



Aproximação de canais via cadeia de reticulados algébricos encaixados baseado na técnica compute and forward

Edson Donizete de Carvalho¹

Departamento de Matemática, Unesp, Ilha Solteira, SP

Azucena Mireya Duarte Zelaya²

Programa de Pós-Graduação em Engenharia Elétrica, PUC-Rio, Rio de Janeiro, RJ

Miller Acosta Osório³

Programa de Pós-Graduação em Engenharia Elétrica, Unesp, Ilha Solteira, SP

Jozué Vieira Filho⁴

Curso de Engenharia de Telecomunicações, Unesp, São João da Boa Vista, SP

Resumo. Através da teoria algébrica dos números, propomos um eficiente método de aproximação de canais via cadeia de reticulados algébricos encaixados por meio da estratégia compute-and-forward em canais que envolvam codificação em redes sem fio. A técnica faz uso de partições de cadeias de reticulados definidos sobre o anel de inteiros $\mathbb{Z}[\zeta_3]$ proveniente de corpos ciclotômicos $\mathbb{Q}(\zeta_{3^s})$ com $s \geq 2$, onde ζ_3 e ζ_{3^s} denotam as raízes terceira e a 3^s -ésima da unidade, respectivamente.

Palavras-chave. Anéis de Inteiros, Reticulados Algébricos, Corpos de Números, Aproximação de Canal, Técnica Compute and Forward.

1 Introdução

Os modelos de canais utilizados em transmissão de informação em uma rede sem fio, tem como característica principal que qualquer receptor captura além do sinal transmitido a partir de seu transmissor designado, também sinais provenientes de outros transmissores (interferência). Diversos algoritmos e protocolos foram desenvolvidos na literatura para contornar problemas desta natureza. Dentre estes, destaca-se a estratégia denominada de calcule e transmite (do inglês compute-and-forward) que tira proveito da interferência para obter altos ganhos de taxas entre os transmissores em uma rede de comunicação sem fio [2].

¹edson@mat.feis.unesp.br

²azucenaduarte23@gmail.com

³macosta13@gmail.com

⁴jozue@sjbv.unesp.br

A construção e procura destes protocolos é uma área ativa de pesquisa dentro da temática de transmissão de informação em redes sem fio.

Os relés (dispositivos intermediários utilizados em uma rede de comunicação) indexados por $m = 1, 2, \dots, M$, analisa as combinações ruidosas dos sinais transmitidos por meio do canal

$$y_m = \sum_{l=1}^L h_{ml}x_l + z_m, \quad (1)$$

onde y_m e x_m denotam os sinais recebido e transmitido, respectivamente. Já h_{ml} e z_m denotam os coeficientes do canal e do ruído, respectivamente.

Em [2] os autores mostraram que ao aplicarmos uma transformação unitária U no vetor y_m da Equação (1), recebemos o vetor $\bar{y}_m = Uy_m = \sum_{l=1}^L a_{ml}Ut_l + Uz_{eq,m}$, onde $z_{eq,m}$ é um ruído Gaussiano que é circular complexo. No equivalente modelo de canal virtual considerado, cada relé analisa os pontos reticulados por meio de combinações lineares sobre o anel de inteiros $\mathbb{Z}[\zeta_3]$.

Neste contexto, a expressão $\sum a_{ml}t_l$ pode ser vista sob a ação de um ruído efetivo $z_{eq,m}$. Assim, consideraremos os vetores da forma $a_{ml}Ut_l$, $h = a_{ml}$ é o coeficiente do canal e Ut_l é matriz geradora de um reticulado. Assim, esta codificação será realizada via códigos reticulados N -dimensionais [5], isto é, reticulados obtidos por meio de mergulhos de códigos lineares em $\mathbb{R}^N$ ou $\mathbb{C}^N$. As regiões fundamentais destes códigos reticulados complexos Λ , do ponto de vista geométrico apresenta um formato cúbico. Estes reticulados são isomorfos a $\omega\mathbb{Z}[i]^N$ para algum $\omega \in \mathbb{Z}[i]$ ou a $\omega'\mathbb{Z}[\zeta_3]^N$ para algum $\omega' \in \mathbb{Z}[\zeta_3]$. Também são ditos versões escalonadas de $\mathbb{Z}[i]^N$ e de $\mathbb{Z}[\zeta_3]^N$.

Nesta codificação faremos uso de cadeias de reticulados algébricos encaixadas que sejam versões escalonadas $\mathbb{Z}[\zeta_3]^N$ que construiremos a partir de famílias de corpos ciclotômicos $\mathbb{Q}(\zeta_{3^s})$. Dentre as contribuições deste trabalho destaca-se a geração de um pré-codificador para canais desta natureza, possibilitando desta forma que a codificação seja realizada via matrizes derivadas de reticulados algébricos e uma técnica de construção da cadeia de reticulados encaixadas será baseada na ação dos homomorfismos do grupo de Galois $G = \text{Gal}(\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_3))$ sobre os geradores dos ideais em $\mathbb{Z}[\zeta_{3^s}]$ de norma relativa 3^k para todo $k \in \{0, 1, \dots, N-1\}$.

O trabalho também traz como inovação dentro desta linha de pesquisa compute and forward de como as cadeias de reticulados algébricos encaixados são usados em aplicações de como calcular a soma ponderada de sinais e como encaminha-lá.

A partir da raiz 3^s -ésima da unidade ζ_{3^s} e no elemento $\gamma = 1 - \zeta_{3^s}$, tomaremos cadeias de ideais principais $\gamma^k\mathbb{Z}[\zeta_{3^s}]$ nos anéis de inteiros $\mathbb{Z}[\zeta_{3^s}]$ proveniente de corpos ciclotômicos do tipo $\mathbb{Q}(\zeta_{3^s})$. Tais ideais são $\mathbb{Z}[\zeta_{3^s}]$ -módulos gerados por bases expressas na forma $\{\gamma^k, \gamma^k\zeta, \dots, \gamma^k\zeta^{N-1}\}$, onde $k \in \{0, \dots, N-1\}$. Através do mergulho canônico de cada ideal $\gamma^k\mathbb{Z}[\zeta_{3^s}]$ em $\mathbb{C}^N$, obteremos cadeias de reticulados algébricos encaixados $\Lambda_{N-1}/\dots/\Lambda_1/\Lambda_0$, onde cada Λ_k é uma versão escalonada do reticulado complexo $\mathbb{Z}[\zeta_3]^N$, isto é, $\Lambda_k \simeq (1 - \zeta_3)^k\mathbb{Z}[\zeta_3]^N$.

O protocolo dado pela Equação (1) interpreta o sinal recebido em cada relé como sendo a soma ponderada dos sinais (dados pelos coeficientes do desvanecimento) visto como uma

soma de pontos do reticulado. Para isto se faz necessário aproximar o sinal recebido por um ponto do reticulado. A construção acima é usada neste contexto. Em particular, o mergulho canônico γ^k é utilizado para realizar tal aproximação.

O trabalho está organizado da seguinte forma. Na seção 2 é apresentado a teoria básica de corpos de números, inteiros algébricos, reticulados algébricos e é proposta uma construção de cadeia de reticulados algébricos encaixados a partir de família de corpos de números $\mathbb{Q}(\zeta_3^N)$. Na seção 3 são construídos pré-codificadores para aproximação de canais a partir da cadeia de reticulados algébricos proposta na seção 2. Finalmente, na seção são apresentados as conclusões do trabalho.

2 Teoria Algébrica dos Números e Reticulados Algébricos

Seja $\mathbb{Q} \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \mathbb{L}_3 \subset \dots \subset \mathbb{L}_s$ uma cadeias de corpos ciclotômicos satisfazendo a condição de que $\mathbb{L}_1 = \mathbb{Q}, \mathbb{L}_j = \mathbb{Q}(\zeta_{3^j})$ para todo $s \geq 2$. Essa cadeia também pode ser denotada por $\mathbb{L}_s/\mathbb{L}_{s-1}/\dots/\mathbb{L}_2/\mathbb{L}_1$. Cada corpo $\mathbb{L}_s$ pode ser visto como um espaço vetorial de dimensão finita sobre $\mathbb{Q}$ ou sobre corpo ciclotômico $\mathbb{L}_{s-1}$, ou seja, temos que $\mathbb{L}_s/\mathbb{L}_{s-1}$ é uma extensão finita de corpos.

Como consequência, segue-se que ζ_{3^s} é uma raiz do polinômio minimal $p_s(x) = x^3 - \zeta_{3^j}^3$. Logo, o corpo $\mathbb{L}_s$ pode ser visto como um espaço vetorial sobre $\mathbb{L}_s$ de dimensão 3 que denotamos por $[\mathbb{L}_s : \mathbb{L}_{s-1}] = 3$, onde $\mathbb{L}_s = \mathbb{L}_{s-1}(\zeta_3)$. Na cadeia de $\mathbb{L}_s/\mathbb{L}_{s-1}/\dots/\mathbb{L}_2/\mathbb{L}_1$ são verificadas as seguintes relações:

1. $\{1, \zeta_{3^j}, \zeta_{3^j}^2\}$ é uma base de $\mathbb{L}_s$ sobre $\mathbb{L}_{s-1}$ tendo ζ_{3^s} como raiz do polinômio minimal $p_s(x) = x^3 - \zeta_{3^j}^3 = (x - \zeta_{3^j})(x - \zeta_{3^j}\zeta_3)(x - \zeta_{3^j}\zeta_3^2)$ e com o grupo de Galois $Gal(\mathbb{L}_s/\mathbb{L}_{s-1}) = \{\sigma_0, \sigma_s, \sigma_s^2\}$ associado a extensão $\mathbb{L}_s/\mathbb{L}_{s-1}$, onde $\sigma_s^3 = \sigma_0, \sigma_s(\zeta_{3^s}) = \zeta_3\zeta_{3^s}$ e σ_0 denota o homomorfismo identidade. [3]
2. $\{1, \zeta_{3^s}, \dots, \zeta_{3^s}^{N-1}\}$ é uma base de $\mathbb{L}_s$ sobre $\mathbb{K}$ tendo ζ_{3^s} como raiz do polinômio minimal $\mu_{\zeta_{3^s}}(x) = \prod_{k=0}^{N-1} (x - \zeta_{3^s}^k)$. As raízes de $\mu_{\zeta_{3^s}}(x)$ e com o grupo de Galois associado a extensão de corpos $\mathbb{L}/\mathbb{K}$ é dado por $Gal(\mathbb{L}/\mathbb{K}) = \{\sigma_j : \sigma_j(\zeta_{3^s}) = \zeta_{3^s}^j, \forall j = 0, 1, \dots, N-1\}$, onde $N = 3^{s-1}$ se $\mathbb{K} = \mathbb{Q}$ e $N = 3^{s-2}$ se $\mathbb{K} = \mathbb{Q}(\zeta_3)$. [3]
3. O conjunto dos elementos de $\mathbb{L}$ que são inteiros sobre $\mathbb{Z}$ formam um $\mathbb{Z}$ -módulo, isto é, os elementos gerados pelos elementos de $\mathbb{L}$ dados por $\{1, \zeta_{3^s}, \zeta_{3^s}^2, \dots, \zeta_{3^s}^{3^{s-1}-1}\}$ denotado por $\mathcal{O}_{\mathbb{L}}$ ou $\mathbb{Z}[\zeta_{3^s}]$, chamado de anel de inteiros de $\mathbb{L}$. Convém, ressaltar que $\mathcal{O}_{\mathbb{L}}$ também pode ser visto como um $\mathbb{Z}[\zeta_3]$ -módulo com os elementos por $\{1, \zeta_{3^s}, \zeta_{3^s}^2, \dots, \zeta_{3^s}^{3^{s-2}-1}\}$ que é justamente o caso de interesse neste trabalho.

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

Consideremos o mergulho dado por

$$\sigma : \mathbb{L} \Rightarrow \mathbb{C}^N, \text{ com } \sigma(x) = (\sigma_0(x), \dots, \sigma_{N-1}(x)), \quad (2)$$

onde $\sigma_i \in \text{Gal}(\mathbb{L}/\mathbb{Q}(\zeta_3))$, $\forall i \in \{0, \dots, N-1\}$.

Através deste mergulho canônico do corpo ciclotômico de $\mathbb{L} = \mathbb{Q}(\zeta_{3^s})$ em $\mathbb{C}^N$, construiremos cadeias de reticulados algébricos encaixados Λ_k em $\mathbb{C}^N$ associados aos ideais $\gamma^k \mathbb{Z}[\zeta_{3^s}]$ gerados por $\mathbb{Z}[\zeta_{3^s}]$ bases da forma $\{\gamma^k, \gamma^k \zeta_{3^s}, \dots, \gamma^k \zeta_{3^s}^{N-1}\}$, $\forall k \in \{0, \dots, N-1\}$. A matriz geradora de cada reticulado Λ_k é descrita na forma:

$$M_k = \begin{pmatrix} \sigma_0(\gamma^k) & \sigma_0(\gamma^k \zeta_{3^s}) & \cdots & \sigma_0(\gamma^k \zeta_{3^s}^{N-1}) \\ \sigma_1(\gamma^k) & \sigma_1(\gamma^k \zeta_{3^s}) & \cdots & \sigma_1(\gamma^k \zeta_{3^s}^{N-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{N-1}(\gamma^k) & \sigma_{N-1}(\gamma^k \zeta_{3^s}) & \cdots & \sigma_{N-1}(\gamma^k \zeta_{3^s}^{N-1}) \end{pmatrix}. \quad (3)$$

Por outro lado, a matriz M_k pode ser reescrita na forma $M_k = B_k M_0$, onde,

$$B_k M_0 = \begin{pmatrix} \gamma^k & 0 & \cdots & 0 \\ 0 & \sigma_1(\gamma^k) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_{N-1}(\gamma^k) \end{pmatrix} \cdot \begin{pmatrix} 1 & \zeta_{3^s} & \cdots & \zeta_{3^s}^{N-1} \\ 1 & \sigma_1(\zeta_{3^s}) & \cdots & \sigma_1(\zeta_{3^s}^{N-1}) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_{N-1}(\zeta_{3^s}) & \cdots & \sigma_{N-1}(\zeta_{3^s}^{N-1}) \end{pmatrix}. \quad (4)$$

Por simplicidade de notação, denotaremos B_k na forma $B_k = \text{diag}(\gamma^k, \sigma(\gamma^k), \dots, \gamma^{N-1}(\gamma^k))$.

Por outro lado, há uma outra matriz associado a cada reticulado algébrico Λ_k que chamaremos de matriz Gram e dada por $G_k = M_k \overline{M}_k^t$, onde $\overline{M}^t$ denota a matriz transposta conjugada da matriz M . A notação $\bar{a}$ denota o conjugado complexo do elemento $a = a_1 + a_2 \zeta_3 \in \mathbb{Z}[\zeta_3]$ dada por $\bar{a} = a_1 + a_2 \zeta_3^2$. Sem muita dificuldade, mostra-se que a matriz Gram do reticulado Λ_k é escrita na forma $G_k = M \cdot B_k \overline{M B_k}$.

Seja Λ' um subreticulado de Λ . Sejam M e M' as matrizes geradoras dos reticulados Λ e Λ' , respectivamente. Assim, Λ' pode ser expresso por $\Lambda' = \{x = UM\lambda \mid \lambda \in \mathbb{Z}[\zeta_3]^N\}$, para matriz complexa U de posto N . Logo, o cálculo do índice da partição Λ_0/Λ' é dado por $|\Lambda_0/\Lambda'| = |\det(U)|$.

2.1 Construção de cadeia de reticulados algébricos encaixados dados por versões escalonadas de $\mathbb{Z}[\zeta_3]^N$

Dizemos que uma cadeia de reticulados $\Lambda_{N-1}, \dots, \Lambda_1$ está encaixado no reticulado Λ se $\Lambda_{N-1} \subseteq \Lambda_{N-2} \subseteq \dots \subseteq \Lambda_1 \subset \Lambda$. Faremos uso da teoria algébrica dos números para construir explicitamente cadeias de reticulados encaixados para serem utilizados em problemas voltados para aproximação de canais.

Proposição 2.1. *A norma relativa $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_3)}(1 - \zeta_{3^s}) = 1 - \zeta_3$, para todo $s > 1$.*

Demonstração: Se $s = 2$, assim $N_{\mathbb{Q}(\zeta_{3^2})/\mathbb{Q}(\zeta_3)}(1 - \zeta_{3^2}) = (1 - \zeta_{3^2})(1 - \zeta_{3^2} \zeta_3)(1 - \zeta_{3^2} \zeta_3^2) = 1 - \zeta_{3^2}^3 = 1 - \zeta_3$. Por indução, supomos que $N_{\mathbb{Q}(\zeta_{3^{s-1}})/\mathbb{Q}(\zeta_3)}(1 - \zeta_{3^{s-1}}) = 1 - \zeta_3$. Agora, desde que $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_{3^{s-1}})}(1 - \zeta_{3^s}) = (1 - \zeta_{3^s}) \sigma_s(1 - \zeta_{3^s}) \sigma_s^2(1 - \zeta_{3^s}) = (1 - \zeta_{3^s})(1 - \zeta_{3^s} \zeta_3)(1 - \zeta_{3^s} \zeta_3^2) = 1^3 - \zeta_{3^s}^3$, segue-se que $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_{3^{s-1}})}(1 - \zeta_{3^s}) = 1 - \zeta_{3^{s-1}}$.

Então, $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_3)}(1 - \zeta_{3^s}) = (1 - \zeta_{3^s})(1 - \zeta_{3^s} \zeta_3)(1 - \zeta_{3^s} \zeta_3^2) = 1^3 - \zeta_{3^s}^3 = 1 - \zeta_{3^{s-1}}$. Portanto, $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_3)}(1 - \zeta_{3^s}) = 1 - \zeta_3$.

Proposição 2.2. *O ideal $\mathfrak{S} = (1 - \zeta_{3^s})\mathbb{Z}[\zeta_{3^s}]$ é um ideal primo no anel de inteiros $\mathbb{Z}[\zeta_{3^s}]$ e $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}}(1 - \zeta_{3^s}) = 3$, para todo $s \geq 1$.*

Demonstração: Para $s = 1$, temos que $N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(1 - \zeta_3) = (1 - \zeta_3)\sigma(1 - \zeta_3) = (1 - \zeta_3)(1 - \zeta_3^2) = 3$, segue-se então que $\mathfrak{S} = (1 - \zeta_3)\mathbb{Z}[\zeta_3]$ é um ideal primo no anel de inteiros $\mathbb{Z}[\zeta_3]$. Por indução, supomos que $N_{\mathbb{Q}(\zeta_{3^{s-1}})/\mathbb{Q}}(1 - \zeta_{3^{s-1}}) = 3$. Agora, desde que

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

segue então que $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}}(1 - \zeta_{3^s}) = N_{\mathbb{Q}(\zeta_{3^{s-1}})/\mathbb{Q}}(1 - \zeta_{3^{s-1}}) = 3$. Portanto, $\mathfrak{S} = (1 - \zeta_{3^s})\mathbb{Z}[\zeta_{3^s}]$ é um ideal primo em $\mathbb{Z}[\zeta_{3^s}]$.

Proposição 2.3. *O índice da partição do reticulado Λ_0 sobre o subreticulado Λ_k é dado por $\Lambda_0/\Lambda_k = 3^k$, para todo $k = 0, 1, \dots, N - 1$.*

Demonstração: A matriz geradora M_k de Λ_k é dado por $M_k = MU^k$, onde M é a matriz geradora do reticulado algébrico Λ_0 . Assim, $U^k = \text{dig}(\sigma_0(\gamma^k), \dots, \sigma_{N-1}(\gamma^k))$. Portanto, $|\Lambda_0/\Lambda_k| = |\det(U^k)| = |(\prod_{i=0}^{N-1} \sigma_i(\gamma^k))| = (N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}}(\gamma^k))^k = 3^k$.

Proposição 2.4. *O índice da partição de reticulados algébricos $\Lambda_{k-1}/\Lambda_k = 3$, para cada $k = 0, 1, \dots, N - 1$.*

Demonstração: A matriz Gram $M_k = MU^k$ de Λ_k associado ao ideal $\mathfrak{S}^k$ pode ser reescrita na forma $M_k = MU^{k-1}U$. Desde que MU^{k-1} é a matriz do reticulado Λ_{k-1} , segue-se que $|\Lambda_{k-1}/\Lambda_k| = |\det(U)| = |\prod_{i=0}^{N-1} \sigma_i(1 - \zeta_{3^s})| = N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}}(1 - \zeta_{3^s}) = 3$.

Proposição 2.5. *O reticulado algébrico Λ_k associado ao ideal $(1 - \zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]$ é isomorfo ao reticulado complexo ternário $(1 - \zeta_3)^k\mathbb{Z}[\zeta_3]^N$, para todo $k = 0, 1, \dots, N - 1$.*

Demonstração: Sejam $\gamma = 1 - \zeta_{3^s}$ e a $\{\gamma^k, \gamma^k\zeta_{3^s}, \dots, \gamma^k\zeta_{3^s}^{N-1}\}$ $\mathbb{Z}[\zeta_3]$ -base do reticulado algébrico Λ_k . Se M_k é a matriz geradora associado ao reticulado Λ_k , então

$$G_k = M_k \overline{M_k^t} = \begin{pmatrix} \sum_{i=0}^{N-1} \sigma_i(\gamma^k) \overline{\sigma_i(\gamma^k)} & \cdots & \sum_{i=1}^N \sigma_i(\alpha^k) \overline{\sigma_i(\gamma^k \zeta_{3^s}^{N-1})} \\ \vdots & \ddots & \vdots \\ \sum_{i=0}^{N-1} \sigma_i(\gamma^k) \overline{\sigma_i(\gamma^k)} & \cdots & \sum_{i=1}^N \sigma_i(\gamma^k) \overline{\sigma_i(\gamma^k \zeta_{3^s}^{N-1})} \end{pmatrix}, \quad (5)$$

onde G_k a matriz Gram do reticulado algébrico Λ_k . Sendo o corpo de números $\mathbb{Q}(\zeta_{3^s})$ um CM-field, segue-se que G_k pode ser reescrita na forma

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

onde M é a matriz geradora do reticulado $\Lambda_0 \cong \mathbb{Z}[\zeta_3]^N$. Pela Proposição 2.1 e pelas propriedades de norma relativa, segue-se que $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}}(\gamma^k) = (1 - \zeta_3)^k$ e $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}}(\overline{\gamma^k}) = \overline{(1 - \zeta_3)^k}$. Assim, $G_k = M_k \overline{M_k^t} = (1 - \zeta_3)^k M (1 - \zeta_3)^k \overline{M^t}$. Portanto, $(1 - \zeta_3)^k M$ é a matriz Gram do reticulado ternário complexo $(1 - \zeta_3)^k \mathbb{Z}[\zeta_3]^N$, para cada $k = 0, 1, \dots, N - 1$.

Observação 2.1. Para obtermos um reticulado algébrico dado por uma transformação unitária a partir do reticulado Λ_k dado pela Proposição 3.1, basta tomarmos o volume fundamental de Λ_k normalizado (divido) pela constante $\nu = \text{vol}(\Lambda_k)/(1 - \zeta_3)^N$ [1].

3 Construção de Pré-Codificadores para Aproximação de Canais a Partir de Reticulados Algébricos

Como vimos na subseção 2.1, a construção dos reticulados algébricos encaixados associados a cadeias de ideais principais $\gamma^k \mathbb{Z}[\zeta_{3^s}]$ está intimamente relacionados com as potências do elemento γ que são os geradores destes ideais. Por outro lado, pela Teoria Algébrica dos Números, sabemos que todos os possíveis geradores de $\gamma^k \mathbb{Z}[\zeta_{3^s}]$ são da forma $\zeta_{3^s}^{k_1} (1 - \zeta_{3^s}^{k_2}) \alpha$, onde $\alpha \in \mathbb{Z}[\zeta_{3^s}]$ com $k_1, k_2 \in \{0, 1, \dots, N-1\}$. Ao analisarmos os elementos da forma $\zeta_{3^s}^{k_1} (1 - \zeta_{3^s}^{k_2})$ há N^2 possibilidades para estes valores.

Desde que sejam conhecidos k_1 e k_2 , temos $2(N-2)$ bits, isto é, $(N-2)$ bits para k_1 e $(N-2)$ bits para k_2 .

No sentido, de realizar a pré-codificação, consideraremos as próximas proposições:

Proposição 3.1. *Seja G o grupo de Galois associado a extensão de corpos $\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_3)$ dada por $G = \text{Gal}(\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_3)) = \{\sigma_j : \sigma_j(\zeta_{3^s}) = \zeta_{3^s}^j, \forall j = 0, 1, \dots, N-1\}$, Então: a ação dos homomorfismo de G em $\gamma \in \mathbb{Z}[\zeta_{3^s}]$ é dada por $\sigma_j(\alpha \zeta_{3^s}^{k_1} (1 - \zeta_{3^s}^{k_2})) = \alpha (\zeta_{3^s}^j)^{k_1} (1 - (\zeta_{3^s}^j)^{k_2})$ para todo $\alpha \in \mathbb{Z}[\zeta_3], \gamma \in \mathbb{Z}[\zeta_{3^s}]$ e para todo $k_1, k_2 \in \{0, 1, \dots, N-1\}$.*

Demonstração: Primeiro, observemos que $\sigma_j(\zeta_{3^s}) = \zeta_{3^s}^j$. Ao considerarmos $(1 - \zeta_{3^s})^k = \sum_{j=0}^k \binom{k}{j} 1^{k-j} (-\zeta_{3^s})^j$, temos $\sigma_j(1 - \zeta_{3^s})^k = \sigma_j(\sum_{j=0}^k \binom{k}{j} 1^{k-j} (-\zeta_{3^s})^j) = (1 - \zeta_{3^s}^j)^k$. Assim, $\sigma_j(\alpha \zeta_{3^s}^{k_1} (1 - \zeta_{3^s}^{k_2})) = \alpha \sigma_j(\zeta_{3^s}^{k_1} - \zeta_{3^s}^{k_1+k_2}) = \alpha (\sigma_j(\zeta_{3^s}^{k_1}) - \sigma_j(\zeta_{3^s}^{k_1+k_2})) = \alpha (\zeta_{3^s}^j)^{k_1} - (\zeta_{3^s}^j)^{k_1+k_2} = \alpha ((\zeta_{3^s}^j)^{k_1} (1 - (\zeta_{3^s}^j)^{k_2}))$.

A partir da Proposição 3.1, aproximaremos os canais dados pela Equação (1) dada por uma matriz H de ordem N , por cadeias matrizes B_k dadas pela Equação (5) derivadas de cadeias de reticulados encaixados isomorfos $\zeta_{3^s}^{k_1} (1 - \zeta_{3^s}^{k_2}) \mathbb{Z}[\zeta_{3^s}]$.

Para isto é necessário realizar uma pré-codificação, para cada coeficiente h na posição i da diagonal de H , temos que matriz diagonal dada pela j -linha e j -coluna por uma constante por $\beta = \frac{(\zeta_{3^s}^j)^{k_1} (1 - \zeta_{3^s}^j)^{k_2}}{\zeta_{3^s}^{k_1} (1 - \zeta_{3^s})^{k_2}} = \sigma_j(\gamma)$.

Assim, obtemos

$$\begin{pmatrix} h\beta_1 & 0 & \cdots & 0 \\ 0 & h\beta_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h\beta_{N-1} \end{pmatrix} \rightarrow \begin{pmatrix} \sigma_0(\gamma^{k_2}) & 0 & \cdots & 0 \\ 0 & \sigma_1(\gamma^{k_2}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_{N-1}(\gamma^{k_2}) \end{pmatrix} = B_{k_2} \quad (6)$$

onde B_{k_2} é a matriz dada pela Equação (5). Seja $h \in \mathbb{Z}[\zeta_3]$. A partir da metodologia descrita neste trabalho, o natural é considerar a aproximação $|h| \rightarrow |1 - \zeta_{3^s}|^{k_2}$, onde $k_2 \in \mathbb{Z}$, ou melhor, encontrar um apropriado k_2 tal que $\frac{\log h}{\log |1 - \zeta_{3^s}|} \rightarrow \mathbb{Z}$.

4 Conclusões

Propomos uma novo método para aproximar os coeficientes de um canal a partir de cadeias de partições de reticulados sobre $\mathbb{Z}[\zeta_3]$. O trabalho também traz como inovação dentro desta linha de pesquisa compute and forward de como as cadeias de reticulados algébricos encaixados são usados em aplicações de como calcular a soma ponderada de sinais e como encaminha-lá.

Agradecimentos

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

Referências

- [1] F. Oggier; *Algebraic methods for channel coding*, Phd dissertation École Polytechnique Fédérale de Lausanne, Lausanne, 2005.
- [2] N. E. Tunali; K. R. Narayanan; J. J. Boutros and Y.C. Huang, *Lattices over Eisenstein integer for compute-and-forward*, Fiftieth Annual Conference Allerton House, UIUC, Illinois, USA, October 1-5, 2012, pp. 33-40.
- [3] L. Washington, *Introduction to cyclotomic fields*. Springer-Verlag, New-York (1982).
- [4] I. N. Stewart, D. O. Tall, *Algebraic number Theory*, Chapman and Hall (1987).
- [5] J.H. Conway and N.J.A. Sloane; *Sphere packings, lattices and groups*, Springer-Verlag, New York, 1988.