Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, v. 6, n. 1, 2018.

Trabalho apresentado no XXXVII CNMAC, S.J. dos Campos - SP, 2017.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Novas construções de códigos reticulados encaixados via corpos ciclotômicos

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.do Rio de Preto, SP

Resumo. Neste trabalho, faremos uso de cadeia de reticulados ideais complexos encaixados provenientes de famílias de corpos ciclotômicos $\mathbb{Q}(\zeta_{3^s})$ que são extensões finitas de $\mathbb{Q}(\zeta_3)$ de grau $N = 3^{s-2}$. A partir deste reticulados, obtemos novas classes de códigos reticulados encaixadas que correspondam a cadeia de códigos ternários encaixados no anel de polinômios finito $\mathbb{F}_3[x]/(x^N - 1)$ por meio da técnica conhecida por Construção A.

Palavras-chave. Códigos Reticulados, Códigos Lineares, Corpos de Números

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 $\mathbb{C}^N$.

Dado um espaço vetorial $\mathbb{F}_3^N$ de dimensão N definido sobre o corpo finito $\mathbb{F}_3$, podemos obter uma cadeia de códigos ternários encaixados

$$\mathcal{C}_N/\mathcal{C}_{N-1}/\cdots/\mathcal{C}_2/\mathcal{C}_1,$$

onde cada código $\mathcal{C}_r$ é um subespaço vetorial em $\mathbb{F}_3^N$ de dimensão r com parâmetros (N, r), onde $r = N - k$ satisfazendo $1 \leq r \leq N$.

A partir desta cadeia de códigos encaixados, Forney [2] propôs uma maneira prática de codificar reticulados complexos encaixados em $\mathbb{C}^N$ por meio da *Construção A*, onde cada código reticulado associado a $\mathcal{C}_r$ em $\mathbb{C}^N$, é obtido via as classes de resíduos de $\mathbb{Z}[\zeta_3]$ módulo $(1 - \zeta_3)^k\mathbb{Z}[\zeta_3]$ em cada uma das N coordenadas. Do ponto de vista da teoria de anéis de polinômios finitos, estes códigos ternários encaixados são dados por ideais encaixados em $\mathbb{F}_3[x]/(x^N - 1)$.

Códigos reticulados de Eisenstein formam uma classe de reticulados complexos, do ponto vista geométrico, as regiões fundamentais destes reticulados apresentam formato cúbico no espaço complexo de dimensão N. O que é equivalente a considerar o reticulado $\mathcal{A}_2^N$ que é isomorfo a uma versão escalonada do reticulado $\mathbb{Z}[\zeta_3]^N$.

[1] edson@mat.feis.unesp.br
[2] andrade@ibilce.unesp.br

Reticulados ideais foram propostos por [3] como uma nova ferramenta algébrica para se construir versões escalonadas do reticulado $\mathbb{Z}[\zeta_3]^N$, a partir de corpos de números complexos que sejam extensões finitas dos corpos complexos $\mathbb{Q}(i)$ ou $\mathbb{Q}(\zeta_3)$.

Consideramos extensões de corpos do tipo $\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_3)$ de grau $N = 3^{s-2}$. Tomamos cadeias de ideais no anel de inteiros $\mathbb{Z}[\zeta_{3^s}]$ de $\mathbb{Q}(\zeta_{3^s})$ do tipo $\mathbb{Z}[\zeta_{3^s}]/\gamma\mathbb{Z}[\zeta_{3^s}]/\cdots/\gamma^{N-1}\mathbb{Z}[\zeta_{3^s}]$, onde $\gamma = 1 - \zeta_{3^s}$.

Cada ideal $\gamma^k\mathbb{Z}[\zeta_{3^s}]$ pode ser gerado pela $\mathbb{Z}[\zeta_3]$-base dada por $\{\gamma^k\omega_0, \ldots, \gamma^k\omega_{N-1}\}$, onde $\{\omega_0, \ldots, \omega_{N-1}\}$ denota a $\mathbb{Z}[\zeta_3]$-base do anel de inteiros $\mathbb{Z}[\zeta_{3^s}]$ visto com um $\mathbb{Z}[\zeta_3]$-módulo. Mergulhamos, esta cadeia encaixada de ideais em $\mathbb{C}^N$, obtendo uma cadeia de reticulados ideais encaixados, onde cada reticulado Λ_k tem como matriz Gram dada por $G_k = Tr_{\mathbb{L}/\mathbb{Q}(\zeta_3)}(\gamma^k\omega_i\overline{\gamma^k\omega_j})$ para cada $k \in \{0, 1, \ldots, N-1\}$. Mostramos cada reticulado ideal é isomorfo uma versão escalonada do reticulado $\gamma^k\mathbb{Z}[\zeta_3]^N$. O que possibilita a construção de classes de códigos reticulados encaixados via corpos de números $\mathbb{Q}(\zeta_{3^s})$.

2 Formulação Matemática de Problema

Consideramos uma cadeia de corpos ciclotômicos dada por $\mathbb{L}_s/\subset \ldots /\mathbb{L}_2/\mathbb{L}_1/\mathbb{Q}$, satisfazendo a condição de que $\mathbb{L}_2 = \mathbb{Q}(\zeta_3)$ e $\mathbb{L}_s = \mathbb{Q}(\zeta_{3^s})$ para todo $s \geq 2$, onde ζ_{3^s} denota a raíz 3^s-ésima da unidade.

Associado a cada extensão finita de corpos $\mathbb{L}_s/\mathbb{L}_{s-1}$, temos como consequência que do fato de que $\zeta_{3^s}^3 = \zeta_{3^{s-1}}$ e $L_s = L_{s-1}(\zeta_{3^s})$, que o polinômio minimal $p_j(x)$ de ζ_{3^j} sobre $\mathbb{L}_{j-1}$ é dado por $p(x) = x^3 - \zeta_{3^j}^3 = (x-\zeta_{3^j})(x-\zeta_{3^j}\zeta_3)(x-\zeta_{3^j}\zeta_3^2)$ e $\{1, \zeta_{3^j}, \zeta_{3^j}^2\}$ é uma base de $\mathbb{L}_j$ sobre $\mathbb{L}_{j-1}$, para $j = 2, 3, \cdots, s$. O grupo de Galois é dado por $Gal(\mathbb{L}_j : \mathbb{L}_{j-1}) =< \sigma_j >= \{id, \sigma_j, \sigma_j^2, \}$, onde $\sigma_j^3 = id$, id é a identidade e σ_j é determinado por $\sigma_j(\zeta_{3^j}) = \zeta_3\zeta_{3^j}$. Assim, $[\mathbb{L}_j : \mathbb{Q}(\zeta_3)] = 3^{j-2}$, $\mathbb{L}_s = \mathbb{Q}(\zeta_3)(\zeta_{3^s})$ e $\{1, \zeta_{3^s}, \zeta_{3^s}^2, \cdots, \zeta_{3^s}^{3^{s-2}-1}\}$ é uma base de $\mathbb{L}_s$ sobre $\mathbb{Q}(\zeta_3)$. O polinômio minimal $\mu(x)$ de ζ_{3^s} sobre $\mathbb{Q}(\zeta_3)$ têm grau 3^{s-2} e é dado por $\mu(x) = x^N - \zeta_3 = \prod_{k=0}^{N-1}\mu_k$, onde $\mu_k = x - \zeta_{3^s}^k$ e $N = 3^{s-2}$. As raízes complexas de $\mu_{\zeta_{3^s}}(x)$ define 3^{s-2} distintos $\mathbb{Q}(\zeta_3)$-homomorphisms, isto é, $\sigma_0(\zeta_{3^s}) = \zeta_{3^s}, \sigma_1(\zeta_{3^s}) = \zeta_{3^s}^2, \cdots, \sigma_{3^{s-2}-1}(\zeta_{3^s}) = \zeta_{3^s}^{3^{s-2}}$. Os 3^{s-2} distintos $\mathbb{Q}(\zeta_3)$-homomorphisms de corpos σ_j podem serem reescritos na forma $\sigma_j(\zeta_{3^s}) = \zeta_{3^s}\zeta_{3^s}^j$, para todo $j = 0, 1, \cdots, 3^{s-2} - 1$.

Seja $\mathbb{L}$ uma extensão de corpos de grau $N = 3^{s-2}$ sobre $\mathbb{Q}(\zeta_3)$. A partir do corpo de números $\mathbb{L}$, podemos obter um reticulado complexo dado por $\Lambda = \{x = \lambda M : \lambda \in \mathbb{Z}[\zeta_3]^N\}$, onde $M \in M_N(\mathbb{C})$ é a matriz geradora do reticulado.

Proposição 2.1. *[3] Seja $\Im$ o ideal dado pelo anel de inteiros $\mathcal{O}_\mathbb{L}$. Um reticulado ideal complexo Λ definido sobre $\mathbb{Z}[\zeta_3]$, tem matriz geradora $G = T_{\mathbb{L}/\mathbb{Q}(\zeta_3)}(\omega_i\overline{\omega_j})$, onde ω_i e ω_j pertence a $\mathbb{Z}[\zeta_3]$-base $\{\omega_0, \ldots, \omega_{N-1}\}$ do anel de inteiros $\mathbb{Z}[\zeta_{3^s}]$ visto com um $\mathbb{Z}[\zeta_3]$-módulo. A notação $\overline{a} = \overline{a_1 + a_2\zeta_3} = a_1 + a_2\zeta_3^2$ denota a conjugação complexa em $\mathbb{Z}[\zeta_3]$.*

A matriz

$$G = M\overline{M}^t = \begin{pmatrix} \sum_{i=0}^{N-1}\sigma_i(\omega_0)\overline{\sigma_i(\omega_0)} & \cdots & \sum_{i=0}^{N-1}\sigma_i(\omega_0)\overline{\sigma_i(\omega_{N-1})} \\ \vdots & \ddots & \vdots \\ \sum_{i=0}^{N-1}\sigma_i(\omega_{N-1})\overline{\sigma_i(\omega_0)} & \cdots & \sum_{i=0}^{N-1}\sigma_i(\omega_{N-1})\overline{\sigma_i(\omega_{N-1})} \end{pmatrix}, \qquad (1)$$

é chamada de matriz Gram do reticulado ideal.

Como consequência da proposição, obtemos a seguinte observação.

Observação 2.1. *Seja* $\{\gamma^k w_0, w_1, \cdots, \gamma^k w_{N-1}\}$ *uma* $\mathbb{Z}[\zeta_3]$*-base do ideal* $\gamma^k \mathcal{O}_{\mathbb{L}}$*. A matriz Gram* G_k *associado ao reticulado ideal* Λ_k *é dado por* $G =_k (T_{\mathbb{L}/\mathbb{Q}(\zeta_3)}(\gamma^k w_j \overline{\gamma^k}\overline{w_j}))_{j=0}^{N-1}$*, que pode ser reescrita como um produto de matrizes da forma* $MU\overline{U}^t\overline{M}^t$ *e*

$U = dig(\sigma_0(\gamma^k), \cdots, \sigma_{N-1}(\gamma^k))$.

3 Resultados

Nesta seção, construímos cadeias de códigos reticulados encaixados a partir da extensão de corpos $\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_3)$ de grau $N = 3^{s-2}$.

3.1 Versões escalonadas de reticulados $\mathbb{Z}[\zeta_3]^N$

Nesta subseção, construímos reticulados complexos encaixados a partir de uma cadeia de ideais encaixados, onde cada reticulado complexo seja uma versão escalonada do reticulado $\mathbb{Z}[\zeta_3]^N$. Neste sentido, consideramos a Proposição 3.1.

Proposição 3.1. $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_3)}(1-\zeta_{3^s}) = 1-\zeta_3$*, para todo* $s > 1$.

Demonstração. Note que para $s = 2$, tem-se que $N_{\mathbb{Q}(\zeta_{3^2})/\mathbb{Q}(\zeta_3)}(1-\zeta_{3^2}) = (1-\zeta_{3^2})(1-\zeta_{3^2}\zeta_3)(1-\zeta_{3^2}\zeta_3^2) = 1-\zeta_{3^2}^3 = 1-\zeta_3$. Suponhamos, por indução sobre $s-1$, que $N_{\mathbb{Q}(\zeta_{3^{s-1}})/\mathbb{Q}(\zeta_3)}(1-\zeta_{3^{s-1}}) = 1-\zeta_3$. Assim, $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(3^{s-1})}(1-\zeta_{3^s}) = (1-\zeta_{3^s})(1-\zeta_{3^s}\zeta_3)(1-\zeta_{3^s}\zeta_3^2) = 1^3-\zeta_{3^s}^3 = 1-\zeta_{3^{s-1}}$. Pela propriedade transitiva da norma relativa, segue que $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_3)}(1-\zeta_{3^s}) = 1-\zeta_3$.

□

Seja $\Lambda = \Lambda_0$. Nosso objetivo é de mostrar como é dado o reticulado complexo Λ_k a partir de uma partição de reticulados dada por $\Lambda_0/\Lambda_1/\cdots/\Lambda_{N-2}/\Lambda_{N-1}$, Nesta direção, consideramos a matriz geradora M do reticulado complexo Λ_0 de posto completo N. Assim, Λ pode ser expresso por $\Lambda_0 = \{x = M\lambda | \lambda \in \mathbb{Z}[\zeta_3]^N\}$ e o subreticulado Λ' de Λ pode ser escrito na forma $\Lambda' = \{x = UM\lambda | \lambda \in \mathbb{Z}[\zeta_3]^N\}$, para alguma matriz complexa U de posto N.

Seja $\{1, \zeta_{3^s}, \ldots, \zeta_{3^s}\}$ a $\mathbb{Z}[\zeta_3]$-base do anel de inteiros $\mathbb{Z}[\zeta_{3^s}]$ vista como um módulo sobre $\mathbb{Z}[\zeta_3]$. Consideramos o elemento $\gamma = 1-\zeta_{3^s}$ de $\mathbb{Z}[\zeta_{3^s}]$ com norma relativa dada por $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_3)}(\gamma) = 1-\zeta_3$. Para cada $k = 0, 1, \cdots, N-1$, tomamos α^k. Assim, a matriz Gram matrix G_k do reticulado ideal Λ_k associada ao ideal $\gamma^k\mathbb{Z}[\zeta_{3^s}]$ e dada por $G_k = M_k\overline{M_k}^t$, onde M_k é a matriz geradora de Λ_k é dada por

$$M_k = \begin{pmatrix} \gamma^k & \gamma^k\zeta_{3^s} & \cdots & \gamma^k\zeta_{3^s}^{N-1} \\ \sigma_2(\gamma^k) & \sigma_2(\gamma^k\zeta_{3^s}) & \cdots & \sigma_2(\gamma^k\zeta_{3^s}^{N-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\gamma^k) & \sigma_n(\gamma^k\zeta_{3^s}) & \cdots & \sigma_n(\gamma^k\zeta_{3^s}^{N-1}) \end{pmatrix}.$$

DOI: 10.5540/03.2018.006.01.0403

A matriz geradora G_k pode ser reescrita na forma $G_k = MU^k\overline{M}^t\overline{U^k}^t$, onde M denota a matriz generadora associada ao reticulado ideal $\Lambda \cong \mathbb{Z}[\zeta_3]^N$ e $U^k = dig(\sigma_0((1-\zeta_{3^s})^k), \cdots, \sigma_{N-1}((1-\zeta_{3^s})^k))$.

Proposição 3.2. *O reticulado ideal Λ_k associado ao ideal $(1-\zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]$ é isomorfo ao reticulado ternário complexo $(1-\zeta_3)^k\mathbb{Z}[\zeta_3]^N$, para $k = 0, 1, \cdots, N-1$.*

Demonstração. Sejam $\alpha = 1-\zeta_{3^s}$ e $\{\alpha^k, \alpha^k\zeta_{3^s}, \cdots, \alpha^k\zeta_{3^s}^{N-1}\}$ uma base sobre $\mathbb{Z}[\zeta_3]$ do reticulado ideal Λ_k. Se M_k é a matriz geradora associada a Λ_k, então

$$G_k = M_k\overline{M_k^t} = \begin{pmatrix} \sum_{i=0}^{N-1}\sigma_i(\alpha^k)\overline{\sigma_i(\alpha^k)} & \cdots & \sum_{i=1}^{N}\sigma_i(\alpha^k)\overline{\sigma_i(\alpha^k\zeta_{3^s}^{N-1})} \\ \vdots & \ddots & \vdots \\ \sum_{i=0}^{N-1}\sigma_i(\alpha^k)\overline{\sigma_i(\alpha^k)} & \cdots & \sum_{i=1}^{N}\sigma_i(\alpha^k)\overline{\sigma_i(\alpha^k\zeta_{3^s}^{N-1})} \end{pmatrix}, \tag{2}$$

onde G_k é a matriz Gram matrix do reticulado ideal Λ_k. Note que G_k pode ser reescrita na forma $G_k = M_k\overline{M_k}^t = \sum_{i=0}^{N-1}\sigma_i(\alpha^k)M\sum_{i=0}^{N-1}\overline{\sigma_i(\alpha^k)}\overline{M}^t = \sum_{i=0}^{N-1}\sigma_i(\alpha^k)\sum_{i=0}^{N-1}\overline{\sigma_i(\alpha^k)}M\overline{M}^t$, onde M é a matriz geradora do reticulado $\Lambda_0 \cong \mathbb{Z}[\zeta_3]^N$. Pelas propriedades de norma relativa, segue-se que $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_3)}(\alpha^k) = (1-\zeta_3)^k$ e $N_{\mathbb{Q}(\zeta_{3^s})/\mathbb{Q}(\zeta_3)}(\overline{\alpha^k}) = \overline{(1-\zeta_3)}^k$. Assim, $G_k = M_k\overline{M_k}^t = (1-\zeta_3)^k\overline{(1-\zeta_3)}^kM\overline{M}^t$. Então, $(1-\zeta_3)^kM$ é a matriz Gram do reticulado complexo $(1-\zeta_3)^k\mathbb{Z}[\zeta_3]^N$, para cada $k = 0, 1, \cdots, N-1$. □

3.2 Códigos Reticulados

Nesta seção, por meio de códigos lineares definidos sobre anéis de polinômios finito $\mathbb{F}_3[x]/(x^N-1)$ e da Construção A vamos obter códigos reticulados complexos que sejam versões escalonadas do reticulado $\mathbb{Z}[\zeta_3]^N$.

O conjunto $\mathcal{L}(\mathcal{C}) = \{\varphi(x)|\ x \in \mathcal{C}\} \subset \mathbb{Z}[\zeta_3]^N\}$ é um código reticulado obtido através da aplicação $\varphi(\sum_{j=0}^{N-1}a_jx^j) = \sum_{j=0}^{N-1}\varphi((a_j)\varphi((x))^j$ para todo $x \in \mathbb{F}_3[x]/(x^N-1)$, onde $\mathcal{C}$ é um código ternário que pode ser visto como um ideal em $\mathbb{F}_3[x]/(x^N-1)$.

Vamos estabelecer uma conexão entre ideais encaixados em $\mathbb{Z}[\zeta_{3^s}]$ e códigos ternários encaixados em $\mathbb{F}_3[x]/(x^N-1)$.

Proposition 3.1. *O polinômio minimal $\mu(x) = x^N - \zeta_3$ associado ao elemento primitivo ζ_{3^s} é identificado pelo polinômio $t(x) = x^N - 1 \in \mathbb{F}_3[x]$ via a operação módulo $(1-\zeta_3)$.*

Demonstração. Se $\zeta_{3^s}^N = \zeta_3$ e $\mu(x) = x^N - \zeta_3$, então $\zeta_{3^s}^N = \zeta_3$, uma vez que $\mu(x)$ é o polinômio minimal associado ao elemento primitivo ζ_{3^s}. Logo, ζ_{3^s} é raíz de $t(x) = x^N - 1$, desde que $\zeta_3 = 1$ modulo $(1-\zeta_3)$. Portanto, o polinômio $\mu(x) = x^N - \zeta_3$ é identificado pelo polinômio $t(x) = x^N - 1 \in \mathbb{F}_3[x]$ por meio da operação módulo $(1-\zeta_3)$. □

Seja $t(x) = x^N - 1 \in \mathbb{F}_3[x]$. Desde que $3/N$, por meio da aritmética operação módulo 3, segue que $x^N - 1 = (x-1)^N$. Pela Proposição 3.1, o polinômio $\mu(x) = x^N - \zeta_3$ é identificado pelo polinômio $t(x) = x^N - 1 \in \mathbb{F}_3[x]$ via a operação módulo $(1-\zeta_3)$. Entretanto, na Seção 2, vimos que $\mu(x) = x^N - \zeta_3 = \prod_{k=0}^{N-1}\mu_k(x)$, onde $\mu_k = x - \zeta_{3^s}^k$. O que nos leva a concluir que cada polinômio mônico $\mu_k = x - \zeta_{3^s}^k$ é identificado pelo

polinômio mônico $t_1(x) = x - 1 \in \mathbb{F}_3[x]$ para todo $k \in \{0, \cdots, N-1\}$ via a operação módulo $1 - \zeta_3$. Consequentemente, $t(x) \in \mathbb{F}_3[x]$ pode ser reescrito na forma $t(x) = t_1(x)^N$ em $\mathbb{F}_3[x]$.

Da teoria dos códigos, segue que um código ternário $\mathcal{C}_r = (N, r)$, onde $r = N - k$, é caracterizado por polinômio ideal no anel de polinômios $\mathbb{F}_3[x]/x^N - 1$, onde o gerador $g(x)$ é de grau k e divide $x^N - 1$.

Agora, apresentamos um resultado geral que estabelece uma correspondência para cada polinômio $g(x)$ $\mathbb{F}_3[x]$ que divide $x^N - 1$ via a operação módulo $(1 - \zeta_3)$.

Proposition 3.2. *1. O polinômio $\mu(x) = x^N - \zeta_3$ com coeficientes em $\mathbb{Z}[\zeta_3]$ é identificado pelo polinômio código $t(x) = x^N - 1 \in \mathbb{F}_3[x]/(x^N - 1)$ via a operação módulo $(1 - \zeta_3)$.*

2. Cada polinômio $\mu_1(x)^k = (x - \zeta_3^k)^k$ com coeficientes no anel de inteiros $\mathbb{Z}[\zeta_3]$ é identificado por cada polinômio código $g(x)^k = (x-1)^k \in \mathbb{F}_3[x]/(x^N - 1)$ via a operação módulo $(1 - \zeta_3)$ para todo $k = 1, \cdots, N-1$.

Observação 3.1. *Se $v = a_0 + a_1\zeta_{3^s} + \cdots + a_{N-1}\zeta_{3^s}^{N-1} \in \mathbb{Z}[\zeta_{3^s}]$, com $a_t \in \mathbb{Z}[\zeta_3]$ e $t = 0, 1, \cdots, N-1$. Desde que $N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(1 - \zeta_3) = 3$, segue-se que $a_t = (\zeta_3 - 1)b_t + c_t$, onde $b_t \in \mathbb{Z}[\zeta_3]$ and $c_t = 0, \pm 1, \zeta_3$. Assim, $v = ((\zeta_3 - 1)b_0 + c_0) + ((\zeta_3 - 1)b_1 + c_1)\zeta_{3^s} + \cdots + ((\zeta_3 - 1)b_{N-1} + c_{N-1})\zeta_{3^s}^{N-1}$ e v módulo $(\zeta_3 - 1) = c_0 + c_1\zeta_{3^s} + \cdots + c_{N-1}\zeta_{3^s}^{N-1}$.*

Proposição 3.3. *Cada ideal $(1 - \zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]$ em $\mathbb{Z}[\zeta_{3^s}]$ corresponde a um código ternário $\mathcal{C}_{N-k} = (N, N-k)$, para todo $k = 1, \cdots, N-1$.*

Demonstração. Para cada $k \in \{1, \ldots, N-1\}$, consideramos ideais dados por $(\zeta_{3^s} - 1)^k\mathbb{Z}[\zeta_{3^s}]$ no anel de inteiros $\mathbb{Z}[\zeta_{3^s}]$. Agora, seja $v = a_0 + a_1\zeta_{3^s} + \cdots + a_{N-1}\zeta_{3^s}^{N-1} \in (\zeta_{3^s} - 1)^k\mathbb{Z}[\zeta_{3^s}]$, onde $a_t \in \mathbb{Z}[\zeta - 3]$ e $t = 0, 1, \cdots, N-1$. Ao considerarmos o reticulado quociente $\mathbb{Z}[\zeta_3]/(\zeta_3 - 1)\mathbb{Z}[\zeta_3]$, podemos escrever v na forma $v = (\zeta_{3^s} - 1)^k[((\zeta_3 - 1)b_0 + c_0) + ((\zeta_3 - 1)b_1 + c_1)\zeta_{3^s} + \cdots + ((\zeta_3 - 1)b_{N-1} + c_{N-1})\zeta_{3^s}^{N-1}]$, onde $a_t = (\zeta_3 - 1)b_t + c_t$, $b_t \in \mathbb{Z}[\zeta_3]$ e $c_t = 0, \pm 1$. Assim, v pode ser reescrito na forma $v = (\zeta_{3^s} - 1)^k[((\zeta_3 - 1)b_0 + c_0) + ((\zeta_3 - 1)b_1 + c_1)\zeta_{3^s} + \cdots + ((\zeta_3 - 1)b_{N-1} + c_{N-1})\zeta_{3^s}^{N-1}]$, isto é, v módulo $(\zeta_3 - 1) = (\zeta_{3^s} - 1)^k(c_0 + c_1\zeta_{3^s} + \cdots + c_{N-1}\zeta_{3^s}^{N-1})$. Logo, os elementos do ideal $(\zeta_{3^s} - 1)^k\mathbb{Z}[\zeta_{3^s}]$ são identificados pelos elementos do polinômio $g^k(x) = (1-x)^k(d_0 + d_1x + \cdots + d_{N-1}x^{N-1})$, para cada $k = 1, 2, \cdots, N-1$, onde $g(x) = (x-1)(d_0 + d_1x + \cdots + d_{N-1}x^{N-1})$ e $d_j = c_j$ módulo $(\zeta_3 - 1)$, para todo $j \in \{0, \ldots, N-1\}$. Portanto, existe uma correspondência entre os ideais $(\zeta_{3^s} - 1)^k\mathbb{Z}[\zeta_{3^s}]$ no anel de inteiros $\mathbb{Z}[\zeta_{3^s}]$ e os polinômios ideais $g(x)^k = (x-1)^k$ no anel $\mathbb{F}_3[x]/(x^N - 1)$. Como consequência, obtemos uma identificação entre os ideais $(\zeta_{3^s} - 1)^k\mathbb{Z}[\zeta_{3^s}]$ em $\mathbb{Z}[\zeta_{3^s}]$ e os códigos ternários $\mathcal{C}_{N-k} = (N, N-k)$, desde que os ideais polinômios $g(x)^k = (x-1)^k$ in $\mathbb{F}_3[x]/(x^N - 1)$ correspondente aos códigos ternários $\mathcal{C}_r = (N, N-k)$ para cada $k = 1, 2, \ldots, N-1$. □

Assim, existe uma correspondência entre os ideais $(1-\zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]$ em $\mathbb{Z}[\zeta_{3^s}]$ e os códigos ternários $\mathcal{C}_{N-k} = (N, N-k)$ via a operação módulo $(1 - \zeta_3)$, para $k = 0, \cdots, N-1$.

A propriedade do formato cubico é uma das condições necessárias para se obter códigos reticulados via a aplicação definida de um anel de polinômios finito $\mathbb{F}_3[x]/(x^N - 1)$ no

espaço Euclidiano complexo $\mathbb{C}^N$. Para isto, consideramos uma cadeia de ideais tomados da forma

$$\mathbb{Z}[\zeta_{3^s}]/(1-\zeta_{3^s})/\mathbb{Z}[\zeta_{3^s}]/\dots(\zeta_{3^s}-1)^{N-1}/\mathbb{Z}[\zeta_{3^s}]. \tag{3}$$

Aplicamos um mergulho dado pela Equação (2) do ideal gerado por $\{\gamma^k, \gamma^k\zeta_{3^s}, \cdots, \gamma^k\zeta_{3^s}\}$. A matriz geradora é dada por

$$M_k = \begin{pmatrix} \gamma^k & \gamma^k\zeta_{3^s} & \cdots & \gamma^k\zeta_{3^s}^{N-1} \\ \sigma_2(\gamma^k) & \sigma_2(\gamma^k\zeta_{3^s}) & \cdots & \sigma_2(\gamma^k\zeta_{3^s}^{N-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\gamma^k) & \sigma_n(\gamma^k\zeta_{3^s}) & \cdots & \sigma_n(\gamma^k\zeta_{3^s}^{N-1}) \end{pmatrix}.$$

Assim, o reticulado ideal Λ_k corresponde a um ideal tomado na cadeia de deals dados pela Equação (3). Pela Proposição 3.2, segue que o reticulado ideal Λ_k é uma versão escalonada do reticulado sobre $\mathbb{Z}[\zeta_3]^N$. Sem perda de generalidade, denotamos o reticulado ideal Λ_k por $(1-\zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]^N$.

Lemma 3.1. *Se Λ e Λ_N são reticulados ternários tal que Λ_N é um sub-reticulado de Λ $|\Lambda/\Lambda_N| = 3^N$, então a sequência de reticulados $\Lambda_0 = \Lambda, \Lambda_1, \cdots, \Lambda_N$ tal que $\Lambda_0/\Lambda/\Lambda_1/\cdots/\Lambda_N$ é uma cadeia de partição, onde cada partição Λ_k/Λ_{k+1} tem ordem 3, para $k = 0, 1, \cdots, N-1$. Além disso, Λ tem uma decomposição em classes laterais dada por $\Lambda = \Lambda_N + \{\sum_{k=1}^{N-1} a_k x_k\}$, onde $a_k \in \mathbb{F}_3$, $a_k x_k \in \{0, 1, 2\}$ é um sistema completo de representantes de classes laterais para $[\Lambda_k/\Lambda_{k+1}]$ and $k = 0, 1, \cdots, N-1$.*

Demonstração. A prova deste Lema é uma consequência direta da definição de reticulado e de partição de reticulados. □

Pelo Lema 3.1, segue que a partição de reticulados pode ser dividida em cadeias de partição de reticulados Λ_k/Λ_{k+1} de ordem 3 para $k = 0, 1, \cdots, N-1$. Consequentemente, se $u \in \mathbb{F}_3[x]/(x^N-1)$, então existe um rotulamento $\varphi(u) = \sum_{k=1}^{N} a_k x_k$, onde a_k é a k-th coordenada da N-upla x_k, é um elemento de Λ_k mas que não pertence as outras classes laterais em Λ_k/Λ_{k+1}. Logo, os vetores $\{a_k x_k | a_k \in \mathbb{F}_3\}$ formam um sistema completo de classes laterais Λ_k em uma partição de ordem 3. Portanto, existem 3^k linear combinações lineares do geradores x_k que formam um sistema completo de classes laterais $[\Lambda_k/\Lambda_{k+1}]$.

Remark 3.1. *Se Λ é um reticulado complexo de Eisenstein de dimensão N e $\Lambda_k = (1-\zeta_3)^k\mathbb{Z}[\zeta_3]^N$ é um subreticulado do reticulado Λ, então,*

1. $\Lambda = (1-\zeta_3)^k\mathbb{Z}[\zeta_3]^N + [\Lambda/(1-\zeta_3)^k\mathbb{Z}[\zeta_3]^N]$,
2. *como consequência do Lema 3.1, obtemos um código reticulado $\mathcal{C}$ com parâmetros (N, k) que é identificado pela partição de reticulados $[\Lambda/(1-\zeta_3)^k\mathbb{Z}[\zeta_3]^N]$ que tem ordem 3^k.*
3. *para cada $u = \sum_{j=0}^{k-1} a_k x^k \in \mathbb{F}_3[x]/(x^N-1)$, existe um mapeamento natural $\varphi : \mathbb{F}_3[x]/(x^N-1) \to \mathbb{Z}[\zeta_3]$ dado por $\varphi(\sum_{j=0}^{k-1} a_k x^k) = \varphi(a_k)(\varphi(x))^j$, onde $\varphi : \mathbb{F}_3[x] \to \mathbb{Z}[\zeta_3]$ é dado por $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(2) = 2$ and $\varphi(x) = 1-\zeta_3$.*

DOI: 10.5540/03.2018.006.01.0403

Proposition 3.3. *Sejam* Λ *e* $(1-\zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]^N$ *um reticulado ideal complexo tal que* $(1-\zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]^N$ *é um subreticulado de* Λ *e* $|\Lambda/(1-\zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]^N| = 3^k$*, onde* $k = 0, 1, \cdots, N-1$*. Então existe uma sequência de reticulados* $\Lambda_0 = \Lambda, (1-\zeta_{3^s})\mathbb{Z}[\zeta_{3^s}]^N, \cdots, (1-\zeta_{3^s})^N\mathbb{Z}[\zeta_{3^s}]^N$ *tal que* $\Lambda_0/\Lambda/(1-\zeta_{3^s})\mathbb{Z}[\zeta_{3^s}]^N/\cdots/(1-\zeta_{3^s})^N\mathbb{Z}[\zeta_{3^s}]^N$ *é uma cadeia de partição de reticulados e cada partição* $(1-\zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]^N/(1-\zeta_{3^s})^{K-1}\mathbb{Z}[\zeta_{3^s}]^N$ *tem ordem* 3*, onde* $k = 0, 1, \cdots, N-1$*. Além disso,* Λ *tem uma decomposição em classes laterais dada por*

$$\Lambda = (1-\zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]^N + \{\sum_{k=0}^{N-1} a_k x_k\},$$

onde $a_k \in \mathbb{F}_3$ *and* $a_k x_k \in \{0, 1, 2\}$ *é um sistema completo de representantes de classes laterais para* $(1-\zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]^N/(1-\zeta_{3^s})^{k+1}\mathbb{Z}[\zeta_{3^s}]^N$*, com* $k = 0, 1, \cdots, N-1$*.*

Demonstração. Pelo Lema 3.1, seque que $\Lambda = (1-\zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]^N + \{\sum_{k=0}^{N-1} a_k x_k\}$ é uma decomposição de classes laterais $\Lambda = \Lambda_k + \{\sum_{k=0}^{N-1} a_k x_k\}$ a menos de isomorfismo, onde $a_k \in \mathbb{F}_3$ e $a_k x_k \in \{0, 1, 2\}$ é um sistema completo de representantes para $(1-\zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]^N/(1-\zeta_{3^s})^{k+1}\mathbb{Z}[\zeta_{3^s}]^N$, onde $k = 0, 1, \cdots, N-1$. □

Seque da Proposição 3.3, que a cadeia $(1-\zeta_{3^s})^k\mathbb{Z}[\zeta_{3^s}]^N/(1-\zeta_{3^s})^{k+1}\mathbb{Z}[\zeta_{3^s}]^N$ ´é uma partição de ordem 3 para $k = 0, 1, \cdots, N-1$. Consequentemente, se $u \in \mathbb{F}_3[x]/(x^N-1)$, então existe um rotulamento $\varphi(u) = \sum_{k=0}^{N-1} a_k x_k$, onde a_k é a k-ésima coordenada da N-upla x_k, que é um elemento de Λ_k mas que não pertence Λ_{k+1} tal que os vetores $\{a_k x_k | a_k \in \mathbb{F}_3\}$ formam sistema completo de classes laterias de Λ_k em uma cadeia de partição de ordem 3. Assim, existem 3^k combinações lineares $\{a_k x_k\}$ dos geradores x_k e formam um sistema completo de classes laterais de $[\Lambda_k/\Lambda_{k+1}]$.

4 Conclusões

A contribuição deste trabalho é de apresentar novas classes de códigos reticulados encaixados via reticulados ideais proveniente de famílias de corpos ciclotômicos $\mathbb{Q}(\zeta_{3^s})$.

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

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

