UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

ANA PAULA DE SOUZA

Sobre constelações de Voronoi para códigos em reticulados e problemas de codificação de índice

Campinas

2021

Ana Paula de Souza

Sobre constelações de Voronoi para códigos em reticulados e problemas de codificação de índice

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestra em Matemática Aplicada.

Orientadora: Sueli Irene Rodrigues Costa

Este trabalho corresponde à versão final da Dissertação defendida pela aluna Ana Paula de Souza e orientada pela Profa. Dra. Sueli Irene Rodrigues Costa.

Campinas

2021

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

So89s

Souza, Ana Paula de, 1997-
Sobre constelações de Voronoi para códigos em reticulados e problemas de codificação de índice / Ana Paula de Souza. – Campinas, SP : [s.n.], 2021.

Orientador: Sueli Irene Rodrigues Costa.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos reticulados. 2. Teoria da codificação. 3. Códigos corretores de erros (Teoria da informação). 4. Reticulado de modelagem. I. Costa, Sueli Irene Rodrigues. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: About Voronoi constellations for lattice codes and index coding problems
Palavras-chave em inglês:
Lattice theory
Coding theory
Error-correcting codes (Information theory)
Shaping lattice
Área de concentração: Matemática Aplicada
Titulação: Mestra em Matemática Aplicada
Banca examinadora:
Sueli Irene Rodrigues Costa [Orientador]
João Eloir Strapasson
Renato da Rocha Lopes
Data de defesa: 26-02-2021
Programa de Pós-Graduação: Matemática Aplicada

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: 0000-0001-8214-9447
- Currículo Lattes do autor: http://lattes.cnpq.br/7873823198026860

Dissertação de Mestrado defendida em 26 de fevereiro de 2021 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). SUELI IRENE RODRIGUES COSTA

Prof(a). Dr(a). JOÃO ELOIR STRAPASSON

Prof(a). Dr(a). RENATO DA ROCHA LOPES

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Agradecimentos

A Deus pelas oportunidades durante o mestrado.

À minha orientadora Sueli pela orientação, por toda preocupação pessoal e acadêmica e pelos incansáveis incentivos ao longo deste percurso. Por mesmo distante fisicamente, devido a pandemia, se fazer tão presente. Minha eterna gratidão!

Aos meus familiares. Sem o apoio de vocês isto não seria possível. Esta conquista também é de vocês!

À Livia, minha namorada, pelo colo acolhedor, paciente e compreensível. Pelo carinho e toda parceria. Sem dúvidas, esta trajetória foi mais leve porque teve você!

Aos meus amigos pelo companheirismo e trocas compartilhadas. Não me esquecerei dessas amizades!

À Unicamp e ao IMECC por me possibilitarem uma formação pública e de qualidade!

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Também à Universidade Virtual do Estado de São Paulo - Univesp por disponibilizar recursos para o desenvolvimento deste trabalho.

Resumo

Neste trabalho estudamos construções de constelações de Voronoi para codificação em reticulados. São considerados reticulados aninhados, $\Lambda_g \subseteq \Lambda_f$, com Λ_f obtido por construção A a partir de um código linear sobre $\mathbb{Z}_p$, com p primo. Também exploramos uma generalização desta abordagem propondo uma adaptação para reticulados q-ários Λ_f obtidos por construção D, com $q \in \mathbb{N}^*$. Estudamos um esquema de codificação e de mapeamento inverso iterativo que aplica essas técnicas para reticulados com bom ganho de codificação e modelagem. Por fim, investigamos o problema de codificação de índice com perspectiva futura de utilizar as estratégias aqui exploradas para obter códigos reticulados de índice com bons resultados quanto ao ganho de informação lateral em canais AWGN.

Palavras-chave: Códigos Reticulados; Constelação de Voronoi; Codificação de Índice; Construção A; Construção D.

Abstract

In this work we study constructions of Voronoi constellations for lattice coding. It is considered nested lattices, $\Lambda_g \subseteq \Lambda_f$, where Λ_f is obtained by construction A from a linear code over a prime field $\mathbb{Z}_p$. We also explore a generalization of this approach and propose an adaptation for Λ_f q-ary lattices obtained by construction D, where $q \in \mathbb{N}^*$. We study a coding and iterative demapping scheme that applies these techniques to lattices with good coding and shaping gains. Finally, we investigate the index coding problem with a future perspective of using the strategies explored here to obtain lattice index codes that achieve good results regarding side information gain in AWGN channels.

Keywords: Lattice Codes; Voronoi Constellations; Index Coding; Construction A; Construction D.

Sumário

Introdução

Reticulados são conjuntos discretos no espaço euclidiano n-dimensional formados por todas as combinações inteiras de vetores linearmente independentes. São objetos de estudo em matemática e têm diversas aplicações. Na área de comunicações vêm sendo considerados para codificação em transmissão de sinais em canais gaussianos e com desvanecimento e também na proposição de sistemas criptográficos que compõe uma das modalidades da chamada criptografia pós-quântica.

Neste trabalho abordamos dois temas específicos relacionados ao uso de reticulados em codificação: a construção de constelações de Voronoi e a codificação de índice através de reticulados. No primeiro são considerados dois reticulados aninhados $\Lambda_g \subseteq \Lambda_f$, chamados de reticulados de modelagem e de codificação e é discutida a construção da constelação finita de pontos a serem utilizados na codificação. No segundo são considerados vários sub-reticulados de um mesmo reticulado num processo de codificação onde é assumido que os receptores tenham também informação lateral.

Os próximos capítulos estão organizados como descrito a seguir. No Capítulo 1 apresentamos conceitos e resultados preliminares a serem utilizados. Mais especificamente introduzimos noções sobre reticulados; códigos lineares e construções de reticulados a partir de códigos lineares. No Capítulo 2 estudamos a construção de constelações de Voronoi proposta no artigo de Pietro e Boutros (2017), estendendo e apresentando resultados relacionados. No Capítulo 3 detalhamos e ilustramos os códigos de índice baseados em reticulados propostos no Capítulo 6 de Costa et al. (2017) e em Natarajan, Hong e Viterbo (2015) visando numa pesquisa futura discutir possíveis ganhos de codificação através das construções de Voronoi como as descritas no Capítulo 2. No Capítulo 4 listamos brevemente algumas perspectivas de continuidade da pesquisa nos temas aqui abordados.

1 Conceitos e Propriedades Preliminares

Neste capítulo, apresentamos conceitos e propriedades preliminares sobre reticulados, particularmente a obtenção destes pelas construções A e D a partir de códigos lineares. O intuito desse capítulo é fornecer a base e possibilitar uma familiarização com as notações usadas no desenvolvimento deste trabalho. As principais referências utilizadas foram Costa et al. (2017), Conway e Sloane (1998), Zamir e Nazer (2014), Strey e Costa (2017), Strey (2017) e Pietro e Boutros (2017).

1.1 Reticulados

Um reticulado $\Lambda \subseteq \mathbb{R}^n$ é um subgrupo aditivo discreto de $\mathbb{R}^n$. Isto é, um conjunto não vazio discreto de vetores de $\mathbb{R}^n$ que satisfazem as condições

(i) se $\mathbf{x}, \mathbf{y} \in \Lambda$ então $\mathbf{x} + \mathbf{y} \in \Lambda$;

(ii) para todo vetor $\mathbf{x} \in \Lambda$, temos que $-\mathbf{x} \in \Lambda$.

O reticulado é discreto no sentido que, para qualquer ponto do reticulado, sempre é possível obter ao seu redor uma vizinhança que possui nenhum outro ponto do reticulado. Ainda, da definição de reticulado, temos que o ponto $\mathbf{0} = (0, \ldots, 0)$ sempre pertencerá ao reticulado pois ele é a soma de qualquer $\mathbf{x} \in \Lambda$ com $-\mathbf{x}$.

Uma definição equivalente (CASSELS, 1997) e mais construtiva de reticulado é dada a seguir.

Definição 1.1. *Sejam $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_m$ vetores linearmente independentes de $\mathbb{R}^n$. Um reticulado Λ é definido como todas as combinações inteiras desses vetores. Ou seja, $\boldsymbol{x} \in \Lambda$ se, e somente se, $\boldsymbol{x} = \alpha_1 \boldsymbol{b}_1 + \cdots + \alpha_m \boldsymbol{b}_m$, com $\alpha_j \in \mathbb{Z}$ para todo $j = 1, \ldots, m$. Em outras palavras, podemos escrever*

$$\Lambda \quad = \quad \left\{ \sum_{j=1}^{m} \alpha_j \boldsymbol{b}_j, \ \textit{com } \alpha_j \in \mathbb{Z} \right\}.$$

O conjunto de vetores linearmente de vetores independentes geradores é denominado uma *base* do reticulado e m chamado *posto* de Λ. Quando $m = n$ o reticulado é dito de *posto completo*. Também, o conjunto $\{(0, \ldots, 0)\} \subset \mathbb{R}^n$ pode ser considerado como um reticulado (degenerado) de posto 0. Um reticulado é *degenerado* quando $m < n$, isto é, quando o número de vetores linearmente independentes que geram o reticulado é menor que a dimensão de $\mathbb{R}^n$.

A definição de reticulados pode ser reescrita em termos de uma matriz contendo os vetores linearmente independentes.

Definição 1.2. *Uma matriz geradora G para um reticulado Λ é uma matriz cujas colunas formam uma base para Λ, isto é,*

$$G = [\boldsymbol{b}_1\ \boldsymbol{b}_2\ \cdots\ \boldsymbol{b}_m].$$

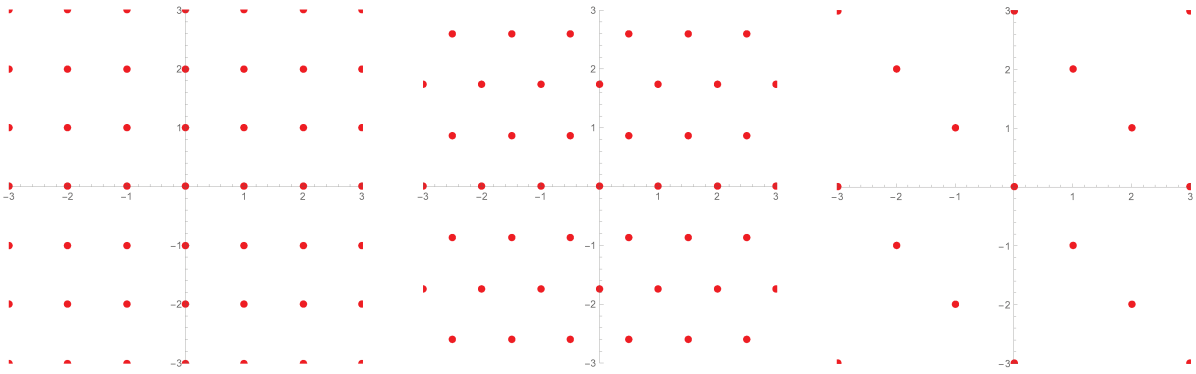
Um vetor $\boldsymbol{x} \in \Lambda$ se, e somente se, pode ser escrito como

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \boldsymbol{b}_1 & \boldsymbol{b}_2 & \cdots & \boldsymbol{b}_m \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}, \text{ com } \alpha_i \in \mathbb{Z}.$$

A Figura 1 ilustra três reticulados em $\mathbb{R}^2$. O primeiro é o reticulado quadrado $\mathbb{Z}^2$, que são os pontos com coordenadas inteiras em $\mathbb{R}^2$ e que tem como uma de suas bases o conjunto $\{(1,0),(0,1)\}$. O segundo é o reticulado hexagonal, Λ_2, com uma base $\left\{(1,0), \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)\right\}$. E o terceiro é um reticulado que possui base $\{(1,2),(0,-3)\}$.

Figura 1 – Reticulados no plano.

(a) Reticulado quadrado $\mathbb{Z}^2$ (b) Reticulado hexagonal Λ_2 (c) Reticulado gerado por $\{(1,2),(0,-3)\}$.



Observamos que uma outra base para o reticulado $\mathbb{Z}^2$ é $\{(1,3),(0,1)\}$. Para o reticulado hexagonal, uma outra base que pode ser considerada é $\left\{\left(\frac{7}{2}, \frac{3\sqrt{3}}{2}\right), \left(\frac{3}{2}, \frac{\sqrt{3}}{2}\right)\right\}$ Vemos assim que a matriz geradora de um reticulado não é única, como caracterizado a seguir.

Proposição 1.1 ((COSTA et al., 2017)). *Seja Λ um reticulado gerado por uma matriz G. Uma matriz G' gera o mesmo reticulado que G se, e somente se, $G' = GU$ para alguma matriz U unimodular, isto é, uma matriz com entradas inteiras e com $det(U) = \pm 1$.*

Demonstração. ($\Rightarrow$) Sejam $\beta_1 = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ e $\beta_2 = \{\mathbf{b}'_1, \ldots, \mathbf{b}'_m\}$ bases de Λ e Λ' associadas às matrizes geradoras G e G', respectivamente. Suponha que G e G' gerem o mesmo

reticulado, isto é, que $\Lambda = \Lambda'$. Por um lado, $\Lambda' \subseteq \Lambda$ se, e somente se, os vetores de β_1 puderem ser escritos como combinação inteira do vetores de β_2, ou seja,

$$\mathbf{b}'_j = \sum_{i=1}^{m} \mathbf{b}_i \alpha_{ij}, \text{para j} = 1, \ldots, \text{m e } \alpha_{ij} \in \mathbb{Z}.$$

Em outras palavras, $G' = GU$, com U uma matriz inteira tendo em cada entrada os valores de α_{ij}.

Por outro lado, analogamente conclui-se que $\Lambda \subseteq \Lambda'$ se, e somente se, $G = G'V$, para alguma matriz inteira V. Resta mostrar que $det(U) = det(V) = \pm 1$.

Como $G' = GU$ e $G = G'V$, segue que

$$G' = G'VU \Leftrightarrow G'(I - VU) = 0$$

Portanto, cada coluna de $I - VU$ define os coeficientes de uma equação linear em $\mathbf{b}'_1, \ldots, \mathbf{b}'_m$ e, lembrando que esses vetores são linearmente independentes, esses coeficientes correspondentes devem ser todos iguais a 0. Assim,

$$I - VU = 0 \Leftrightarrow VU = I.$$

Consequentemente, $det(V)det(U) = det(I) = 1$ que, juntamente com o fato que U, V são matrizes com entradas inteiras, tem-se $det(U) = det(V) = \pm 1$. Portanto, U é unimodular.

($\Leftarrow$) Se existe U unimodular tal que $G' = GU$, então $\Lambda' \subseteq \Lambda$. Além disso, como U é unimodular então possui inversa, pois $det(U) = \pm 1$ e, assim, segue que $G = G'U^{-1}$, com U^{-1} também com entradas inteiras, uma vez que no processo da obtenção da inversa o cálculo das matrizes de cofatores envolve apenas as entradas de U, que são inteiras. Isso implica que $\Lambda \subseteq \Lambda'$. Logo, $\Lambda = \Lambda'$. □

Deste resultado, podemos concluir que o valor absoluto do determinante das matrizes geradoras de um reticulado de posto máximo é invariante, pois

$$det(G') = det(GU) = det(G)det(U) = \pm det(G).$$

Observação 1. *Como um reticulado Λ possui infinitas bases, para reticulados inteiros, ou seja, para $\Lambda \subseteq \mathbb{Z}^n$, de posto máximo consideramos bases especiais, que utilizaremos no Capítulo 2, que sempre podem ser obtidas da que é chamada Forma Normal de Hermite por colunas da matriz geradora com entradas inteiras G (COHEN, 1996): $H = GU$ com U unimodular e $H = [h_{i,j}]$ uma matriz quadrada que satisfaz*

1. *$h_{i,j} = 0$ para $i < j$, ou seja, H é uma matriz triangular inferior.*
2. *$0 \leqslant h_{i,j} < h_{i,i}$ para $i > j$, isto é, as entradas são não negativas e o elemento da diagonal é o de maior valor em cada linha.*

Exemplo 1. *Seja* $G = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ *uma matriz geradora para* $\Lambda \subset \mathbb{Z}^2$. *Outra matriz geradora para este reticulado obtida na Forma Normal de Hermite por colunas é*

$$H = GU = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}.$$

Essas matrizes foram obtidas pelo software Mathematica (INC.,).

É importante ressaltar aqui que existem algoritmos computacionais muito eficientes em tempo polinomial para encontrar a Forma Normal de Hermite e que estes são encontrados em programas tais como o Mathematica, Maple, MatLab e Phyton.

Para reticulados de posto qualquer, definimos o *determinante de* Λ como o determinante de uma de suas matrizes de Gram definida a seguir. Este é sempre um número positivo e novamente como consequência da Proposição 1.1 o determinante de Λ não depende da base escolhida.

Definição 1.3. *Dado uma matriz geradora* G *para o reticulado* Λ, *definimos a matriz de Gram associada à* G *por* $B = G^tG$.

Definição 1.4. *O volume de um reticulado* Λ, *denotado por* $Vol(\Lambda)$ *é a raiz quadrada do determinante de uma matriz de Gram, isto é,* $Vol(\Lambda) = \sqrt{det(G^tG)}$.

O volume de um reticulado é igual ao volume euclidiano m-dimensional de um *paralelotopo fundamental* de Λ definido a seguir.

Definição 1.5. *Um paralelotopo fundamental de* Λ *associado a uma matriz geradora* G, *denotado por* $\mathcal{P}(G)$, *é o conjunto*

$$\mathcal{P}(G) = \{\alpha_1 \boldsymbol{b}_1 + \alpha_2 \boldsymbol{b}_2 + \cdots + \alpha_m \boldsymbol{b}_m; 0 \leqslant \alpha_i < 1, i = 1, \ldots, m\}.$$

Observação 2. *Ao longo deste trabalho estaremos assumindo, a menos de menção em contrário, que os reticulados são de posto máximo e os conceitos a seguir são definidos para tais reticulados. Um conjunto* $\mathcal{R} \subset \mathbb{R}^n$ *cujo bordo tem medida nula é chamado região fundamental para um reticulado* Λ *se, e somente se,*

(i) $\bigcup_{\boldsymbol{x} \in \Lambda} (\boldsymbol{x} + \mathcal{R}) = \mathbb{R}^n$;

(ii) dados $\boldsymbol{x}, \boldsymbol{y} \in \Lambda$, $\boldsymbol{x} \neq \boldsymbol{y}$, *os conjuntos* $\boldsymbol{x} + \mathcal{R}$ *e* $\boldsymbol{y} + \mathcal{R}$ *se interseccionam no máximo em seus bordos.*

O volume de uma região fundamental é $Vol(\Lambda)$. Um paralelotopo fundamental é um exemplo de região fundamental. Uma outra região fundamental importante que usaremos no Capítulo 2 é a região de Voronoi do reticulado definida a seguir, que é independente da base escolhida.

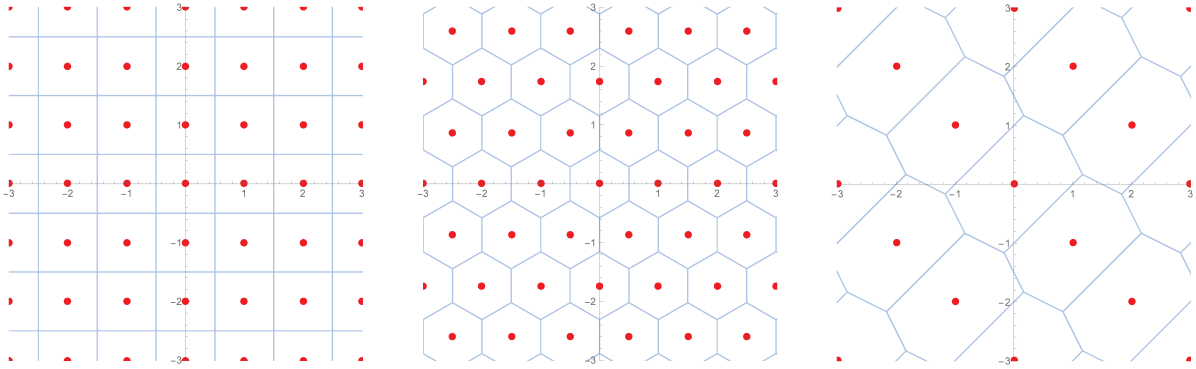
Definição 1.6. *A região de Voronoi de um reticulado Λ de um ponto $\boldsymbol{x} \in \Lambda$ é o conjunto de todos os pontos de $\mathbb{R}^n$ que estão mais próximos de $\boldsymbol{x}$ do que qualquer outro ponto de Λ, isto é,*

$$\mathcal{V}_\Lambda(\boldsymbol{x}) = \{\boldsymbol{y} \in \mathbb{R}^n; ||\boldsymbol{x} - \boldsymbol{y}|| \leqslant ||\boldsymbol{z} - \boldsymbol{y}||, \text{ para todo } \boldsymbol{z} \in \Lambda\}.$$

Ao cobrir o $\mathbb{R}^n$ com regiões de Voronoi sobre os pontos de Λ temos a *partição de Voronoi*. A Figura 2 ilustra as regiões de Voronoi dos reticulados mencionados anteriormente.

Figura 2 – Exemplos de região de Voronoi de reticulados no plano.

(a) Reticulado $\mathbb{Z}^2$ (b) Reticulado A_2 (c) Reticulado $\Lambda = \langle(1,2),(0,-3)\rangle$



Devido à natureza periódica do reticulado, todas as regiões de Voronoi são versões transladadas (pelos pontos do reticulado Λ) da região de Voronoi $\mathcal{V}_\Lambda(\mathbf{0})$, que é a região de Voronoi associada com a origem, chamada simplesmente de *região de Voronoi do reticulado*.

Definição 1.7. *Uma aplicação de quantização*

$$\begin{aligned} \mathcal{Q}_\Lambda(\cdot) : \mathbb{R}^n &\longrightarrow \Lambda \\ \boldsymbol{x} \in \mathbb{R}^n &\longmapsto \arg\min_{\boldsymbol{z} \in \Lambda} ||\boldsymbol{z} - \boldsymbol{x}|| \end{aligned}$$

é uma função que leva qualquer ponto do espaço $\mathbb{R}^n$ para um ponto do reticulado Λ mais próximo deste.

Observação 3. *Esta aplicação está claramente definida para os pontos no interior das regiões de Voronoi. Para os que estiverem no bordo é feita uma escolha.*

Outros parâmetros importantes em reticulados que são associados em diversas aplicações, como as que veremos no Capítulos 2 e 3, são a *distância mínima de um reticulado, raio de empacotamento, densidade de empacotamento, raio de cobertura e densidade de cobertura.*

A *distância mínima* de um reticulado é a menor distância entre dois pontos de um reticulado e esta corresponde à menor entre todas as normas de vetores diferentes de

zero em Λ, isto é,

$$d_{min}(\Lambda) = \min_{0 \neq \mathbf{x} \in \Lambda} ||\mathbf{x}||.$$

Utilizamos essa distância para determinar o maior raio, denotado por λ, de bolas disjuntas centradas nos pontos do reticulado Λ que cobrem a maior porção possível de $\mathbb{R}^n$. É fácil ver que λ, chamado *raio de empacotamento*, é

$$\lambda = \frac{d_{min}}{2}.$$

A *densidade de empacotamento*, denotada por $\Delta(\Lambda)$, determina a proporção de $\mathbb{R}^n$ coberta pelo o empacotamento. Pela homogeneidade do reticulado é expressa como

$$\Delta(\Lambda) = \frac{Vol\mathcal{B}^n(\lambda)}{Vol(\Lambda)},$$

com $\mathcal{B}^n(\lambda)$ a bola euclidiana de raio λ ao redor da origem.

O *raio de cobertura* é definido como o menor μ tal que translações de bolas $\mathcal{B}^n(\mu)$ por pontos de Λ cobrem o espaço, isto é,

$$\bigcup_{\mathbf{x} \in \Lambda} (\mathcal{B}^n(\mu) + \mathbf{x}) = \mathbb{R}^n.$$

A densidade ou taxa de cobertura é então definida como

$$\theta(\Lambda) = \frac{Vol\mathcal{B}^n(\mu)}{Vol(\Lambda)}.$$

1.2 Códigos lineares

Nesta seção, apresentamos uma breve introdução a códigos lineares q-ários.

Para $q \geqslant 2$ um inteiro positivo, consideramos o conjunto $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$ de inteiros módulo q. Quando q é um número composto, o conjunto $\mathbb{Z}_q$ é estruturalmente diferente de quando q é primo, pois no primeiro nem todos os elementos são invertíveis, consequentemente não temos um corpo. Por esse motivo, usaremos a notação $\mathbb{F}_q$ para indicar essa diferença, sendo que $\mathbb{F}_q = \mathbb{Z}_q$, quando q é primo.

Definição 1.8. *Um código linear q-ário $\mathcal{C}$ em $\mathbb{Z}^n$ de comprimento n é um subgrupo aditivo de $\mathbb{Z}_q^n$.*

Por exemplo, $\mathcal{C} = \{\alpha(1,3); a \in \mathbb{Z}_5\} = \{(0,0), (1,3), (2,1), (3,4), (4,2)\}$ é um código linear em $\mathbb{Z}_5^2$.

Observação 4. *Se $q = p$ primo, um código linear é um subespaço de dimensão k no espaço vetorial $\mathbb{Z}_p^n = \mathbb{F}_p^n$, chamado um código (n, k). No exemplo anterior o código $\mathcal{C}$ é um subespaço de $\mathbb{Z}_5^2$ de dimensão 1 gerado pelo vetor (1,3) e usamos a notação $\mathcal{C} = \langle(1,3)\rangle$.*

A seguir estabelecemos uma conexão entre códigos lineares em $\mathbb{Z}_q^n$ e reticulados. Seja

$$\begin{aligned} \rho : \mathbb{Z} &\longrightarrow \mathbb{Z}_q \\ \mathbf{x} &\longmapsto \mathbf{x}(\bmod q) \end{aligned}$$

o mapeamento de redução à modulo q. Dado $a(\bmod q)$ sua pré-imagem ρ^{-1} é o conjunto de inteiros que são mapeados para a por ρ

Este mapeamento ρ pode ser definido componente a componente sobre um número arbitrário de n cópias de $\mathbb{Z}_q$, isto é,

$$\begin{aligned} \rho : \mathbb{Z}^n &\longrightarrow \mathbb{Z}_q^n \\ \mathbf{x} &\longmapsto \rho(\mathbf{x}) \end{aligned}$$

reduzindo à modulo q cada uma das n componentes.

Proposição 1.2. *Dado um subconjunto $\mathcal{S} \subset \mathbb{Z}_q^n$ então $\rho^{-1}(\mathcal{S})$ é um reticulado se, e somente se, $\mathcal{S}$ é um código linear em $\mathbb{Z}_q^n$.*

A demonstração desta Proposição pode ser encontrada no Capítulo 3 de (COSTA et al., 2017).

1.3 Reticulados obtidos a partir de códigos lineares

Nesta seção, descrevemos como construir reticulados pelas construções A e D a partir de códigos lineares q-ários, $q \in \mathbb{N}^*$. Apresentamos algumas propriedades dessas construções que serão utilizadas no Capítulos 2, as quais podem ser encontradas em Costa et al. (2017) no Capítulo 3.

1.3.1 Construção A

A construção A associa um reticulado Λ em $\mathbb{R}^n$ à um código linear em $\mathbb{Z}_q^n$, com $\mathbb{Z}_q$ sendo o conjunto de números inteiros módulo q.

Definição 1.9. *Seja $\mathcal{C}$ um código linear em $\mathbb{Z}_q^n$ os inteiros modulo um positivo inteiro $q \geqslant 2$. Seja $\rho : \mathbb{Z}^n \longrightarrow \mathbb{Z}_q^n$ o mapeamento de redução à modulo q coordenada a coordenada. Então, o reticulado $\Lambda_A(\mathcal{C}) = \rho^{-1}$ é dito obtido via construção A de um código linear q-ário.*

Um reticulado obtido por construção A também pode ser expresso como

$$\Lambda_A(\mathcal{C}) = \mathcal{C} + q\mathbb{Z}^n = \{\mathbf{x} \in \mathbb{R}^n; \mathbf{x} = \mathbf{c} + q\mathbf{z}, \text{com } \mathbf{c} \in \mathcal{C}, \mathbf{z} \in \mathbb{Z}^n\}.$$

Exemplo 2. *Consideremos* $\mathcal{C} = \langle(1,3)\rangle$ *em* $\mathbb{Z}_5^2$. *O reticulado obtido por construção A é a translação por pontos de* $5\mathbb{Z}^2$ *dos pontos*

$$\mathcal{C} = \langle(1,3)\rangle = \{(0,0),(1,3),(2,1),(3,4),(4,2)\}.$$

A Figura 2 ilustra o reticulado $\Lambda_A(\mathcal{C})$.

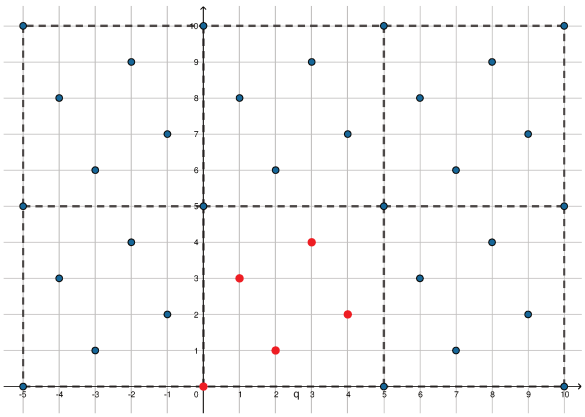


Figura 3 – Reticulado $\Lambda_A(\mathcal{C})$, com $\mathcal{C} = \langle(1,3)\rangle$ em $\mathbb{Z}_5$ destacado pelos pontos em vermelho.

Observação 5. *A distância mínima de reticulado* $\Lambda_A(\mathcal{C})$ *obtido por construção A de um código linear* $\mathcal{C}$ *para algum* $q \in \mathbb{Z}^*$ *é expressa como*

$$d_{min}(\Lambda_A(\mathcal{C})) = \min\{d_{min}(\mathcal{C}), q\}.$$

Proposição 1.3. *Se* $\Lambda_A(\mathcal{C})$ *é um reticulado q-ário associado com o código* $\mathcal{C} \subseteq \mathbb{Z}_q^n$ *então*

$$|\Lambda_A(\mathcal{C})/q\mathbb{Z}^n| = \frac{q^n}{Vol(\Lambda_A(\mathcal{C}))} = |\mathcal{C}|,$$

com $|\mathcal{C}|$ *o número de palavras código de* $\mathcal{C}$.

1.3.2 Construções D e $\bar{D}$

Referências para os resultados listados nesta subseção são Strey (2017) e Strey e Costa (2017). No decorrer do texto, utilizamos a inclusão natural $\sigma : \mathbb{Z}_q^n \to \mathbb{Z}^n$.

Definição 1.10 (Construção D)**.** *Seja* $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ *uma cadeia de códigos lineares. Dados números inteiros* $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_a \geqslant 0$ *e um conjunto de vetores* $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_l}\}$ *em* $\mathbb{Z}_q^n$ *tais que* $C_l = \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_{k_l}\rangle$, *para* $l = 1, 2, \ldots, a$. *O conjunto* Λ_D *consiste de todos os vetores da forma*

$$q\boldsymbol{z} + \sum_{l=1}^{a}\sum_{j=1}^{k_l} \beta_j^{(l)} \frac{1}{q^{l-1}} \sigma(\boldsymbol{b}_j),$$

com $\boldsymbol{z} \in \mathbb{Z}^n$ *e* $\beta_j^{(l)} \in \{0, 1, \cdots, q-1\}$.

Teorema 1.1. *Podemos reescrever o reticulado Λ_D como*

$$\Lambda_D = \left\{ \boldsymbol{z} + \sum_{s=1}^{a} \sum_{i=k_{s+1}+1}^{k_s} \alpha_i^{(s)} \frac{1}{q^{s-1}} \sigma(\boldsymbol{b}_i); \boldsymbol{z} \in q\mathbb{Z}^n, \alpha_i^{(s)} \in \mathbb{Z} \ \ e \ \ 0 \leqslant \alpha_i^{(s)} < q^s \right\}.$$

Teorema 1.2. *O conjunto Λ_D é um reticulado em $\mathbb{R}^n$ de posto completo.*

Exemplo 3. *Dados $k_1 = 2$, $k_2 = 1$, $\boldsymbol{b}_1 = (1,2)$, $\boldsymbol{b}_2 = (1,0) \in \mathbb{Z}_4^2$, temos a cadeia de códigos lineares $\mathbb{Z}_4^2 \supseteq C_1 \supseteq C_2$ tais que*

$$\begin{aligned} C_1 &= \langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle = \langle (1,2), (1,0) \rangle \\ C_2 &= \langle \boldsymbol{b}_1 \rangle = \langle (1,2) \rangle. \end{aligned}$$

Aplicando o Teorema 1.1, obtemos

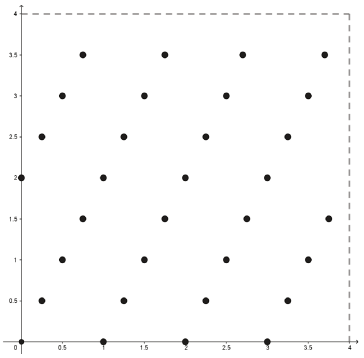
$$\Lambda_D = \{ \boldsymbol{z} + \alpha_1^{(2)}(1/4, 1/2) + \alpha_2^{(1)}(1,0); \boldsymbol{z} \in 4\mathbb{Z}^2, 0 \leqslant \alpha_2^{(1)} < 4, 0 \leqslant \alpha_1^{(2)} < 4^2 \}.$$

isto é,

$$\Lambda_D = \bigcup_{\boldsymbol{z} \in 4\mathbb{Z}^2} (\boldsymbol{z} + \Lambda_D \cap [0,4)^2)$$

e os elementos de $\Lambda_D \cap [0,4)^2$ estão representados na Figura 4

Figura 4 – Conjunto $\Lambda_D \cap [0,4)^2$.



Observação 6. *Um reticulado obtido pela Construção D depende dos parâmetros $k_1, \ldots, k_a$ e $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1}$.*

Teorema 1.3. *Se $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1} \in \mathbb{Z}_q^n$ são vetores linearmente independentes, então*

$$|\Lambda_D \cap [0,q)^n| = \prod_{s=1}^{a} (q^s)^{k_s - k_{s+1}}.$$

Observação 7. *No Exemplo 3, os vetores $\boldsymbol{b}_1 = (1,2)$ e $\boldsymbol{b}_2 = (0,1)$ são linearmente dependentes sobre $\mathbb{Z}_4$ e $|\Lambda_D \cap [0,4)^2| = 32 \neq 64 = \prod_{s=1}^{2} (4^s)^{k_s - k_{s+1}}$. Isto nos mostra que a hipótese de Teorema 1.3 é fundamental.*

Teorema 1.4. *Sejam $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_a \geqslant 0$ e $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_l} \in \mathbb{Z}_q^n$ não nulos tais que*

1. *$C_l = \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_{k_l} \rangle$, para $l = 1, 2, \ldots, a$.*
2. *Alguma permutação das colunas da matriz $M = (\sigma(\boldsymbol{b}_1) \cdots \sigma(\boldsymbol{b}_{k_1}))$ forma uma matriz triangular inferior na forma escalonada.*
3. *Para cada $j \in \{1, \ldots k_1\}$, a primeira componente não nula do vetor $\sigma(\boldsymbol{b}_j)$, digamos α_j, divide q e todas as demais componentes do mesmo.*

Se Λ_D é o reticulado obtido via Construção D a partir da cadeia $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ usando os parâmetros $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_a \geqslant 0$ e um conjunto de vetores $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_l}\}$ em $\mathbb{Z}_q^n$, então existe uma base para Λ_D formada pelos k_1 vetores $(1/q^{i-1})\sigma(\boldsymbol{b}_j)$, $1 \leqslant i \leqslant a$ e $k_{i+1} < j \leqslant k_i$, mais $n - k_1$ vetores da forma $(0, \cdots, 0, q, 0, \cdots, 0)^t$.

Corolário 1.1. *Sejam $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_a \geqslant 0$ e $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_l} \in \mathbb{Z}_q^n$ não nulos satisfazendo as condições 1, 2 e 3 do Teorema 1.4. Temos que*

$$det(\Lambda_D) = \left(\prod_{j=1}^{k_1} \alpha_j \right)^2 (q^2)^{n - \sum_{l=1}^{a} k_l}.$$

Exemplo 4. *Dados $k_1 = 2$, $k_2 = 1$, $\boldsymbol{b}_1 = (2, 2)$, $\boldsymbol{b}_2 = (0, 2) \in \mathbb{Z}_4^2$, temos a cadeia de códigos lineares $\mathbb{Z}_4^2 \supseteq C_1 \supseteq C_2$ tais que*

$$\begin{aligned} C_1 &= \langle (2,2), (0,2) \rangle \\ C_2 &= \langle (2,2) \rangle. \end{aligned}$$

Aplicando o Teorema 1.1, obtemos

$$\Lambda_D = \{ \boldsymbol{z} + \alpha_1^{(2)}(1/2, 1/2) + \alpha_2^{(1)}(0, 2); \boldsymbol{z} \in 4\mathbb{Z}^2, 0 \leqslant \alpha_2^{(1)} < 4, 0 \leqslant \alpha_1^{(2)} < 4^2 \}.$$

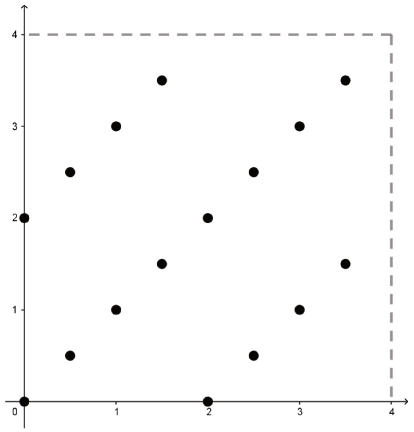
Os elementos de $\Lambda_D \cap [0, 4)^2$ estão representados na Figura 5

As condições 1, 2 e 3 do Teorema 1.4 são satisfeitas com $M = \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}$ e $\alpha_1 = \alpha_2 = 2$ dividindo q e, respectivamente, os outros componentes de b_j, com j = 1,2. Então, existe uma base para Λ_D formada pelos $k_1 = 2$ vetores da forma $(1/q^{i-1})\sigma(b_j)$, para $1 \leqslant i \leqslant 2$ e $k_{i+1} < j \leqslant k_i$. Ou seja, $\{(0, 2), (1/2, 1/2)\}$ é uma base para Λ_D e não necessitamos adicionar mais vetores pois $n = k_1$. Pelo Corolário 1.1,

$$det(\Lambda_D) = \left(\prod_{j=1}^{2} \alpha_j \right)^2 (q^2)^{n - \sum_{l=1}^{2} k_l} = (4^2) \cdot (4^2)^{-1} = 1.$$

Exemplo 5. *Reticulados importantes como $E_8, \Lambda_{16}, \Lambda_{24}$ podem ser obtidos via Construção D (STREY, 2017).*

Figura 5 – Conjunto $\Lambda_D \cap [0,4)^2$.



Teorema 1.5. *Sejam G_1 a matriz cujas colunas são os vetores $\sigma(\boldsymbol{b}_1), \ldots, \sigma(\boldsymbol{b}_{k_1})$ e $\mathcal{C}$ o código linear q^a-ário gerado pelas colunas da matriz $G = G_1 D$, em que $D = (d_{ij})$ é a matriz diagonal com*

$$d_{jj} = \begin{cases} 1, & \text{se } 1 \leqslant j \leqslant k_a \\ q, & \text{se } k_a \leqslant j \leqslant k_{a-1} \\ \vdots & \\ q^{a-1}, & \text{se } k_2 < j \leqslant k_1. \end{cases}$$

Temos que $q^{a-1}\Lambda_D = \Lambda_A(\mathcal{C})$.

Exemplo 6. *Consideremos novamente o reticulado obtido com $k_1 = 2$, $k_2 = 1$, $\boldsymbol{b}_1 = (2,2)$, $\boldsymbol{b}_2 = (0,2) \in \mathbb{Z}_4^2$, isto é,*

$$\Lambda_D = \{\boldsymbol{z} + \alpha_1^{(2)}(1/2, 1/2) + \alpha_2^{(1)}(0,2); \boldsymbol{z} \in 4\mathbb{Z}^2, 0 \leqslant \alpha_2^{(1)} < 4, 0 \leqslant \alpha_1^{(2)} < 4^2\}.$$

O reticulado $4\Lambda_D$ é um 16-ário, podendo ser obtido por Construção A a partir do código gerado por

$$G = \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 8 & 8 \end{pmatrix}.$$

Corolário 1.2. *A distância mínima do reticulado Λ_D é*

$$d_{min}(\Lambda_D) = \frac{d_{min}(\Lambda_A(C))}{q^{a-1}}.$$

A chamada Fórmula Código ou Construção $\bar{D}$ definida a seguir por Strey (2017) foi introduzida por Forney (a) e Forney (b) e tem sido usada em diversas aplicações. Mesmo quando construída para códigos binários, nem sempre é um reticulado (KOSITWATTANARERK; OGGIER., 2014), (KOSITWATTANARERK; OGGIER., 2013).

Definição 1.11 (Construção $\bar{D}$)**.** *Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq \cdots C_a$ uma cadeia de códigos lineares. O conjunto $\Gamma_{\bar{D}}$ é definido da seguinte forma*

$$\Gamma_{\bar{D}} = q^a\mathbb{Z}^n + q^{a-1}\sigma(C_1) + \cdots + q^1\sigma(C_{a-1}) + \sigma(C_a).$$

Exemplo 7. *Por exemplo, considerando $k_1 = 2$, $k_2 = 1$, $\boldsymbol{b}_1 = (1,2)$, $\boldsymbol{b}_2 = (3,1) \in \mathbb{Z}_5^2$, temos a cadeia de códigos lineares $\mathbb{Z}_5^2 \supseteq C_1 \supseteq C_2$ com*

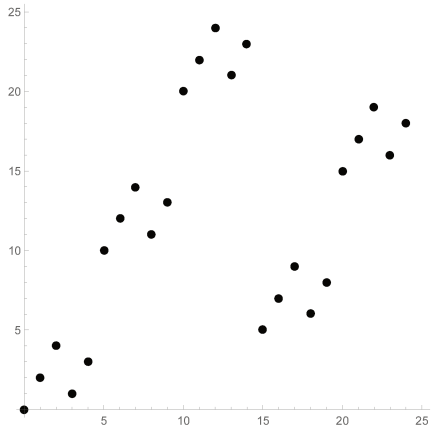
$$\begin{aligned} C_1 &= \langle (1,2),(3,1) \rangle = \{(0,0),(1,2),(2,4),(3,1),(4,3)\} \\ C_2 &= \langle (1,2) \rangle = \{(0,0),(1,2),(2,4),(3,1),(4,3)\}. \end{aligned}$$

Assim,

$$\Gamma_{\bar{D}} = 5^2\mathbb{Z}^2 + 5C_1 + C_2.$$

A Figura 6 ilustra os elementos de $\Gamma_{\bar{D}} \cap [0,5^2)^2$. Observamos que não é um reticulado.

Figura 6 – Elementos de $\Gamma_{\bar{D}}$ em $[0,5^2)^2$.



2 Constelações de Voronoi

Neste capítulo, apresentamos e ilustramos um resultado de Pietro e Boutros (2017) que nos permite construir constelações de Voronoi a partir de dois reticulados aninhados, isto é, $\Lambda_g \subseteq \Lambda_f$, com Λ_f obtido por construção A de códigos p-ários, p primo. Descrevemos e ilustramos o processo proposto neste artigo de codificação e mapeamento inverso para constelações de Voronoi. Generalizamos esta construção para Λ_f obtido de construções A e D de códigos q-ários, $q \in \mathbb{N}^*$. As principais referências utilizadas neste capítulo foram Pietro e Boutros (2017), Strey e Costa (2017), Zamir e Nazer (2014), Buglia e Lopes (2021), Costa et al. (2017).

2.1 Construção de constelações de Voronoi

Para construir constelações de Voronoi utilizamos dois reticulados, $\Lambda_g, \Lambda_f \subset \mathbb{R}^n$, ditos *reticulados aninhados*, isto é, $\Lambda_g \subseteq \Lambda_f$. Como Λ_g é um subgrupo de Λ_f podemos particionar Λ_f em classes laterais que formam o grupo quociente $\Lambda_f/\Lambda_g = \{\mathbf{x}+\Lambda_g; \mathbf{x} \in \Lambda_f\}$. O grupo quociente é o conjunto gerado pelas diferentes translações de Λ_g sobre os pontos de Λ_f. Cada classe lateral $\mathbf{x} + \Lambda_g = \{\mathbf{x} + \mathbf{y}; \mathbf{y} \in \Lambda_g\}$ é representada por $\mathbf{x}$, que é chamado de *líder da classe*. O número de elementos de Λ_f/Λ_g é igual a $\dfrac{Vol(\Lambda_g)}{Vol(\Lambda_f)}$ e todas as classes laterais estão representadas de maneira única pelos líderes que são os pontos de Λ_f que estão contidos num paralelotopo fundamental de Λ_g ((COSTA et al., 2017), Cap. 3).

Os pontos de Λ_f dentro da região de Voronoi na origem de Λ_g, $\mathcal{V}_{\Lambda_g}(\mathbf{0})$, também representam todas as classes do quociente Λ_f/Λ_g, mas podemos ter mais do que um líder da mesma classe para os pontos situados no bordo desta região.

Uma *constelação de Voronoi* para um par de reticulados aninhados, $\Lambda_g \subseteq \Lambda_f$, é uma seleção de líderes de Λ_f que representem univocamente todas as classes laterais de Λ_f/Λ_g e que tenham a menor norma dentro de cada classe. Ela será então composta por todos os elementos de Λ_f que estão no interior de $\mathcal{V}_{\Lambda_g}(\mathbf{0})$ mais uma seleção de pontos de Λ_f que estão no bordo de $\mathcal{V}_{\Lambda_g}(\mathbf{0})$ de modo a termos um único líder para cada classe.

A Figura 7(a) a ilustra um exemplo em duas dimensões de um par de reticulados aninhados com $\Lambda_f = \mathbb{Z}^2$ gerado pela matriz identidade 2×2 e Λ_g gerado pela matriz $M = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$.

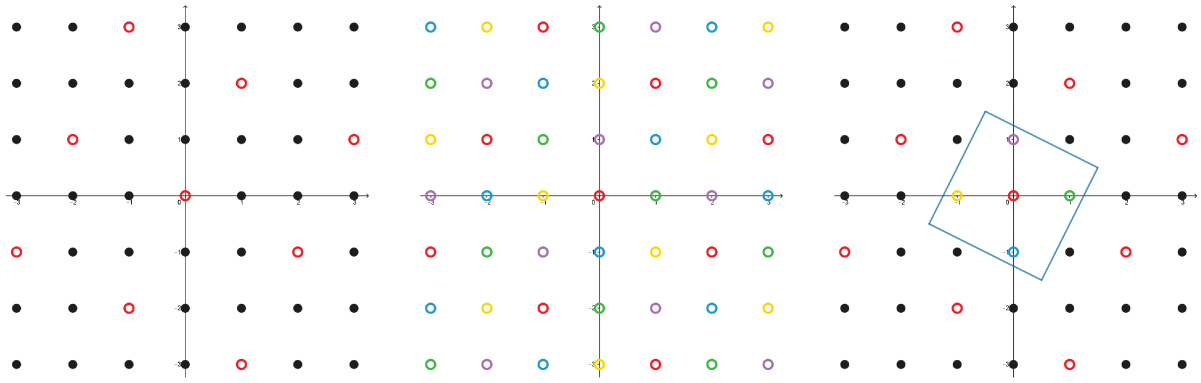
A Figura 7(b) ilustra as classes laterais $\mathbf{x} + \Lambda_g$ que particionam o reticulado Λ_f. Cada cor representa pontos de Λ_f em uma mesma classe lateral e podemos escolher qualquer ponto de uma classe como seu representante.

Figura 7 – Exemplo 1 de reticulados aninhados com as classes laterais de Λ_f/Λ_g e a constelação de Voronoi resultante.

(a) Par de reticulados aninhados $\Lambda_g \subset \Lambda_f$. Os pontos vermelhos representam Λ_g.

(b) Classes laterais de Λ_f/Λ_g. Cada cor representa elementos de Λ_f em uma classe lateral.

(c) Os cinco pontos no interior de $\mathcal{V}_{\Lambda_g}(\mathbf{0})$ formam a constelação de Voronoi $\mathcal{P} = \Lambda_f \cap \mathcal{V}_{\Lambda_g}(\mathbf{0})$.



A Figura 7(c) mostra um exemplo em que podemos obter univocamente um representante de cada classe lateral no interior da região de Voronoi de Λ_g centrada na origem. Mas, caso algum estivesse no bordo região de Voronoi, certamente haveria outro representante da mesma classe também no bordo e deveríamos fazer uma escolha entre eles. Por exemplo, se Λ_f e Λ_g são gerados, respectivamente, pelas matrizes

$$G_{\Lambda_f} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{e} \qquad M = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$$

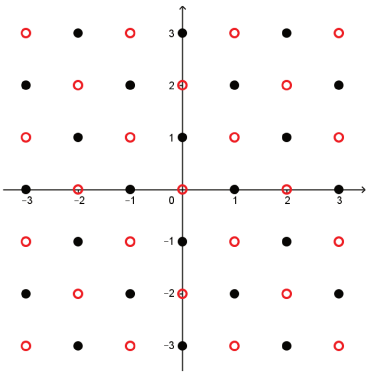
teremos pontos no bordo da região de Voronoi. A figura 8 ilustra esta situação. Observemos que neste caso há apenas duas classes laterais. A região de Voronoi de Λ_g na Figura 8(c) possui quatro representantes de uma mesma classe no bordo. Devemos considerar apenas um representante e, consequentemente, uma constelação de Voronoi é formada por um ponto vermelho e outro lilás.

As constelações de Voronoi também são conhecidas como *códigos reticulados*. Em termos de comunicação, o reticulado Λ_f é chamado de *reticulado de codificação* ou *reticulado fino* e Λ_g é conhecido como *reticulado de modelagem* ou *reticulado grosso*. Uma primeira ideia para balancear as grandezas que influenciam no processo de transmissão é modificar a distribuição dos pontos da constelação, alterando o espaçamento relativo entre eles. Isso é possível alterando o reticulado de codificação. Essa diminuição na potência mantendo a distância mínima ou o aumento da distância mínima mantendo a potência através da alteração relativa do espaçamento (densidade) dos pontos é chamado de ganho de codificação (*coding gain*) (FORNEY, 1989).

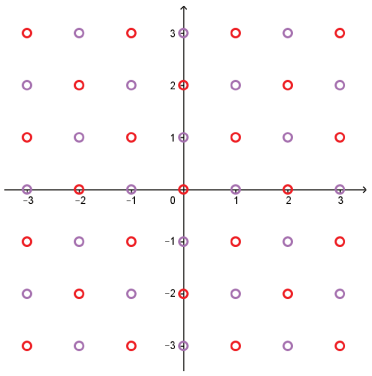
O reticulado de modelagem Λ_g determina a região que limita o código $\mathcal{C}$ e, consequentemente, a potência exigida para transmitir uma quantidade de palavras código. Assim, a segunda maneira é alterar a escolha dos pontos, sem modificar o posicionamento relativo entre eles é escolhendo o reticulado grosso com pequeno raio de cobertura. A

Figura 8 – Exemplo 2 de reticulados aninhados com as classes laterais de Λ_f/Λ_g e a constelação de Voronoi resultante.

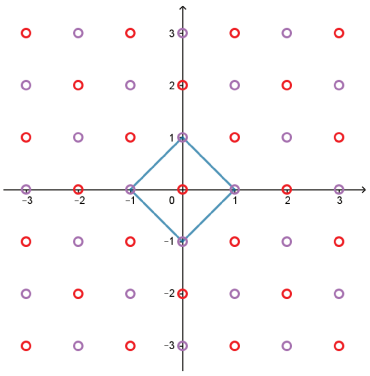
(a) Par de reticulados aninhados $\Lambda_g \subset \Lambda_f$. Os pontos em vermelho representam Λ_g.



(b) Classes laterais de Λ_f/Λ_g. Cada cor representa elementos de Λ_f em uma classe lateral.



(c) A origem e um dos pontos em lilás no bordo formam uma constelação de Voronoi.



redução resultante na potência do sinal é chamada ganho de modelagem (*shaping gain*). Como destacado em Forney (1989) bons reticulados para codificação estão em geral associados a boa taxa de empacotamento, enquanto para reticulados de modelagem um parâmetro importante é a taxa de cobertura (para detalhes sobre esses parâmetros ver Costa et al. (2017)).

A busca pelos representantes das classes laterais com menor norma euclidiana não é simples. Pietro e Boutros (2017) apresentam um resultado que nos permite encontrar inicialmente um conjunto completo de representantes de cada classe lateral quando Λ_f é obtido por Contrução A de um código p-ário e o reticulado Λ_g está contido em $p\mathbb{Z}^n$, p primo. Entretanto, esses não estão na região de Voronoi. Assim, após determinar este conjunto é necessário realizar uma operação para encontrar os líderes com menor norma euclidiana.

Vimos na Observação 1 que todo reticulado em $\mathbb{Z}^n$ de posto máximo admite uma matriz geradora triangular inferior obtida pela Forma Normal de Hermite. Por outro lado, se considerarmos a base associada à esta matriz na ordem inversa teremos também uma matriz geradora triangular superior para estes reticulados, como é assumido na próxima proposição.

Proposição 2.1 ((PIETRO; BOUTROS, 2017)). *Sejam $\Lambda_f = \mathcal{C} + p\mathbb{Z}^n$ um reticulado obtido pela construção A de um código linear p-ário, $\Gamma \subseteq \mathbb{Z}^n$ um reticulado inteiro e $\Lambda_g = p\Gamma \subseteq p\mathbb{Z}^n$, p primo. Consideramos T uma matriz geradora de Γ triangular superior*

com $t_{i,i} > 0$ *para todo* i*:*

$$T = \begin{pmatrix} t_{1,1} & t_{1,2} & \cdots & t_{1,n} \\ 0 & t_{2,2} & \cdots & t_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & t_{n,n} \end{pmatrix}, \text{ com } t_{i,j} \in \mathbb{Z}.$$

e $\mathcal{S} = \{0, \ldots, t_{1,1} - 1\} \times \cdots \times \{0, \ldots, t_{n,n} - 1\}$.

Então, $\mathcal{C} + p\mathcal{S} = \{\boldsymbol{c} + p\boldsymbol{s} \in \mathbb{Z}^n; \boldsymbol{c} \in \mathcal{C}, \boldsymbol{s} \in \mathcal{S}\}$ *é um conjunto completo de líderes das classes laterais de* Λ_f/Λ_g.

Demonstração. Vamos primeiramente mostrar que $\mathcal{C} + p\mathcal{S}$ e Λ_f/Λ_g possuem a mesma cardinalidade. Inicialmente, temos que $|\mathcal{C} + p\mathcal{S}| \leqslant |\mathcal{C}||\mathcal{S}|$. A igualdade também é valida uma vez que supondo $\mathbf{c} + p\mathbf{s} = \mathbf{d} + p\mathbf{t}$ para $\mathbf{c}, \mathbf{d} \in \mathcal{C} \subseteq \{0, 1, \ldots, p-1\}^n$ e $\mathbf{s}, \mathbf{t} \in \mathcal{S}$, temos que $\mathbf{c} - \mathbf{d} = p(\mathbf{t} - \mathbf{s})$. Então, $\mathbf{c} \equiv \mathbf{d} \bmod p$. Isso significa que $\mathbf{c} = \mathbf{d}$, pois todos $c_i's$ e $d_i's$ estão em $\{0, 1, \ldots, p-1\}$, para todo $i = 1, \ldots, n$.

Assim, $\mathbf{c} - \mathbf{d} = \mathbf{0} = p(\mathbf{t} - \mathbf{s})$. O que nos diz que $\mathbf{t} - \mathbf{s} = \mathbf{0}$ e, portanto, $\mathbf{t} = \mathbf{s}$. Logo, cada par $(\mathbf{c}, \mathbf{s}) \in \mathcal{C} \times \mathcal{S}$ representa um ponto diferente em $\mathcal{C} + p\mathcal{S}$ e, assim, $|\mathcal{C} + p\mathcal{S}| = |\mathcal{C}||\mathcal{S}|$.

Agora, pelo fato de T ser triangular e pela definição de $\mathcal{S}$ temos que

$$\begin{aligned} Vol(\Lambda_g) = Vol(p\Gamma) &= p^n Vol(\Gamma) \\ &= p^n det(T) \\ &= p^n \prod_{i=1}^{n} t_{i,i} = p^n |\mathcal{S}|. \end{aligned}$$

Pela Proposição 2.5.1 de Zamir e Nazer (2014) temos que $Vol(\Lambda_f) = p^{n-k}$. Assim,

$$|\Lambda_f/\Lambda_g| = \frac{Vol(\Lambda_g)}{Vol(\Lambda_f)} = \frac{Vol(\Lambda_g)}{p^{n-k}}.$$

Portanto,

$$|\mathcal{C} + p\mathcal{S}| = |\mathcal{C}||\mathcal{S}| = p^k \frac{Vol(\Lambda_g)}{p^n} = \frac{Vol(\Lambda_g)}{p^{n-k}} = |\Lambda_f/\Lambda_g|.$$

Por fim, é suficiente mostrar agora que cada dois elementos de $\mathcal{C} + p\mathcal{S}$ pertencem a classes laterais distintas ou, equivalentemente, que se $\mathbf{x}, \mathbf{y} \in \mathcal{C} + p\mathcal{S}$ pertencem a uma mesma classe lateral então $\mathbf{x} = \mathbf{y}$. De fato, $\mathbf{x} = \mathbf{c} + p\mathbf{s}$ e $\mathbf{y} = d + p\mathbf{t}$ estão em uma mesma classe lateral se, e somente se, $\mathbf{x} - \mathbf{y} = \mathbf{c} - \mathbf{d} + p(\mathbf{s} - \mathbf{t}) \in \Lambda_g \subseteq p\mathbb{Z}^n$. Isso vale somente se $\mathbf{c} - \mathbf{d} \in p\mathbb{Z}^n$ e consequentemente se $c_i - d_i = 0$ para $i = 1, \ldots, n$, pois 0 é o único elemento de $p\mathbb{Z}$ que pode ser obtido subtraindo dois números de $\{0, 1, \ldots, p-1\}$. Então $\mathbf{x}$ e $\mathbf{y}$ estão na mesma classe lateral somente se $\mathbf{c} = \mathbf{d}$ e $\mathbf{x} - \mathbf{y} = p(\mathbf{s} - \mathbf{t}) \in \Lambda_g = p\Gamma$. Isso nos diz que $\mathbf{s} - \mathbf{t} = T\mathbf{z}$ para algum $z \in \mathbb{Z}^n$.

Seja U a inversa de T: que também é triangular superior e $u_{i,i} = t_{i,i}^{-1}$. Temos que $U(s-t) = z$ implica que

$$z_i = \sum_{j=1}^{n} (s_j - t_j)u_{i,j} \in \mathbb{Z}, \text{para cada i} = 1, \ldots, \text{n}.$$

Quando $i = n$, temos $(s_n - t_n)t_{n,n}^{-1} \in \mathbb{Z}$, o que implica que $s_n - t_n = 0$ pois, pela definição de $\mathcal{S}$ temos que $|s_n - t_n| \leqslant t_{n,n} - 1 < t_{n,n}$. Usando a igualdade $s_n = t_n$ no caso $i = n-1$, obtemos que $s_{n-1} = t_{n-1}$. Repetindo esse processo recursivamente para $i = n-2, n-3, \ldots, 1$ concluímos que $s_i = t_i$ para cada $i = 1, \ldots, n$ e, consequentemente, $s = t$. Portanto, $x = y$. □

Exemplo 8. *Escolhendo $n = 2$, $k = 1$ e $p = 5$ e tomando o reticulado Γ com matriz geradora dada por*

$$T = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \in \mathbb{Z}^{2\times 2},$$

portanto o conjunto $\mathcal{S} = \{0,1\} \times \{0,1\}$.

Definimos $\Lambda_g = 5\Gamma \subseteq 5\mathbb{Z}^2$. Assim, uma matriz geradora para esse reticulado é

$$5T = \begin{pmatrix} 10 & 5 \\ 0 & 10 \end{pmatrix}.$$

Agora, para construir Λ_f é necessário um código linear $\mathcal{C} \in \mathbb{Z}_5^2$, para ser utilizado na construção A. Consideremos $\mathcal{C} = \langle (1,2) \rangle = \{(0,0), (1,2), (2,4), (3,1), (4,3)\}$. Consequentemente, $\Lambda_f = \mathcal{C} + 5\mathbb{Z}^2$. Neste caso, uma matriz geradora para Λ_f é ((COSTA et al., 2017))

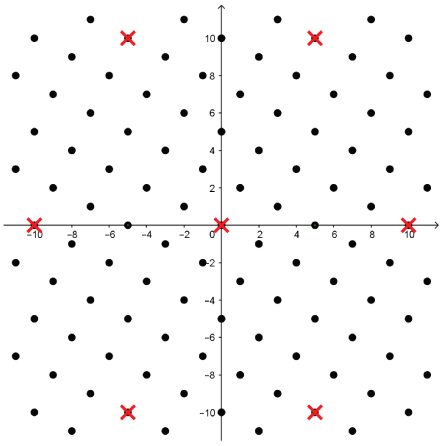
$$G_{\Lambda_f} = \begin{pmatrix} 1 & 0 \\ 2 & 5 \end{pmatrix}.$$

A Figura 9(a) ilustra os reticulados Λ_g e Λ_f, os pontos " • " indicam o reticulado Λ_f e os "×" o reticulado Λ_g. Pelo Lema, o conjunto $\mathcal{C} + p\mathcal{S} = \{\boldsymbol{c} + p\boldsymbol{s} \in \mathbb{Z}^2; \boldsymbol{c} \in \mathcal{C}, \boldsymbol{s} \in \mathcal{S}\} = \{(0,0), (1,2), (2,4), (3,1), (4,3), (0,5), (1,7), (2,9), (3,6), (4,8), (5,0), (6,2), (7,4), (8,1), (9,3), (5,5), (6,7), (7,9), (8,6), (9,8)\}$ é um conjunto completo de líderes das classes de Λ_f/Λ_g. A Figura 9(b) ilustra esse conjunto.

Observamos neste exemplo que os pontos de $C + p\mathcal{S}$ não pertencem ao paralelotopo associado à matriz geradora que usamos para construir Λ_g, como pode ser visto na Figura 10(a). Entretanto, esses pontos pertencem a uma outra região fundamental que também ladrilha do plano. Isto pode ser observado na Figura 10(b).

Figura 9 – Exemplo para reticulados Λ_g e Λ_f no plano.

(a) Reticulados Λ_g e Λ_f.



(b) Conjunto $C + p\mathcal{S}$ destacado.

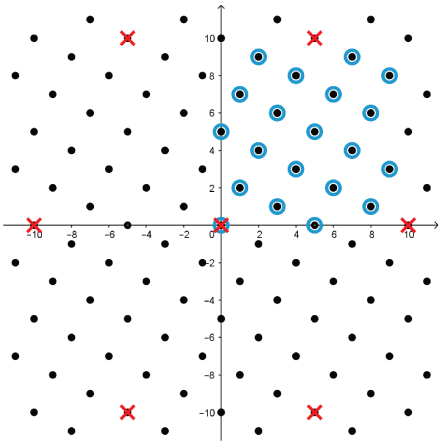
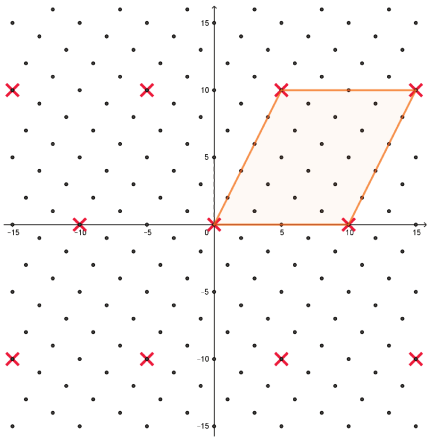
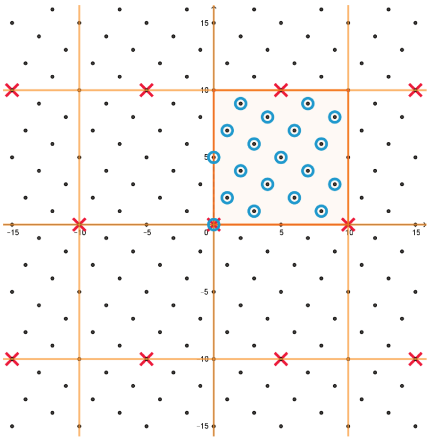


Figura 10 – Regiões fundamentais do reticulado Λ_g.

(a) Paralelotopo associado à matriz geradora de Λ_g.



(b) Um exemplo de região fundamental ladrilhando o plano.



Para construir a constelação de Voronoi, precisamos encontrar os líderes das classes laterais que possuem norma euclidiana mínima, que estarão no interior da região de Vornoi de Λ_g. Para isto, consideramos

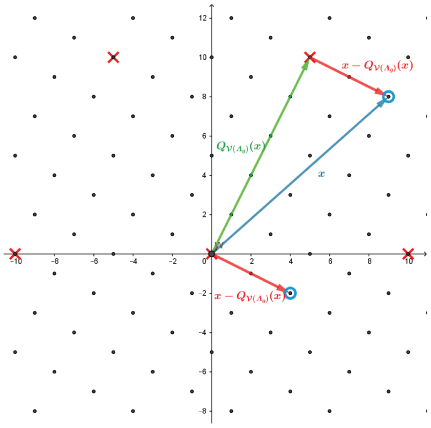
$$\begin{aligned} \mathcal{Q}_{\mathcal{V}(\Lambda)}(\cdot) : \mathbb{R}^n &\longrightarrow \Lambda_g \\ \boldsymbol{y} &\longmapsto arg\ min_{\boldsymbol{z}\in\Lambda_g}||\boldsymbol{z}-\boldsymbol{y}|| \end{aligned}$$

Assim, dado um líder $\boldsymbol{y}$ da classe lateral , o seu representante com norma euclidiana mínima é obtido fazendo $\boldsymbol{y} - \mathcal{Q}_{\mathcal{V}(\Lambda_g)}(\boldsymbol{y})$. A Figura 11(a) ilustra essa operação para o ponto $\boldsymbol{x} = (9, 8)$ em especial, com $\mathcal{Q}_{\mathcal{V}(\Lambda_g)}(\boldsymbol{x}) = (5, 10)$. Assim, temos $\boldsymbol{x} - \mathcal{Q}_{\mathcal{V}(\Lambda_g)}(\boldsymbol{x}) = (9, 8) - (5, 10) = (4, -2)$. A Figura 11(b) ilustra a constelação de Voronoi obtida com esse exemplo ao realizar essa operação para todos os pontos do conjunto $\mathcal{C} + 5\mathcal{S}$.

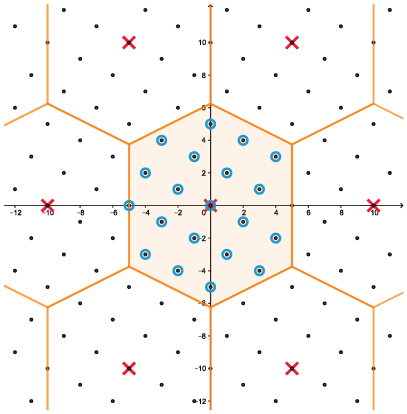
No Exemplo 8 a quantização do ponto $(5, 0)$ pode ser tanto o ponto $(10, 0) \in \Lambda_g$ quanto $(0, 0) \in \Lambda_g$. Nesses casos, escolhemos arbitrariamente qual ponto tomar e essa escolha

Figura 11 – Construção da constelação de Voronoi.

(a) Operação para $\mathbf{x} = (9, 8)$.



(b) Constelação de Voronoi resultante.



determinará qual representante será considerado. No caso, escolhemos $\mathcal{Q}_{\mathcal{V}(\Lambda_g)}(5, 0) = (10, 0)$ gerando o líder $(-5, 0)$. Caso escolhêssemos $\mathcal{Q}_{\mathcal{V}(\Lambda_g)}(5, 0) = (0, 0)$, o líder gerado seria $(5, 0)$, ambos estão na borda. Vale ressaltar que a estratégia adotada aqui automaticamente soluciona as ambiguidades da borda.

2.2 Codificação

A codificação de constelações de Voronoi pode ser feita com base na Proposição 2.1. Como detalhado em Pietro e Boutros (2017) esse procedimento difere do que normalmente é feito para reticulados obtidos por construção A, possibilitando construir constelações de Voronoi com complexidade de codificação linear, enquanto que, normalmente, a complexidade possui ordem n^2. Descrevemos e ilustramos a seguir esse processo:

1. Cada uma dos elementos da Constelação de Voronoi será representado por vetores inteiros do conjunto $\mathcal{M} = \mathbb{F}_p^k \times \mathcal{S}$.

2. Seja $\mathbf{m} = (\mathbf{u}, \mathbf{s}) \in \mathcal{M}$ uma palavra a ser codificada com $\mathbf{u} \in \mathbb{F}_p^k$ e $\mathbf{s} \in \mathcal{S}$. Seja $\mathbf{c}$ a palavra código de $\mathcal{C}$ associada com $\mathbf{u}$, isto é, $\mathbf{c} = enc_{\mathcal{C}}(\mathbf{u})$ com $enc_{\mathcal{C}} : \mathbb{F}_p^k \longrightarrow \mathbb{F}_p^n$.

3. Consideramos $\mathbf{x}' = \mathbf{c} + p\mathbf{s} \in \Lambda_f$.

4. Seja $\mathcal{Q}_{\mathcal{V}(\Lambda)}(\cdot)$ o quantizador associado com a região de Voronoi do reticulado de modelagem. Então, a mensagem $\mathbf{m}$ é codificada para

$$\mathbf{x} = \mathbf{x}' - \mathcal{Q}_{\mathcal{V}(\Lambda_g)}(\mathbf{x}') \in \mathcal{C} = \Lambda_f \cap \mathcal{V}_{\Lambda_g}(0).$$

Notemos que $\mathbf{x}'$ e $\mathbf{x}' - \mathcal{Q}_{\mathcal{V}(\Lambda_g)}(\mathbf{x}')$ representam a mesma classe lateral. Isso garante que cada duas mensagens diferentes sejam codificadas para diferentes elementos da constelação de Voronoi.

Exemplo 9. *Seja* Γ *obtido por* $T = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$, $\Lambda_g = 5\Gamma$ *e* $\Lambda_f = \mathcal{C} + 5\mathbb{Z}^2$, *com* $\mathcal{C} = \langle (1,2) \rangle$ *em* $\mathbb{Z}_5^2$.

1. $\mathcal{M} = \mathbb{Z}_5 \times \{0,1\} \times \{0,1\}$.
2. *Suponhamos* $\boldsymbol{m} = (\boldsymbol{u}, \boldsymbol{s}) = (2|0,1)$. *Então, a palavra código* $\boldsymbol{c}$ *associada a* $\boldsymbol{u}$ *é*

$$\boldsymbol{c} = (G\boldsymbol{u}) \bmod 5 = (2(1,2)) \bmod 5 = (2,4).$$

3. *Seja* $\boldsymbol{x'} = \boldsymbol{c} + 5\boldsymbol{s} = (2,4) + 5(0,1) = (2,9)$
4. *Assim, a mensagem* $\boldsymbol{m}$ *é codificada para a palavra código do reticulado* Λ_f

$$\boldsymbol{x} = \boldsymbol{x'} - Q_{\mathcal{V}(\Lambda_g)}(\boldsymbol{x'}) = (2,9) - (5,10) = (-3,-1) \in \mathcal{P} = \Lambda_f \cap \mathcal{V}_{\Lambda_g}(0).$$

2.3 Mapeamento inverso

No processo de comunicação baseado em codificação de pontos da constelações de Voronoi é necessário especificar como se realiza o mapeamento inverso. Nesta seção, descrevemos como recuperar $\mathbf{m} = (\mathbf{u}, \mathbf{s})$ de uma palavra $\mathbf{x}$ da constelação de Voronoi. Para isso, aplicamos as seguintes etapas:

1. Temos que $\mathbf{x} = \mathbf{x}' - \mathcal{Q}_{\mathcal{V}(\Lambda)}(\mathbf{x}') = \mathbf{c} + p\mathbf{s} - \mathcal{Q}_{\mathcal{V}(\Lambda)}(\mathbf{x}')$. Notemos que para qualquer $\mathbf{y} \in \mathbb{R}^n$ temos que $\mathcal{Q}_{\mathcal{V}(\Lambda)}(\mathbf{y}) \in \Lambda_g = p\Gamma \subseteq p\mathbb{Z}^n$. Portanto, é possível obter $\mathbf{c}$ simplesmente reduzindo $\mathbf{x}$ módulo p.

2. De modo geral, vamos supor que as palavras códigos de $\mathcal{C}$ foram codificadas com a matriz geradora na forma sistemática. Assim, $\mathbf{u}$ é obtido automaticamente considerando as k primeiras entradas de $\mathbf{c}$.

3. Agora precisamos calcular $\mathbf{s}$. Como conhecemos $\mathbf{x}$ e $\mathbf{c}$ podemos calcular

$$\mathbf{r} = \frac{(\mathbf{x} - \mathbf{c})}{p} = \frac{\mathbf{c} + p\mathbf{s} - \mathcal{Q}_{\mathcal{V}(\Lambda)}(\mathbf{x}') - \mathbf{c}}{p} = \mathbf{s} - \frac{1}{p}\mathcal{Q}_{\mathcal{V}(\Lambda)}(\mathbf{x}') = \mathbf{s} - \mathbf{q} \in \mathbb{Z}^n,$$

   para algum $\mathbf{q} \in \Gamma = p^{-1}\Lambda_g$. Particularmente, como T é uma matriz geradora de Γ triangular superior, podemos reescrever $\mathbf{r} = \mathbf{s} - T\mathbf{z}$ para algum $\mathbf{z} \in \mathbb{Z}^n$.

4. Pela triangularidade da matriz T temos que a i-ésima coordenada de $\mathbf{r}$ é expressa como
$$r_i = s_i - z_i t_{i,i} - \sum_{j=i+1}^{n} z_j t_{i,j}.$$
Para $i = n$ temos
$$s_n = r_n + z_n t_{n,n}. \tag{2.1}$$
Nossa intenção é determinar s_n. Da expressão 2.1 e da maneira como definimos o conjunto $\mathcal{S}$ podemos determinar s_n unicamente pelas seguintes condições:
   - $s_n \equiv r_n \mod t_{n,n}$;
   - $0 \leqslant s_n \leqslant t_{n,n} - 1$.

   Assim, depois de calcular s_n podemos obter z_n em 2.1.

5. Para $i = n - 1$ temos
$$s_{n-1} = r_{n-1} + z_{n-1} t_{n-1,n-1} + z_n t_{n-1,n}. \tag{2.2}$$
Os únicos desconhecidos são s_{n-1} e z_{n-1} e, similarmente, podemos determinar s_{n-1} pelas condições:
   - $s_{n-1} \equiv r_{n-1} + z_n t_{n-1,n} \mod t_{n-1,n-1}$;
   - $0 \leqslant s_{n-1} \leqslant t_{n-1,n-1} - 1$.

   Obtido s_{n-1} podemos calcular z_{n-1} de 2.2.

6. Usando essa estratégia recursivamente para $i = n-2, n-3, \ldots, 1$ obtemos s_i e recuperamos $\mathbf{m} = (\mathbf{u}, \mathbf{s})$.

Exemplo 10. *1. Dado $\boldsymbol{x} = (-3, -1)$ obtemos $\boldsymbol{c}$ reduzindo $\boldsymbol{x}$ à $\mod 5$, isto é, $\boldsymbol{c} = (2, 4)$.*

2. Supondo que a codificação foi feita com a matriz geradora de $\mathcal{C}$ na forma sistemática, então $\boldsymbol{u} = (2)$.

3. Temos $\boldsymbol{r} = \dfrac{\boldsymbol{x} - \boldsymbol{c}}{5} = \dfrac{(-3, -1) - (2, 4)}{5} = (-1, -1)$.
Dai, quando $i = 2$:
   - $s_2 \equiv r_2 \mod t_{2,2}$
   - $0 \leqslant s_2 < t_{2,2}$

   Ou seja, $s_2 \equiv -1 \mod 2$ e $0 \leqslant s_2 < 2$ então $s_2 = 1$.

   Quando $i = 1$:

- $s_1 \equiv r_1 + z_1 t_{1,2} \mod t_{1,1}$
- $0 \leqslant s_2 < t_{1,1}$

Assim, $s_1 \equiv -1 - 1 \mod 2$ *e* $0 \leqslant s_2 < 2$. *Então,* $s_1 = 0$. *Logo,* $\boldsymbol{m} = (2|0, 1)$.

2.4 Extensões da Proposição 2.1

Para um código linear q-ário, $\mathcal{C} \subset \mathbb{N}_q^n, q \in \mathbb{N}^*$, sabemos que ((COSTA et al., 2017), Cap. 2) para o reticulado Λ_f obtido de construção A de $\mathcal{C}$, temos $\frac{q^n}{Vol(\Lambda_f)} = |\mathcal{C}|$, ou seja, $Vol(\Lambda_f) = \frac{q^n}{|\mathcal{C}|}$.

Observamos então que todos os argumentos usado na demonstração da Proposição 2.1 são ainda válidos para códigos lineares em $\mathbb{Z}_q^n$, com a única diferença que para um código $\mathcal{C}$ gerado por k elementos não satisfaz necessariamente $|\mathcal{C}| = q^{n-k}$. Isto irá ocorrer quando estes geradores forem linearmente independentes em $\mathbb{Z}_q^n$.

Desta forma, considerando os vetores geradores linearmente independentes em $\mathbb{Z}_q^n$, a construção proposta na Proposição 2.1 para obtenção de um conjunto completo de líderes de Λ_f/Λ_g pode ser estendida para códigos lineares q-ários e apresentamos esta extensão a seguir.

Proposição 2.2 (Extensão da Proposição 2.1 para códigos lineares q-ários)**.** *Sejam* $\Lambda_f = \mathcal{C} + q\mathbb{Z}^n$ *um reticulado obtido pela construção A de um código linear q-ário gerado por vetores linearmente independentes,* $\Gamma \subseteq \mathbb{Z}^n$ *um reticulado inteiro e* $\Lambda_g = q\Gamma \subseteq q\mathbb{Z}^n$, $q \in \mathbb{N}^*$. *Consideramos* T *uma matriz geradora de* Γ *triangular superior com* $t_{i,i} > 0$ *para todo* i*:*

$$T = \begin{pmatrix} t_{1,1} & t_{1,2} & \cdots & t_{1,n} \\ 0 & t_{2,2} & \cdots & t_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & t_{n,n} \end{pmatrix}, \text{ com } t_{i,j} \in \mathbb{Z}.$$

e $\mathcal{S} = \{0, \ldots, t_{1,1} - 1\} \times \cdots \times \{0, \ldots, t_{n,n} - 1\}$.

Então, $\mathcal{C} + q\mathcal{S} = \{\boldsymbol{c} + p\boldsymbol{s} \in \mathbb{Z}^n; \boldsymbol{c} \in \mathcal{C}, \boldsymbol{s} \in \mathcal{S}\}$ *é um conjunto completo de líderes das classes laterais de* Λ_f/Λ_g.

Observação 8. *É importante notar na Proposição anterior que como existe um conjunto de* k *geradores linearmente independentes em* $\mathbb{Z}_q$ *para o código* $\mathcal{C} \subseteq \mathbb{Z}_q^n$, *teremos* $|\mathcal{C}| = q^k$ *e, além disso, a menos de uma troca de linhas teremos (COSTA et al., 2017) matrizes geradoras na forma padrão para o código e para o reticulado na forma*

$$\begin{pmatrix} I_{k\times k} \\ B \end{pmatrix} e \begin{pmatrix} I_{k\times k} & O \\ B & qI_{(n-k)\times(n-k)} \end{pmatrix}, \text{ em que } B \text{ tem elementos inteiros entre 0 e q-1.}$$

Portanto, considerando os termos da base na ordem inversa temos uma matriz geradora na forma triangular superior.

De qualquer forma, mesmo para códigos lineares quaisquer podemos obter uma matriz geradora para Λ_f a partir da Forma Normal de Hermite (1) por colunas, invertendo a ordem da base, de uma matriz que contém nas colunas geradores do código e os vetores do tipo qe_i, para $i = 1, \ldots, n$.

A proposição 2.1 pode ser estendida para reticulados Λ_f obtidos por construção D e apresentamos esta extensão a seguir. A vantagem em utilizar essa construção está em realizar uma decodificação multi-estágio que apresenta bom desempenho e eficiência em esquemas de codificação multinível (MATSUMINE B. M. KURKOSKI, 2018), (SILVA; SILVA, 2019). Além disso, é possível construir reticulados importantes utilizando códigos mais simples. Para essa extensão, vamos usar o fato que dado um reticulado Λ_D obtido por construção D de uma sequência de a códigos q-ários e que $q^{a-1}\Lambda_D$ pode ser identificado como construção A do código q^a-ário $\mathcal{X}$ expresso como o conjunto $\mathcal{X} = q^{a-1}\Lambda_D \cap [0, q^a)^n$ (STREY, 2017).

Proposição 2.3 (Extensão da Proposição 2.1 para reticulados obtidos por Construção D)**.** *Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ uma cadeia de códigos q-ários lineares e seja $\Lambda_f = q^{a-1}\Lambda_D$, com Λ_D obtido por construção D. Seja Γ um reticulado inteiro e T uma matriz geradora triangular superior de Γ com entradas t_{ij} e $\Lambda_g = q^a\Gamma$. Temos então que para*

$$\mathcal{X} = \Lambda_f \cap [0, q^a)^n = \left(\sum_{s=1}^{a} \sum_{i=k_{s+1}+1}^{k_s} \alpha_i^{(s)} q^{a-s} \sigma(b_i) \right) \bmod q^a$$

com $\alpha_i^{(s)} \in \mathbb{Z}$ e $0 \leqslant \alpha_i^{(s)} < q^s$, um conjunto completo de representantes de Λ_f/Λ_g é dado por

$$\mathcal{X} + q^a\mathcal{S}$$

com $\mathcal{S} = \{0, \ldots, t_{1,1} - 1\} \times \cdots \times \{0, \ldots, t_{n,n} - 1\}$.

Observação 9. *O número de classes laterais em Λ_f/Λ_g na Proposição anterior é $|\mathcal{X}| \cdot t_{1,1} \cdot \cdots \cdot t_{n,n}$. No caso em que o código C_1 é gerado por um conjunto de vetores linearmente independentes em $\mathbb{Z}_q$ fica mais simples determinar o código $\mathcal{X}$ que gera Λ_f por construção A. Ilustramos isto no exemplo a seguir.*

Exemplo 11. *Sejam $\boldsymbol{b}_1 = (2, 1, 0)$, $\boldsymbol{b}_2 = (0, 1, 3) \in \mathbb{Z}_4^3$ e $k_1 = 2$ e $k_2 = 1$. Temos a cadeia de códigos lineares $\mathbb{Z}_4^3 \supseteq C_1 \supseteq C_2$ com*

$$\begin{aligned} C_1 &= \langle (2, 1, 0), (0, 1, 3) \rangle \\ C_2 &= \langle (2, 1, 0) \rangle. \end{aligned}$$

Pela Proposição 2.3, utilizamos $\Lambda_f = 4\Lambda_D$ *com*

$$\Lambda_f = 4\Lambda_D = \{z + \alpha_1^{(2)}(2,1,0) + \alpha_2^{(1)}4(0,1,3); z \in 4^2\mathbb{Z}^2, 0 \leqslant \alpha_2^{(1)} < 4, 0 \leqslant \alpha_1^{(2)} < 4^2\}.$$

Pelo Teorema 1.5, $4\Lambda_D$ *é um 16-ário gerado pelo código* $\mathcal{X}$ *obtido pela matriz*

$$G = G_1 D = \begin{pmatrix} 2 & 0 \\ 1 & 1 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}.$$

Como b_1 *e* b_2 *são linearmente independentes em* $\mathbb{Z}_{16}$ *e, a menos por uma troca de linhas, podemos reescrever a matriz* $\bar{G}_1$ *do código equivalente na forma sistemática com* $\bar{G}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 2 & 2 \end{pmatrix}$.

Isto nos permite calcular a quantidade de palavras códigos que existem em $\mathcal{X}$. *De fato, temos agora*

$$\bar{G} = \bar{G}_1 D = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 4 \\ 2 & 8 \end{pmatrix}.$$

As palavras códigos de $\mathcal{X}$ *são da forma*

$$\alpha_1 \boldsymbol{w}_1 + \alpha_2 \boldsymbol{w}_2 = \alpha_1(1,0,2) + \alpha_2(0,4,8), \text{ com } \alpha_i \in \mathbb{Z}_{16}, i = 1,2.$$

A quantidade de palavras códigos de $\mathcal{C}$, $|\mathcal{C}|$, *é o números de combinações lineares distintas que podemos obter de* $\boldsymbol{w}_1$ *e* $4\boldsymbol{w}_2$ *com* $\boldsymbol{w}_1$ *e* $\boldsymbol{w}_2$ *L.I. em* $\mathbb{Z}_{16}$. *Para* α_1 *há* $4^2 = 16$ *possibilidades e para* α_2 *são 4 (pois, a partir do 4 as palavras começam a se repetirem). Logo,* $|\mathcal{X}| = 4^2 \cdot 4 = 64$.

Assim, pela Proposição 1.3, temos que

$$Vol(\Lambda_f) = \frac{(q^a)^n}{|\mathcal{C}|} = \frac{(4^2)^3}{4^2 \cdot 4} = 64.$$

Agora, seja Γ *gerado pela matriz* $T = \begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \end{pmatrix}$ *e* $\Lambda_g = 4^2\Gamma$ *com* $G_{\Lambda_g} = \begin{pmatrix} 32 & 16 & 16 \\ 0 & 16 & 16 \\ 0 & 0 & 48 \end{pmatrix}$ *e* $\mathcal{S} = \{0,1\} \times \{0\} \times \{0,1,2\}$.

Assim, temos

$$Vol(\Lambda_g) = (4^2)^3 \cdot 6$$

$$\textit{Logo, } |\Lambda_f/\Lambda_g| = \frac{Vol(\Lambda_g)}{\Lambda_f} = (4^2)^3 \cdot 6 \cdot \frac{4^2 \cdot 4}{(4^2)^3} = 4^3 \cdot 6 = |\mathcal{C}||\mathcal{S}|.$$

Recentemente, Buglia e Lopes (2021) propuseram a generalização que colocamos a seguir e que foi usada para construções do tipo Fórmula Código, também conhecidas como construção $\bar{D}$

Teorema 2.1 ((BUGLIA; LOPES, 2021)). *Seja $\Gamma \subseteq \mathbb{Z}^n$ um reticulado inteiro com T sendo uma matriz triangular superior, com $t_{i,i} > 0$ para $i = 1, \ldots, n$ e seja K uma matriz diagonal com entradas k_i. Defina $\Lambda_g = KT \subseteq K\mathbb{Z}^n$ e o conjunto*

$$\begin{aligned} \mathcal{S} &= \{0, \ldots, t_{1,1} - 1\} \times \{0, \ldots, t_{2,2} - 1\} \times \cdots \times \{0, \ldots, t_{n,n} - 1\} \\ &= \{0, \ldots, \frac{g_{1,1}}{k_1} - 1\} \times \{0, \ldots, \frac{g_{2,2}}{k_2} - 1\} \times \cdots \times \{0, \ldots, \frac{g_{n,n}}{k_n} - 1\}, \end{aligned}$$

com $g_{i,i}$ os elementos da diagonal de G_{Λ_g}, para $i = 1, \ldots, n$. Sejam Λ_f um reticulado que satisfaça $\Lambda_g \subseteq K\mathbb{Z}^n \subseteq \Lambda_f$ e $\mathcal{X} = \Lambda_f \cap \mathcal{P}(K)$ o conjunto de pontos de Λ_f no interior de $\mathcal{P}(K)$, com

$$\mathcal{P}(K) = \{K\boldsymbol{m}; 0 \leqslant m_i < 1, i = 1, \ldots, n\}.$$

Então, um conjunto completo de representantes do grupo quociente Λ_f/Λ_g é dado por

$$\mathcal{X} + K\mathcal{S} = \{\boldsymbol{x} + K\boldsymbol{s}; \textit{com } \boldsymbol{x} \in \mathcal{X}, \boldsymbol{s} \in \mathcal{S}\}.$$

Exemplo 12. *Podemos pensar o Exemplo 8 em termos dessa generalização. Como $\Lambda_g \subseteq K\mathbb{Z}^n$, existe uma matriz T triangular superior, na qual podemos reescrever a matriz geradora de Λ_g como $G_{\Lambda_g} = KT$. No Exemplo 8, o reticulado Λ_g é gerado por $G_{\Lambda_g} = \begin{pmatrix} 10 & 5 \\ 0 & 10 \end{pmatrix}$ e existem $K = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$ e $T = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ tais que $G_{\Lambda_g} = KT$. Nos casos em que Λ_f é obtido por construção-A, a matriz K é uma matriz diagonal com $k_{i,i} = p = 5$, o número primo utilizado na construção, para $i = 1, \ldots, n$. A operação de pré-multiplicar $\mathcal{S}$ por K nesse caso, é equivalente à simplesmente multiplicar $\mathcal{S}$ por $p = 5$.*

O conjunto $\mathcal{S}$ é dado por

$$\begin{aligned} \mathcal{S} &= \{0, \ldots, t_{1,1} - 1\} \times \cdots \times \{0, \ldots, t_{n,n} - 1\} \\ &= \{0, 1\} \times \{0, 1\}, \end{aligned}$$

tal como no Exemplo 8.

Escolhendo Λ_f o reticulado gerado por $G_{\Lambda_f} = \begin{pmatrix} 1 & 0 \\ 2 & 5 \end{pmatrix}$, teremos que

$$\mathcal{X} = \Lambda_f \cap \mathcal{P}(K) = \{(0,0), (1,2), (2,4), (3,1), (4,3)\},$$

que é exatamente o código $\mathcal{C}$ escolhido para construir o Λ_f por construção A no Exemplo 8. Assim, o conjunto completo de representantes das classes laterais do grupo quociente Λ_f/Λ_g é

$$\mathcal{X} + K\mathcal{S} = \mathcal{C} + p\mathcal{S}.$$

Exemplo 13. *A matriz K não necessita possuir o mesmo número em toda a diagonal. Seja* $K = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$. *Seja* $\Lambda_g \subseteq K\mathbb{Z}^2$ *gerado pela matriz* $G'_{\Lambda_g} = \begin{pmatrix} 2 & 3 \\ 4 & 0 \end{pmatrix}$. *Pela Forma Normal de Hermite (1), por colunas invertendo a ordem da base,* Λ_g *também pode ser gerado pela matriz* $G_{\Lambda_g} = \begin{pmatrix} 2 & 3 \\ 0 & 6 \end{pmatrix}$.

O Teorema 2.1 nos fornece $t_{1,1} = \dfrac{g_{1,1}}{k_1} = \dfrac{2}{2} = 1$ *e* $t_{2,2} = \dfrac{g_{2,2}}{k_2} = \dfrac{6}{3} = 2$. *Assim,* $\mathcal{S} = \{0, \ldots, t_{1,1} - 1\} \times \{0, \ldots, t_{2,2} - 1\} = \{0\} \times \{0, 1\}$.

Escolhamos $\Lambda_f = \mathbb{Z}^2$. *Precisamos agora identificar o conjunto* $\mathcal{P}(K)$ *e localizar o conjunto de pontos de* Λ_f *que estão em seu interior, ou seja, o conjunto* $\mathcal{X} = \Lambda_f \cap \mathcal{P}(K)$. *A Figura 12(a) ilustra o paralelotopo* $\mathcal{P}(K)$ *obtido pelos vetores da matriz* K *e o conjunto* $\mathcal{X}$.

Notemos que $\mathcal{X} = \Lambda_f \cap \mathcal{P}(K) = \{(0,0), (1,0), (0,1), (1,1), (0,2), (1,2)\}$. *O conjunto de representantes do grupo quociente* Λ_f/Λ_g *ainda não está completo, necessitamos transladar o conjunto* $\mathcal{X}$ *pela operação* $\mathcal{X} + K\mathcal{S}$ *para obter o restante dos representantes. Assim,*

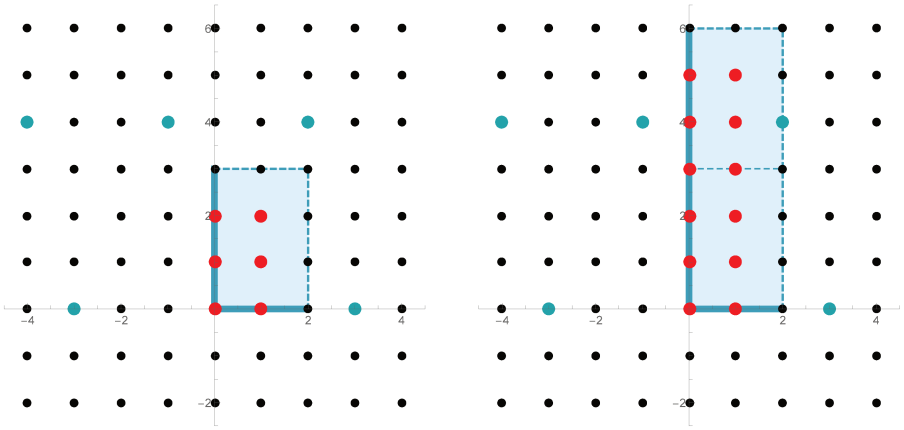
$$\begin{aligned} \mathcal{X} + K\mathcal{S} &= \{\mathcal{X} + K(0,0)^t\} \cup \{\mathcal{X} + K(0,1)^t\} \\ &= \mathcal{X} \cup \{\mathcal{X} + (0,3)\} \\ &= \{(0,0), (1,0), (0,1), (1,1), (0,2), (1,2), (0,3), (1,3), (0,4), (1,4), (0,5), (1,5)\}. \end{aligned}$$

A Figura 12(b) ilustra o conjunto $\mathcal{X} + K\mathcal{S}$, *que é um conjunto completo de representantes do grupo quociente* Λ_f/Λ_g.

Figura 12 – Etapa 1 da construção da constelação de Voronoi.

(a) Paralelotopo $\mathcal{P}(K)$ e conjunto $\mathcal{X} = \Lambda_f \cap \mathcal{P}(K)$ destacados.

(b) Conjunto $\mathcal{X} + K\mathcal{S}$.



Concluímos esta seção com uma observação sobre a construção $\bar{D}$ e o possível uso da Proposição 2.1 neste caso.

Na construção $\bar{D}$, definida em 1.11, quando $a = 1$ temos que $\Gamma_{\bar{D}} = \Lambda_A(C_1)$, ou seja, é a construção A e, neste caso, é um reticulado. Para $a \geqslant 2$ esta construção em geral não é um reticulado. Mas como demonstrado em Strey e Costa (2017) esta construção coincide com o reticulado $q^{a-1}\Lambda_D$ se, e somente se, $\mathbb{Z}_q^n \supseteq C_1 \supseteq \cdots \supseteq C_a$ é fechado sob a adição zero-um [1].

Uma das perspectivas de sequência deste trabalho é analisar as particularidades das constelações de Voronoi da construção $\bar{D}$ quando temos esta propriedade.

[1] Uma cadeia de códigos lineares $\mathbb{Z}_q^n \supseteq C_1 \supseteq \cdots C_a$ é dita fechada sob a adição zero-um quando a adição zero-um de quaisquer dois elementos de C_i sempre pertence à C_{i-1} para $i = 2, \ldots, a$.

3 Códigos Reticulados de Índice

Neste capítulo, tendo como referências o capítulo 6 de Costa et al. (2017) e Natarajan, Hong e Viterbo (2015), apresentamos o problema de codificação de índice e o uso de reticulados nesse problema. Inicialmente, descrevemos as figuras de mérito para determinar a qualidade de um código de índice e, em seguida, abordamos o problema com o uso de reticulados, analisando algumas restrições que precisam ser consideradas. Abordamos mais especificamente uma construção de códigos reticulados de índice que utiliza o Teorema Chinês dos Restos e possibilita que o código resultante atinja o limitante para o ganho de informação lateral.

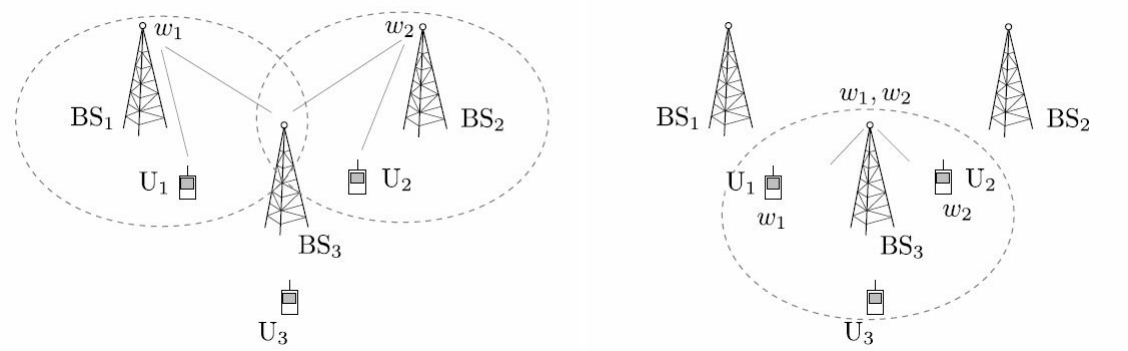
O problema clássico de codificação de índice consiste de um remetente com K mensagens independentes $\mathbf{w}_1, \ldots, \mathbf{w}_K$ e receptores que demandam um subconjunto dessas mensagens enquanto conhecem os valores de um subconjunto diferente de mensagens. A este conhecimento prévio dos receptores chamamos de *informação lateral*. Consideramos aqui a versão ruidosa desse problema, em que a transmissão é feita através de um canal com ruído aditivo gaussiano branco, o canal AWGN.

A figura 13 ilustra um caso especial de codificação de índice em um canal ruidoso em que os receptores demandam todas as mensagens da fonte. Esta é uma rede de retransmissão sem fio com duas fontes BS_1 e BS_2, um repetidor BS_3 e três receptores U_1, U_2 e UR_3. A transmissão precisa ocorrer em duas fases, pois os receptores não estão no alcance de transmissão de todas as fontes. Na primeira fase, BS_1 e BS_2 transmitem $\mathbf{w}_1$ e $\mathbf{w}_2$ respectivamente. U_1 recebeu $\mathbf{w}_1$, U_2 recebeu $\mathbf{w}_2$ e BS_1, que está no alcance de transmissão de BS_1 e BS_2, recebeu ambos. Na segunda fase, podemos realizar a codificação de índice transformando as informações laterais que U_1 e U_2 possuem em ganho de desempenho e atender a demanda de todos receptores. O objetivo na codificação de índice é transmitir um pacote de mensagens com menor comprimento possível que atenda a demanda de todos os receptores.

3.1 Codificação de índice em canal AWGN

Consideremos o canal de transmissão AWGN contendo um transmissor e uma quantidade finita e grande de receptores que desejam decodificar todas as mensagens da fonte. Vamos assumir que a fonte possui K mensagens independentes $\mathbf{w}_1, \ldots, \mathbf{w}_K$, com cada uma pertencendo aos conjuntos $\mathcal{W}_1, \ldots, \mathcal{W}_K$, respectivamente. A codificação de cada K-upla $(\mathbf{w}_1, \ldots, \mathbf{w}_K)$ será feita para a palavra código $\Psi(\mathbf{w}_1, \ldots, \mathbf{w}_K) = \mathbf{x} \in \mathcal{C}$ usando a

Figura 13 – Transmissão de mensagens com receptores possuindo informação lateral.



Fonte: Natarajan, Hong e Viterbo (2015).

correspondência um a um

$$\begin{aligned} \Psi : \mathcal{W}_1 \times \cdots \times \mathcal{W}_K &\longrightarrow \mathcal{C} \\ (\mathbf{w}_1, \ldots, \mathbf{w}_K) &\longmapsto \mathbf{x} \end{aligned}$$

Como a demanda de todos os receptores é igual, um receptor será caracterizado por sua razão sinal ruído (SNR) e pelo subconjunto $S \subset \{1, \ldots, K\}$ que indica quais as mensagens que ele possui como informação lateral, por exemplo, se um receptor conhece as mensagens $\mathbf{w}_1$, $\mathbf{w}_3$ e $\mathbf{w}_4$ teremos $S = \{1, 3, 4\}$.

Agora, consideremos um receptor com parâmetros (SNR,S) com a saída de canal $\mathbf{y}$ tal que

$$\mathbf{y} = \mathbf{x} + \mathbf{z},$$

com $\mathbf{x} \in \mathcal{C}$ sendo a palavra código transmitida e $\mathbf{z}$ um vetor aleatório gaussiano. O receptor conhece as mensagens $\mathbf{w}_j = \mathbf{a}_j, \in S$. Assim, no momento da decodificação, o decodificador desse receptor se utiliza do fato de que a palavra código transmitida $\mathbf{x}$ é correspondente a uma mensagem $(\mathbf{w}_1, \cdots, \mathbf{w}_K)$ e, então, a busca pela mensagem que foi transmitida se restringe ao subcódigo

$$C_{\mathbf{a}_S} = \{\Psi(\mathbf{w}_1, \ldots, \mathbf{w}_K)\,;\, \mathbf{w}_j = \mathbf{a}_j, j \in S \,\mathrm{e}\, \mathbf{w}_j \in \mathcal{W}_j, j \notin S\}.$$

Assim, a palavra $\mathbf{y}$ recebida será decodificada para a palavra código mais próxima $\bar{\mathbf{x}}$ em $C_{\mathbf{a}_S}$, isto é,

$$\bar{\mathbf{x}} = \arg \min_{\mathbf{x} \in C_{\mathbf{a}_S}} ||\mathbf{y} - \mathbf{x}||^2.$$

A qualidade de $\mathcal{C}$ como um código de índice pode ser medida. Para isso, precisamos calcular a menor distância possível que a informação lateral pode assumir, isto é,

$$d_S = \min\{d_{\mathbf{a}_S}; \mathbf{a}_j \in \mathcal{W}_j, j \in S\},$$

com $d_{\mathbf{a}_S} = \min\{||\mathbf{x}_1 - \mathbf{x}_2||; \mathbf{x}_1, \mathbf{x}_2 \in \mathcal{C}_{\mathbf{a}_S}, \mathbf{x}_1 \neq \mathbf{x}_2\}$. Também, precisamos medir a quantidade de informações secundárias em um receptor (SNR,S), que é dada por

$$R_S = \sum_{j \in S} R_j,$$

com $R_j = \dfrac{1}{n} \log_2 |\mathcal{W}_j| b/dim$ sendo a taxa de transmissão da j-ésima mensagem.

Assim, o *ganho de informação* $\Gamma(\mathcal{C})$ que um código $\mathcal{C}$ possui ao utilizar as informações laterais dos receptores é medido por

$$\Gamma(\mathcal{C}) = \min_{S \subset \{1,\ldots,K\}} \frac{10 \log_{10}(d_S^2/d_0^2)}{R_S} dB/b/dim.$$

com d_0 sendo a distância mínima do código de canal $\mathcal{C}$.

Exemplo 14. *Consideremos* $\mathcal{W}_1 = \{0,1\}$, $\mathcal{W}_2 = \{0,1,2\}$ *e* $\mathcal{W}_3 = \{0,1,2,3,4\}$ *e a correspondência*

$$\begin{aligned} \Psi : \mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{W}_3 &\longrightarrow \mathcal{C} \\ (\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3) &\longmapsto (15\boldsymbol{w}_1 + 10\boldsymbol{w}_2 + 6\boldsymbol{w}_3) \bmod 30 \end{aligned}$$

Essa aplicação leva uma 3-upla em um número inteiro em $[0, 29]$*, que são os possíveis restos da operação* $\bmod 30$*. Porém, escolheremos para cada valor em* $[0, 29]$ *o seu representante equivalente em* $[-15, 14]$ *pois, mais adiante, olharemos esse exemplo em termos de reticulados.*

A mensagem $(0,1,2) \longmapsto (15 \cdot 0 + 10 \cdot 1 + 6 \cdot 2) \bmod 30 = 22$ *e, seu representante equivalente em* $[0, 29]$ *é* -8*. Repetindo essa operação para todas as combinações* $(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3)$*, teremos que* $\mathcal{C} = \{-15, -14, \ldots, 13, 14\}$*.*

Sem informação lateral o receptor decodifica a mensagem recebida para o ponto mais próximo em $\mathcal{C}$*.*

Agora, se o receptor conhece a mensagem $\boldsymbol{w}_1 = \boldsymbol{a}_1$ *isto é,* $S = \{1\}$*, o decodificador restringirá a busca pela mensagem transmitida ao subcódigo*

$$C_{\boldsymbol{a}_1} = \{\Psi(\boldsymbol{a}_1, \boldsymbol{w}_2, \boldsymbol{w}_3); \boldsymbol{w}_1 = \boldsymbol{a}_1 \, e \, \boldsymbol{w}_j \in \mathcal{W}_j, j \notin S\}.$$

Suponhamos que $\boldsymbol{w}_1 = \boldsymbol{a}_1 = \boldsymbol{0}$*, então* $\mathcal{C}_{\boldsymbol{a}_1} = \{\Psi(0, \boldsymbol{w}_2, \boldsymbol{w}_3); \boldsymbol{w}_j \in \mathcal{W}_j, j \notin S\}$*. Ou seja,*

$$\begin{aligned} \mathcal{C}_{\boldsymbol{a}_1} &= \{(10\boldsymbol{w}_2 + 6\boldsymbol{w}_3) \mod 30; \boldsymbol{w}_2 \in \mathcal{W}_2 \, e \, \boldsymbol{w}_3 \in \mathcal{W}_3\} \\ &= \{(2(5\boldsymbol{w}_2 + 3\boldsymbol{w}_3)) \bmod 30; \boldsymbol{w}_2 \in \mathcal{W}_2 \, e \, \boldsymbol{w}_3 \in \mathcal{W}_3\}. \end{aligned}$$

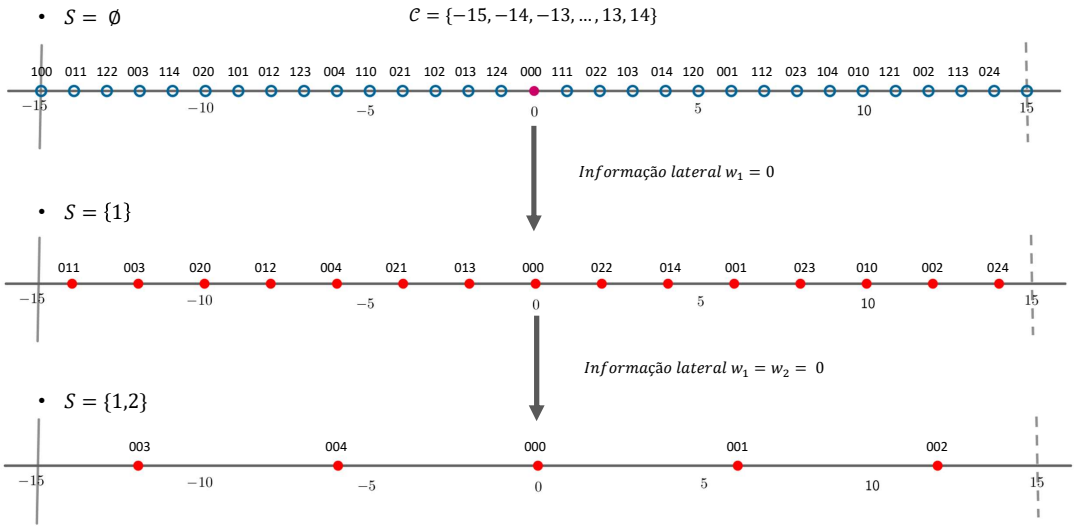
A operação $(5\boldsymbol{w}_2 + 3\boldsymbol{w}_3)$*, com* $\boldsymbol{w}_2 \in \mathcal{W}_2$ *e* $\boldsymbol{w}_3 \in \mathcal{W}_3$ *atinge todas as combinações possíveis para que* $(2(5\boldsymbol{w}_2 + 3\boldsymbol{w}_3)) \bmod 30$ *seja um número inteiro par em* $[-15, 14]$*. Logo,* $\mathcal{C}_{\boldsymbol{a}_1}$ *é o conjunto de todos os inteiros pares em* $[-15, 14]$*.*

Quanto mais informação lateral o receptor possuir, mais restringiremos a busca do decodificador. Por exemplo, se $S = \{1, 2\}$ *e* $\boldsymbol{w}_1 = \boldsymbol{w}_2 = \boldsymbol{0}$ *teremos* $C_{(\boldsymbol{a}_1, \boldsymbol{a}_2)}$ *como os múltiplos de 6 em* $[-15, 14]$*, isto é,*

$$C_{(\boldsymbol{a}_1, \boldsymbol{a}_2)} = \{\Psi(\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{w}_3); \boldsymbol{w}_j = \boldsymbol{a}_j, j \in S \, e \, \boldsymbol{w}_3 \in \mathcal{W}_3\} = \{-12, -6, 0, 6, 12\}.$$

A Figura 14 ilustra o código $\mathcal{C}$ *e os subcódigos* C_{a_1} *quando* $\boldsymbol{w}_1 = \boldsymbol{a}_1 = \boldsymbol{0}$ *e* $C_{(\boldsymbol{a}_1, \boldsymbol{a}_2)}$ *quando* $\boldsymbol{w}_1 = \boldsymbol{w}_2 = \boldsymbol{0}$*.*

Figura 14 – Exemplo unidimensional de codificação de índice.



Como a dimensão de $\mathcal{C}$ *é* $n = 1$*, temos que as taxas da j-ésima mensagem, para* $j = 1, 2$ *e* 3 *são* $R_j = \log_2 |\mathcal{W}_j| b/dim$*, ou seja,*

$$R_1 = 1, R_2 = \log_2 3 \, e \, R_3 = \log_2 5 b/dim.$$

Quando $S = \{1\}$*, por exemplo, o subcódigo* $\mathcal{C}_{\boldsymbol{a}_1}$ *é o conjunto de todos os inteiros pares em* $[-15, 14]$*. Então, a distância mínima correspondente a esse subconjunto de informação lateral* S *é* $d_S = 2$ *e a taxa de informação* $R_S = R_1 = 1 b/dim$*. Consequentemente, o ganho de informação quando o receptor conhece as informações* $S = \{1\}$ *sobre* $S = \varnothing$ *é* $\dfrac{10 \log_{10}(2^2/1)}{1} \approx 20 \log_{10} 2 \approx 6 dB/b/dim$*.*

Se $S = \{3\}$*, isto é, o receptor conhece apenas uma informação mas agora* $w_3 = a_3 \in \mathcal{W}_3$*, a distância mínima e a taxa de informação são diferentes. Os elementos do subcódigo* $\mathcal{C}_{\boldsymbol{a}_3}$ *estão distantes um do outro* $15\alpha w_1 + 10\alpha w_2$*, com* αw_1 *e* αw_2 *inteiros e ambos diferentes de zero simultaneamente. Desta forma, a menor distância que temos*

entre dois pontos de $\mathcal{C}_{a_3}$ *é dada pelo* $mdc(15, 10) = 5$. *Assim, a distância mínima nesse caso é* $d_S = 5$, *isto será detalhado em 3.4, e taxa de informação* $R_S = R_3 = \log_2 5 b/dim$. *Neste caso, o ganho de informação quando o receptor conhece as informações* $S = \{3\}$ *sobre* $S = \varnothing$ *é* $\dfrac{10\log_{10}(5^2/1)}{\log_2 5} \approx 6dB/b/dim$.

Analisando, de maneira similar, qualquer escolha de $S \subset \{1, 2, 3\}$ *temos que*

$$\Gamma(\mathcal{C}) = \min_{S\subset\{1,\ldots,K\}} \frac{10\log_{10}(d_S^2/d_0^2)}{R_S} \approx 20\log_{10} 2 \approx 6dB/b/dim,$$

com $d_0 = 1$ *sendo a distância mínima do código de canal* $\mathcal{C}$.

Para $\mathcal{C}$ ser um bom código de índice para um canal de transmissão AWGN precisamos que

1. $\mathcal{C}$ seja um bom código de canal para o canal AWGN, ou seja, deve ter uma grande distância mínima d_0;
2. $\Gamma(\mathcal{C})$ seja grande.

3.2 Códigos Reticulados de Índice

O objetivo agora é utilizar reticulados para construir bons códigos de índice, que chamaremos de *códigos reticulados de índice*. Mais especificamente, construiremos constelações, em qualquer dimensão, para codificar K mensagens independentes tal que o código resultante possua grande distância mínima d_0 e grande ganho de informação $\Gamma(\mathcal{C})$. Para isso, utilizaremos um conjunto de K reticulados $\Lambda_1, \ldots, \Lambda_K$ tais que todos possuam um subreticulado Λ' em comum, isto é,

$$\Lambda' \subset \Lambda_j, j = 1, \ldots, K.$$

O reticulado Λ' será utilizado como reticulado de modelagem na construção das constelações de Voronoi $\Lambda_1/\Lambda', \ldots, \Lambda_K/\Lambda'$.

Cada mensagem $\mathbf{w}_j$ será representada como um único ponto $\mathbf{x}_j \in \Lambda_j/\Lambda'$, e a palavra código transmitida será gerada como $\mathbf{x} = (\mathbf{x}_1 + \cdots + \mathbf{x}_K) \bmod \Lambda'$. Para que a decodificação seja única, exigiremos que a correspondência entre uma K-upla de mensagem $(\mathbf{w}_1, \ldots, \mathbf{w}_K)$ e a palavra código $\mathbf{x}$ seja biunívoca.

Definição 3.1 (Códigos reticulados de índice)**.** *Um código reticulado de índice* $\mathcal{C}$ *para* K *mensagens consiste de* K *constelações de reticulado* $\Lambda_1/\Lambda', \ldots, \Lambda_K/\Lambda'$, *sendo que* $\Lambda_1, \ldots, \Lambda_K$ *possuem todos um subreticulado* Λ' *em comum como reticulado de modelagem e de uma aplicação bijetiva* Ψ *dada por*

$$\begin{aligned} \Psi : \Lambda_1/\Lambda' \times \cdots \times \Lambda_K/\Lambda' &\longrightarrow \mathcal{C} \\ (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_K) &\longmapsto (\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_K) \bmod \Lambda' \end{aligned}$$

com $\boldsymbol{x}_j \in \Lambda_j/\Lambda'$ *e* $\mathcal{C}$ *sendo o conjunto de todos os possíveis valores para* $\boldsymbol{x} = \Psi(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_K)$.

No exemplo a seguir, ilustramos e exploramos um código reticulado de índice.

Exemplo 15. *Consideremos os reticulados* Λ_1 *e* Λ_2 *obtidos pelas seguintes matrizes geradoras, respectivamente,*

$$G_1 = \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix} \qquad G_2 = \begin{pmatrix} 0 & 3 \\ 3 & 2 \end{pmatrix}$$

e o subreticulado Λ' *tal que* $\Lambda' \subset \Lambda_1$ *e* $\Lambda' \subset \Lambda_2$ *gerado pela matriz* $B = \begin{pmatrix} 9 & 0 \\ 0 & 9 \end{pmatrix}$.

Para mostrar que a escolha de Λ_1, Λ_2 *e* Λ' *definem um código reticulado de índice, vamos mostrar que* Λ' *é subreticulado de* Λ_1 *e* Λ_2, *identificar as constelações* Λ_1/Λ' *e* Λ_2/Λ', *o código* $\mathcal{C}$ *e mostrar que o aplicação* Ψ *é injetiva (a sobrejetividade já está garantida, pois o contradomínio da aplicação é sua imagem).*

Observamos que os vetores da base $(9,0)^t$ *e* $(0,9)^t$ *de* Λ' *podem ser expressos como combinação linear inteira das colunas de* G_1, *então* $\Lambda' \subset \Lambda_1$*:*

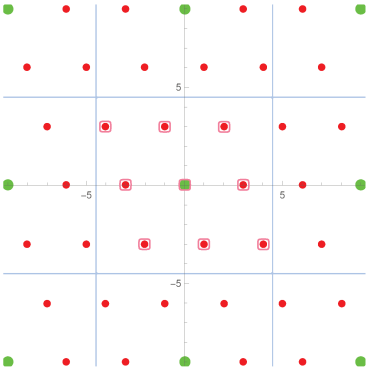
$$\begin{pmatrix} 9 \\ 0 \end{pmatrix} = 3\begin{pmatrix} 3 \\ 0 \end{pmatrix} \qquad e \qquad \begin{pmatrix} 0 \\ 9 \end{pmatrix} = 3\begin{pmatrix} 2 \\ 3 \end{pmatrix} - 2\begin{pmatrix} 3 \\ 0 \end{pmatrix}.$$

Similarmente, temos que $\Lambda' \subset \Lambda_2$ *pois os vetores da base de* Λ' *também podem ser escritos como combinação linear inteira dos vetores coluna de* G_2.

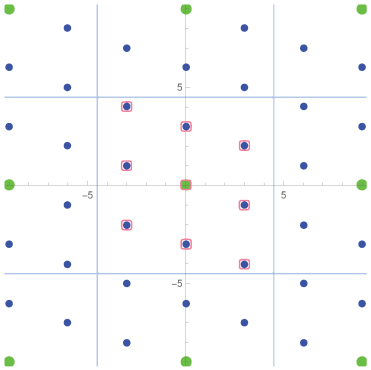
A Figura 15 ilustra os reticulados Λ_1 *e* Λ_2 *representados pelos pontos em vermelho, o subreticulado* Λ' *pelos pontos verde e os conjuntos* Λ_1/Λ' *e* Λ_2/Λ' *destacados pelos pontos com quadrados. Os conjuntos* Λ_1/Λ' *e* Λ_2/Λ' *são formados pelos seus representantes das classes laterais que estão no interior da região de Voronoi de* Λ', *respectivamente.*

Figura 15 – Reticulados Λ_1 e Λ_2 com o subreticulado Λ' e os conjuntos Λ_1/Λ' e Λ_2/Λ', respectivamente.

(a) Reticulados Λ_1 e Λ' e o código Λ_1/Λ' destacado.



(b) Reticulados Λ_2 e Λ' e código Λ_2/Λ' destacado.

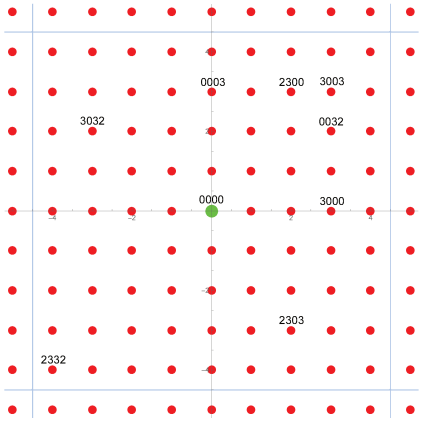


O código reticulado de índice neste caso é a imagem da aplicação

$$\begin{aligned} \Psi : \Lambda_1/\Lambda' \times \Lambda_2/\Lambda' &\longrightarrow \mathcal{C} \\ (\boldsymbol{x}_1, \boldsymbol{x}_2) &\longmapsto (\boldsymbol{x}_1 + \boldsymbol{x}_2) \bmod \Lambda' \end{aligned}$$

com $\boldsymbol{x}_j \in \Lambda_j/\Lambda'$, *para* $j = 1, 2$ *e* $\mathcal{C}$ *sendo o conjunto de todos os possíveis valores para* $\boldsymbol{x} = \Psi(\boldsymbol{x}_1, \boldsymbol{x}_2)$. *Por exemplo, tomando* $\boldsymbol{x}_1 = (3,0) \in \Lambda_1/\Lambda'$ *e* $\boldsymbol{x}_2 = (0,3) \in \Lambda_2/\Lambda'$ *teremos* $\boldsymbol{x} = \Psi(3,0,0,3) = ((3,0) + (0,3)) \bmod \Lambda' = (3,3) - \mathcal{Q}_{\Lambda'}(3,3) = (3,3) - (0,0) = (3,3) \in \mathcal{C}$. *A Figura 16 ilustra todas as palavras códigos obtidas que serão transmitidas no interior da região de Voronoi destacada. Para melhor visualização, o rotulamento feito na Figura 16 é apenas da aplicação de* Ψ *nos elementos* $\{(0,0),(3,0),(2,3)\} \subset \Lambda_1/\Lambda'$ *e* $\{(0,0),(3,2),(0,3)\} \subset \Lambda_2/\Lambda'$.

Figura 16 – Palavras códigos obtidas que serão transmitidas destacadas pela região de Voronoi de Λ'.



Observamos que o código $\mathcal{C}$ *também é uma constelação de Voronoi, porém do reticulado* $\Lambda = \Lambda_1 + \Lambda_2 = \mathbb{Z}^2$ *com* Λ' *como reticulado de modelagem, isto é,* $\mathcal{C} = \Lambda/\Lambda'$. *De fato, como* $\Lambda_1, \Lambda_2 \subset \mathbb{Z}^2$, *temos que* $\Lambda = \Lambda_1 + \Lambda_2 \subset \mathbb{Z}^2$.

Como os vetores bases $(1,0)^t$ *e* $(0,1)^t$ *de* $\mathbb{Z}$ *são escritos como combinação linear das colunas de* G_1 *e* G_2 *concluímos que* $\mathbb{Z}^2 \subset \Lambda = \Lambda_1 + \Lambda_2$:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \end{pmatrix} - \begin{pmatrix} 2 \\ 3 \end{pmatrix} - \begin{pmatrix} 0 \\ 3 \end{pmatrix} \qquad e \qquad \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \end{pmatrix} - \begin{pmatrix} 3 \\ 2 \end{pmatrix} - \begin{pmatrix} 3 \\ 0 \end{pmatrix}.$$

Logo, $\Lambda = \mathbb{Z}^2$.

Resta concluirmos a injetividade de Ψ. *A cardinalidade do domínio* $\Lambda_1/\Lambda' \times \Lambda_2/\Lambda'$ *é*

$$|\Lambda_1/\Lambda'| \cdot |\Lambda_2/\Lambda'| = \frac{Vol(\Lambda')}{Vol(\Lambda_1)} \cdot \frac{Vol(\Lambda')}{Vol(\Lambda_2)} = \frac{81}{9} \cdot \frac{81}{9} = 81,$$

e a cardinalidade da imagem é

$$|\mathcal{C}| = |\Lambda/\Lambda'| = \frac{Vol(\Lambda')}{Vol(\Lambda)} = \frac{81}{1} = 81.$$

Portanto, a aplicação Ψ é injetiva, pois o domínio e a imagem possuem a mesma cardinalidade.

Sem informação lateral, um receptor decodificará a saída do canal para o ponto mais próximo em $\mathcal{C}$, com distância mínima entre as palavras códigos $d_0 = d_{min}(\Lambda) = 1$.

Agora, se o receptor conhece o valor de um conjunto de mensagens $\boldsymbol{w}_j$, com $j \in S \subset \{1, \cdots, K\}$, a busca pela mensagem que foi transmitida se restringe ao subcódigo

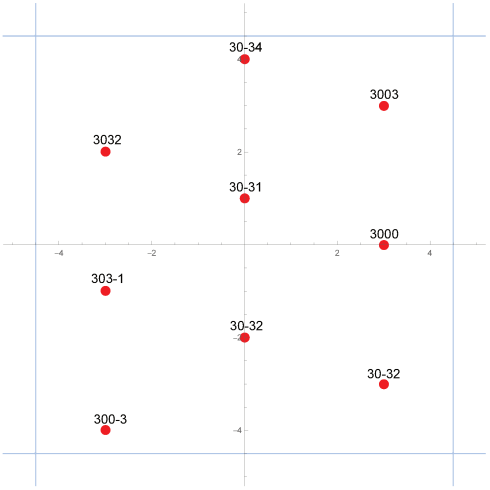
$$C_{\boldsymbol{a}_1} = \{\Psi(\boldsymbol{w}_1, \cdots, \boldsymbol{w}_K)\,;\, \boldsymbol{w}_j = \boldsymbol{a}_j, j \in S \, e \, \boldsymbol{w}_j \in \Lambda_j/\Lambda', j \notin S\}.$$

Por exemplo, se $S = \{1\}$, ou seja, se um receptor conhece $\boldsymbol{w}_1 = \boldsymbol{a}_1$, suponhamos $\boldsymbol{w}_1 = (3,0) \in \Lambda_1/\Lambda$ teremos que

$$C_{\boldsymbol{a}_1} = \{\Psi((3,0), \boldsymbol{w}_2)\,;\, \boldsymbol{w}_2 \in \Lambda_2/\Lambda'\} = \{((3,0) + w_2) \bmod \Lambda'\,;\, \boldsymbol{w}_2 \in \Lambda_2/\Lambda'\}.$$

A Figura 17 ilustra o subcódigo que o receptor com informação lateral restringe sua busca quando $S = \{1\}$ e $\boldsymbol{w}_1 = (3,0)$.

Figura 17 – Conjunto $C_{\mathbf{a}_1}$.



A propriedade $\mathcal{C} = \Lambda/\Lambda'$ com $\Lambda = \Lambda_1 + \cdots + \Lambda_K$ em virtude da bijeção requerida não se restringe a esse exemplo. Essa é uma propriedade de um código reticulado de índice em termos de suas constelações de reticulados Λ_1/Λ', ..., Λ_K/Λ'. De fato, seja

$$\Lambda = \Lambda_1 + \cdots + \Lambda_K = \{\mathbf{v}_1 + \cdots + \mathbf{v}_K; \mathbf{v}_j \in \Lambda_j, j = 1, \ldots, K\}$$

o reticulado obtido como a soma de componentes dos reticulados. Para todo $j = 1, \ldots, K$, temos que $\Lambda_j \subset \Lambda$ e, portanto, para cada escolha de $\mathbf{x}_j \in \Lambda_j/\Lambda'$ temos que $\mathbf{x}_1 + \cdots + \mathbf{x}_K \in \Lambda$. Disso, segue que

$$\mathbf{x} = \Psi(\mathbf{x}_1 + \cdots + \mathbf{x}_K) = (\mathbf{x}_1 + \cdots + \mathbf{x}_K) \mod \Lambda' \in \Lambda/\Lambda'.$$

Portanto, temos que $\mathcal{C} \subset \Lambda/\Lambda'$. Por outro lado, se $\mathbf{v} \in \Lambda/\Lambda'$, temos que $\mathbf{v} \in \Lambda$. Isto nos diz que existem $\mathbf{v}_j \in \Lambda_j$, para $j = 1, \ldots, K$ tal que $\mathbf{v} = \mathbf{v}_1 + \cdots + \mathbf{v}_K$. Pelo fato de $\mathbf{v} \in \mathcal{V}_{\Lambda'}(\mathbf{0})$, obtemos

$$\begin{aligned} \mathbf{v} = \mathbf{v} \bmod \Lambda' &= (\mathbf{v}_1 + \cdots + \mathbf{v}_K) \bmod \Lambda' \\ &= (\mathbf{v}_1 \bmod \Lambda' + \cdots + \mathbf{v}_K \bmod \Lambda') \bmod \Lambda' \\ &= \Psi(\mathbf{v}_1 \bmod \Lambda' + \cdots + \mathbf{v}_K \bmod \Lambda') \end{aligned}$$

com $\mathbf{v}_j \bmod \Lambda' \in \Lambda_j/\Lambda'$, para $j = 1, \cdots, K$. Logo, $\mathbf{v} \in \mathcal{C}$ e, portanto, $\Lambda/\Lambda' \subset \mathcal{C}$. Assim, mostramos que o código $\mathcal{C}$ transmitido pode ser identificado como uma constelação de Voronoi e é dada por $\mathcal{C} = \Lambda/\Lambda'$.

Outra propriedade dos códigos reticulados de índice é caracterizar os subcódigos C_{a_S} em função dos reticulados Λ_k, com $k \notin S$, isto é,

$$\begin{aligned} C_{\mathbf{a}_S} &= \{\Psi(\mathbf{w}_1, \ldots, \mathbf{w}_K)\,;\, \mathbf{w}_j = \mathbf{a}_j, j \in S \,\mathrm{e}\, \mathbf{w}_j \in \Lambda_j/\Lambda', j \notin S\} \\ &= \{(\mathbf{w}_1 + \cdots + \mathbf{w}_K) \mod \Lambda';\ \mathbf{w}_j = \mathbf{a}_j, j \in S \,\mathrm{e}\, \mathbf{w}_j \in \Lambda_j/\Lambda', j \in S^c\} \\ &= \left\{ \left(\sum_{j\in S} \mathbf{a}_j + \sum_{j\in S^c} \mathbf{x}_j \right) \mod \Lambda';\ \mathbf{w}_j \in \Lambda_j/\Lambda', j \in S^c \right\} \\ &= \left\{ \left(\sum_{j\in S} \mathbf{a}_j + \sum_{j\in S^c} \mathbf{v}_j \right) \mod \Lambda';\ \mathbf{v}_j \in \Lambda_j, j \in S^c \right\} \end{aligned} \tag{3.1}$$

sendo que a última igualdade segue da seguinte observação

$$\left(\sum_{j\in S} \mathbf{a}_j + \sum_{j\in S^c} \mathbf{v}_j \right) \mod \Lambda' = \left(\sum_{j\in S} \mathbf{a}_j + \sum_{j\in S^c} \mathbf{v}_j \mod \Lambda' \right) \mod \Lambda'$$

com $\mathbf{v}_j \bmod \Lambda' \in \Lambda_j/\Lambda'$.

Denotando por Λ_{S^c} o reticulado soma das componentes de Λ_j, com $j \in S^c$, isto é,

$$\Lambda_{S^c} = \sum_{j\in S^c} \Lambda_j = \left\{ \sum_{j\in S^c} \mathbf{v}_j\,;\, \mathbf{v}_j \in \Lambda_j, j \in S^c \right\},$$

podemos expressar 3.1 como

$$C_{\mathbf{a}_S} = \left(\sum_{j\in S} \mathbf{a}_j + \Lambda_{S^c} \right) \mod \Lambda'.$$

Assim, o subcódigo $\mathcal{C}_{\mathbf{a}_1}$ do exemplo 15 pode ser expresso como $\mathcal{C}_{\mathbf{a}_1} = (\mathbf{a}_1 + \Lambda_2) \bmod \Lambda'$.

Voltando à Definição 3.1 é importante observar que a injetividade requerida da aplicação Ψ nem sempre é garantida. Isto significa que para algumas escolhas dos reticulados $\Lambda_1, \ldots, \Lambda_K$ podem existir pontos de $\mathcal{C}$ rotulados por mais de uma mensagem $(\mathbf{x}_1, \ldots, \mathbf{x}_K)$ e nesta situação não teremos um código reticulado de índice. Os exemplos 16 e 17 ilustram situações em que a aplicação Ψ não é bijetiva.

Exemplo 16. *Tomando* $\Lambda_1 = 4\mathbb{Z}$, $\Lambda_2 = 6\mathbb{Z}$, $\Lambda_3 = 10\mathbb{Z}$ *e escolhendo* $\Lambda' = 60\mathbb{Z}$ *teremos*

$$\begin{aligned} \Psi : 4\mathbb{Z}/60\mathbb{Z} \times 6\mathbb{Z}/60\mathbb{Z} \times 10\mathbb{Z}/60\mathbb{Z} &\longrightarrow \mathcal{C} \\ (\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3) &\longmapsto (\boldsymbol{x}_1 + \boldsymbol{x}_2 + \boldsymbol{x}_3) \bmod 60. \end{aligned}$$

Observemos que $\mathcal{C} = 2\mathbb{Z}/60\mathbb{Z}$ *uma vez que* $\Lambda = \Lambda_1 + \Lambda_2 + \Lambda_3 = 2\mathbb{Z}$. *Logo, a cardinalidade do domínio é*

$$|4\mathbb{Z}/60\mathbb{Z}| \cdot |6\mathbb{Z}/60\mathbb{Z}| \cdot |10\mathbb{Z}/60\mathbb{Z}| = 15 \cdot 10 \cdot 6 = 900,$$

e $|\mathcal{C}| = |2\mathbb{Z}/60\mathbb{Z}| = 30$. *Portanto, não obtemos a injetividade com este exemplo, consequentemente,* $\mathcal{C}$ *não é um código reticulado de índice.*

Este exemplo nos indica que, no caso unidimensional, em situações em que o mdc entre os fatores que geraram os reticulados $\Lambda_1, \ldots, \Lambda_K$ *for diferente de* 1 *teremos uma bijeção quando o menor reticulado que contém todos os reticulados* $\Lambda_1, \ldots, \Lambda_K$ *é o* $\mathbb{Z}$. *O que não acontece neste exemplo, pois temos que* $mdc(4, 6, 10) = 2$ *e* $2\mathbb{Z}$ *é o menor reticulado que contém* Λ_1, Λ_2 *e* Λ_3.

Exemplo 17. *Consideremos os reticulados* Λ_1 *e* Λ_2 *com as matrizes geradoras*

$$G_1 = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \qquad\qquad G_2 = \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix},$$

respectivamente, e o reticulado Λ' *gerado pela matriz* $B = \begin{pmatrix} 4 & 2 \\ 0 & 2 \end{pmatrix}$.

A aplicação Ψ *tem domínio* $\Lambda_1/\Lambda' \times \Lambda_2/\Lambda'$ *e o código* $\mathcal{C}$ *como imagem. Desejamos que essa aplicação seja bijetiva mas, da forma como está definida, há rotulamentos diferentes sendo associados a um mesmo ponto de* $\mathcal{C}$, *uma vez que*

$$|\Lambda_1/\Lambda'| \cdot |\Lambda_2/\Lambda'| = \frac{Vol(\Lambda')}{Vol(\Lambda_1)} \cdot \frac{Vol(\Lambda')}{Vol(\Lambda_2)} = \frac{8}{2} \cdot \frac{8}{2} = 16,$$

enquanto que a cardinalidade da imagem é

$$|\mathcal{C}| = |\Lambda/\Lambda'| = \frac{Vol(\Lambda')}{Vol(\Lambda)} = \frac{8}{1} = 8,$$

com $\Lambda = \Lambda_1 + \Lambda_2 = \mathbb{Z}$. *Isto pode ser visto considerando uma matriz que representa os elementos de* $\Lambda = \Lambda_1 + \Lambda_2$, *por exemplo,*

$$G' = \begin{pmatrix} 2 & 1 & 0 & 1 \\ 0 & 1 & 2 & 2 \end{pmatrix},$$

e tomando sua Forma Normal de Hermite. Assim, a matriz geradora de Λ *equivalente obtida pela FNH é*

$$G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

3.3 Um limitante superior para o ganho de informação lateral

Detalhamos agora um resultado apresentado em Natarajan, Hong e Viterbo (2015) em que o ganho de informação lateral de um reticulado código de índice é limitado superiormente por $20\log_{10} 2 \approx 6dB/b/dim$ quando escolhemos Λ que nos fornece o melhor empacotamento em $\mathbb{R}^n$.

Vamos assumir que $\Lambda_1/\Lambda', \ldots, \Lambda_K/\Lambda'$ define um reticulado código de índice para K mensagens tal que o reticulado soma $\Lambda = \Lambda_1 + \cdots + \Lambda_K$ possui ótima densidade de empacotamento entre todos os reticulado em n dimensões. Vamos agora considerar um receptor com $S = \{1, \ldots, K-1\}$, isto é, o receptor conhece o valor de todas as mensagens exceto de w_K. Para esse receptor, $\Lambda_{S^c} = \sum_{j \in S^c} \Lambda_j = \Lambda_K$ e sua distância mínima é

$$d_S = 2\rho(\Lambda_{S^c}) = 2\rho(\Lambda_K).$$

Sendo R a soma da taxa de todas as K mensagens, isto é,

$$R = R_1 + \cdots + R_K = \sum_{k=1}^{K} \frac{1}{n} \log_2 |\Lambda_k/\Lambda'|,$$

podemos reescrever a taxa como

$$nR = \log_2(|\Lambda_1/\Lambda'| \cdot \cdots \cdot |\Lambda_K/\Lambda'|),$$

que nos fornece $|\Lambda_1/\Lambda'| \cdot \cdots \cdot |\Lambda_K/\Lambda'| = 2^{nR}$. Logo, como as mensagens são unicamente mapeadas para as palavras códigos em Λ/Λ', temos que

$$|\Lambda/\Lambda'| = |\Lambda_1/\Lambda'| \cdot \cdots \cdot |\Lambda_K/\Lambda'| = 2^{nR} \Leftrightarrow R = \frac{1}{n} \log_2 |\Lambda/\Lambda'|.$$

A taxa de informação desse receptor é

$$R_S = R_1 + \cdots + R_{K-1} = R - R_K.$$

Usando o fato de $|\Lambda_K/\Lambda'| = 2^{nR_K}$, obtemos

$$\begin{aligned} R_S = R - R_K &= \frac{1}{n} \log_2 |\Lambda/\Lambda'| - \frac{1}{n} \log_2 |\Lambda_K/\Lambda'| \\ &= \frac{1}{n} \log_2 \frac{Vol(\Lambda')}{Vol(\Lambda)} - \frac{1}{n} \log_2 \frac{Vol(\Lambda')}{Vol(\Lambda_K)} \\ &= \frac{1}{n} \log_2 \frac{Vol(\Lambda_K)}{Vol(\Lambda)}. \end{aligned} \tag{3.2}$$

Agora relacionaremos R_S às densidades de empacotamento de Λ e Λ_K por meio de seus raios de empacotamento. Da definição de densidade de empacotamento, temos que

$$Vol(\Lambda) = \frac{Vol\mathcal{B}^n(\rho(\Lambda))}{\Delta(\Lambda)} = Vol\mathcal{B}^n(1)\frac{\rho^n(\Lambda)}{\Delta(\Lambda)},$$

com $\mathcal{B}^n(r)$ sendo a bola n-dimensional Euclidiana de raio r. Assim, reescrevemos 3.2 como

$$\begin{aligned} R_S = \frac{1}{n}\log_2 \frac{\rho^n(\Lambda_K)}{\Delta(\Lambda_K)}\frac{\Delta(\Lambda)}{\rho^n(\Lambda)} &= \frac{1}{n}\log_2 \frac{\rho^n(\Lambda_K)}{\rho^n(\Lambda)} + \frac{1}{n}\log_2 \frac{\Delta(\Lambda)}{\Delta(\Lambda_K)} \\ &= \log_2 \frac{\rho(\Lambda_K)}{\rho(\Lambda)} + \frac{1}{n}\log_2 \frac{\Delta(\Lambda)}{\Delta(\Lambda_K)}. \end{aligned}$$

Como assumimos que Λ tem a maior densidade de empacotamento entre todos os reticulados n-dimensionais, observamos que $\Delta(\Lambda) \geqslant \Delta(\Lambda_K)$ e, portanto,

$$R_S \geqslant \log_2 \frac{\rho(\Lambda_K)}{\rho(\Lambda)}.$$

Como $d_S = 2\rho(\Lambda_K)$ e $d_0 = 2\rho(\Lambda)$ temos, portanto, $R_S \geqslant \log_2(d_S/d_0)$. Assim, concluímos que

$$\frac{d_S}{d_0} \leqslant 2^{R_S} = 2^{R-R_K}.$$

Assim, podemos limitar superiormente o ganho de informação lateral de Λ/Λ' por

$$\begin{aligned} \Gamma(\Lambda/\Lambda') &= \min_{S\subset\{1,\ldots,K\}} \frac{10\log_{10}(d_S^2/d_0^2)}{R_S} \\ &\leqslant \frac{10\log_{10}(2^{2(R-R_K)})}{R-R_k} \\ &= \frac{20(R-R_K)\log_{10} 2}{R-R_K} \\ &= 20\log_{10} 2 \approx 6dB/b/dim. \end{aligned} \tag{3.3}$$

3.4 Uma construção de Códigos Reticulados de Índice usando o Teorema Chinês dos Restos

Uma vez conhecido[1] um reticulado com ótima densidade de empacotamento entre todos os reticulados em n dimensões, não é simples determinar bons reticulados $\Lambda_1, \ldots, \Lambda_K$ que definam o código reticulado de índice associado. O Teorema Chinês dos Restos nos permite determinar tais reticulados e com eles construir um código reticulado de índice que atinge o limitante para o ganho de informação, como mostrado no capítulo 6 de (COSTA et al., 2017). Para esta construção são necessários K números inteiros positivos primos entre si, digamos $p_1, \ldots, p_K$, e um reticulado Λ arbitrário n-dimensional. Usaremos versões escalares de Λ para obter $\Lambda_1, \ldots, \Lambda_K$ e Λ', com coeficientes escalares dados pelo

[1] É importante observar que reticulados com densidade máxima só são conhecidos em dimensões até 8 e em dimensão 24 (CONWAY; SLOANE, 1998).

Teorema Chinês dos Restos. Isto é, com $M = \prod_{j=1}^{K} p_j$ e $M_j = M/p_j$ seja

$$\Lambda_j = M_j\Lambda, \text{para j} = 1, \ldots, \text{K e } \Lambda' = M\Lambda.$$

De fato, o código de índice obtido dos reticulados construídos pelo Teorema Chinês dos Restos atinge o limitante para o ganho de informação 3.3. Com essa construção, podemos reescrever a taxa de transmissão da j-ésima mensagem uma vez que

$$|\Lambda_j/\Lambda'| = \left|\frac{Vol(\Lambda')}{Vol(\Lambda_j)}\right| = \left|\frac{det(G_{\Lambda'})}{det(G_{\Lambda_k})}\right| = \left|\frac{M^n det(G_\Lambda)}{M_k^n det(G_\Lambda)}\right| = p_j^n$$

e então

$$R_j = \frac{1}{n}\log_2|\Lambda_j/\Lambda'| = \frac{1}{n}\log_2 p_j^n = \log_2 p_j$$

Assim, para qualquer escolha de $S \subset \{1, \ldots, K\}$ teremos

$$R_S = \sum_{j\in S} R_j = \sum_{j\in S} \log p_j = \log_2 \prod_{j\in S} p_j.$$

Optamos por usar R_S em termos na base 10 para comparar com a expressão do ganho de informação. Assim,

$$R_S = \log_2 \prod_{j\in S} p_j = \frac{\log_{10}\prod_{j\in S} p_j}{\log_{10} 2}.$$

Logo, podemos reescrever a expressão para o ganho de informação como

$$\Gamma(\Lambda/\Lambda') = \min_{S\subset\{1,\ldots,K\}} \frac{10\log_{10}(d_S^2/d_0^2)}{R_S} = \min_{S\subset\{1,\ldots,K\}} 20\frac{\log_{10}(d_S/d_0)}{\frac{\log_{10}\prod_{j\in S} p_j}{\log_{10} 2}}.$$

Ou equivalentemente como

$$\Gamma(\Lambda/\Lambda') = \min_{S\subset\{1,\ldots,K\}} 20\frac{\log_{10}(d_S/d_0)\cdot\log_{10} 2}{\log_{10}\prod_{j\in S} p_j}.$$

Como $20\log_{10} 2$ é um limitante superior para ganho de informação lateral, para que ele seja atingido devemos ter $\log_{10}(d_S/d_0) = \log_{10}\prod_{j\in S} p_j$ ou, equivalentemente, $d_S/d_0 = \prod_{j\in S} p_j$ para toda escolha de $S \subset \{1, \ldots, K\}$. Primeiramente, observemos que para qualquer escolha de $S \subset \{1, \ldots, K\}$, o código $\mathcal{C}_{a_S}$ é um subcódigo de $\mathcal{C}$ com d_S igual à d_0 multiplicada por um fator de escala, α, pois apenas retiramos alguns elementos do código inicial.

Afirmação: Sob as hipóteses do Teorema Chinês dos Restos, $d_S = \alpha d_0$, com $\alpha = mdc(M_j, j \in S^c)$, para qualquer $S \subset \{1, \ldots, K\}$. Isso segue do fato de $p_1, \ldots, p_K$ serem primos entre si.

Assim, $d_S/d_0 = mdc(M_j, j \in S^c)$. Queremos que $mdc(M_j, j \in S^c) = \prod_{j\in S} p_j$, o que é imediato, uma vez que $\prod_{j\in S} p_j$, é a parcela em comum em cada $M_j, j \in S^c$. No

Exemplo 14 quando $S = \{1\}$ obtemos que a distância entre os pontos de C_{a_S} é 2, uma vez que os pontos distam $10\Delta w_2 + 6\Delta w_3$ um do outro, com $\Delta \in \mathbb{Z}$, fazendo com que o $d_S = mdc(10, 6) = 2 = p_1 = \prod_{j \in S} p_j$.

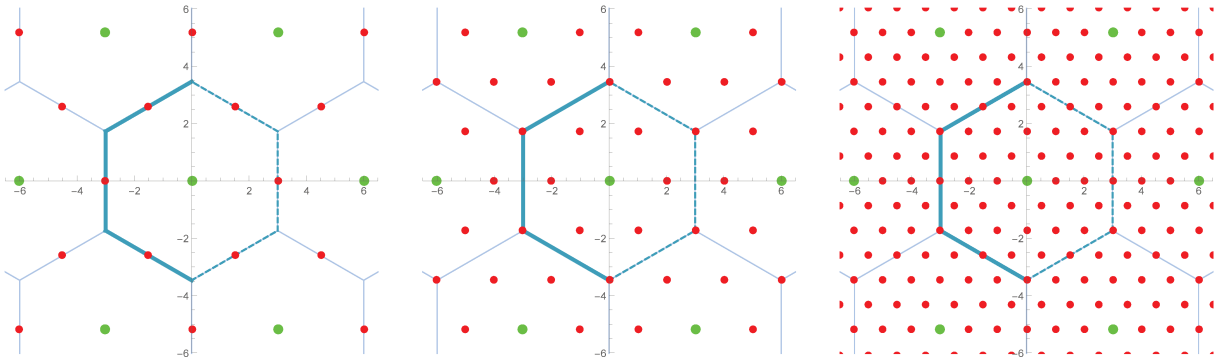
Portanto, os códigos reticulados de índice construídos pelo Teorema Chinês dos Restos atingem o limitante para o ganho de informação.

Exemplo 18. *No Exemplo 14, $p_1 = 2$, $p_2 = 3$ e $p_3 = 5$ e $\Lambda = \mathbb{Z}$. Assim, $M = 2 \cdot 3 \cdot 5 = 30$, $M_1 = 15$, $M_2 = 10$ e $M_3 = 6$ e, portanto, $\Lambda_1 = 15\mathbb{Z}$, $\Lambda_2 = 10\mathbb{Z}$, $\Lambda_3 = 6\mathbb{Z}$ e $\Lambda' = 30\mathbb{Z}$.*

Exemplo 19. *Suponhamos que desejamos transmitir $K = 2$ mensagens em dimensão $n = 2$. Escolhendo $p_1 = 2$ e $p_2 = 3$, que são primos entre si, obteremos pelo Teorema Chinês dos Restos os escalares $M = 2 \cdot 3 = 6$ e $M_1 = 3$, $M_2 = 2$. Vamos escolher $\Lambda = \Lambda_2$, o reticulado hexagonal, gerado pela matriz $G = \begin{pmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{pmatrix}$. Assim, os reticulados que serão utilizados são $\Lambda_1 = 3\Lambda$ e $\Lambda_2 = 2\Lambda$. A Figura 18 ilustra os reticulados Λ_1 e Λ_2, com suas respectivas constelações de Voronoi Λ_1/Λ' e Λ_2/Λ' e o código reticulado de índice $\mathcal{C} = \Lambda/\Lambda'$.*

Figura 18 – Reticulados Λ_1 e Λ_2 com o subreticulado Λ' e os conjuntos Λ_1/Λ', Λ_2/Λ' e $\mathcal{C} = \Lambda/\Lambda'$, respectivamente.

(a) Código Λ_1/Λ'. (b) Código Λ_2/Λ'. (c) Código $\mathcal{C} = \Lambda/\Lambda'$.



Para ilustrar o rotulamento nesse exemplo, escolheremos $(-3, 0) \in \Lambda_1/\Lambda'$ e $(-2, 0) \in \Lambda_2/\Lambda'$. A aplicação que define $\mathcal{C}$ é

$$\begin{aligned} \Psi : \Lambda_1/\Lambda' \times \Lambda_2/\Lambda' &\longrightarrow \mathcal{C} \\ (\boldsymbol{x}_1, \boldsymbol{x}_2) &\longmapsto (\boldsymbol{x}_1 + \boldsymbol{x}_2) \bmod \Lambda' \end{aligned}$$

Assim,

$$\begin{aligned} \Psi(-3, 0, -2, 0) &= ((-3, 0) + (-2, 0)) \mod \Lambda' = (-5, 0) - \mathcal{Q}_{\mathcal{V}(\Lambda')}(-5, 0) \\ &= (-5, 0) - (-6, 0) = (1, 0). \end{aligned}$$

Comentário final:

Um dos propósitos do estudo e ilustrações de códigos reticulados de índice feitos neste capítulo é o da perspectiva que temos de conexão deste tema com o do Capitulo 2. Pretendemos na continuidade deste trabalho analisar possíveis ganhos de codificação e decodificação de índice em sequências especiais de subreticulados de reticulados quando consideramos as construções de constelações de Voronoi discutidas no Capítulo 2.

4 Considerações Finais

Neste trabalho procuramos entender e ilustrar como reticulados aninhados, $\Lambda_g \subseteq \Lambda_f$, auxiliam no processo de seleção de pontos para transmissão de informações e no problema de codificação de índice.

Estudamos a construção de constelações de Voronoi proposta em Pietro e Boutros (2017) para reticulados dados por construção A de um código sobre $\mathbb{Z}_p$, p primo e apresentamos extensões desta para reticulados obtidos por construções A e D de códigos q-ários, com $q \in \mathbb{N}^*$. Perspectivas futuras de pesquisa que consideramos nos temas aqui abordados incluem:

- Analisar as particularidades das constelações de Voronoi obtidas pela construção $\bar{D}$ (Fórmula Código) quando esta satisfaz as condições para gerar um reticulado.

- Estudar construções de constelações de Voronoi como as estudadas no Capítulo 2 no contexto de códigos reticulados de índice, analisando possíveis ganhos de codificação e decodificação.

- Aprofundar o estudo sobre a construção de constelações mais gerais para códigos reticulados analisando os ganhos de codificação e de modelagem e figuras de mérito que os impactam. No caso específico de reticulados construídos a partir de códigos q-ários lineares discutir possíveis especificidades quando q é primo ou potência de primo.

Referências

BUGLIA, H.; LOPES, R. Voronoi shaping for lattices with efficient encoding. *IEEE Communications Letters*, 2021. Citado 2 vezes nas páginas 22 e 34.

CASSELS, J. W. S. *An Introduction to the Geometry of Numbers*. [S.l.]: Springer-Verlag, 1997. Citado na página 10.

COHEN, H. *A Course in Computational Algebraic Number Theory*. [S.l.]: Springer, New York, 1996. Citado na página 12.

CONWAY, J. H.; SLOANE, N. J. A. *Sphere Packings, Lattices and Groups*. [S.l.]: Springer, New York, 1998. Citado 2 vezes nas páginas 10 e 48.

COSTA, S. I. R.; OGGIER, F.; CAMPELLO, A.; BELFIORE, J. C.; VITERBO, E. *Lattices Applied to Coding for Reliable and Secure Communication*. [S.l.]: Springer, New York, 2017. Citado 10 vezes nas páginas 9, 10, 11, 16, 22, 24, 26, 31, 37 e 48.

FORNEY, G. D. Coset codes-part i: introduction and geometrical classification. *IEEE Trans. Inf. Theory*, v. 34(5). Citado na página 20.

_____. Coset codes-part ii: binary lattices and related codes. *IEEE Trans. Inf. Theory*, v. 34(5). Citado na página 20.

_____. Multidimensional constellations. ii. voronoi constellations. *IEEE Journal on Selected Areas in Communications*, v. 7, n. 6, p. 941–958, 1989. Citado 2 vezes nas páginas 23 e 24.

INC., W. R. *Mathematica, Version 12.1*. Disponível em: <https://www.wolfram.com/mathematica>. Citado na página 13.

KOSITWATTANARERK, W.; OGGIER., F. On construction d and related constructions of lattices from linear codes. *Proc. of the Int. Workshop on Coding and Cryptography*, p. 428–437, 2013. Citado na página 20.

_____. Connections between construction d and related constructions of lattices. *Des. Codes Cryptogr.*, v. 73, p. 441–455, 2014. Citado na página 20.

MATSUMINE B. M. KURKOSKI, H. O. T. Construction D Lattice Decoding and Its Application to BCH Code Lattices. *2018 IEEE Global Communications Conference (GLOBECOM)*, p. 1–6, 2018. Citado na página 32.

NATARAJAN, L.; HONG, Y.; VITERBO, E. Lattice index coding. *IEEE Trans. Inf. Theory*, v. 61(12), p. 6505–6525, 2015. Citado 4 vezes nas páginas 9, 37, 38 e 47.

PIETRO, N.; BOUTROS, J. J. Leech constellations of construction-a lattices. *IEEE Transactions on Communication*, v. 65, p. 4622–4631, 2017. Citado 6 vezes nas páginas 9, 10, 22, 24, 28 e 52.

SILVA, P. R. B.; SILVA, D. Multilevel ldpc lattices with efficient encoding and decoding and a generalization of construction D′. *IEEE Transactions on Information Theory*, v. 65, n. 5, p. 3246–3260, 2019. Citado na página 32.

STREY, E. *Construções de reticulados a partir de códigos q-ários*. Tese (Doutorado) — Universidade Estadual de Campinas, Campinas, São Paulo, 2017. Acesso em: 25 nov. 2020. Citado 5 vezes nas páginas 10, 17, 19, 20 e 32.

STREY, E.; COSTA, S. I. R. Lattices from codes over $\mathbb{Z}_q$: generalization of constructions D, D' and $\bar{D}$. *Des. Codes Cryptogr.*, v. 85, p. 77–95, 2017. Citado 4 vezes nas páginas 10, 17, 22 e 36.

ZAMIR, R.; NAZER, B. *Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation and Multiuser Information Theory*. [S.l.]: Cambridge Univ. Press, New York, 2014. Citado 3 vezes nas páginas 10, 22 e 25.