Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Novas construções de códigos reticulados via o anel de polinômios generalizados $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]$

Edson Donizete de Carvalho[1]

Departamento de Matemática, Feis-Unesp, Ilha Solteira, SP

Antônio Aparecido de Andrade[2]

Departamento de Matemática, Ibilce-Unesp, S.J.Rio Preto, SP

Cibele Cristina Trinca[3]

Departamento de Engenharia Florestal, UFT, Gurupi-TO

Resumo. Tradicionalmente, códigos-reticulados são obtidos através do anel de polinômios $\mathbb{F}_p[x]$, onde $\mathbb{F}_p$ denota um corpo finito. Neste artigo, mostraremos para o caso $p = 2$, uma nova construção de códigos-reticulados a partir do anel de pseudo-polinômios $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]$. Para isto primeiro, construíremos códigos reticulados sobre o corpo $\mathbb{F}_2$ via o anel de inteiros $\mathcal{O}_L$ de um corpo de números $L = \mathbb{Q}(\zeta_{2^s})$. Como consequência, utilizaremos as mesmas ferramentas algébricas obtidos a partir de $\mathcal{O}_L$ para construirmos códigos reticulados via anéis de polinômios generalizados $\mathbb{F}_2[x;\frac{1}{2}\mathbb{Z}_0]$.

Palavras-chave. Anéis de polinômios generalizados, Códigos Reticulados, Códigos Lineares, Corpos de Números e Codificação de Canal

1 Introdução

Códigos reticulados [1] são construídos por meio da *Construção A*, isto é, a técnica que possibilita a construção de reticulados através do mergulho de um código linear definido sobre um corpo finito $\mathbb{F}_p$ em $\mathbb{R}^N$ ou em $\mathbb{C}^N$.

Eres e Zamir [2] mostraram que para esquemas de codificação baseados em códigos reticulados desde que combinados com a decodificação de reticulados apresentam desempenhos próximos aos limitantes teóricos demonstrados por Shannon em codificação de canal envolvendo problemas seja eles de quantização de canal quanto de codificação em redes. O que tem dispertando um grande interesse da comunidade de teoria de códigos nesta temática.

Uma importante classe de códigos reticulados podem serem obtidos a partir de $\mathbb{Z}[i]^N$. Para isto basta que consideremos o código $\mathcal{C}$ como sendo o conjunto de todos as N-uplas de $\mathbb{Z}[i]^N$ como sendo congruente modulo $\phi = 1 + i$. Neste caso, temos $\mathcal{C} \simeq \mathbb{Z}[i]^N/\phi\mathbb{Z}[i]^N$.

[1]edson@mat.feis.unesp.br
[2]andrade@ibilce.unesp.br
[3]cibtrinca@yahoo.com.br

Note que a partir do reticulado complexo $\mathbb{Z}[i]^N$ podemos uma cadeia de partição infinita de subreticulados na forma $\mathbb{Z}[i]^N/\phi\mathbb{Z}[i]^N/\phi^2\mathbb{Z}[i]^N/\cdots$

Forney [3] mostrou que podemos expressar $\phi^k\mathbb{Z}[i]^N$ por meio de uma fórmula código complexa

$$\phi^k\mathbb{Z}[i]^N = \phi^{k-1}\mathbb{Z}[i]^N + \phi^{k-2}\mathcal{C}_{k-1} + \cdots \mathcal{C}_0, \tag{1}$$

e que estes reticulados complexos $\phi^k\mathbb{Z}[i]^N$ são identificados por códigos lineares sobre o corpo finito $\mathbb{F}_2$ e que podem serem vistos como um ideal primo no anel fatorial $\mathbb{F}_2[x]/(x^N - 1) \simeq \mathbb{F}_2^N$

Por outro lado, Shah et al. [7] proporam uma nova maneira de construir códigos lineares sobre anéis de polinômios generalizados.

O objetivo deste artigo é de mostrar que reticulados complexos $\phi^k\mathbb{Z}[i]^N$ também são identificados por códigos lineares sobre o anel de polinômios generalizados B e que podem serem vistos como um ideal primo no anel fatorial $B/(x^N - 1)$.

2 Códigos lineares provenientes de anéis comutativos

Um código linear $\mathcal{C}$ de comprimento n sobre um anel comutativo B com identidade é um submódulo B no espaço de todas as n-uplas de B^n, e código linear $\mathcal{C}$ sobre B é um código cíclico, se $v = (v_0, v_1, \cdots, v_{n-1}) \in \mathcal{C}$, para todo shift $v_1^{(1)} = (v_{n-1}, v_1, \cdots, v_{n-2}) \in \mathcal{C}$, onde $v_i \in B$ para $0 \leq i \leq n-1$.

Por [4] temos para um anel comutativo B com identidade, $\Re = \frac{B[x,\frac{1}{2}\mathbb{Z}_0]}{((x^{\frac{1}{2}})^{2n}-1)}$ é um anel finito. Um código linear $\mathcal{C}$ de comprimento $2n$ sobre B é um submódulo no espaço de todas as $2n$-uplas de B^{2n} e $\mathcal{C}$ é um código cíclico, se $v = (v_0, v_{\frac{1}{2}}, v_1, \cdots, v_{\frac{2n-1}{2}}) \in \mathcal{C}$, para shift cíclico $v^{(1)} = (v_{\frac{2n-1}{2}}, v_0, v_{\frac{1}{2}}, \cdots, v_{n-1}) \in \mathcal{C}$, onde $v_i \in B$ for $i = 0, 1, \cdots, \frac{2n-1}{2}$.

O próximo teorema descreve quando um subconjunto $\Re = \frac{B[x,\frac{1}{2}\mathbb{Z}_0]}{((x^{\frac{1}{2}})^{2n}-1)}$ é um código cíclico.

Theorem 2.1. *[7] Um subconjunto $\mathcal{C}$ de $\Re = \frac{B[x,\frac{1}{2}\mathbb{Z}_0]}{((x^{\frac{1}{2}})^{2n}-1)}$ é um código cíclico se e somente se $\mathcal{C}$ é um ideal de $\Re$.*

3 Formulação e Solução Matemática do Problema

A formulação e resolução do problema em questão será baseado na teoria algébrica dos números.

Neste sentido, consideremos uma cadeias de corpos ciclotômicos dados por $\mathbb{Q} \subset L_2 \subset \ldots \subset L_s$, satisfazendo a condição de que $L_2 = \mathbb{Q}(\zeta_{2^2}) = \mathbb{Q}(i)$ e para todo $s \geq 3$ temos $L_s = \mathbb{Q}(\zeta_{2^s})$, onde ζ_{2^s} denota 2^s-ésima da unidade.

A cadeia acima também pode ser denotada por $L_s/L_{s-1}/\cdots/L_2/\mathbb{Q}$. Cada corpo L_s pode ser visto como um espaço vetorial sobre $\mathbb{Q}$ ou sobre corpo ciclotômico L_{s-1}.

DOI: 10.5540/03.2016.004.01.0106

Diremos que L_s/L_{s-1} é uma extensão finita de corpos se L_s visto como espaço vetorial sobre L_s tem dimensão finita. Associado a cada extensão finita de corpos L_s/L_{s-1}, temos como consequência do fato de que $\zeta_{2^s}^2 = \zeta_{2^{s-1}}$ e $L_s = L_{s-1}(\zeta_{2^s})$ as sequintes relações:

1. $\{1, \zeta_{2^s}\}$ é uma base de L_s sobre L_{s-1} tendo ζ_{2^s} como raiz do polinômio minimal $p_s(x) = (x - \zeta_{2^s})(x + \zeta_{2^s})$ e com o grupo de Galois associado a extensão dado por $Gal(L_s/L_{s-1}) = \{id, \sigma_s\}$ onde σ_s denota as permutações das raízes do polinômio minimal p_s.

2. $\{1, \zeta_{2^s}, \ldots, \zeta_{2^s}^{N-1}\}$ é uma base de L_s sobre K tendo ζ_{2^s} como raiz do polinômio minimal $\mu_{\zeta_{2^s}}(x) = \prod_{k=0}^{N-1}(x - \zeta_{2^s}^k)$. As raízes de $\mu_{\zeta_{2^s}}(x)$ e com o grupo de Galois associado a extensão de corpos L/K dado por $Gal(L/F) = \{\sigma_j : \sigma_j(\zeta_{2^s}) = \zeta_{2^s}^j, \forall j = 0, 1, \ldots, N-1\}$, onde $N = 2^{s-1}$ se $K = \mathbb{Q}$ e $N = 2^{s-2}$ se $K = \mathbb{Q}(i)$.

3. O conjunto dos elementos de L obtido como um módulo sobre $\mathbb{Z}$ gerado pela base integral $\{1, \zeta_{2^s}, \zeta_{2^s}^2, \cdots, \zeta_{2^s}^{2^{s-1}}\}$ é chamado de anel de inteiros de L denotado por $\mathcal{O}_L$ ou $\mathbb{Z}[\zeta_{2^s}]$ e β é chamada de base integral. Convém, desde que $\mathcal{O}_L$ também pode ser visto como um módulo sobre $\mathbb{Z}[i]$ gerado pela base integral $\{1, \zeta_{2^s}, \zeta_{2^s}^2, \cdots, \zeta_{2^s}^{2^{s-2}}\}$.

A partir de uma extensão finita de corpos L/K de grau t, podemos definir o traço e a norma relativa de um elemento $\alpha \in \mathcal{O}_L$ como sendo os inteiros algébricos $Tr_{L/K}(\alpha) = \sum_{i=0}^{t-1} \sigma_i(\alpha)$ and $N_{L/K}(\alpha) = \prod_{i=0}^{t-1} \sigma_i(\alpha)$, respectivamente. Observe que $Tr_{L/K}(\alpha)$ e $N_{L/K}(\alpha)$ pertence a $\mathcal{O}_K$. Caso $L/K/\mathbb{Q}$ seja uma cadeia de extensões finitas de corpos, então para cada elemento $\alpha \in L$ vale $N_{L/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(N_{L/K}(\alpha))$.

Se $\alpha, \beta \in L$, então $N_{L/\mathbb{Q}}(\alpha\beta) = N_{L/\mathbb{Q}}(\alpha)N_{L/\mathbb{Q}}(\beta)$.

Exemplo 3.1. *1. Seja $\alpha = 1 - i \in \mathbb{Q}(i)$ então $N_{\mathbb{Q}(i)/\mathbb{Q}}(1 - i) = id(1 - i)\sigma(1 - i) = 1 - i^2 = 2$, onde $\sigma^2 = id$ e $\sigma \in Gal(\mathbb{Q}(i)/\mathbb{Q}) = \{id, \sigma\}$.*

2. Seja $\alpha = 1 - \zeta_{2^s} \in \mathbb{Z}[\zeta_{2^s}]$, então, temos que $N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(9.2^{s-1})}(1 - \zeta_{2^s}) = id(1 - \zeta_{2^s})\sigma_r(1 - \zeta_{2^s}) = (1 - \zeta_{2^s})(1 + \zeta_{2^s}) = 1 - \zeta_{2^s}^2 = 1 - \zeta_{2^{s-1}}$.

Os trabalhos [5] e [6] mostraram maneiras de se obter reticulados algébricos Λ isomorfos a reticulados $\mathbb{Z}[i]^N$ via famílias de corpos ciclotômicos $\mathbb{Q}(\zeta_{2^s})$.

A partir de um ideal $\Im \subseteq \mathcal{O}_L$, podemos obter um reticulado algébrico complexo Λ como consequência dos mergulhos complexos de L em $\mathbb{C}^N$ definido da seguinte maneira

$$\sigma : L \Rightarrow \mathbb{C}^N, \text{ with } \sigma(x) = (\sigma_0(x), \cdots, \sigma_{N-1}(x)), \tag{2}$$

onde $\sigma_i \in Gal(L/\mathbb{Q}(i)), \forall i \in \{0, 1, \ldots N-1\}$.

Seja $\{w_0, \cdots, w_{N-1}\}$ a base integral de $\mathcal{O}_L$ sobre $\mathbb{Z}[i]$. No caso particular em que o ideal $\Im = \mathcal{O}_L$, obtemos o reticulado complexo associado dado por

$$\Lambda = \{x = \lambda M | \lambda \in \mathbb{Z}[i]^N\},$$

onde M chamada de matriz geradora do reticulado algébrica Λ e é dada por:

$$M = \begin{pmatrix} \sigma_0(w_0) & \cdots & \sigma_{N-1}(w_0) \\ \vdots & \ddots & \vdots \\ \sigma_0(w_{N-1}) & \cdots & \sigma_{N-1}(w_{N-1}) \end{pmatrix}. \quad (3)$$

Por outro lado, há uma outra matriz associado a um reticulado algébrico que chamamos de matriz Gram e dada por $G = M.\overline{M}^t$, onde $\overline{M}^t$ denota a matriz transposta conjugada da matriz M.

O próximo Proposição 3.1 estabelece a conexão entre reticulados algébricos obtidos a partir de um anel de inteiros $\mathbb{Z}[\zeta_{2^s}]$ e reticulados escalonados da forma $\mathbb{Z}[i]^N$.

Proposição 3.1. *[5] A matriz geradora $M_0 = (\frac{1}{\sqrt{N}})M$ do reticulado algébrico associado a $\mathbb{Z}[\zeta_{2^s}]$ é unitária e a matriz Gram $G = M_0\overline{M_0}^t = Id$, onde $N = 2^{s-2}$.*

3.1 Construção de cadeia de reticulados aninhados

Dizemos que uma cadeia de reticulados $\Lambda_{n-1}, \cdots, \Lambda_1$ está aninhado no reticulado Λ se $\Lambda_{n-1} \subseteq \Lambda_{n-2} \subseteq \cdots \subseteq \Lambda_1 \subset \Lambda$. Faremos uso da teoria algébrica dos números para construir explicitamente cadeias de reticulados aninhados.

Caso os reticulados desta cadeia de reticulados sejam códigos reticulados, temos uma cadeia de códigos reticulados aninhados. Uma importante classe de códigos reticulados da forma $\phi^k\mathbb{Z}[i]^N$ podem serem obtidos a partir de $\mathbb{Z}[i]^N$, como os descritos na Equação 1. Do ponto de vista geométrico os códigos reticulados aninhados são caracterizados da forma $\phi^k\mathbb{Z}[i]^N$, também chamados de versão escalonada do reticulado $\mathbb{Z}[i]^N$.

Consideremos uma cadeia de ideais em $\mathbb{Z}[\zeta_{2^s}]$ rotulados por rotulados por $\Im^k = (\alpha)^k\mathbb{Z}[\zeta_{2^s}]$, onde $\alpha = 1 - \zeta_{2^s}$.

Desde que $\{w_0, \ldots, w_{N-1}\}$ é uma base integral do anel de inteiros $\mathbb{Z}[\zeta_{2^s}]$ sobre $\mathbb{Z}[i]$. Da teoria de reticulados algébricos, temos que $\{\alpha^k w_0, \ldots, \alpha^k w_{N-1}\}$ é uma base integral de ideal $\Im^k\mathbb{Z}[\zeta_{2^s}]$ visto como um módulo sobre $\mathbb{Z}[i]$, onde $w_i = \zeta_{2^s}^i \ \ i \in \{0, 1, \ldots, N-1\}$.

Note que para $k = 0$, obtemos o reticulado trivial $\Im^0 = \mathbb{Z}[\zeta_{2^s}]$, onde temos a matriz geradora M_0 associada ao reticulado algébrico que denotaremos por Λ. A próxima Observação 3.1 que é baseada nos resultados de [5] e [6] que estabelecem uma importante conexão entre reticulados algébricos Λ_k associados aos ideais $\Im^k$ e a matrizes geradoras de reticulados obtidos via a forma traço.

Observação 3.1. *A matriz Gram $G = M_k\overline{M_k}^t$ concide a matriz $T_{L/\mathbb{Q}(\omega)}(\alpha w_j\overline{\alpha w_j})_{j=0}^{N-1}$ para reticulados ideais, isto é reticulados obtidos a através de ideais gerados por α via forma fórmula traço a partir de famílias de corpos ciclotômicos $\mathbb{Q}(\zeta_{2^s})$.*

Assim, matriz Gram do reticulado Λ_k é escrita na forma $G_k = M.B^k\overline{M}\overline{B^k}$, onde $B^k = diag(\alpha^k, \sigma(\alpha^k), \ldots, \sigma^{N-1}(\alpha^k))$.

No sentido de caracterizarmos exlpicitamente de forma algébrica os reticulados obtidos via a cadeia de ideais $\Im^k = (\alpha^k)\mathbb{Z}[\zeta_{2^s}]$ é que consideraremos a Proposição 3.2.

Proposição 3.2. *A norma relativa $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(i)}$ aplicada sobre o elemento $1 - \zeta_{2^s}$ é dada por $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(i)}(1 - \zeta_{2^s}) = 1 - i, \forall s \geq 3$.*

DOI: 10.5540/03.2016.004.01.0106

Demonstração. 1. Para $s = 3$, segue-se que $N_{\mathbb{Q}(\zeta_8)/\mathbb{Q}(i)}(1-\zeta_8) = id(1-\zeta_8)\sigma_3(1-\zeta_8) = (1-\zeta_{2^3})(1+\zeta_{2^3}) = 1-\zeta_{2^3}^2 = 1-i$.

2. Por indução sobre $s-1$, segue-se que $N_{\mathbb{Q}(\zeta_{2^{s-1}})/\mathbb{Q}(i)}(1-\zeta_{2^{s-1}}) = 1-i$.

   Pelo item (2) do Exemplo 3.1, temos que $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(2^{s-1})}(1-\zeta_{2^s}) = 1-\zeta_{2^{s-1}}$.

   Pela propriedade de norma relativa em uma extensão finita de corpos dada pela Equação , temos que $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(i)}(1-\zeta_{2^s}) = N_{\mathbb{Q}(\zeta_{2^{s-1}})/\mathbb{Q}(i)}(N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(2^{s-1})}(1-\zeta_{2^s}))$.

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

□

Proposição 3.3. *Seja $\alpha = 1-\zeta_{2^s}$. Para cada reticulado ideal Λ_k in $\mathbb{C}^N$ associado a um ideal $\Im^k = (\alpha)^k\mathbb{Z}[\zeta_{2^s}]$ é isomorfo a um código reticulado $(1+i)^k\mathbb{Z}[i]^N$ para todo inteiro $k \geq 1$.*

Demonstração. Analisaremos primeiro a matriz Gram matrix $G = M_k\overline{M_k}^t$ associada ao reticulado ideal Λ_k. Temos que a matriz M_k pode ser escrita na forma
$M_k = \sigma_\alpha(\zeta_{9.2^s}^j)_{j=0}^{N-1}.diag(\alpha^k,\ldots,\sigma_k(\alpha^k))$ and $\overline{M_k}^t = \overline{\sigma_{\alpha^k}(w_j))}_{j=0}^{N-1}.diag(\overline{\alpha^k},\ldots,\overline{\sigma_k(\alpha^k)})$
Usando de forma conveniente as propriedades da transposta conjugada do produto de matrizes, podemos expressar a matriz Gram por:

$$G = (\sigma_\alpha(\zeta_{2^s}^j)_{j=0}^{N-1}).(\overline{\sigma_j(\zeta_{2^s}^j)})_{j=0}^{N-1})^t \prod_{i=0}^{N-1}\sigma_i(\alpha^2)\prod_{i=0}^{N-1}\overline{\sigma_i(\alpha^k)}.$$

No entanto, temos que $M_0 = (\sigma_j(\zeta_{2^s}^j)_{j=0}^{N-1})$ e $\prod_{i=0}^{N-1}\sigma_i(\alpha) = N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(i)}(\alpha^k)$.
Pelo Exemplo 3.2, temos $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(i)}(\alpha) = 1-i$.
Assim, obtemos $N_{\mathbb{Q}(\zeta_{2^s})/\mathbb{Q}(i)}(\alpha)^k = (1-i)^k$.
O que nos permite reescrever G na forma

$$G = (1-i)^k M_0(\overline{(1-i)})^k M_0\overline{M_0}^t = M_0\overline{M_0}^t = (1-i)^k M_0\overline{(1-i)^k M_0} \tag{4}$$

Desde que M_0 é a matriz geradora do código reticulado $\mathbb{Z}[i]^N$ e como $(1-i) = i(1+i)$. Então, podemos concluir que $i^k(1+i)^k M_0$ denota a matriz geradora do código reticulado $(1+i)^k\mathbb{Z}[i]^N$.

□

4 Códigos reticulados provenientes de anéis de pseudo polinômios

Inicialmente, mostraremos que existe uma relação entre polinômios de um anel de polinômios finito $\frac{\mathbb{F}_2[x]}{(x^N-1)}$ e polinômios generalizados pertencente a um anel de pseudo polinômios. $\mathbb{F}_2[x,\frac{1}{2}\mathbb{Z}_0]/((x^{\frac{1}{2}})^{2N}-1)$. Por fim estabeleceremos esta relação por meio das as raízes 2^s-ésimas da unidades.

Proposição 4.1. *As classes de resíduos de polinômios generalizados pertencentes ao anel de pseudo polinômios finito* $\mathbb{F}_2[x, \frac{1}{2}\mathbb{Z}_0]/((x^{\frac{1}{2}})^{2N} - 1)$ *é isomorfo as classes de resíduos de polinômios pertecentes ao anel de polinômios finito* $\mathbb{F}_2[x]/(x^N - 1)$.

Demonstração. Note que cada elemento (da classe de resíduos de polinômios generalizados) de $\mathbb{F}_2[x, \frac{1}{2}\mathbb{Z}_0]/((x^{\frac{1}{2}})^{2N} - 1)$ podem serem escritas na forma $\overline{a}(x^{\frac{1}{2}}) = \overline{a}_0 + \overline{a}_{\frac{1}{2}}x^{\frac{1}{2}} + \overline{a}_1 x + \cdots + \overline{a}_{\frac{2n-1}{2}}x^{\frac{2n-1}{2}}$. Defindo a aplicação $\varphi(\overline{a}(x^{\frac{1}{2}})) = \overline{b}(x)$, onde $\overline{b}(x) = \overline{b}_0 + \overline{b}_1 x + \cdots + \overline{b}_{2n-1}x^{2n-1}$ corresponde a classe de resíduos de polinômios em $\frac{B[x]}{(x^{2N}-1)}$, com $\overline{b}_i = \frac{\overline{a}_i}{2}$, para todo $i = 0, 1, \cdots, 2n-1$. Não é difícil mostrar que φ é um isomorfismo entre $\mathbb{F}_2[x, \frac{1}{2}\mathbb{Z}_0]/((x^{\frac{1}{2}})^{2N} - 1)$ e $\frac{\mathbb{F}_2[x]}{(x^{2N}-1)}$. □

Denotemos $2N = 2^{s+1}$ e $N = 2^s$, respectivamente. Por conveniência, escreveremos $\zeta = \zeta_{2^s}$ e $\zeta^{\frac{1}{2}} = \zeta_{2^{s+1}}$, onde $\zeta_{2^s}, \zeta_{2^{s+1}}$ são 2^{s+1} e 2^s-ésimas raízes da unidade, respectivamente.

Observação 4.1. *Se* $\zeta = \zeta_{2^s}$, *então* ζ *é uma raiz do polinômio* $m_1(x) = x^N - 1 \in B[x]/(x^N - 1)$. *Podemos fatorar* $m_1(x)$ *em* $m_1(x) = m_2(x^{\frac{1}{2}})m_3(x^{\frac{1}{2}})$, *onde* $m_2(x^{\frac{1}{2}}) = (x^{\frac{1}{2}})^N - 1$ *e* $m_3(x^{\frac{1}{2}}) = (x^{\frac{1}{2}})^N + 1$. *Também,* $m_2(x^{\frac{1}{2}})$ *e* $m_3(x^{\frac{1}{2}})$ *são polinômios generalizados no anel finito* $B[x, \frac{1}{2}\mathbb{Z}_0]/((x^{\frac{1}{2}})^{2N} - 1)$. *Temos, também que* $\zeta^{\frac{1}{2}}$ *é uma raiz do polinômio generalizado* $m_2(x^{\frac{1}{2}})$ *que pertence* $B[x, \frac{1}{2}\mathbb{Z}_0]/((x^{\frac{1}{2}})^{2N} - 1)$ *e ao mesmo tempo é raiz do polinômio* $p(x) = x^{2^{s+1}} - 1$ *que pertence* $B[x]/(x^{2N} - 1)$.

5 Resultados

Uma consequência direta da Proposição 4.1 e da Observação 4.1 estabelecemos uma correspondência entre a sequência de ideals $\mathbb{Z}[\zeta_{2^{s+1}}]$ dadas pela Equação (5)

$$\cdots \subset \Im^k \subset \Im^{k-1} \subset \cdots \Im^2 \subset \Im \subset \mathbb{Z}[\zeta_{2^{s+1}}] \tag{5}$$

e a sequência de subreticulados complexos $\Lambda \simeq \mathbb{Z}[i]^{2N}$ dados pela Equação (6)

$$\cdots \subset \Lambda_k \subset \Lambda_{k-1} \subset \cdots \Lambda_2 \subset \Lambda_1 \subset \Lambda \simeq \mathbb{Z}[i]^{2N} \tag{6}$$

e a sequência de ideais dados pelos polinômios generalizados de $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_0]$ dados por

$$\cdots \subset (1 + x^{1/2})^k \subset (1 + x^{1/2})^{k-1} \subset \cdots (1 + x^{1/2})^2 \subset (1 + x^{1/2}) \subset \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_0.] \tag{7}$$

6 Conclusões

A grande contribuição deste trabalho é de mostrar que códigos reticulados também podem serem obtidos via anéis de pseudo polinômios finitos. Desta forma extendendo a técnica da *Construção A* para outras estruras algébricas.

Agradecimentos

Os autores agradecem a Fapesp pelo apoio financeiro, Processo Fapesp 2013/25977-7.

Referências

[1] J.H. Conway and N.J.A. Sloane; *Sphere packings, lattices and groups*, Springer-Verlag, New York, 1988.

[2] U. Eres, S. Litsyn and R. Zamir, *Lattices which are good for (almost(everything)*, IEEE Trans. Inform. Theory, **51**(10), (2005) 3401-3416.

[3] G. D. Forney; *Coset Codes - Part I: Introduction and geometrical classification*, IEEE Trans. Inform. Theory, 34, 1123-1151, 1988.

[4] R. Gilmer; *Multiplicative ideal theory*, Marcel Dekker, New York, 1972.

[5] X. Giraud; E. Boutilon and J. C. Belfiore, *Algebraic tools to built modulation schemes for fading channels*, IEEE Trans. Inform. Theory, **43**(3), (1997) 938-952.

[6] F. Oggier; *Algebraic methods for channel coding*, Phd dissertation École Polytechnique Fédérale de Lausanne, Lausanne, 2005.

[7] T. Shah, A. Khan and A.A. Andrade; *Encoding through generalized polynomial codes*, Computational and Applied Mathematics, 30(2), 349-366, 2011.

