0]/((x^{\frac{1}{3}})^{3n} - 1)$ can be represented as $\overline{a}(x^{\frac{1}{3}}) = \overline{a}_0 + \overline{a}_{\frac{1}{3}}x^{\frac{1}{3}} + \overline{a}_{\frac{2}{3}}x^{\frac{2}{3}} + \overline{a}_1 x + \cdots + \overline{a}_{\frac{3n-1}{3}}x^{\frac{3n-1}{3}}$. We can be defined an application $\phi(\overline{a}(x^{\frac{1}{3}})) = \overline{b}(x)$, where $\overline{b}(x) = \overline{b}_0 + \overline{b}_1 x + \cdots + \overline{b}_{3n-1}x^{3n-1}$ correspond to the residue classes of polynomial in $\frac{B[x]}{(x^{3n}-1)}$, with $\overline{b}_i = \frac{\overline{a}_i}{3}$, for all $i = 0, 1, \cdots, 3n-1$. It is not difficult to check ϕ established an isomorphism between $B[x, \frac{1}{3}\mathbb{Z}_0]/((x^{\frac{1}{3}})^{3n} - 1)$ and $\frac{B[x]}{(x^{3n}-1)}$. □

Now, we fixed the cyclic fields $\mathbb{Q}(\zeta_{3^{s+1}})$ and $\mathbb{Q}(\zeta_{3^s})$ of degree $3n = 3^{s+1}$ and $n = 3^s$, respectively. Here, for our convenience, let $\zeta = \zeta_{3^s}$ and $\zeta^{\frac{1}{3}} = \zeta_{3^{s+1}}$, where ζ_{3^s} and $\zeta_{3^{s+1}}$ are 3^{s+1} and 3^s-th root of unity, respectively.

Remark 5. *Consider $\zeta = \zeta_{3^s}$. Observe that ζ is a root of the polynomial $m_1(x) = x^n - 1 \in B[x]/(x^n - 1)$.*

(i) *We can factored* $m_1(x)$ *as* $m_1(x) = m_2(x^{\frac{1}{3}})m_3(x^{\frac{1}{3}})$, *where* $m_2(x^{\frac{1}{3}}) = (x^{\frac{1}{3}})^n - 1$ *and* $m_3(x^{\frac{1}{3}}) = (x^{\frac{2}{3}})^n + (x^{\frac{1}{3}})^n + 1$.

(ii) $m_2(x^{\frac{1}{3}})$ *and* $m_3(x^{\frac{1}{3}})$ *are pseudo polynomial in finite ring* $B[x, \frac{1}{3}\mathbb{Z}_0]/((x^{\frac{1}{3}})^{3n} - 1)$.

(iii) $\zeta^{\frac{1}{3}}$ *is a root of the pseudo polynomial* $m_2(x^{\frac{1}{3}})$ *belong to* $B[x, \frac{1}{3}\mathbb{Z}_0]/((x^{\frac{1}{3}})^{3n} - 1)$ *and at the same time is a root of polynomial* $p(x) = x^{3^{s+1}} - 1$ *belong to* $B[x]/(x^{3n} - 1)$.

Theorem 6. *Each complex ideal lattice* C_r *of Remark 3 correspond to a cyclic code generated by* $(1 - x^{\frac{1}{3}})^r$, *where* $0 < r = 3n - k \leq 3n$ *and* r *is the dimension of the cyclic code.*

Proof. Since $\zeta^{\frac{1}{3}} = \zeta_{3^{s+1}}$, it follows that $\Im^r = (1 + \zeta_{3^{s+1}})^r \mathcal{O}_L$ is an ideal of the ring $\mathcal{O}_L$ and its correspondent complex lattice is $\Lambda(\Im^r)$, where $\mathbb{L} = \mathbb{Q}(\zeta_{3^{s+1}})$ of degree $3n$, with $n = 3^{s-1}$. As consequence, of Remark 3 and Theorem 4, it follows that C_r is the coset representative $[\Lambda(\Im^r)/(1 + \zeta_3)\Lambda(\Im^r)]$ correspond to cyclic code given by an ideal in $B[x]/(x^{3n} - 1)$ generated by the polynomial $(1 - x)^r$. By Remark 5, it follows that the polynomial $(1 - x)^r$ in the quotient polynomial ring $B[x]/(x^{3n} - 1)$ correspond to the pseudo polynomial $(1 - x^{\frac{1}{3}})^r$ in the quotient semi ring $B[x, \frac{1}{3}\mathbb{Z}_0]/((x^{\frac{1}{3}})^{3n} - 1)$. Finally, as consequence of Theorem 1, it follows that $(1 - x^{\frac{1}{3}})^r$ generate a cyclic codes. Consequently, we obtain a correspondence between the family of cyclic codes obtained as ideal of the monoid ring and the family of lattices codes. □

References

[1] 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), pp. 37-50, 2012.

[2] A.A. Andrade and R. Palazzo Jr.; *Linear codes over finite rings*, Tend. Mat. Apl. Comput., 6(2), pp. 207-217, 2005.p

[3] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, New York: Springer-Verlag, 1988.

[4] C.C. Trinca,E.D. Carvalho, J. Vieira Filho, and A.A. Andrade. *On the construction of perfect codes from HEX signal constellations* Journal of the Franklein in Institute 349, pp 3060-3077, 2012.

[5] G. D. Forney, "Coset Codes - Part I: Introduction and Geometrical Classification," *IEEE Trans. Inform. Theory*, v. 34, pp. 1123–1151, September 1988.