Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 10, n. 1, 2023.

Trabalho apresentado no XLII CNMAC, Universidade Federal de Mato Grosso do Sul - Bonito - MS, 2023

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Códigos Quase-perfeito no Reticulado Algébrico Bidimensional

Jessica R. de O. Moreira[1], João E. Strapasson[2]
UNICAMP, Campinas, SP

Um campo de estudo muito explorado, chamado de reticulado, por ter aplicações em diversas áreas como criptografia, redes e em comunicação. Outro motivo seria os problemas em abertos, principalmente em dimensões superiores à 8, tanto em empacotamento de esfera quanto de cobertura. Essa estrutura pode ser considerado um código linear, em que são construídos a partir de uma transformação linear com uma matriz geradora, para usar elementos da Álgebra Linear para codificação e decodificação de mensagens.

O reticulado é subgrupo aditivo e discreto que está contido no espaço $\mathbb{R}^n$. Isto implica na existência de m vetores linearmente independentes que geram os pontos pertencentes a esse espaço. Por definição, o reticulado Λ é dado por todas as combinações inteiras desses vetores. A matriz geradora M do reticulado Λ é a matriz que contém, por linha, esses vetores. Tem como um nome especial a matriz de Gram G, obtida pela multiplicação da matriz geradora pela sua transposta.

Sejam Λ e Λ_a reticulados tal que $\Lambda \subset \Lambda_a$. Diz que Λ_a é o reticulado ambiente para o reticulado Λ. A proposta é investigar Λ considerando o ambiendo sendo uma familia de reticulado algébrico tomando a métrica euclidiana, tal que Λ seja código quase-perfeito em Λ_a. Essa ideia se deu com base na tese [4], em que exploraram a existência de códigos perfeitos em reticulados ambientes gerais considerando a métrica euclidiana.

A construção dessa família de reticulados algébricos $\Lambda_{a,l}$ é dado via extensão de corpos quadrático, para mais detalhe dessa construção encontra-se em [1]. Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{-l})$ um corpo quadrático, em que $l > 0$ e l é um inteiro livre de quadrados e $-l \equiv 1(\mod 4)$. Então, o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ sobre $\mathbb{Z}$ é igual a $\mathbb{Z}\left[\frac{1+\sqrt{-l}}{2}\right]$ e uma $\mathbb{Z}-$base de $\mathcal{O}_{\mathbb{K}}$ é $\left\{1, \frac{1+\sqrt{-l}}{2}\right\}$. Sendo assim, obtêm-se uma matriz geradora (1) para $\Lambda_{a,l}$.

$$M_l = \sqrt{2}\begin{pmatrix} 1 & 0 \\ -\frac{1}{2} & \frac{\sqrt{l}}{2} \end{pmatrix} \tag{1}$$

Para caracterizar um código quase-perfeito no ambiente geral, é importante definir as bolas de empacotamento e de cobertura discreto. Essas definições podem ser encontrado também em [3].

Definição 1. *Seja $\mathcal{D}$ um conjunto definido como todas as distâncias atingíveis em Λ_a com métrica l_2, isso é,*

$$\mathcal{D} = \mathcal{D}(\Lambda_a) = \{||x|| \ / \ x \in \Lambda_a\} \tag{2}$$

Definição 2. *Considere $\Lambda \subset \Lambda_a$ um reticulado. O raio de empacotamento(discreto), denotado por $r(\Lambda)$, é o maior r tal que*

$$i) \qquad ((\tilde{B}_r + \lambda) \cap \tilde{B}_r) \cap \Lambda_a = \varnothing, \text{ em que } 0 \neq \lambda \in \Lambda \tag{3}$$

$$ii) \qquad r \in \mathcal{D}(\Lambda_a) \tag{4}$$

[1] j230106@dac.unicamp.br
[2] strapass@unicamp.br

Definição 3. *Seja $\Lambda \subset \Lambda_a$ um reticulado. O raio de Cobertura (discreto), denotado por $R(\Lambda)$, é o menor $R \in \mathcal{D}(\Lambda_a)$ tal que*

$$\bigcup_{\lambda \in \Lambda} (\tilde{B}_R + \lambda) = \Lambda_a. \tag{5}$$

Definição 4. *Um reticulado Λ tem grau de imperfeição t se a distância entre o raio de empacotamento e de cobertura for igual a t, ou seja,*

$$d(r(\Lambda), R(\Lambda)) = t \tag{6}$$

Definição 5. *Seja $\Lambda \subset \Lambda_a$, um reticulado contido em um reticulado ambiente qualquer. Diz que Λ é um código quase-perfeito em Λ_a se a $d(r(\Lambda), R(\Lambda)) = 1$, em que $r(\Lambda)$ é o raio de empacotamento e $R(\Lambda)$ é o raio de cobertura (discreto).*

O teorema 1 garante a existência de código quase-perfeitos em um reticulado ambiente geral, foi desenvolvido em [5] para o $\mathbb{Z}^n$, por homomorfismo pode ser estendido para ambiente geral. Esse resultado foi fundamental para construção do algoritmo, que também foi adaptado de trabalhos anteriores [2] e [4]. Esse algoritmo listará todos os $\Lambda \subset \Lambda_a$ que são códigos desse tipo em Λ_a.

Teorema 1. *Há código quase-perfeito $(n, \bar{r}_i, A)$ com a métrica l_p para algum inteiro i se existir um grupo abeliano G de ordem A com $|\tilde{B}^n(\bar{r})| < A < |\tilde{B}^n(r_{i+1})|$ e homomorfismo $\phi : \Lambda_a \to G$ tal que ϕ em $\tilde{B}^n(r_i)$ é injetiva e para $\tilde{B}^n(\bar{r}_{i+1})$ é sobrejetiva.*

Com isso, foi explorado a lista de $\Lambda \subset \Lambda_{a,l}$ obtido pelo algoritmo, a fim de vincular a quantidade de códigos quase-perfeitos com o aumento no valor de l. Para realizar essa análise, foram separados em três formatos principais, em que esses formatos está associado à quantidade de camada de poli-hexágono na bola de empacotamento de Λ.

Realizando uma investigação em cada formato, constatou-se que no tipo 1 e no tipo 2, em que possuem uma e três camadas de poli-hexágono respectivamente, com aumento de l obtêm-se um aumento proporcional desses códigos. Já no tipo 3 com 5 camadas de poli-hexágono, não pôde ser determinado essa quantidade.

Agradecimentos

Processo nº 20/09838-0, Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP).

Referências

[1] C. W. De O. Benedito. "Famílias de reticulados algébricos e reticulados ideais". Dissertação de mestrado. São José do Rio Preto: Universidade Estadual Paulista "Júlio de Mesquita Filho", 2010.

[2] N. M. L. B. Da G. Morais. "Estudo sobre o grau de imperfeição em sub-reticulados do reticulado inteiro". Dissertação de mestrado. Campinas: Universidade Estadual de Campinas, 2015.

[3] J. E. Strapasson et al. "Quasi-perfect codes in the l_p metric". Em: **Heidelberg** 37.2 (2018), pp. 852–866. URL: https://arxiv.org/pdf/1509.05348v1.pdf.

[4] G. R. A. Da S. Strey. "Códigos Perfeitos e Ladrilhamentos em Diversos Reticulados Ambientes". Tese de doutorado. campinas: Universidade Estadual de Campinas, 2020.

[5] F. Zhao e S. Qiao. "Radius Selection Algorithms for Sphere Decoding". Em: **Proceedings of C3S2E-09, ACM International Conference Proceedings Series** (mai. de 2009), pp. 169–174. URL: https://www.cas.mcmaster.ca/~qiao/publications/ZQ09.pdf.