Sobre parâmetros das Construções D e D'

Franciele do Carmo Silva

Trabalho em conjunto com Ana Souza, Eleonesio Strey e Sueli Costa

Encontro de Códigos, Reticulados e Informação

15 de Junho de 2023

Sumário

Construção A

Exemplo:

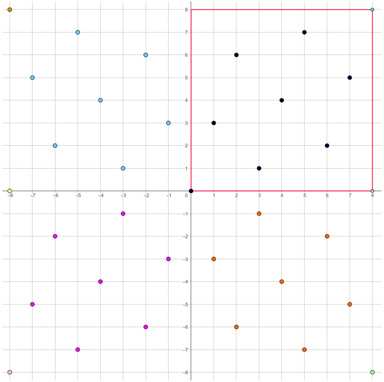

Figure 1: Construção A do código $\mathcal{C} = \langle(\overline{1}, \overline{3})\rangle \subseteq \mathbb{Z}_8^2$.

Construção A

Proposição [Costa et al, 2017]

Seja $n \in \mathbb{N}$ e consideremos a aplicação:

$$\begin{aligned} \rho : \mathbb{Z}^n &\rightarrow \mathbb{Z}_q^n \\ x &\mapsto (x_1 \mod q, \ldots, x_n \mod q). \end{aligned}$$

Dado um subconjunto $S \subset \mathbb{Z}_q^n$, então $\rho^{-1}(S)$ é reticulado em $\mathbb{R}^n$ se, e somente se, S é um código linear em $\mathbb{Z}_q^n$.

Construção A: propriedades básicas

Definição

Seja $C \subseteq \mathbb{Z}_q^n$ um código linear com $q \geq 2$. O reticulado $\Lambda_A(C) = \rho^{-1}(C)$ é dito ser obtido da **Construção A** e chamado **reticulado q-ário**.

Propriedades: [Costa et al, 2017]

- Valem as inclusões: $q\mathbb{Z}^n \subseteq \Lambda_A(C) \subseteq \mathbb{Z}_q^n$.
- Tem-se:

$$\begin{aligned} \left|\frac{\Lambda_A(C)}{q\mathbb{Z}^n}\right| &= \frac{q^n}{\mathrm{vol}\ \Lambda_A(C)} = |C|; \\ d_{\mathrm{p}}(\Lambda_A(\mathcal{C})) &= \min\left\{d_{\mathrm{p}}(\mathcal{C}), q\right\}. \end{aligned}$$

Construção $\overline{D}$

Definição

Seja $\mathcal{C}_a \subseteq \mathcal{C}_{a-1} \subseteq \ldots \subseteq \mathcal{C}_1 \subseteq \mathbb{Z}_q^n$ uma cadeia de códigos lineares. O conjunto obtido pela construção $\overline{D}$ (*code formula*) é definido como:

$$\Gamma_{\overline{D}} := q^a\mathbb{Z}^n + q^{a-1}\sigma(\mathcal{C}_1) + \ldots + q^{a-i}\sigma(\mathcal{C}_i) + q\sigma(\mathcal{C}_{a-1}) + \sigma(\mathcal{C}_a).$$

Observações:

- Se $a = 1$, essa definição coincide com a Construção A.
- Em geral, $\Gamma_{\overline{D}}$ não é um reticulado.
- Define-se $\Lambda_{\overline{D}}$ como o menor reticulado que contém $\Gamma_{\overline{D}}$.

Construção $\overline{D}$: Condições para obtermos um reticulado

Teorema [Teo. 9, Strey]

Dada uma cadeia de códigos lineares $\mathcal{C}_a \subseteq \mathcal{C}_{a-1} \subseteq \ldots \subseteq \mathcal{C}_1 \subseteq \mathbb{Z}_q^n$, as seguintes condições são equivalentes:

1. $\Gamma_{\overline{D}}$ é um reticulado.
2. $\mathcal{C}_a \subseteq \mathcal{C}_{a-1} \subseteq \ldots \subseteq \mathcal{C}_1 \subseteq \mathbb{Z}_q^n$ é fechada sob adição zero-um.
3. $\Gamma_{\overline{D}} = \Lambda_{\overline{D}} = \Lambda_D$.

Dados $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_q^n$, a adição zero-um é definida coordenada a coordenada como:

$$x_i * y_i = \begin{cases} 0, & \text{se } 0 \leq \sigma(x_i) + \sigma(y_i) < q; \\ 1, & \text{se } q \leq \sigma(x_i) + \sigma(y_i) \leq 2(q-1). \end{cases}$$

Construção D

Definição

Consideremos uma cadeia de códigos lineares em $\mathbb{Z}_q^n$ dada por:

$$\mathcal{C}_a \subseteq \mathcal{C}_{a-1} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathcal{C}_0 = \mathbb{Z}_q^n.$$

Dados números inteiros $k_1 \geq k_2 \geq \cdots \geq k_a \geq 0$ e um conjunto de n-uplas $\{\mathbf{b}_1, \ldots, \mathbf{b}_{k_1}\}$ em $\mathbb{Z}_q^n$ tais que $\mathcal{C}_\ell = \langle \mathbf{b}_1, \ldots, \mathbf{b}_{k_\ell} \rangle$ para $\ell = 1, 2, \ldots, a$, temos que

$$\Lambda_D = \left\{ q^a \boldsymbol{z} + \sum_{s=1}^{a} \sum_{i=k_{s+1}+1}^{k_s} \alpha_i^{(s)} q^{a-s} \sigma(\boldsymbol{b}_i) : \ \boldsymbol{z} \in \mathbb{Z}^n \text{ e } 0 \leq \alpha_i^{(s)} < q^s \right\}.$$

Construção D'

Definição

Seja

$$\mathcal{C}_a \subseteq \mathcal{C}_{a-1} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathcal{C}_0 = \mathbb{Z}_q^n$$

uma família de códigos lineares q-ários sobre $\mathbb{Z}_q$.

Construção D'

Definição

Seja

$$\mathcal{C}_a \subseteq \mathcal{C}_{a-1} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathcal{C}_0 = \mathbb{Z}_q^n$$

uma família de códigos lineares q-ários sobre $\mathbb{Z}_q$.

Considere

$$\underbrace{\langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_1} \rangle}_{\mathcal{C}_1^\perp} \subseteq \underbrace{\langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_1}, \boldsymbol{h}_{r_1+1}, \ldots, \boldsymbol{h}_{r_2} \rangle}_{\mathcal{C}_2^\perp} \subseteq \cdots \subseteq \underbrace{\langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_a} \rangle}_{\mathcal{C}_a^\perp} \subseteq \mathbb{Z}_q^n.$$

Matriz de verificação

$$\boldsymbol{H} := \begin{bmatrix} \sigma(\boldsymbol{h}_1) \\ \vdots \\ \sigma(\boldsymbol{h}_{r_1}) \\ q\sigma(\boldsymbol{h}_{r_1+1}) \\ \vdots \\ q\sigma(\boldsymbol{h}_{r_2}) \\ \vdots \\ q^{a-1}\sigma(\boldsymbol{h}_{r_{a-1}+1}) \\ \vdots \\ q^{a-1}\sigma(\boldsymbol{h}_{r_a}) \end{bmatrix}_{r_a \times n}.$$

Construção D' para códigos q-ários [Strey, 2017]

Definição

Seja

$$\mathcal{C}_1^\perp \subseteq \mathcal{C}_2^\perp \ldots \subseteq \mathcal{C}_{a-1}^\perp \subseteq \mathcal{C}_a^\perp \subseteq \mathbb{Z}_q^n$$

uma família de códigos lineares q-ários.

Considere

$$\underbrace{\langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_1} \rangle}_{\mathcal{C}_1^\perp} \subseteq \underbrace{\langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_1}, \boldsymbol{h}_{r_1+1}, \ldots, \boldsymbol{h}_{r_2} \rangle}_{\mathcal{C}_2^\perp} \subseteq \cdots \subseteq \underbrace{\langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_a} \rangle}_{\mathcal{C}_a^\perp} \subseteq \mathbb{Z}_q^n.$$

Então, a Construção D' corresponde a

$$\Lambda_{D'} = \left\{ \boldsymbol{x} \in \mathbb{Z}^n : \boldsymbol{H}\boldsymbol{x} \equiv 0 \mod q^a \right\}.$$

Construção D'

Definição

Seja

$$\mathcal{C}_a \subseteq \mathcal{C}_{a-1} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathcal{C}_0 = \mathbb{Z}_q^n$$

uma família de códigos lineares q-ários.

Sejam $r_0 := 0 \leq r_1 \leq r_2 \leq \ldots \leq r_a$ inteiros não negativos e $\{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_a}\}$ um subconjunto de $\mathbb{Z}_q^n$ tal que $\mathcal{C}_\ell^\perp = \langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_\ell} \rangle$ para cada $1 \leq \ell \leq a$.

A Construção D', denotada por $\Lambda_{D'}$, é o conjunto de todos os vetores $\boldsymbol{x} \in \mathbb{Z}^n$ satisfazendo:

$$\boldsymbol{x} \cdot \sigma(\boldsymbol{h}_j) \equiv 0 \mod q^{i+1} \text{ para todo } 0 \leq i \leq a-1 \text{ e } r_{a-i-1} < j \leq r_{a-i},$$

onde $\sigma : \mathbb{Z}_q^n \to \mathbb{Z}^n$ é o mergulho natural.

Construção D' como Construção A

Proposição

Seja $\Lambda_{D'}$ o reticulado obtido via Construção D'. Então,

$$\Lambda_{D'} = \Lambda_A(\mathcal{C}^{\perp}) = q^a \Lambda_A^*(\mathcal{C}),$$

em que $\mathcal{C} \subseteq \mathbb{Z}_{q^a}^n$ é o código q^a-ário linear gerado pelas linhas de $\rho_{q^a}(\boldsymbol{H})$.

Construção D' como Construção A

Proposição

Seja $\Lambda_{D'}$ o reticulado obtido via Construção D'. Então,

$$\Lambda_{D'} = \Lambda_A(\mathcal{C}^{\perp}) = q^a \Lambda_A^*(\mathcal{C}),$$

em que $\mathcal{C} \subseteq \mathbb{Z}_{q^a}^n$ é o código q^a-ário linear gerado pelas linhas de $\rho_{q^a}(\boldsymbol{H})$.

Sejam

$$\begin{aligned} \mathcal{C}_a &\subseteq \ldots \subseteq \mathcal{C}_1 \subseteq \mathbb{Z}_q^n \ \textbf{(Cadeia 1)} \\ \mathcal{C}_1^{\perp} &\subseteq \ldots \subseteq \mathcal{C}_a^{\perp} \subseteq \mathbb{Z}_q^n \ \textbf{(Cadeia 2)}. \end{aligned}$$

$$\Lambda_{D'} = \Lambda_{D^{\perp}}^*.$$

Construção D'

Exemplo:

Consideremos a cadeia

$$\begin{aligned} \mathcal{C}_1^{\perp} &= \langle (4,2) \rangle \subseteq \mathcal{C}_2^{\perp} = \langle (4,2), (0,1) \rangle; \\ \hat{\mathcal{C}}_1^{\perp} &= \langle (2,4) \rangle \subseteq \hat{\mathcal{C}}_2^{\perp} = \langle (2,4), (0,1) \rangle. \end{aligned}$$

Temos que

$$\boldsymbol{H} = \begin{bmatrix} 4 & 2 \\ 0 & 6 \end{bmatrix} \quad \text{e} \quad \hat{\boldsymbol{H}} = \begin{bmatrix} 2 & 4 \\ 0 & 6 \end{bmatrix}$$

são matrizes de verificação de $\Lambda_{D'}$ e $\hat{\Lambda}_{D'}$, respectivamente.

$$\Lambda_{D'} = \left\{ \boldsymbol{x} \in \mathbb{Z}^2 : \boldsymbol{H}\boldsymbol{x} \equiv 0 \mod 36 \right\}$$

Construção D'

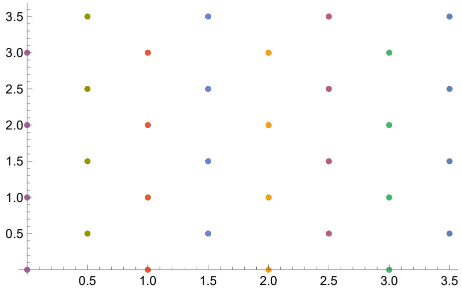

Figure 2: Reticulado $\Lambda_{D'}$.

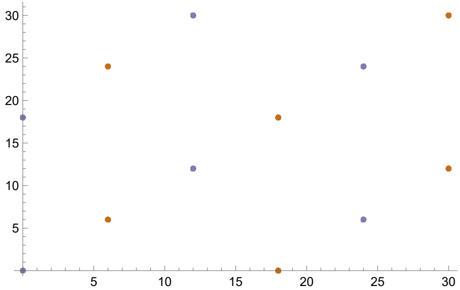

Figure 3: Reticulado $\hat{\Lambda}_{D'}$.

Volume

Teorema

Seja $\Lambda_D = \Lambda_A(\mathcal{C})$ o reticulado obtido via Construção D, em que $\mathcal{C} \subseteq \mathbb{Z}_{q^a}^n$ é o código gerado pelas linhas da matriz $\rho_{q^a}(\boldsymbol{G})$. Então,

$$|\mathcal{C}| \leq q^{\sum_{\ell=1}^{a} k_\ell} \prod_{i=1}^{k_1} \mathcal{O}(\boldsymbol{b}_i),$$

e, consequentemente, o volume de Λ_D satisfaz

$$\mathrm{vol}\, \Lambda_D \geq q^{an - \sum_{\ell=1}^{a} k_\ell} \left(\prod_{i=1}^{k_1} \frac{q}{\mathcal{O}(\boldsymbol{b}_i)} \right),$$

em que $\mathcal{O}(\boldsymbol{b}_i)$ é a ordem de $\boldsymbol{b}_i$ sobre $\mathbb{Z}_q$ para cada i.

Volume

Teorema

Seja $\Lambda_{D'} = \Lambda_A(\mathcal{C}^{\perp})$ o reticulado obtido via Construção D', em que $\mathcal{C} \subseteq \mathbb{Z}_{q^a}^n$ é o código com matriz de verificação $\rho_{q^a}(\boldsymbol{G})$. Então,

$$\operatorname{vol} \Lambda_{D'} = |\mathcal{C}| \leq \frac{q^{\sum_{\ell=1}^{a} r_\ell}}{\prod_{i=1}^{r_a} \frac{q}{\mathcal{O}(\boldsymbol{h}_i)}},$$

em que $\mathcal{O}(\boldsymbol{h}_i)$ é a ordem de $\boldsymbol{h}_i$ sobre $\mathbb{Z}_q$ para cada i.

Volume

Voltando no exemplo anterior...

$$\begin{aligned}
\mathcal{C}_1^{\perp} &= \underbrace{\langle (4,2) \rangle}_{\langle \boldsymbol{h}_1 \rangle} \subseteq \mathcal{C}_2^{\perp} = \underbrace{\langle (4,2), (0,1) \rangle}_{\langle \boldsymbol{h}_1, \boldsymbol{h}_2 \rangle}; \\
\hat{\mathcal{C}}_1^{\perp} &= \underbrace{\langle (2,4) \rangle}_{\langle \hat{\boldsymbol{h}}_1 \rangle} \subseteq \hat{\mathcal{C}}_2^{\perp} = \underbrace{\langle (2,4), (0,1) \rangle}_{\langle \hat{\boldsymbol{h}}_1, \hat{\boldsymbol{h}}_2 \rangle}.
\end{aligned}$$

A partir do volume de $\Lambda_{D'}$ e $\hat{\Lambda}_{D'}$ verifica-se que

$$108 = \operatorname{vol} \hat{\Lambda}_{D'} = \frac{6^3}{\frac{6}{3} \cdot \frac{6}{6}} \quad \text{mas} \quad 54 = \operatorname{vol} \Lambda_{D'} < \frac{6^3}{\frac{6}{3} \cdot \frac{6}{6}}.$$

Volume

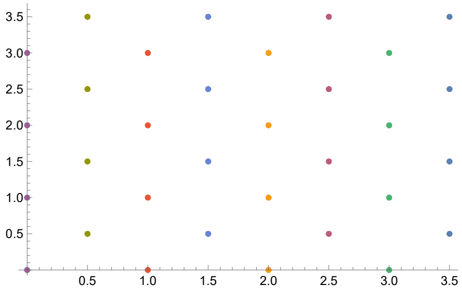

Figure 4: Reticulado $\Lambda_{D'}$.

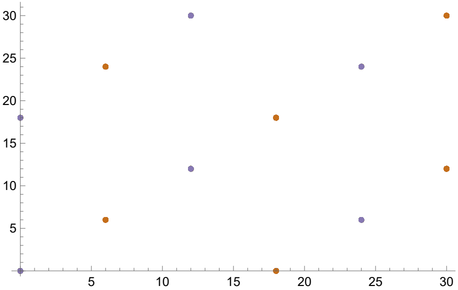

Figure 5: Reticulado $\hat{\Lambda}_{D'}$.

Distância Mínima L_p

Teorema

Seja $0 \subsetneq \mathcal{C}_a \subseteq \mathcal{C}_{a-1} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathbb{Z}_q^n$ uma cadeia de códigos lineares. Considere a distância L_p, com $1 \leq \mathrm{p} \leq \infty$, e denote a distância L_p de $\mathcal{C}_\ell$ por $d_\mathrm{p}(\mathcal{C}_\ell)$. Então, a distância L_p de $\Gamma_{\overline{D}}$ é dada por

$$d_\mathrm{p}(\Gamma_{\overline{D}}) = \min\left\{q^a, q^{a-1} d_\mathrm{p}(\mathcal{C}_1), \ldots, d_\mathrm{p}(\mathcal{C}_a)\right\}.$$

- A condição de ser uma cadeia pode ser removida.

Distância Mínima L_{p}

Teorema

Seja $0 \subsetneq \mathcal{C}_a \subseteq \mathcal{C}_{a-1} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathbb{Z}_q^n$ uma cadeia de códigos lineares. Considere a distância L_{p}, com $1 \leq \mathrm{p} \leq \infty$, e denote a distância L_{p} de $\mathcal{C}_\ell$ por $d_{\mathrm{p}}(\mathcal{C}_\ell)$. Então, a distância L_{p} de $\Gamma_{\overline{D}}$ é dada por

$$d_{\mathrm{p}}(\Gamma_{\overline{D}}) = \min\left\{q^a, q^{a-1} d_{\mathrm{p}}(\mathcal{C}_1), \ldots, d_{\mathrm{p}}(\mathcal{C}_a)\right\}.$$

Se a cadeia é fechada sob adição zero-um, vale:

$$d_{\mathrm{P}}(\Lambda_D) = \min\left\{q^a, q^{a-1} d_{\mathrm{P}}(\mathcal{C}_1), \ldots, d_{\mathrm{P}}(\mathcal{C}_a)\right\}.$$

Distância Mínima L_{p}

Teorema

Seja $0 \subsetneq \mathcal{C}_a \subseteq \mathcal{C}_{a-1} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathbb{Z}_q^n$ uma cadeia de códigos lineares. Se a cadeia de duais é **fechada sob adição zero-um**, vale:

$$d_{\mathrm{P}}(\Lambda_{D'}^*) = \min\left\{1, q^{-1} d_{\mathrm{P}}(\mathcal{C}_a^{\perp}), \ldots, q^{-a} d_{\mathrm{P}}(\mathcal{C}_1^{\perp})\right\} =: d.$$

Em particular,

$$\frac{1}{d} \leq d_2(\Lambda_{D'}) \leq \frac{\gamma_n}{d},$$

onde γ_n é a constante de Hermite na dimensão n.

Distância Mínima L_{p}

Teorema

Seja $0 \subsetneq \mathcal{C}_a \subseteq \mathcal{C}_{a-1} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathbb{Z}_q^n$ uma cadeia de códigos lineares. Se a cadeia de duais é **fechada sob adição zero-um**, vale:

$$d_{\mathrm{P}}(\Lambda_{D'}^*) = \min\left\{1, q^{-1} d_{\mathrm{P}}(\mathcal{C}_a^\perp), \ldots, q^{-a} d_{\mathrm{P}}(\mathcal{C}_1^\perp)\right\} =: d.$$

Em particular,

$$d_{\mathrm{P}}(\Lambda_{D'}) \leq \frac{\gamma_n}{d} \qquad \text{se } 2 < \mathrm{p} \leq \infty,$$

onde γ_n é a constante de Hermite na dimensão n.

Distância Mínima L_{p}

Teorema

Seja $0 \subsetneq \mathcal{C}_a \subseteq \mathcal{C}_{a-1} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathbb{Z}_q^n$ uma cadeia de códigos lineares. Se a cadeia de duais é **fechada sob adição zero-um**, vale:

$$d_{\mathrm{P}}(\Lambda_{D'}^*) = \min\left\{1, q^{-1} d_{\mathrm{P}}(\mathcal{C}_a^\perp), \ldots, q^{-a} d_{\mathrm{P}}(\mathcal{C}_1^\perp)\right\} =: d.$$

Em particular,

$$d_{\mathrm{P}}(\Lambda_{D'}) \leq \left(n^{\frac{1}{p}-\frac{1}{2}}\right)^2 \cdot \frac{\gamma_n}{d} \qquad \text{se } 1 < \mathrm{p} < 2,$$

onde γ_n é a constante de Hermite na dimensão n.

Distância Mínima $L_{\rm p}$

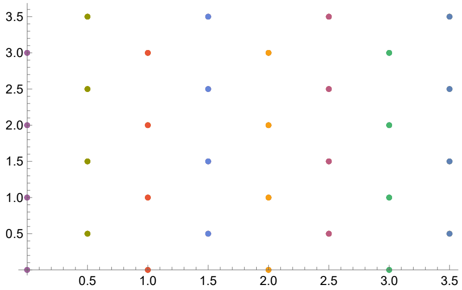

Figure 6: Reticulado $\Lambda_{D'}$.

$$\mathcal{C}_1^{\perp} = \langle (4,2) \rangle \subseteq \mathcal{C}_2^{\perp} = \langle (4,2), (0,1) \rangle$$

Verifica-se que

$$d_2(\Lambda^*_{D'}) = \min\left\{\sqrt{5}/18, 36\right\} = \sqrt{5}/18,$$

porém

$$\min\left\{1, 6^{-1} d_2(\mathcal{C}_2^{\perp}), d_2(\mathcal{C}_1^{\perp})\right\} = 1/6.$$

Cadeia não fechada sob adição zero-um

Ganho de Codificação

Teorema

Seja $\mathcal{C}_a \subseteq \ldots \subseteq \mathcal{C}_1 \subseteq \mathbb{Z}_q^n$ cadeia de códigos lineares. Se a cadeia de duais é fechada sob adição zero-um, tem-se

$$\gamma(\Lambda_{D'}) \geq \frac{q^{2a} \cdot \left(\prod_{i=1}^{r_a} \frac{q}{\mathcal{O}(\boldsymbol{h}_i)}\right)^{2/n}}{(q^2)^{\sum_{\ell=1}^{a} \frac{r_\ell}{n}} \min\left\{q^{2a}, q^{2(a-1)} d_2^2(\mathcal{C}_a^\perp), \ldots, d_2^2(\mathcal{C}_1^\perp)\right\}},$$

sendo que vale igualdade se os geradores são linearmente independentes sobre $\mathbb{Z}_q$.

Questões em aberto

- Sobre o volume:
  - Obter uma fórmula geral e não apenas limitantes.
  - Critério para escolher entre geradores de mesma ordem.
- Sobre a distância L_{p}:
  - Restringimos às cadeias fechadas sob adição zero-um.
  - Cadeias mais gerais podem produzir reticulados *melhores*?
- Análise assintótica das Construções D e D'.
- Possíveis aplicações em criptografia.

Referências I

[1] S. I. R. Costa , F. Oggier, A. Campello, J.C. Belfiore, E, Viterbo; Lattices Applied to Codiging for Reliable and Secure Communications, Springer, 2017.

[2] Kositwattanarerk, W.; Oggier, F. Connections between construction D and related constructions of lattices. Designs, codes and cryptography, v. 73, n. 2, p. 441-455, 2014.

[3] Strey, E. Construções de reticulados a partir de códigos q-ários. Diss. Tese de Doutorado, Imecc-Unicamp, 2017.

[4] Silva, F.C.; Souza, A.; Strey, E., Costa, S. I. R. "On Lattice Constructions D and D' from q-ary Linear Codes". In: arXiv preprint arXiv:2303.16879 (2023)

Muito obrigada!

francielecs@ime.unicamp.br