Trabalho apresentado no XXXIX CNMAC, Uberlândia - MG, 2019.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Decodificação de Reticulados via Fatoração QR

Daniela dos Santos de Oliveira [1]
Universidade Estadual Paulista (UNESP), São João da Boa Vista, SP, Brasil
Cintya Wink de Oliveira Benedito[2]
Universidade Estadual Paulista (UNESP), São João da Boa Vista, SP, Brasil

1 Introdução

A estrutura e as propriedades dos reticulados vêm sendo exploradas em diversas áreas, dentre elas a telecomunicações e, em particular, a teoria da informação e codificação. O estudo dos reticulados surgiu a partir do problema de como cobrir o espaço no $\mathbb{R}^n$ com esferas de mesmo raio, de forma que quaisquer duas esferas se toquem em apenas um ponto e ocupem o maior espaço possível, [1]. O objetivo deste trabalho é apresentar uma estratégia de decodificação para reticulados conhecida como *Sphere Decoding* que faz uso da fatoração QR na matriz geradora do reticulado para decodificá-lo utilizando a métrica euclidiana, [2].

2 Desenvolvimento

Seja $\beta = \{v_1, \cdots, v_m\}$ um conjunto de vetores no $\mathbb{R}^n$ linearmente independentes, com $m \leq n$. Chamamos de **reticulado** de dimensão m e base β ao subconjunto do $\mathbb{R}^n$ da forma:

$$\Lambda = \left\{ x \in \mathbb{R}^n, \text{ tal que } x = \sum_{i=1}^{m} a_i \cdot v_i, \text{ com } a_i \in \mathbb{Z} \right\}. \tag{1}$$

A **matriz geradora** M de Λ é definida como sendo a matriz cujas linhas são os vetores de β, $v_i = (v_{i1}, v_{i2}, \cdots, v_{in})$, para $i = 1, \cdots, m$. Dado um reticulado Λ, **decodificar** um ponto $z \in \mathbb{R}^n$ corresponde a encontrar o ponto de Λ mais próximo de z, ou seja, encontrar $x \in \Lambda$ tal que $d(x, z) = min\{d(y, z) \ : \ y \in \Lambda\}$. Uma forma de decodificação de reticulados é através do algoritmo chamado *Sphere Decoding*, que utiliza a fatoração QR na matriz geradora M do reticulado. O algoritmo consiste em procurar os pontos do reticulado Λ que estão em uma esfera euclidiana de raio $\mathcal{R}$ em torno do vetor dado z. Se $\mathcal{R}$ for muito grande, obtêm-se muitos pontos do reticulado dentro da esfera, porém se for muito pequeno, não se têm certeza da existência do ponto dentro da esfera. Uma boa estimativa para o raio, é utilizar a estimativa de *Babai*, [3].

[1] danielaoliveira52@yahoo.com.br
[2] cintya.benedito@unesp.br

Se $x \in \Lambda$, temos que $x = Ms$, onde M é a matriz geradora de Λ e $s \in \mathbb{Z}^m$. Então, os pontos deste reticulado que estão em uma esfera n-dimensional de raio $\mathcal{R}$ e centro z, na métrica euclidiana é dado por $d(Ms, z) =\| z - Ms \|^2 \leq \mathbb{R}^2$. Para obtermos os pontos $s \in \mathbb{Z}^m$ que satisfazem $d(Ms, z) \leq \mathbb{R}^2$, iremos considerar a fatoração QR da matriz M, ou seja, consideramos $M = Q \begin{pmatrix} R \\ 0_{(n-m)\times m} \end{pmatrix}$, onde R será uma matriz triangular superior, e $Q = [Q_1\ Q_2]$ é uma matriz $n \times n$ ortogonal, com Q_1 e Q_2 representando as primeiras m e $m - n$ colunas ortogonais de Q. Assim,

$$\| z - Ms \|^2 =\| z - [Q_1\ Q_2] \begin{bmatrix} R \\ 0 \end{bmatrix} s \|^2 =\| Q_1^t z - Rs \|^2 + \| Q_2^t z \|^2 \leq \mathcal{R}^2. \tag{2}$$

Desta forma, passamos a buscar $s \in \mathbb{Z}^n$ tal que

$$\| Q_1^t z - Rs \|^2 \leq \mathcal{R}^2 - \| Q_2^t z \|^2 . \tag{3}$$

Exemplo 2.1. *Considere o reticulado Λ com base $\beta = \{(2, 0), (1, 3)\}$ e o vetor $z = (2, 3)$. A matriz geradora M de Λ com sua respectiva fatoração QR é dada por*

$$M = \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} \frac{2}{\sqrt{5}} & -\frac{2}{5} \\ \frac{1}{\sqrt{5}} & \frac{4}{5} \end{pmatrix} \begin{pmatrix} \frac{5}{\sqrt{5}} & -\frac{3}{\sqrt{5}} \\ 0 & 3 \end{pmatrix}. \tag{4}$$

Na métrica euclidiana, com base na estimativa de Babai, obtemos $\mathcal{R} = \sqrt{10}$. Assim, a Figura 1 representa a esfera euclidiana centrada em $z = (2, 3)$ e de raio $\mathcal{R} = \sqrt{10}$ contendo os pontos do reticulado, os quais foram obtidos utilizando (3).

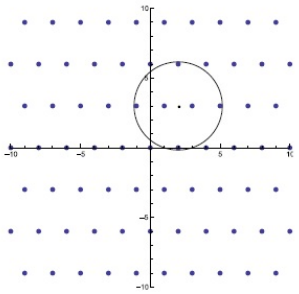

Figura 1: Esfera euclidiana contendo os pontos do Λ.

Referências

[1] J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, 1988.

[2] B. Hassid and H. Vikalo. On the sphere-decoding Algorithm I, Expected Complexity, *IEEE Transactions on Information Theory*, 53:2806-2818, 2005.

[3] L. Y. Tsuchiya. Um estudo de reticulados q-ários com a métrica da soma, Dissertação de Mestrado, Unicamp, 2012.