Trabalho apresentado no XL CNMAC, Evento Virtual - Co-organizado pela Universidade do Mato Grosso do Sul (UFMS).

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Códigos perfeitos na métrica p-Lee

Lucas Eduardo Nogueira Gonçalves[1]
Instituto de Ciência e Tecnologia, Unifesp, São José dos Campos, SP
Grasiele Cristiane Jorge[2]
Instituto de Ciência e Tecnologia, Unifesp, São José dos Campos, SP

1 Introdução

A teoria dos Códigos Corretores de Erros surgiu na década de 40 quando foram construídos códigos na métrica de Hamming. A métrica de Lee foi introduzida em 1957/1958 para transmissão de sinais sobre $\mathbb{Z}_p$, p primo. Depois, em 1970 ela foi generalizada para $\mathbb{Z}_q$, $q \geq 2$ natural, e foi enunciada a famosa conjectura de Golomb-Welch, que afirma que não existem códigos perfeitos na métrica de Lee para qualquer dimensão $n \geq 3$ e qualquer raio $r \geq 2$ [3]. Esta conjectura tem sido a principal responsável pelo desenvolvimento do estudo de códigos na métrica de Lee e embora existam vários resultados parciais relacionados a ela, acredita-se que ainda está longe de ser demonstrada. Neste trabalho, vamos apresentar alguns resultados obtidos em [2] em 2016 sobre códigos lineares perfeitos em $\mathbb{Z}_q^n$ na métrica p-Lee, $1 \leq p < \infty$, que é uma generalização da métrica de Lee.

Através da Construção A é possível demostrar que estudar códigos lineares perfeitos em $\mathbb{Z}_q^n$ na métrica p-Lee com raio de empacotamento r_p satisfazendo $2r_p < q$ é equivalente a estudar reticulados em $\mathbb{Z}^n$ que são códigos perfeitos na métrica ℓ_p. Foi mostrado em [2] que trabalhando em $\mathbb{Z}^n$ é possível limitar o raio de empacotamento de um código linear perfeito em função do supremo de todas as densidades de empacotamento de reticulados na dimensão n na métrica ℓ_p. Para $p = 2$ a métrica ℓ_2 é a métrica euclidiana e, neste caso, a densidade de empacotamento máxima entre reticulados é conhecida para algumas dimensões e, então, é possível encontrar limitantes para o raio de empacotamento de códigos lineares perfeitos. Em [2] foi implementado um algoritmo no *software Wolfram Mathematica* para buscar códigos lineares perfeitos em $\mathbb{Z}^n$ na métrica ℓ_2 para $n = 2$ e $n = 3$.

2 Detalhamento dos conceitos e resultados

Dado $q \in \mathbb{N}$, um código linear $C \subseteq \mathbb{Z}_q^n$ é um subgrupo aditivo de $\mathbb{Z}_q^n$. Por sua vez, um reticulado em $\mathbb{R}^n$ é um subgrupo aditivo discreto de $\mathbb{R}^n$. Um reticulado $\Lambda \subseteq \mathbb{R}^n$ também pode ser definido um conjunto de pontos em $\mathbb{R}^n$ escritos como combinação linear com coeficientes inteiros de m vetores linearmente independentes $\{v_1, \ldots, v_m\}$ em $\mathbb{R}^n$, isto é, $\Lambda = \{\sum_{i=1}^m a_i v_i;\ a_i \in \mathbb{Z}\}$. Um código linear em $\mathbb{Z}^n$ é simplesmente um reticulado contido em $\mathbb{Z}^n$.

Códigos lineares em $\mathbb{Z}_q^n$ podem ser "levantados" para reticulados em $\mathbb{Z}^n$ via a Construção A, definida como segue. Considere $\phi : \mathbb{Z}^n \longrightarrow \mathbb{Z}_q^n$ tal que $\phi(x_1, \ldots, x_n) = (\overline{x_1}, \ldots, \overline{x_n})$. Temos que se $C \subseteq \mathbb{Z}_q^n$ é um código linear, então $\phi^{-1}(C) \subseteq \mathbb{Z}^n$ é um reticulado.

[1] lucasedng@gmail.com
[2] grasiele.jorge@unifesp.br

Relembramos que a distância ℓ_p, $1 \leq p \leq \infty$, entre dois elementos $x, y \in \mathbb{Z}^n$ é $d_p(x,y) := \left(\sum_{i=1}^n |x_i - y_i|^p\right)^{1/p}$. Já a métrica p-Lee é definida para dois elementos $\overline{x}, \overline{y} \in \mathbb{Z}_q^n$ como $d_{p,Lee}(\overline{x}, \overline{y}) = \left(\sum_{i=1}^n \left(d_{Lee}(\overline{x}_i, \overline{y}_i)\right)^p\right)^{1/p}$ onde $d_{Lee}(\overline{x}_i, \overline{y}_i) = \max\{|x_i - y_i|, q - |x_i - y_i|\}$ para $0 \leq x_i, y_i < q$.

Dado um reticulado $\Lambda \subseteq \mathbb{R}^n$, a densidade de empacotamento de Λ na métrica ℓ_p, denotada por $\Delta_p^n(\Lambda)$, é a proporção do espaço coberto por esferas idênticas com o maior raio possível de forma que a intersecção entre quaisquer duas esferas ou é vazia ou ocorre somente no bordo. Seja $\Delta_p^n = \sup_\Lambda \Delta_p^n(\Lambda)$, onde $\Lambda \subseteq \mathbb{R}^n$ é reticulado.

Proposition 2.1. *[2] O raio de empacotamento r_p de um código linear perfeito em $\mathbb{Z}^n$ na métrica ℓ_p satisfaz $r_p \leq \frac{n^{1/p}(1+(\Delta_p^n)^{1/n})}{2(1-(\Delta_p^n)^{1/n})}$.*

Usando este limitante para o raio de empacotamento e a Proposição 2.2 foram demonstradas as Proposições 2.3 e 2.4 com auxílio de um algoritmo computacional.

Proposition 2.2. *[1] Seja $\mathcal{P} \subset \mathbb{Z}^n$, tal que $|\mathcal{P}| = m$. Existe um ladrilhamento de $\mathbb{Z}^n$ por transladados $\mathcal{P}$ se, e somente se, existem um grupo abeliano G de ordem m e um homomorfismo $\phi : \mathbb{Z}^n \to G$ tal que a restrição de ϕ a $\mathcal{P}$ é uma bijeção.*

Proposition 2.3. *[2] Não existem códigos lineares perfeitos em $\mathbb{Z}^2$ com raio r na métrica ℓ_2, a menos que $r = 1, \sqrt{2}, 2,$ ou $2\sqrt{2}$.*

Exemplos de homomorfismos encontrados pelo algoritmo associado à Proposição 2.3 são $\phi(x,y) = x+\overline{2}y \in \mathbb{Z}_5$, $\phi(x,y) = x+\overline{3}y \in \mathbb{Z}_9$, $\phi(x,y) = x+\overline{5}y \in \mathbb{Z}_{13}$ e $\phi(x,y) = x+\overline{5}y \in \mathbb{Z}_{25}$. Os códigos lineares perfeitos associados a estes homomorfismos são seus núcleos, ou seja, os reticulados gerados por $\{(1,2),(0,5)\}$, $\{(3,2),(0,3)\}$, $\{(1,5)),(3,2)\}$ e $\{(5,4),(0,5)\}$, respectivamente. Os códigos lineares associados a tais reticulados via Construção A são $\left\langle(\overline{1},\overline{2})\right\rangle \subset \mathbb{Z}_5^2$, $\left\langle(\overline{3},\overline{2})\right\rangle \subset \mathbb{Z}_9^2$, $\left\langle(\overline{1},\overline{5})\right\rangle \subset \mathbb{Z}_{13}^2$ $\left\langle(\overline{5},\overline{4})\right\rangle \subset \mathbb{Z}_{25}^2$ e eles são perfeitos na métrica 2-Lee.

Proposition 2.4. *[2] Não existem códigos lineares perfeitos em $\mathbb{Z}^3$ com raio r na métrica ℓ_2, a menos que $r = 1,$ ou $\sqrt{3}$.*

Exemplos de homomorfismos encontrados pelo algoritmo associado à Proposição 2.4 são $\phi(x,y,z) = x + \overline{2}y + \overline{3}z \in \mathbb{Z}_7$ e $\phi(x,y,z) = x + \overline{3}y + \overline{9}z \in \mathbb{Z}_{27}$. Os códigos lineares perfeitos associados a estes homomorfismos são seus núcleos, ou seja, os reticulados gerados por $\{(1,0,2),(0,1,4),(0,0,7)\}$ e $\{(3,8,0),(0,3,2),(0,0,3)\}$, respectivamente.

Agradecimentos

Agradecemos a FAPESP, processo 2019/14390-1, pelo auxílio financeiro.

Referências

[1] AlBdaiwi B. F. and Horak P. Diameter Perfect Lee Codes. *IEEE Transactions on Information Theory*, 58(8) : 5490 − 5499, 2012. DOI: 10.1109/TIT.2012.2196257.

[2] Campello A., Costa S. I. R., Jorge G. C. and Strapasson J. E. Perfect codes in the l_p metric. *European Journal of Combinatorics*, 53 : 72 − 85, 2016. DOI: 10.1016/j.ejc.2015.11.002.

[3] Golomb, S. W. and Welch L. R. Perfect Codes in the Lee Metric and the Packing of Polyominoes. *SIAM Journal on Applied Mathematics*, 18(2) : 302 − 317, 1970. DOI: 10.1137/0118025.