Sobre códigos reticulados obtidos a partir das Construções A, D e D′

Ana Paula de Souza

Em parceria com Franciele Carmo, Eleonesio Strey e Sueli I. R. Costa

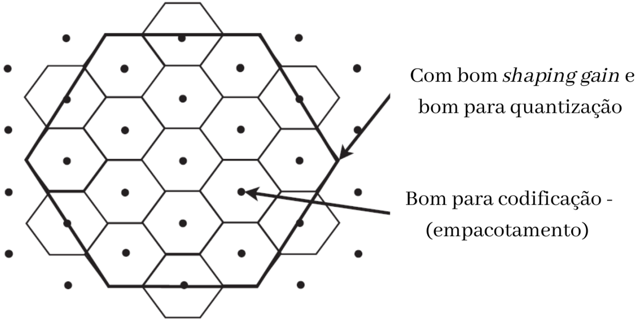
15 de junho de 2023

EnCoRI 2023
Encontro de Códigos, Reticulados e Informação

Conteúdos

Motivação

Um dos desafios em transmissões de sinais: obter códigos capazes de aproximar da capacidade do canal (AWGN) e que possam ser codificados e decodificados de forma computacionalmente eficientes.



Fonte: Adaptada de [Zamir and Nazer, 2014].

Códigos Reticulados

Sejam $\Lambda_f, \Lambda_g \subset \mathbb{R}^n$ reticulados aninhados, isto é, $\Lambda_g \subseteq \Lambda_f$.

Como Λ_g é um subgrupo de Λ_f podemos considerar o grupo quociente

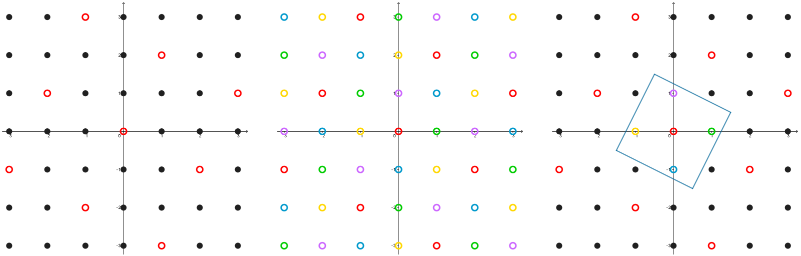
$$\Lambda_f/\Lambda_g = \{x + \Lambda_g : x \in \Lambda_f\}.$$

Chamamos de *Códigos Reticulados* o conjunto $\mathcal{P}$ dado por uma seleção de líderes que represente univocamente todas as classes laterais de Λ_f/Λ_g com menor norma[1].

[1] Introduzido por [Conway and Sloane, 1983], detalhada por [Forney, 1989] e seguimos [Pietro and Boutros, 2017]

Exemplos

Figura 1: Exemplo de reticulados aninhados com as classes laterais de Λ_f / Λ_g e o Código Reticulado resultante.



((a)) Par de reticulados aninhados $\Lambda_g \subset \Lambda_f$. Os pontos vermelhos representam Λ_g.

((b)) Classes laterais de Λ_f / Λ_g. Cada cor representa elementos de Λ_f em uma classe lateral.

((c)) Os cinco pontos no interior de $\mathcal{V}_{\Lambda_g}(\mathbf{0})$ formam o Código Reticulado $\mathcal{P} = \Lambda_f \cap \mathcal{V}_{\Lambda_g}(\mathbf{0})$.

Resumidamente:

Etapa 1: construir as diferentes classes laterais de Λ_g em Λ_f e tomar um líder de cada uma delas.

Etapa 2: encontrar para cada um dos líderes seu representante equivalente com menor norma.

Esse será um ponto do Código Reticulado.

Etapa 1

Proposição [Pietro and Boutros, 2017]

Sejam $\Lambda_f = \mathcal{C} + p\mathbb{Z}^n$ um reticulado obtido pela Construção A de um código linear p-ário, $\Gamma \subseteq \mathbb{Z}^n$ um reticulado inteiro e $\Lambda_g = p\Gamma \subseteq p\mathbb{Z}^n$, p primo.
Consideramos T uma matriz geradora de Γ triangular inferior com $t_{i,i} > 0$ para todo i:

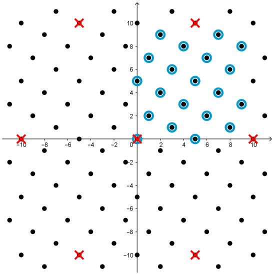
$$T = \begin{pmatrix} t_{1,1} & 0 & \cdots & 0 \\ t_{2,1} & t_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{n,1} & t_{n,2} & \cdots & t_{n,n} \end{pmatrix}, \text{com } t_{i,j} \in \mathbb{Z}.$$

e $\mathcal{S} = \{0, \ldots, t_{1,1} - 1\} \times \cdots \times \{0, \ldots, t_{n,n} - 1\}$.
Então, $\mathcal{C} + p\mathcal{S} = \{c + ps \in \mathbb{Z}^n : c \in \mathcal{C}, s \in \mathcal{S}\}$ é um conjunto completo de líderes das classes laterais de Λ_f / Λ_g.

Ilustração

Sejam $\Lambda_f = \mathcal{C} + 5\mathbb{Z}^2$, com $\mathcal{C} = \langle(1,2)\rangle$ e Γ com matriz geradora $T = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}$. Dela, temos o conjunto $\mathcal{S} = \{0,1\} \times \{0,1\}$. Escolhendo $p = 5$, temos $\Lambda_g = 5\Gamma \subseteq 5\mathbb{Z}^2$.

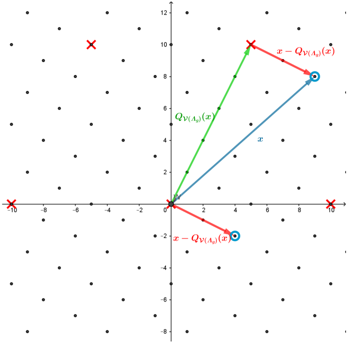
Figura 2: Λ_g e Λ_f e conjunto $C + p\mathcal{S}$.



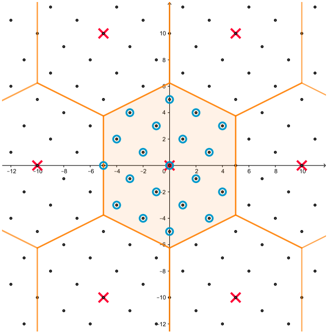
Pela Proposição, $\mathcal{C} + 5\mathcal{S}$ é um conjunto completo de representantes das classes laterais de Λ_f / Λ_g.

Etapa 2

Encontrar para cada um dos líderes seu representante equivalente com menor norma euclidiana.



((a)) Operação para x = (9,8).



((b)) Código reticulado resultante.

Codificação - Encoding

1. A informação será representada por vetores inteiros no conjunto $\mathcal{M} = \mathbb{F}_p^k \times \mathcal{S}$.
2. Seja $\mathbf{m} = (\mathbf{u}, \mathbf{s}) \in \mathcal{M}$ uma mensagem a ser codificada com $\mathbf{u} \in \mathbb{F}_p^k$ e $\mathbf{s} \in \mathcal{S}$. Seja $\mathbf{c}$ a palavra código associada a $\mathbf{u}$, isto é, se $enc_{\mathcal{C}}(\cdot) = \mathbb{F}_p^k \longrightarrow \mathbb{F}_p^n$ é o codificador das palavras de $\mathcal{C}$ então $\mathbf{c} = enc_{\mathcal{C}}(\mathbf{u})$.
3. Seja $\mathbf{x}' = \mathbf{c} + p\mathbf{s} \in \Lambda_f$.
4. Então a mensagem $\mathbf{m}$ é codificada para a palavra código do reticulado
$$\mathbf{x} = \mathbf{x}' - Q_{\mathcal{V}(\Lambda_g)}(\mathbf{x}') \in \mathcal{P} = \Lambda_f \cap \mathcal{V}_{\Lambda_g}(\mathbf{0}),$$
em que $Q_{\mathcal{V}(\Lambda_g)}(\cdot)$ é o quantizador associado à região de Voronoi do reticulado Λ_g.

Obs.: A Proposição garante que mensagens diferentes sejam codificadas para palavras diferentes do código reticulado.

“Desmapeamento” - Demapping

Objetivo: recuperar $\mathbf{m} = (\mathbf{u}, \mathbf{s})$ dado um elemento $\mathbf{x} \in \Lambda_f$.

1. Como $Q_{\mathcal{V}(\Lambda_g)}(\mathbf{y}) \in \Lambda_g = p\Gamma$ para todo $\mathbf{y} \in \mathbb{R}^n$, nós obtemos $\mathbf{c}$ reduzindo a módulo p o ponto $\mathbf{x} = \mathbf{c} + p\mathbf{s} - Q_{\mathcal{V}(\Lambda_g)}(\mathbf{x}')$.
2. Assumindo que a codificação foi feita de forma sistemática, obtemos $\mathbf{u}$ como as primeiras coordenadas de $\mathbf{c} = enc_{\mathcal{C}}(\mathbf{u}) = (\mathbf{u}|\mathbf{c}')$.
3. Resta calcular $\mathbf{s}$. Já conhecemos $\mathbf{x}$ e $\mathbf{c}$, então podemos calcular
$$\mathbf{r} = \frac{(\mathbf{x} - \mathbf{c})}{p} = \mathbf{s} - \frac{1}{p} Q_{\mathcal{V}(\Lambda_g)}(\mathbf{x}') = \mathbf{s} - \mathbf{q} \in \mathbb{Z}^n,$$
para algum $\mathbf{q} \in \Gamma$. Como $\mathbf{T}$ é matriz geradora de Γ, temos $\mathbf{r} = \mathbf{s} - \mathbf{z}\mathbf{T}$ para algum $\mathbf{z} \in \mathbb{Z}^n$.
4. Como $\mathbf{T}$ é triangular, obtemos a i-ésima coordenada de $\mathbf{r} = \mathbf{s} - \mathbf{z}\mathbf{T}$ fazendo, para $i = 1, \ldots, n$,
$$r_i = s_i - z_i t_{i,i} - \sum_{j=i+1}^{n} z_j t_{j,i}.$$

Uma observação...

Para que a complexidade da codificação e do desmapeamento sejam lineares pedem que:

- Λ_f seja um reticulado obtido por Construção A a partir de um código LDPC cuja matriz de paridade tenha uma submatriz esparsa com dupla diagonal. Isto é,

$$\Lambda_f = \mathcal{C} + p\mathbb{Z}^n,$$

em que $\mathcal{C} = \{x \in \mathbb{F}_p^n : \mathbf{H}x^t \equiv \mathbf{0} \mod p\}$ com $\mathbf{H} = (\mathbf{L}|\mathbf{R})$ sendo

$$\mathbf{R} = \begin{pmatrix} h_{1,k+1} & 0 & \cdots & \cdots & 0 \\ h_{2,k+1} & h_{2,k+2} & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & h_{n-k,n-1} & h_{n-k,n} \end{pmatrix},$$

com $h_{i,k+i} \neq 0$ para $i = 1, 2, \ldots, n-k$ e para $h_{i,k+i-1} \neq 0$ para $i = 2, 3 \ldots, n-k$.

Os resultados de [de Souza, 2021, Costa et al., 2017] possibilitaram estender a Proposição e os procedimentos anteriores para códigos q-ários (em $\mathbb{Z}_q$).

Extensão para reticulados obtidos pela Construção A a partir de códigos lineares q-ários

Sejam $\Lambda_f = \mathcal{C} + q\mathbb{Z}^n$ um reticulado obtido pela Construção A de um código linear q-ário, $\Gamma \subseteq \mathbb{Z}^n$ um reticulado inteiro e $\Lambda_g = q\Gamma \subseteq q\mathbb{Z}^n$, $q \in \mathbb{Z}^*$. Consideramos T uma matriz geradora de Γ triangular inferior com $t_{i,i} > 0$ para todo i:

$$T = \begin{pmatrix} t_{1,1} & 0 & \cdots & 0 \\ t_{2,1} & t_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{n,1} & t_{n,2} & \cdots & t_{n,n} \end{pmatrix}, \text{com } t_{i,j} \in \mathbb{Z}.$$

e $\mathcal{S} = \{0, \ldots, t_{1,1} - 1\} \times \cdots \times \{0, \ldots, t_{n,n} - 1\}$.
Então, $\mathcal{C} + q\mathcal{S} = \{c + qs \in \mathbb{Z}^n : c \in \mathcal{C}, s \in \mathcal{S}\}$ é um conjunto completo de líderes das classes laterais de Λ_f / Λ_g.

Conexão entre as Construções D e A

Teorema 5 de [Strey and Costa, 2017]

Sejam $\boldsymbol{G}_1$ a matriz cujas linhas são os vetores $\sigma(\boldsymbol{b}_1), \ldots, \sigma(\boldsymbol{b}_{k_1})$ e $\mathcal{C}$ o código linear q^a-ário gerado pelas linhas da matriz $\boldsymbol{G} = \boldsymbol{D}\boldsymbol{G}_1$, em que $\boldsymbol{D} = (d_{ij})$ é a matriz diagonal com

$$d_{jj} = \begin{cases} 1, & \text{se } 1 \leq j \leq k_a \\ q, & \text{se } k_a < j \leq k_{a-1} \\ \vdots & \\ q^{a-1}, & \text{se } k_2 < j \leq k_1. \end{cases}$$

Temos que $\Lambda_D = \Lambda_A(\mathcal{C})$. Ou seja, Λ_D é um reticulado q^a-ário.

Essa associação permite, a partir da extensão anterior, usar também a Construção D neste processo, com possíveis ganhos de codificação/decodificação [Sakzad et al., 2010, Matsumine et al., 2018].

Extensão para reticulados obtidos pela Construção D [de Souza, 2021]

Seja $\mathbb{Z}_q^n \supseteq \mathcal{C}_1 \supseteq \mathcal{C}_2 \supseteq \cdots \supseteq \mathcal{C}_a$ uma família de códigos lineares com os parâmetros adequados para que $\Lambda_f = \Lambda_D$ seja um reticulado obtido pela Construção D. Seja também $\Gamma \subseteq \mathbb{Z}^n$ um reticulado inteiro com matriz geradora T triangular inferior com $t_{i,i} > 0$ para todo $i = 1, \ldots, n$ e $\Lambda_g = q^a\Gamma$. Então, para $\mathcal{C} = \Lambda_f \cap [0, q^a)^n$ um conjunto completo de representantes das classes laterais de Λ_f/Λ_g é dado por

$$\mathcal{C} + q^a\mathcal{S},$$

com $\mathcal{S} = \{0, \ldots, t_{1,1} - 1\} \times \cdots \times \{0, \ldots, t_{n,n} - 1\}$.

Conexão entre as Construções D′ e A

Teorema 3.17 de [do Carmo Silva et al., 2023]

Sob as notações da definição da Construção D′ temos que

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

em que $\mathcal{C}^{\perp} = \Lambda_{D'} \cap [0, q^a)^n$ é o código dual q^a-ário com matriz de paridade $\rho_{q^a}(\boldsymbol{H})$, em que $\boldsymbol{H} = \boldsymbol{D}\boldsymbol{H}_a$ sendo $\boldsymbol{H}_a$ a matriz cuja as linhas são os elementos $\sigma(\boldsymbol{h}_1), \ldots, \sigma(\boldsymbol{h}_{r_a})$ e $\boldsymbol{D}$ a matriz diagonal semelhante à definida anteriormente para a Construção D.

A partir dessa associação, também é possível utilizar a Construção D′ na proposta para obtenção dos Códigos Reticulados visando ganhos de codificação/decodificação
[Zhou et al., 2021, Zhou and Kurkoski, 2022].

Construção D′ Generalizada[2] [da Silva and Silva, 2018]

Sejam $\mathbf{H}_\ell \in \mathbb{Z}^{m_\ell \times n}$ tal que $\mathbf{H}_\ell \equiv \mathbf{F}_\ell \mathbf{H}_{\ell-1} (\bmod\ 2^\ell)$, para $\ell = 0, \dots, a-1$ e algum $\mathbf{F}_\ell \in \mathbb{Z}^{m_\ell \times m_{\ell-1}}$. O reticulado

$$\Lambda = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{H}_\ell \mathbf{x}^t \equiv \mathbf{0} (\bmod\ 2^{\ell+1}), 0 \leq \ell \leq a-1\}$$

é dito ser obtido pela Contrução D′ Generalizada aplicada a $\mathbf{H}_\ell, \dots, \mathbf{H}_{a-1}$. Equivalentemente, $\Lambda = \mathcal{C} + 2^a \mathbb{Z}^n$.

Vantagens:

- As matrizes $\mathbf{H}_\ell$ para $\ell = 0, \dots, a-1$ dos códigos $\mathcal{C}_\ell$ associados não precisam ser aninhadas.
- As características da Construção D′ são mantidas, mas com codificação e decodificação mais eficientes.

[2] Para códigos binários, aplicável também para códigos p-ários, p primo.

Perspectivas

- Uso da Construção D′ Generalizada como reticulado Λ_f na proposta de [Pietro and Boutros, 2017].
- Análise da viabilidade e complexibilidade computacional ao utilizar as diferentes construções.

[Conway and Sloane, 1983] Conway, J. and Sloane, N. J. A. (1983).
A Fast Encoding Method for Lattice Codes and Quantizers.
IEEE Transactions on Communication, 29.

[Costa et al., 2017] Costa, S. I., Oggier, F., Campello, A., Belfiore, J.-C., and Viterbo, E. (2017).
Lattices Applied to Coding for Reliable and Secure Communications.
Springer.

[da Silva and Silva, 2018] da Silva, P. R. B. and Silva, D. (2018).
Multilevel LDPC Lattices With Efficient Encoding and Decoding and a Generalization of Construction D′ .
IEEE Transactions on Information Theory, 65(5):3246–3260.

[de Souza, 2021] de Souza, A. P. (2021).
Sobre constelações de voronoi para códigos em reticulados e problemas de codificação de índice.
Master's thesis, Universidade Estadual de Campinas.

[do Carmo Silva et al., 2023] do Carmo Silva, F., de Souza, A. P., Strey, E., and Costa, S. I. R. (2023).
On lattice constructions d and d′ from q-ary linear codes.
arXiv e-prints, pages arXiv–2303.

[Forney, 1989] Forney, G. D. (1989).
Multidimensional constellations. ii. voronoi constellations.
IEEE Journal on Selected Areas in Communications, 7(6):941–958.

[Matsumine et al., 2018] Matsumine, T., Kurkoski, B. M., and Ochiai, H. (2018).
Construction D lattice decoding and its application to BCH code lattices.
In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE.

[Pietro and Boutros, 2017] Pietro, N. and Boutros, J. J. (2017).
Leech Constellations of Construction-A Lattices.
IEEE Transactions on Communication, 65:4622–4631.

[Sakzad et al., 2010] Sakzad, A., Sadeghi, M.-R., and Panario, D. (2010).
Construction of turbo lattices.
In *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 14–21. IEEE.

[Strey and Costa, 2017] Strey, E. and Costa, S. I. R. (2017).
Lattices from codes over $\mathbb{Z}_q$: Generalization of Constructions D, D' and $\overline{D}$.
Designs, Codes and Cryptography, 85(1):77–95.

[Zamir and Nazer, 2014] Zamir, R. and Nazer, B. (2014).
Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation and Multiuser Information Theory.
Cambridge Univ. Press, New York, NY, USA.

[Zhou et al., 2021] Zhou, F., Fitri, A., Anwar, K., and Kurkoski, B. M. (2021).
Encoding and Decoding Construction D′ Lattices for Power-Constrained Communications.
In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 1005–1010. IEEE.

[Zhou and Kurkoski, 2022] Zhou, F. and Kurkoski, B. M. (2022).
Construction D' Lattices for Power-Constrained Communications.
IEEE Transactions on Communications, 70(4):2200–2212.