Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 8, n. 1, 2021.

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

Uma ilustração da construção de constelações de Voronoi para codificação em reticulados

Ana Paula de Souza[1]
Sueli I. R. Costa[2]
Instituto de Matemática, Estatística e Computação Científica, IMECC/Unicamp, Campinas, SP

Reticulados têm sido muito estudados devido suas aplicações para transmissões de sinais em especial em subáreas como codificação contínua, transmissões em canais gaussianos e do tipo Rayleigh e na recente subárea chamada criptografia pós quântica [1]. Em particular, para o canal aditivo de ruído gaussiano branco (AWGN), são consideradas constelações finitas que podem ser obtidas por pares de reticulados Λ e Λ_f aninhados, $\Lambda \subseteq \Lambda_f \subseteq \mathbb{R}^n$. Nesse processo, procura-se reticulados tais que o reticulado "fino" tenha a região de Voronoi do "grosso" selecionando seus pontos de tal modo que se tenha ganho de forma. Neste trabalho de pesquisa em andamento procuramos entender e ilustrar o processo de seleção dos pontos do reticulado para codificação.

Dado que um *reticulado* é um *subgrupo discreto aditivo* de $\mathbb{R}^n$, para um par de reticulados aninhados $\Lambda \subseteq \Lambda_f$ podemos considerar o grupo quociente $\Lambda_f/\Lambda = \{x + \Lambda, x \in \Lambda_f\}$. A *constelação de Voronoi* é o código reticulado $\mathcal{P}$ dado por líderes de todos os *cosets* com norma euclidiana mínima. Equivalentemente, são todos os elementos de Λ_f que estão no interior da região de Voronoi de Λ, $\mathcal{V}_\Lambda(\mathbf{0})$, mais uma seleção de pontos de Λ_f que estão no bordo de $\mathcal{V}_\Lambda(\mathbf{0})$ de modo a termos um único líder para cada *coset* [1]. Resumidamente, construir uma constelação de Voronoi consiste em duas etapas: construir os diferentes *cosets* de Λ em Λ_f e, em seguida, encontrar para cada um deles um líder com norma euclidiana mínima, que será um ponto da constelação de Voronoi. Quando Λ_f é obtido por Construção-A e $\Lambda \subseteq p\mathbb{Z}^n$, com p primo, a primeira etapa pode ser realizada através da seguinte proposição:

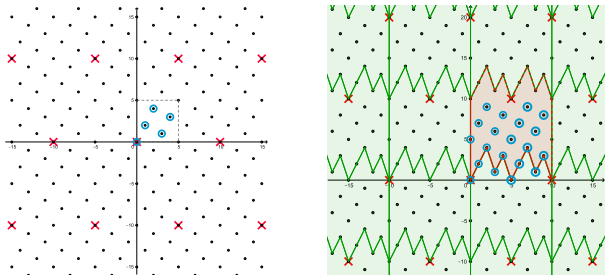
Proposição [2]: *Seja $\Gamma \subseteq \mathbb{Z}^n$ um reticulado $\Lambda = p\Gamma \subseteq p\mathbb{Z}^n$. Sejam T uma matriz geradora para Γ triangular inferior com $t_{i,i} > 0$ para todo i (sempre é possível tomando sua Forma Normal de Hermite, [1]) e $\mathcal{S} = \{0, \ldots, t_{1,1} - 1\} \times \cdots \times \{0, \ldots, t_{n,n} - 1\}$. Se $\Lambda_f = \mathcal{C} + p\mathbb{Z}^n$ é um reticulado obtido de um código linear $\mathcal{C} \subseteq \mathbb{Z}_p^n$ então $\mathcal{C} + p\mathcal{S} = \{c + ps, c \in \mathcal{C}\, e\, s \in \mathcal{S}\}$ é um conjunto completo de líderes de cosets de Λ_f/Λ.*

A seguir interpretamos esse resultado num exemplo em dimensão 2 e analisamos um ladrilhamento envolvido. Consideramos o reticulado Γ com matriz geradora $T = \left(\begin{smallmatrix} 2 & 0 \\ 1 & 2 \end{smallmatrix}\right)$. Dela, temos o conjunto $\mathcal{S} = \{0, 1\} \times \{0, 1\}$. Escolhendo $p = 5$, temos o reticulado $\Lambda = 5\Gamma \subseteq 5\mathbb{Z}^2$, representado pelos pontos " $\times$ " na Figura 1(a). Para construir Λ_f, se considerarmos $\mathcal{C} = \langle(1, 2)\rangle$, teremos $\Lambda_f = \mathcal{C} + 5\mathbb{Z}^2$ representado na Figura 1(a) pelos pontos menores.

Pelo Proposição, $\mathcal{C}+5\mathcal{S} = \{(0,0), (1,2), (2,4), (3,1), (4,3), (0,5), (1,7), (2,9), (3,6), (4,8), (5,0), (6,2), (7,4), (8,1), (9,3), (5,5), (6,7), (7,9), (8,6), (9,8)\}$ é um conjunto completo de líderes de *cosets* de Λ_f/Λ, representado na Figura 1(b) pelos pontos " $\odot$ ". Esses pontos não pertencem à região fundamental de Λ, mas eles pertencem à uma outra região que também ladrilha do plano.

A segunda etapa é feita através de uma operação de quantização associada à região de Voronoi: $\mathcal{Q}_{\mathcal{V}(\Lambda)}(\cdot) : \mathbb{R}^n \longrightarrow \Lambda$, com $\mathcal{Q}_{\mathcal{V}(\Lambda)}(x) = \arg\min_{z\in\Lambda}||z - x||$. Devido a quantidade infinita de

[1] a211975@dac.unicamp.br
[2] sueli@ime.unicamp.br

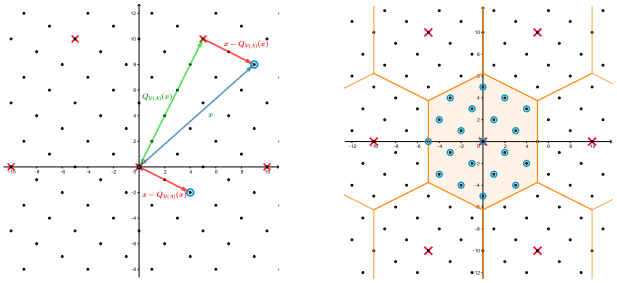


(a) O código $\mathcal{C}$ e os reticulados Λ e Λ_f do exemplo.

(b) Uma região que contém $\mathcal{C} + 5\mathcal{S}$ que ladrilha o plano.

Figura 1: Os reticulados e o conjunto $\mathcal{C} + 5\mathcal{S}$ do exemplo.

pontos do reticulado Λ, essa busca pelo ponto mais próximo é um problema NP-difícil. Assim, é importante que se tenha um algoritmo de quantização para Λ eficiente e implementável para ser usado na codificação e decodificação de informações em grandes dimensões. Com essa operação, se x é representante de um determinado *coset* de Λ em Λ_f, o representante com norma euclidiana mínima é $x - \mathcal{Q}_{\mathcal{V}(\Lambda)}(x)$. A Figura 2(a) ilustra essa operação para o ponto $x = (9, 8)$ em especial, com $\mathcal{Q}_{\mathcal{V}(\Lambda)}(x) = (5, 10)$. Assim, $x - \mathcal{Q}_{\mathcal{V}(\Lambda)}(x) = (4, -2)$. A Figura 2(b) ilustra a constelação de Voronoi obtida com esse exemplo ao realizar a operação para todos os pontos do conjunto $\mathcal{C} + 5\mathcal{S}$.



(a) Operação para $x = (9, 8)$.

(b) Constelação de Voronoi.

Figura 2: Etapa 2 da construção da constelação de Voronoi.

Esse exemplo ilustra em dimensão 2 a construção de constelações de Voronoi proposta em [2]. Como colocado em [3], um dos propósitos de nosso projeto de pesquisa é o uso deste esquema para estudar reticulados aninhados em diversas dimensões buscando constelações que tenham bons parâmetros para codificação de índice ([1], cap.6) e esquemas criptográficos.

Agradecimentos

À Univesp (bolsa de pós-graduação), à CAPES, ao CNPq (313326/2017-7) e ao IMECC-Unicamp.

Referências

[1] Costa, S. I. R. et al. *Lattices Applied to Coding for Reliable and Secure Communication.* Springer, New York, 2017.

[2] Pietro, N., Boutros, J. J. Leech Constellations of Construction-A Lattices, *IEEE Transactions on Communication*, 65:4622–4631, 2017. DOI: 10.1109/ISIT.2017.8006941.

[3] Souza, A. P. Sobre constelações de Voronoi para códigos em reticulados e problemas de codificação de índice. Dissertação de mestrado, Unicamp, 2021.