RETICULADOS E APLICAÇÕES EM COMUNICAÇÕES

Palavras-Chave: RETICULADOS, CODIFICAÇÃO, TRANSMISSÃO DE SINAIS

Autores/as:
Iran Seixas Lopes Neto, FEEC, UNICAMP
Prof.ª Sueli I. R. Costa, IMECC, UNICAMP

INTRODUÇÃO:

Reticulados são conjuntos discretos de pontos no espaço n-dimensional que, por suas propriedades algébricas e geométricas, tem sido usada em diferentes aplicações. Na área de comunicação, são utilizadas para codificação e transmissão confiável e segura de sinais [1]. Criptografia baseada em reticulados é atualmente uma das principais subáreas da chamada criptografia pós-quântica [3].

Esse trabalho é parte inicial do projeto de iniciação científica "Matemática Discreta, Distância Entre Distribuições e Aplicações em Comunicações e Aprendizagem" (PICME 2023-2024), o qual propõe o estudo e pesquisa de tópicos introdutórios de reticulado, aprendizado de máquina e conexões entre estes.

Dentre os tópicos que já abordamos, escolhemos para a apresentação neste congresso conceitos e propriedades de reticulados que são relevantes para codificação de sinais. Destacamos particularmente os conceitos de empacotamento, cobertura, densidade, reticulados equivalentes e reticulados duais.

METODOLOGIA:

Estudo e pesquisa individual de artigos e livros descritos na bibliografia, e uso de recursos computacionais para simulações dos tópicos abordados (Particularmente Mathematica e Python). Encontros e discussões semanais com a orientadora, participação e apresentação de seminários do grupo de pesquisa relacionados aos temas abordados.

RESULTADOS E DISCUSSÃO:

Reticulados são conjuntos discretos de pontos no espaço Euclidiano n-dimensional, que são descritos como todas as combinações lineares inteiras de um conjunto de vetores independentes.

Dados $b_1, b_2, \dots, b_m$ vetores linearmente independentes entre si em $\mathbb{R}^2$, temos que o reticulado Λ de base $\{b_1, b_2, \dots, b_m\}$ é definido como:

$$\boldsymbol{\Lambda} = \{\boldsymbol{u_1 b_1} + \boldsymbol{u_2 b_2} + \dots + \boldsymbol{u_m b_m} : \boldsymbol{u_1}, \dots \boldsymbol{u_m} \in \boldsymbol{Z}\} \quad (1)$$

O inteiro m é dito posto de Λ, e um reticulado tal que $m = n$ é chamado de posto máximo. Neste trabalho, consideraremos apenas reticulados de posto máximo.

Uma matriz geradora B de um reticulado é formada tendo como suas colunas a base do reticulado.

Uma propriedade interessante das matrizes geradoras é a possibilidade de obter bases alternativas de um reticulado usando uma matriz. Se uma matriz B é geradora de um reticulado qualquer, a matriz $B' = BU$, tal que U é uma matriz unimodular (matriz com entradas inteiras cujo determinante é igual a 1 ou -1), também é geradora do mesmo reticulado [1].

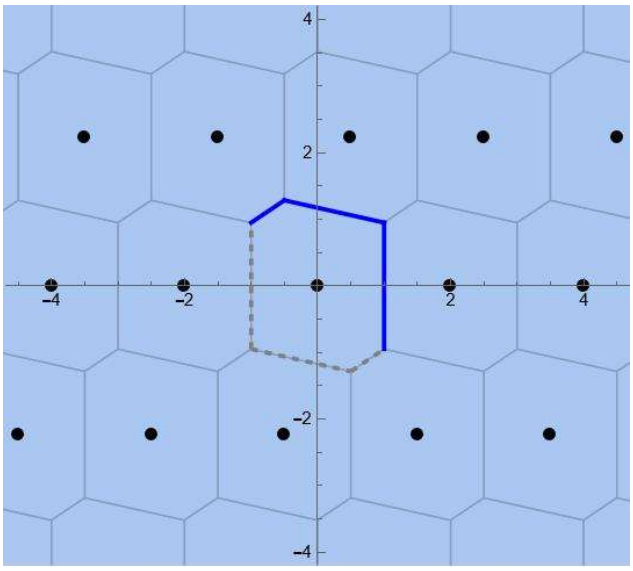
O volume de um reticulado de posto máximo $V(\Lambda)$ é dado pelo módulo do determinante de sua matriz geradora:

$$V(\Lambda) = |\det(B)| \qquad (2)$$

A região de Voronoi $V_\Lambda(x)$ em um ponto $x \in \Lambda$ é o conjunto de todos os pontos em $\mathbb{R}^n$ que estão mais próximos do ponto escolhido do que de qualquer outro ponto do reticulado, e a região de Voronoi do reticulado é dada como a região de Voronoi da origem ($V_\Lambda(0) = V(\Lambda)$). Em $\mathbb{R}^2$, a região de Voronoi assume a forma de um polígono de quatro ou seis lados, dependendo do reticulado. Ao juntar as regiões de Voronoi de todos os pontos de um reticulado, é possível criar uma malha que cobre completamente o espaço $\mathbb{R}^n$.

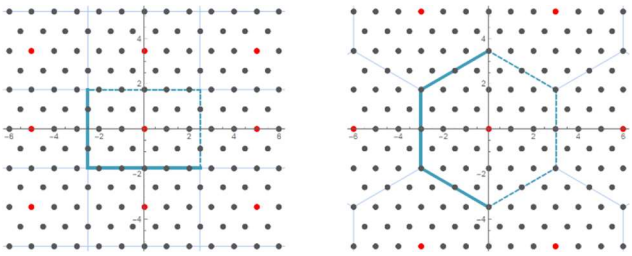
A região de Voronoi de um reticulado independe da base utilizada. Essa propriedade é muito importante para os estudos de comunicações, e ajuda a complementar os conhecimentos do próximo conceito.

Como exemplo, ao usar um reticulado Λ_B de base $B = \{(2,0), (1/2, \sqrt{5})\}$, temos que a matriz geradora associada à base é $\begin{pmatrix} 2 & \frac{1}{2} \\ 0 & \sqrt{5} \end{pmatrix}$, o seu volume é igual a $2\sqrt{5}$, e a sua região de Voronoi é formada da seguinte maneira:



Região de Voronoi do reticulado de base {(2, 0), (1/2, √5)}

A região de Voronoi de um subreticulado costuma ser para selecionar um conjunto finito especial para codificação (constelação de Voronoi)



Constelações de Voronoi do reticulado hexagonal (com base {(1, 0), (1/2, √3/2)}). À esquerda, é usado o subreticulado de base {(5, 0), (0, 2√3)}, e à direita o de base {(6, 0), (3, 3√3)}.

A norma mínima (ou distância mínima) de um reticulado é dada como o mínimo entre todas as normas de vetores não nulos pertencentes a Λ:

$$\lambda = min\{||x||;\ x \in \Lambda, x \neq 0\}, \qquad (3)$$

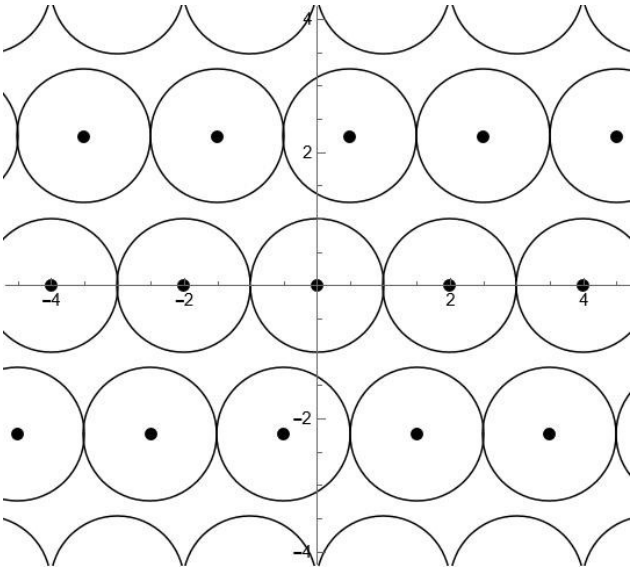
onde $||x||$ é a norma euclidiana padrão do vetor x.

Dado uma bola euclidiana $B^n(x,r)$ em $\mathbb{R}^n$ de raio definido r com centro em um ponto x de um reticulado Λ, definimos o empacotamento do reticulado como a união dessas bolas em todos os pontos de Λ, tal que raio dessas bolas seja igual à metade da norma mínima ($r = \rho = \lambda/2$). O raio ρ é chamado de raio de empacotamento. Este raio define, por exemplo, qual é o tamanho máximo de um vetor ruído para que se possa decodificar corretamente em uma codificação em reticulados.

É importante notar que a bola $B^n(0,\rho)$ está dentro da região de Voronoi $V(\Lambda)$, e toca em seu bordo. Por fim, a densidade de empacotamento Δ de um reticulado é a razão entre o volume da bola $B^n(0,\rho)$ e o volume do reticulado:

$$\Delta(\Lambda) = \frac{V(B^n(0,\rho))}{V(\Lambda)} \qquad (4)$$

Voltando ao exemplo do reticulado Λ_B, temos que $\lambda_B = 2$, $\rho_B = 1$ e $\Delta(\Lambda_B) = 0{,}7025$, com o empacotamento representado abaixo:



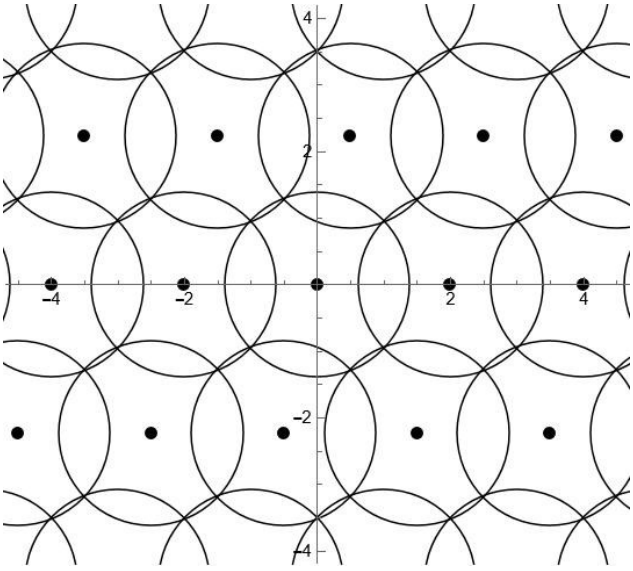
O empacotamento do reticulado de base {(2, 0), (1/2, √5)}

A cobertura de um reticulado é definida como a união de bolas euclidianas $B^n(x,\mu)$ de menor raio μ com centro em todos os pontos x de Λ, de forma que a reunião delas cubra todo o espaço $\mathbb{R}^n$. Não há uma maneira fácil de definir o raio de cobertura; porém, sabemos que $B^n(0,\mu)$ contém a região de Voronoi $V(\Lambda)$ e toca nos seus vértices mais distantes do centro. Por fim, a taxa de cobertura θ de um reticulado é a razão entre o volume da bola $B^n(0,\mu)$ e o volume do reticulado:

$$\theta(\Lambda) = \frac{V(B^n(0,\mu))}{V(\Lambda)} \qquad (5)$$

Para $n \geq 2$, a densidade de empacotamento é sempre menor que um, enquanto a taxa de cobertura é sempre maior que um. Isso acontece porque o empacotamento cobre uma área o máximo possível sem sobrepor, enquanto a cobertura cobre toda a área, sobrepondo o mínimo possível.

Para o reticulado Λ_B, temos que $\mu_B = 1{,}380$ e $\theta(\Lambda_B) = 1{,}337$, com a cobertura representado abaixo:



A cobertura do reticulado de base {(2, 0), (1/2, √5)}

Dois reticulados são ditos equivalentes entre si se um deles for uma dilatação de todos os vetores do outro por um fator k, composta com uma transformação ortogonal. Reticulados equivalentes possuem os raios de empacotamento e cobertura dilatados em k vezes e o volume dilatado em k^n, porém eles tem a mesma densidade de empacotamento e a mesma taxa de cobertura.

Usando as bases geradoras dos reticulados, podemos obter uma relação mais formal entre eles. Dado os reticulados Λ_1 e Λ_2, temos que ambos os reticulados são equivalentes se e somente se existirem duas matrizes B_1 e B_2 geradoras dos respectivos reticulados tais que $B_1 = kA_\theta B_2 U$, onde k é o fator de dilatação ou de contração, A_θ é uma matriz ortogonal, onde $A_\theta^T A_\theta = I_n$, sendo I_n a matriz identidade de dimensão n e U é uma matriz unimodular. Se $|k| = 1$, temos que os reticulados são *congruentes*.

A notação $\Lambda_1 \sim \Lambda_2$ é usada para a equivalência entre dois reticulados.

Um reticulado dual de um reticulado Λ é definido pelo conjunto de vetores $\boldsymbol{y}$ tais que o produto interno desses vetores com qualquer vetor x do reticulado Λ resulte em um valor inteiro, ou seja:

$$\Lambda^* = \{y \in R^n \mid \langle x, y\rangle \in Z \; para \; todo \; x \in \Lambda\} \quad (6)$$

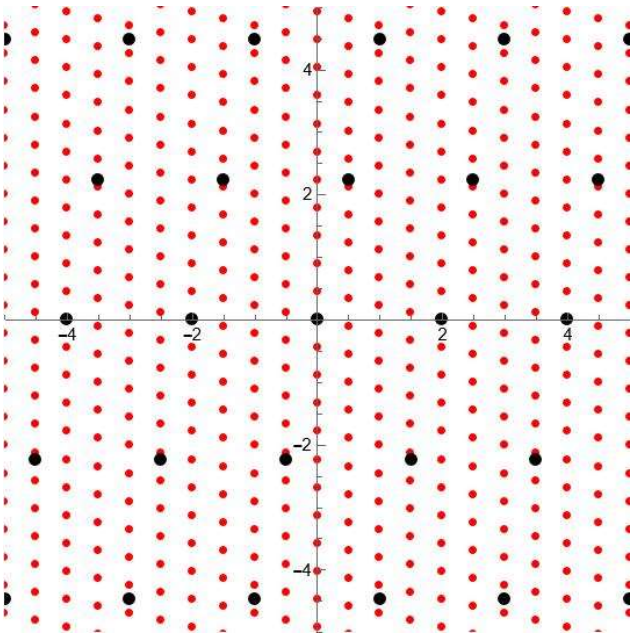
Outra forma de caracterizar o dual de um reticulado é usando sua matriz geradora. Considere um reticulado Λ em $\mathbb{R}^2$ com uma matriz geradora B formada pelas bases v_1 e v_2. Considere também a matriz $(B^T)^{-1}$, composta pelos vetores v_3 e v_4. Usando a propriedade da matriz inversa $AA^{-1} = I_2$, é possível afirmar que $B^T (B^T)^{-1} = I_2$. Simplificando a expressão, obtemos:

$$\begin{pmatrix} < v_1, v_3 > & < v_1, v_4 > \\ < v_2, v_3 > & < v_2, v_4 > \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (7)$$

Da expressão acima, é possível ver que os produtos internos entre as bases v_1 e v_2 e os vetores v_3 e v_4 resultam em valores inteiros. Usando as propriedades do produto interno verificamos então que os vetores linearmente independentes v_3 e v_4 formam uma base para o reticulado dual, portanto a matriz $(B^T)^{-1}$ é matriz geradora desse dual. Apesar da prova estar feita aqui em $\mathbb{R}^2$, é fácil ver que o teorema é válido para quaisquer dimensões.

Se um reticulado Λ possui o reticulado dual equivalente a ele ($\Lambda \sim \Lambda^*$), ele é dito auto dual. De forma semelhante, se Λ for um reticulado auto dual, temos que, para B sendo a matriz geradora desse reticulado:

$$B = kA_\theta^* (B^{-1})^T U \quad (8)$$



O reticulado de base {(2, 0), (1/2, √5)}, junto com o seu dual de base {(1/2, -1/4√5), (0, 1/√5)}

No exemplo do reticulado Λ_B, temos que o seu reticulado dual associado à matriz geradora $\begin{pmatrix} 1/2 & 0 \\ -\frac{1}{4\sqrt{5}} & \frac{1}{\sqrt{5}} \end{pmatrix}$ é equivalente a ele, sendo portanto auto dual.

Observamos através de outros exemplos que reticulados em dimensão 2 eram sempre auto duais. Esta é de fato uma propriedade interessante que demostramos a seguir.

Dada uma matriz geradora B de um reticulado Λ em $\mathbb{R}^2$, podemos provar que ele sempre será um reticulado equivalente ao seu dual, com o fator k sendo igual ao determinante da matriz B e o ângulo de rotação sendo igual a $90°$. Usando a matriz geradora do reticulado dual $(B^{-1})^T = B^*$, também teríamos uma matriz unimodular única:

$$B = \det(B) \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot B^* \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad (9)$$

Isso ocorre por conta da formação única da matriz inversa em $n = 2$ [2], já que com uma matriz $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, ela sempre pode ser dada como $B^{-1} = \frac{1}{\det(B)} \cdot \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$. Calculando então a matriz transposta a essa para obter a matriz do dual $B^* = \frac{1}{\det(B)} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ e substituindo ela na Equação 9, é possível perceber que o produto das matrizes voltará para a matriz geradora B.

Logo, temos que $\Lambda \sim \Lambda^*$ para todo Λ em $\mathbb{R}^2$, com dilatação igual ao determinante da sua matriz geradora e com uma rotação de $90°$.

Note, porém, que esta propriedade só é verdadeira para reticulados em $\mathbb{R}^2$. Para reticulados em maiores dimensões, nem todo reticulado é auto dual. Por exemplo, o reticulado com matriz geradora $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ não é auto dual, pois seu dual, de matriz geradora $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix}$, não é equivalente a ele, o que podemos verificar por exemplo calculando suas densidades de empacotamento, que são diferentes. Para reticulados em dimensões maiores ou iguais a 3, apenas alguns reticulados entram nessa classificação, como os reticulados Z_n, E_8, λ_{24}, etc., que são especiais para certas codificações.

CONCLUSÕES:

Neste trabalho, discutimos e ilustramos parâmetros de reticulados que são relevantes para codificação em transmissão de sinais. Foram estudados particularmente os conceitos de empacotamento, cobertura e reticulado dual.

BIBLIOGRAFIA:

[1] Sueli I. R. Costa, F. Oggier, A. Campello, J-C Belfiore, and E. Viterbo. **Lattices Applied to Coding for Reliable and Secure Comunications.** Springer, 2017.

[2] José L. Boldrini, Sueli I. R. Costa, Vera F. Figueiredo, and Henry G. Wetzler. **Álgebra Linear - 3° Edição**. Editora HARBRA, 1980.

[3] PEIKERT, A. A decade of lattice cryptography. **Foundations and Trends in Theoretical Computer Science**, v. 10, n. 4, p. 283‑424, 2016.

[4] Wolfram Research, Inc. **Mathematica**. Version 13.0, Champaign, IL, 2021.