Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 11, n. 1, 2025.

Trabalho apresentado no XLIII CNMAC, Centro de Convenções do Armação Resort - Porto de Galinhas - PE, 2024

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Relação Entre Reticulados e Códigos Lineares por Meio da Construção A

Gabriel Augusto Alcântara Bezerra,[1] Analisse Magalhães Alves [2], Clarice Dias de Albuquerque [3]
UFCA, Juazeiro do Norte, CE

Dada a grande demanda de armazenamento e transmissão de dados que a vida atual exige, o estudo dos Códigos Corretores de Erros torna-se cada vez mais essencial para garantir a segurança das mensagens que passam por canais ruidosos e podem sofrer interferências.

Em $\mathbb{R}^n$, o problema de encontrar o melhor código possível em $\mathbb{Z}_2^n$ corresponde ao *problema de empacotamento esférico*. Ou seja, encontrar o melhor arranjo de esferas de raio r em $\mathbb{R}^n$, tais que, duas esferas quaisquer só se intersectem em seus bordos, e que esse arranjo de esferas ocupe o maior espaço possível. Em $\mathbb{Z}_2^n$, a solução faz uso da estrutura algébrica de código linear, utilizam-se os vetores do código como os centros das esferas. Em $\mathbb{R}^n$, utiliza-se a estrutura de reticulados. A estrutura algébrico-geométrica de reticulados vem sendo usada a bastante tempo como aliada à Teoria de Códigos Corretores de Erros [2, 4], e também na criptografia [1].

Um reticulado Λ de $\mathbb{R}^n$ é um arranjo de pontos (vetores), tais que, cada $\mathbf{v} \in \Lambda$ é uma combinação linear dos vetores de uma base $\beta = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ de $\mathbb{R}^n$, com coeficientes inteiros, ou seja, $\mathbf{v} = a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \ldots + a_n\mathbf{u}_n$, com $a_i \in \mathbb{Z}$ para $i = 1, 2, \ldots, n$.

Seja Λ um reticulado e $\mathbf{v} \in \Lambda$, o conjunto de pontos no espaço que estão mais próximos de $\mathbf{v}$ do que de qualquer outro ponto de Λ é denominado *região de Voronoi* e é representado por $R(\mathbf{v})$. Considerando que a estrutura de reticulado é geometricamente uniforme, temos que as regiões de Voronoi dos pontos do reticulado são todas iguais. Assim, sendo $R(\mathbf{0})$ a região de Voronoi na origem, todas as outras são obtidas por translações dessa, $R(\mathbf{v}) = R(\mathbf{0}) + \mathbf{v}$, daí, é suficiente estudar a região $R(\mathbf{0})$.

Nesse trabalho, realizamos o estudo no plano $\mathbb{R}^2$. Neste caso, temos que as esferas de raio r passam a ser discos. Considerando o reticulado $\mathbb{Z}^2$, podemos usar discos de raio igual a metade da distância entre os vetores $\mathbf{v}$ do reticulado Λ, dessa forma não temos sobreposição dos discos, e os mesmos se intersectam apenas nos bordos.

A *densidade* de um reticulado nos informa o quanto um plano é preenchido pelos discos, e é dada pela razão entre a área do disco de empacotamento e a área da região de Voronoi. Assim,

$$\Delta = \frac{\acute{a}rea(disco)}{\acute{a}rea(R(0))}, \tag{1}$$

em que Δ é a densidade do reticulado.

Por exemplo, se considerarmos o reticulado quadrado $\mathbb{Z}^2$, gerado pela base $\beta = \{(1,0),(0,1)\}$, temos que a região de Voronoi é o quadrado de lado 2 e o disco de empacotamento tem raio 1, logo, a densidade é $\Delta = \frac{\pi}{4} \cong 0,7804$.

A *construção A* é um método de construção de um reticulado utilizando-se de códigos lineares. Para isso, considera-se a aplicação sobrejetora $\phi : \mathbb{Z}^n \to \mathbb{Z}_q^n$; $\phi(x_1, \ldots, x_n) = (\overline{x_1}, \ldots, \overline{x_n})$, em que

[1] gabriel.bezerra@aluno.ufca.edu.br
[2] analisse.magalhaes@aluno.ufca.edu.br
[3] clarice.albuquerque@ufca.edu.br

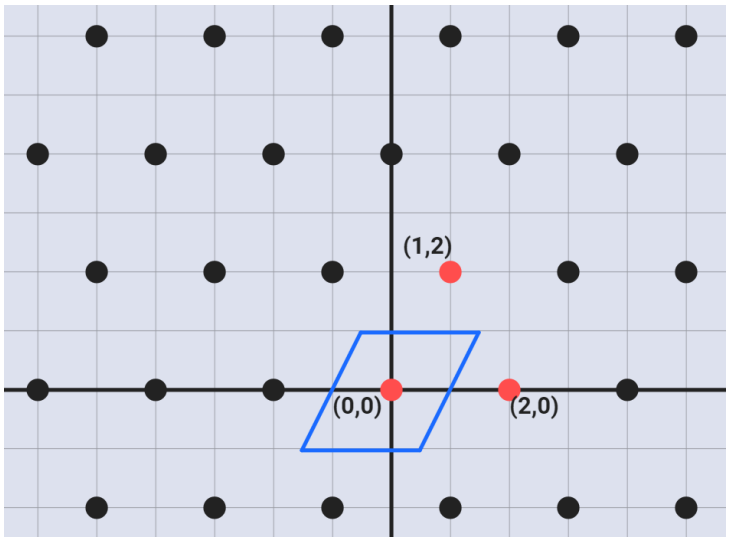

Figura 1: Reticulado formado por código linear.
Fonte: Elaborada pelo autor, baseada na referência [3].

$\overline{x_i}$ é obtido de x_i módulo q. Assim, pode-se mostrar que ϕ é um homomorfismo de grupos que associa a cada código linear binário um reticulado da seguinte forma: $\mathbf{C} \subset \mathbb{Z}_q^n$ é um código linear q-ário se, e somente se, $\phi^{-1}(\mathbf{C})$ é um reticulado em $\mathbb{R}^n$. Reticulados construídos dessa forma são chamados *reticulados q-ários*.

Como ilustração, usaremos um $\mathbf{C} \subseteq \mathbb{Z}_3^2$, que é um código linear q-ário e $\phi^{-1}(\mathbf{C})$ um reticulado, $\phi^{-1}(\mathbf{C})$ é um grupo aditivo [3], desta forma um reticulado q-ário é formado por translações do grupo aditivo formado por $\mathbf{C}$.

A Figura 1 representa o reticulado formado pelo código 3-ário $\langle(\overline{1}, \overline{2})\rangle = \{(0,0), (1,2), (2,0)\}$, onde os pontos vermelhos são os pontos do grupo aditivo, os pretos são as translações de tais pontos, formando o plano reticulado. Em azul temos a de uma região de Voronoi do ponto $(0,0)$ deste reticulado.

Agradecimentos

Esse trabalho teve apoio da Universidade Federal do Cariri.

Referências

[1] D. J. Bernstein, J. Buchmann e E. Dahmen. **Post-Quantum Cryptography**. 1a. ed. Berlin, Heidelberg: Springer, 2009. ISBN: 9783540887010.

[2] S. W. Golomb e L. R. Welch. "Perfect Codes in the Lee Metric and the Packing of Polyominoes". Em: **SIAM Journal on Applied Mathematics** (1970). Aceito. DOI: 10.1137/0118025.

[3] G. C. Jorge. "Reticulados q-ários e algébricos". Tese de doutorado. UNICAMP/IMECC, 2012.

[4] C. C. Lavor, M. M. S. Alves, R. M. de Siqueira e S. I. R. Costa. **Uma Introdução à Teoria de Códigos**. Notas em Matemática Aplicada. SBMAC, 2012. ISBN: 978-85-86883-86-6.