Códigos na métrica p-Lee

Ana Flávia C. M. A. Nogueira & Grasiele C. Jorge

Instituto de Ciência e Tecnologia - Universidade Federal de São Paulo

ana_alckmin@hotmail.com, grasiele.jorge@unifesp.br

UNIFESP 25 ANOS

Universidade pública, conhecimento público

Introdução

Neste trabalho serão abordados códigos lineares q-ários na métrica p-Lee, que é uma generalização da métrica de Lee.

Códigos e reticulados q-ários

Definição 1. *Seja $q \in \mathbb{N}$, $q \geq 2$. Um* **código linear q-ário $C \subseteq \mathbb{Z}_q^n$** *é um $\mathbb{Z}_q$-submódulo de $\mathbb{Z}_q^n$, ou seja, é um subgrupo aditivo de $\mathbb{Z}_q^n$.*

Definição 2. *Seja $\{v_1, \cdots, v_m\}$, $m \leq n$, um conjunto de vetores linearmente independentes em $\mathbb{R}^n$. O conjunto de pontos*

$$\Lambda = \left\{ \sum_{i=1}^{m} \lambda_i v_i,\ \lambda_i \in \mathbb{Z} \text{ para todo } i = 1, \cdots, m \right\}$$

é chamado de **reticulado**.

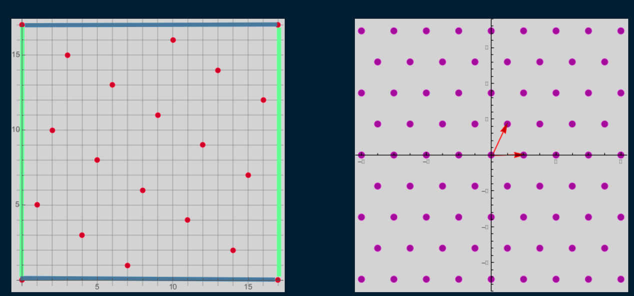

Figura 1: Código 17-ário gerado por $(\overline{1}, \overline{5})$ em $\mathbb{Z}_{17}^2$ e reticulado gerado por $\{(1,0), (1/2, \sqrt{3}/2)\}$.

Proposição 1. *[2] Considere a aplicação sobrejetora*

$$\begin{aligned} \phi :\ \mathbb{Z}^n &\longrightarrow \mathbb{Z}_q^n \\ (x_1, \ldots, x_n) &\longmapsto (\overline{x_1}, \ldots, \overline{x_n}). \end{aligned}$$

Temos que $C \subseteq \mathbb{Z}_q^n$ é um código linear q-ário se, e somente se, $\phi^{-1}(C) = \Lambda_A(C) \subseteq \mathbb{Z}^n$ é um reticulado. Além disso, temos que $q\mathbb{Z}^n \subseteq \Lambda_A(C)$ e $\Lambda_A(C)/q\mathbb{Z}^n \simeq C$.

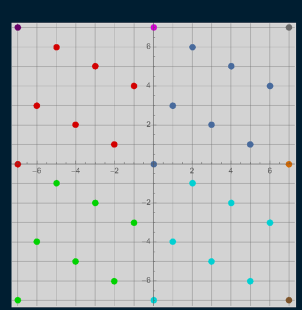

Figura 2: Reticulado 7-ário $\Lambda_A(C)$.

Métrica p-Lee

Definição 3. *Dados $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in \mathbb{R}^n$ e $1 \leq p < \infty$, definimos a métrica d_p como*

$$d_p(a, b) = \left(\sum_{i=1}^{n} |a_i - b_i|^p \right)^{1/p}.$$

Definição 4. *Dados $\overline{a}, \overline{b} \in [\overline{0}, \overline{q})$ com $0 \leq a, b < q$, definimos a métrica de Lee por $d_{Lee}(\overline{a}, \overline{b}) = min\{|a - b|, q - |a - b|\}$.*

Definição 5. *Dados $\overline{a} = (\overline{a_1}, \ldots, \overline{a_n}), \overline{b} = (\overline{b_1}, \ldots, \overline{b_n}) \in [\overline{0}, \overline{q})^n$ e $1 \leq p < \infty$, definimos a métrica p-Lee como*

$$d_{p,Lee}(\overline{a}, \overline{b}) = \left(\sum_{i=1}^{n} \left(d_{Lee}(\overline{a_i}, \overline{b_i}) \right)^p \right)^{1/p}.$$

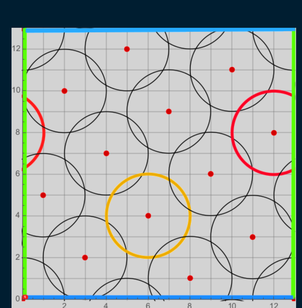

Figura 3: Código gerado por $(\overline{1}, \overline{5})$ em $\mathbb{Z}_{13}^2$ na métrica 2-Lee.

Raio de empacotamento

Proposição 2. *[1] Seja $C \subseteq \mathbb{Z}_q^n$ um código linear q-ário com distância mínima $\mu_p(C)$ na métrica p-Lee. Temos que o reticulado $\Lambda_A(C)$ tem distância mínima $\mu_p(\Lambda_A(C)) = \min\{\mu_p(C), q\}$ na métrica d_p.*

Exemplo 1. *O código $C = \{(\overline{0}, \overline{0}, \overline{0}, \overline{0}, \overline{0}, \overline{0}, \overline{0}), (\overline{1}, \overline{1}, \overline{1}, \overline{1}, \overline{1}, \overline{1}, \overline{1})\}$, contido em $\mathbb{Z}_2^7$, tem distância mínima $\mu_p(C) = 7$ na métrica de Lee e $\Lambda_A(C)$ tem distância mínima $\mu_p(\Lambda_A C) = 2$ na métrica d_1.*

Proposição 3. *[1] Seja $C \subseteq \mathbb{Z}_q^n$ um código linear q-ário com raio de empacotamento $r_p = r_p(C)$ na métrica p-Lee. Se $2\,r_p < q$, então o raio de empacotamento de $\Lambda_A(C)$ na métrica d_p também é r_p.*

Observação 1. *Em geral, para $p > 1$, $r_p(C) \neq \left\lfloor \frac{\mu_p(C)-1}{2} \right\rfloor$.*

Exemplo 2. *Sejam $q = 4$, $n > 2^p$, $p > 1$,*

$$C_1 = \{(\overline{0}, \overline{0}, \ldots, \overline{0}), (\overline{2}, \overline{0}, \ldots, \overline{0})\} \subset \mathbb{Z}_4^n \text{ e}$$

$$C_2 = \{(\overbrace{\overline{1}, \overline{1}, \ldots, \overline{1}}^{2^p}, \overline{0}, \ldots, \overline{0})j;\ \ j = \overline{0}, \overline{1}, \overline{2}, \overline{3}\} \subset \mathbb{Z}_4^n.$$

Temos que $\mu_p(C_1) = \mu_p(C_2) = 2$, $r_p(C_1) = 0$ e $r_p(C_2) = (2^{p-1} - 1)^{1/p}$.

Proposição 4. *[1] A distância mínima e o raio de empacotamento de um reticulado q-ário $\Lambda_A(C)$ na métrica d_p satisfazem*

$$\left\lfloor \frac{\mu_p(\Lambda) - 1}{2} \right\rfloor \leq r_p(\Lambda) < \frac{\mu_p(\Lambda)}{2} + \frac{n^{1/p}}{2}.$$

Decodificação

Proposição 5. *[4] Sejam $\Lambda_A(C)$ um reticulado q-ário e $r = (r_1, \cdots, r_n) \in \mathbb{R}^n$ um vetor. Dado $\overline{x} \in \Lambda_A(C)/q\mathbb{Z}^n$ com $x = (x_1, \cdots, x_n)$, o representante z da classe $\overline{x}$ que está mais próximo de r em $\Lambda_A(C)$, na métrica d_p, $1 \leq p < \infty$, é $z = (z_1, \cdots, z_n)$, onde $z_i = x_i + qw_i$ e $w_i = \left\lceil \frac{r_i - x_i}{q} \right\rfloor$ para cada $i = 1, \cdots, n$.*

Proposição 6. *[4] Sejam $\Lambda_A(C)$ um reticulado q-ário e $r = (r_1, \cdots, r_n) \in \mathbb{R}^n$ um vetor. Se $\overline{x} \in C$ é o elemento do código C mais próximo de r (mod q) considerando a métrica $d_{p,Lee}$, $1 \leq p < \infty$, então $z \in \Lambda_A(C)$ dado pela Proposição 5 tal que $\overline{z} = \overline{x}$ em $\Lambda_A(C)/q\mathbb{Z}^n$, é um elemento de $\Lambda_A(C)$ mais próximo de r na métrica d_p.*

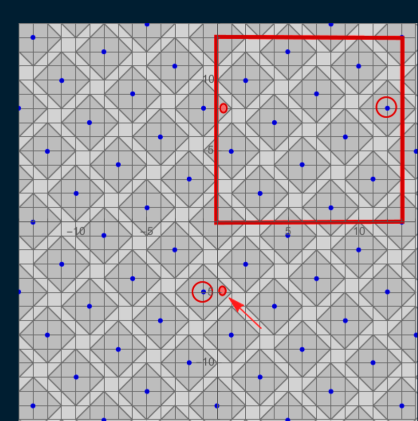

Figura 4: Reticulado $\Lambda_A(C)$, onde C é o código gerado por $(\overline{1}, \overline{5})$ em $\mathbb{Z}_{13}^2$.

Referências

[1] A. Campello, G. C. Jorge, J. E. Strapasson e S. I. R. Costa. Perfect codes in the l_p metric. *European Journal of Combinatorics*, 53:72 – 85, 2016.

[2] J. H. Conway e N. J. A. Sloane. *Sphere packings, lattices and groups*. Springer-Verlag, New York, NY, USA, 1998.

[3] S. W. Golomb e L. R. Welch. Perfect codes in the Lee metric and the packing of polyominoes. *SIAM Journal on Applied Mathematics*, 18(2):302–317, 1970.

[4] G. C. Jorge. Reticulados q-ários e algébricos. *Tese de Doutorado, Universidade Estadual de Campinas*, 2012.

Agradecimentos

CAPES