SOBRE RETICULADOS E APLICAÇÕES EM CRIPTOGRAFIA

Palavras-Chave: RETICULADOS, CODIFICAÇÃO PARA TRANSMISSÃO DE SINAIS, CRIPTOGRAFIA

Autores/as:

Douglas Henrique Ribeiro de Almeida Pereira – IC, UNICAMP

Prof.(ª) Dr.(ª) Sueli Irene Rodrigues Costa (orientador(a)) – IMECC, UNICAMP

INTRODUÇÃO:

Reticulados são utilizados na área de comunicações para transmissão confiável de sinais e em criptografia. Recentemente, no campo de segurança, sistemas de criptografia baseados em problemas computacionais em reticulados foram reconhecidos dentro da área de criptografia pós-quântica. Essas proposições ganharam importância quando foi provada a vulnerabilidade dos sistemas atuais (RSA e Diffie-Hellman) a ataques quânticos[1,2]

Este trabalho faz parte do projeto de iniciação científica em andamento, “Reticulados, distância entre distribuições e aplicações à área de comunicações – Uma introdução” (PICME) que propõe o estudo de tópicos introdutórios de Teoria de Reticulados e Aprendizado de Máquina, conexões entre estes e aplicações na área de comunicações. Dentre os assuntos abordados, foram escolhidos para apresentação neste congresso conceitos e propriedades iniciais de reticulados, problemas computacionais [2] e a aplicação destes no sistema de criptografia GGH [3].

METODOLOGIA:

Estudos individuais mediados por encontros semanais de forma presencial com a orientadora, alguns deles com participação de alunos da pós-graduação do grupo de pesquisa. Os encontros visavam apresentar e discutir os tópicos desenvolvidos. Recursos computacionais (Mathematica[4] e Python) foram utilizados em simulações e exemplos dos temas estudados.

RESULTADOS E DISCUSSÕES:

DEFINIÇÕES:

Um **reticulado** no espaço n-dimensional $\mathbb{R}^n$ é um conjunto discreto de pontos obtidos por todas as combinações lineares inteiras de vetores linearmente independentes. Dado $\{b_1, b_2, \cdots, b_m\}$um conjunto de vetores linearmente independentes em $\mathbb{R}^n$, o reticulado Λ de **Base** $\{b_1, b_2, \cdots, b_m\}$ é definido por:

$$\Lambda = \{a_1 b_1 + \cdots + a_m b_m : a_1, \cdots, a_m \in \mathbb{Z}\}.$$

Os elementos de um reticulado podem ser representados por meio de uma **Matriz Geradora:**

$$B = \begin{bmatrix} b_1 & b_2 & \cdots & b_m \end{bmatrix},$$

em que os vetores são colocados na forma coluna. Dada uma matriz geradora do reticulado, os pontos podem ser obtidos por:

$$\Lambda = \{Bx : x \in \mathbb{Z}^n\}$$

Neste trabalho, consideramos reticulados em que as matrizes geradoras tem posto completo. $m = n$. Duas matrizes geradoras B_1, B_2 geram o mesmo reticulado se, e só se, se existir uma matriz U e entradas inteiras com $\det(U) = \pm 1$, (matriz unimodular) tal que $B_2 = B_1 U$. Dessa forma, existem infinitas bases que geram o mesmo reticulado. Tal propriedade, tem grande importância na área de criptografia baseada em reticulados, em que podemos gerar um reticulado com uma base apropriada, mas, divulgar, em uma chave pública, uma base menos trivial, a fim de dificultar as operações que são necessárias para quebrar a criptografia.

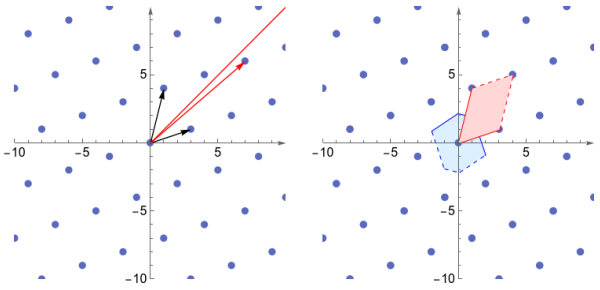
O **volume** de um reticulado $V(\Lambda)$ é o volume do **Paralelotopo Fundamental** de Λ, o qual é definido por:

$$\mathbf{P}(\Lambda) = \{a_1 b_1 + \cdots + a_m b_m, 0 \leq a_i \leq 1\}$$

A **Região de Voronoi** de um ponto $x \in \Lambda$ são os pontos do $\mathbb{R}^n$ que estão mais próximos de x que qualquer outro ponto de Λ. Assim,

$$\mathbb{V}_\Lambda(x) = \{y \in \mathbb{R}^n : ||x - y|| \leq ||z - y|| \quad \forall z \in \Lambda\}$$

Note que a região de Voronoi independe de uma base para ser obtida, diferente do paralelotopo fundamental.



Figuras 1 e 2 - Exemplo de Reticulado no $\mathbb{R}^2$ gerado pelos vetores $\{(3,1),(1,4)\}$ em preto. Os vetores em vermelho $\{(7,6),(11,11)\}$ formam outra base. Na figura 2 (direita), estão destacados o Paralelotopo Fundamental (vermelho) e a Região de Voronoi (azul) do reticulado.

*Algumas propriedades dos reticulados relevantes são: **Norma Mínima** λ que consiste na menor distância de um ponto não nulo à origem; **Raio de Empacotamento** ρ que é o maior valor de raio para esferas centradas em pontos do reticulado não terem sobreposições, exceto no bordo $(\rho = \lambda/2)$; **Raio de Cobertura** μ que é o menor valor de raio tal que as esferas centradas em pontos do reticulado com esse raio cobrem $\mathbb{R}^n$.*

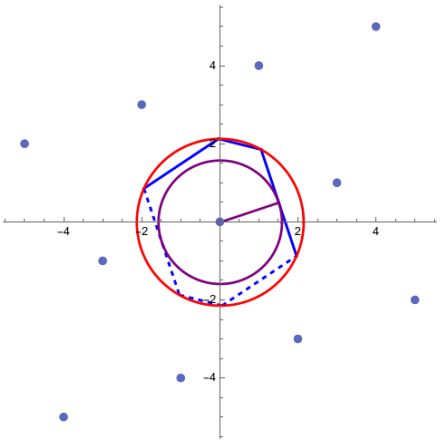


Figura 3 - Na figura (3), estão ilustrados, para o reticulado das figuras (1) e (2), os raios de empacotamento e de cobertura e a região de Voronoi. Note que a região de Voronoi tangencia ambas as circunferências. Os valores obtidos neste caso são:

$$\lambda \approx 3.16,\ \rho \approx 1.58,\ \mu \approx 2.13.$$

Para codificação visando transmissão de sinais, asseguramos a decodificação correta se o tamanho do ruído for menor que o raio de empacotamento.

PROBLEMAS COMPUTACIONAIS:

O reticulado utilizado no exemplo anterior foi definido em $\mathbb{R}^2$ e era conhecida uma base com vetores de normas pequenas e quase ortogonais. Nesse caso, os parâmetros de norma mínima, raio de empacotamento e raio de cobertura foram obtidos com certa facilidade. Sem essas condições e em dimensões grandes, encontrar estes parâmetros torna-se um problema difícil computacionalmente.

Dois problemas que são cruciais para a criptografia baseada em reticulados são:

SVP (Shortest Vector Problem): Dada uma matriz geradora B, encontrar a norma mínima do reticulado Λ gerado por B.

CVP (Closest Vector Problem): Dada uma matriz geradora B de um reticulado $\Lambda \subset R^n$ e um vetor $y \in R^n$, encontrar o ponto de Λ mais próximo de y.

BASES "BOAS" E "BASES RUINS":

Um fator que os torna difíceis computacionalmente é a dependência da matriz geradora B fornecida, o que, em conjunto com a existência de infinitas matrizes geradoras para o mesmo reticulado, possibilita gerar **bases boas** e **bases ruins** para o mesmo reticulado.

Por exemplo, o reticulado $\mathbb{Z}^2$ pode ser gerado por ambas as matrizes B_1, B_2.

$$B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad B_2 = \begin{bmatrix} 4390 & 133 \\ 439033 & 13301 \end{bmatrix}$$

No primeiro caso, a norma de um ponto qualquer $y_1 = B_1 X$ com, $X = (z_1, z_2) \in \mathbb{Z}^2$ do reticulado:

$$|y_1|^2 = \langle B_1 X, B_1 X \rangle = z_1^2 + z_2^2$$

Com essa base, é fácil perceber que a norma mínima é 1, nos vetores $(\pm 1, 0), (0, \pm 1)$.

No segundo caso, a norma de um ponto qualquer $y_2 = B_2 X$ será:

$$|y_2|^2 = 192769247189 z_1^2 + 11680323606 z_1 z_2 + 176934290 z_2^2$$

Com essa base, as combinações de (z_1, z_2) que minimizam a norma seriam:

$$(13301, -439033), (-13301, +439033), (133, -4390), (-133, 4390)$$

Se a matriz B_2 fosse a única fornecida, seria necessário testar muitas combinações para chegar nesse resultado.

RETICULADOS EM CRIPTOGRAFIA DE CHAVE PÚBLICA:

Sistemas de criptografia baseados em reticulados têm relevância na área de criptografia pós-quântica, de modo que três dos finalistas do concurso do órgão NIST (2016-2022) para criptografia pós-quântica eram baseados em reticulados[5]. Nesse tópico, será abordado o método de criptografia de chave pública chamado GGH[3].

A Criptografia de Chave Pública se baseia na existência de duas "chaves", uma pública e outra privada. Qualquer pessoa que tiver a chave pública, poderá Criptografar uma mensagem, mas somente uma pessoa com acesso a chave privada, consegue decripta-la.

Um meio de utilizar um reticulado $\Lambda \in \mathbb{R}^n$ nesse tipo de criptografia é uma adaptação do problema (CVP). Pode-se dizer que "Alice" tem acesso a uma "Boa" matriz geradora $B \in \mathbb{R}^n$ de Λ. Utilizando B, será divulgada uma chave pública constrói uma matriz geradora "Ruim" H, que será disponibilizada ao público enquanto B será mantida em segredo.

Para criptografar uma mensagem, “Bob” deverá escolher um vetor $u \in \mathbb{Z}^n$ que, de alguma maneira, contenha a mensagem e um vetor de ruído $n \in \mathbb{R}^n$. Com os vetores u, n, uma mensagem criptografada é gerada da seguinte maneira:

$$u \to y = Hu + n$$

O processo de descriptografar uma mensagem y consiste em resolver o problema de vetor mais próximo (CVP). Assim, somente “Alice” conseguirá decodificar as mensagens com certa facilidade, por possuir uma “Base Boa”.

No caso do vetor de ruídos for suficientemente pequeno e conhecermos uma base boa, o problema do vetor mais próximo pode ser resolvido por um método de aproximação. O método consiste em:

- Encontrar as coordenadas v de y na base B sem a restrição de números inteiros. $v = B^{-1} y$
- Aproximar cada coordenada obtida para o número inteiro mais próximo $\bar{v}$. $\bar{v} = \lfloor B^{-1} y \rceil$
- Calcular o ponto y' de coordenadas $\bar{v}$ na base B. $y' = B\bar{v}$

A sequência dos passos resulta na seguinte equação:

$$y' = B \lfloor B^{-1}(Hu + n) \rceil$$

Com esse ponto y', os valores iniciais de u e n podem ser obtidos novamente.

$$u = H^{-1} y' \quad n = y - H^{-1} y'$$

Para exemplificar o método, será utilizado o reticulado no $\mathbb{R}^2$ com bases boa (B) e ruim(H):

$B = \{(3,4), (3,-3)\} \quad H = \{(24,-3), (33,-5)\}$

.

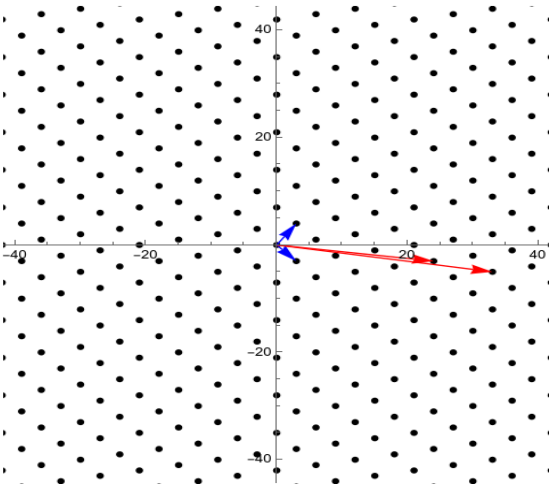


Figura 4- Reticulado no $\mathbb{R}^2$ com duas bases destacadas, $B = \{(3,4), (3,-3)\}$ em azul e $H = \{(24,-3), (33,-5)\}$ em vermelho.

Seja $u = (13, 25)$ e $n_1 = (1.3, 1.2)$, resultando na mensagem criptografada

$y_1 = (1030.3, -138.8)$, ao executar o método de decodificação valor de y é decodificado corretamente. No entanto, se o vetor for utilizado um $n_2 = (-2.1, 1.3)$, com $y_2 = (1026.9, -138.7)$, a mensagem é decodificada para $(1026, -137)$ ao invés de $(1029, -140)$.

Assim, existe uma região no plano, dada uma base específica, em que o vetor de ruído pode ser escolhido para o método funcionar. Para identificar essa região, o método foi realizado para 2500 vetores de ruído igualmente distribuídos na região $(-5, 5) \times (-5, 5)$. E obtivemos o seguinte resultado:

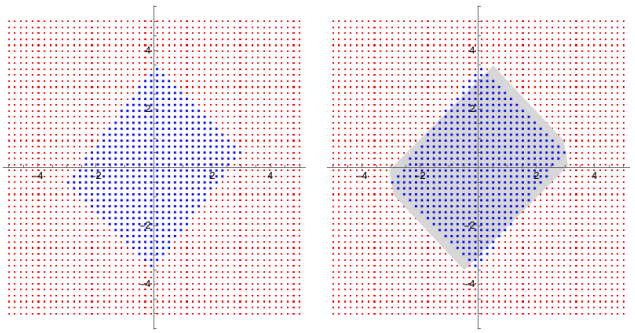


Figura 5 e 6 - Na imagem da esquerda (5), os pontos em azul representam as posições do vetor de ruído que resultaram em decodificações corretas e os pontos em vermelho indicam as posições em que as decodificações foram incorretas, considerando a base B. Na imagem da direita (6) a área destacada é a região de Voronoi do reticulado.

Pela **Imagem 6**, nota-se que o método de aproximação para a base B é praticamente equivalente a resolver de fato o problema (CVP), uma vez que a região de Voronoi, que independe da base utilizada, é muito próxima da região de acerto do método.

Ao realizar o mesmo teste tentando simular que uma pessoa tente decodificar com a base ruim, foi obtido o seguinte resultado:

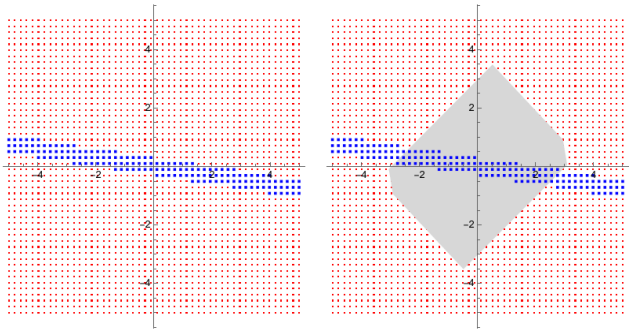


Figura 7 e 8 - Na imagem da esquerda (7), os pontos em azul representam as posições do vetor de ruído que resultaram em decodificações corretas e os pontos em vermelho indicam as posições em que as decodificações foram incorretas para a base H. Na imagem da direita (8) a área destacada é a região de Voronoi do reticulado.

Nesse exemplo, fica claro que o método de aproximação na base H não é tão efetivo quanto na base B.

Essa região de acerto pode ser obtida algebricamente pela seguinte equação:

$$y' = B\lfloor B^{-1}(Hu + n)\rceil = Hu \Leftrightarrow$$
$$BB^{-1}Hu + \lfloor B^{-1}n)\rceil = Hu \Leftrightarrow$$
$$\lfloor B^{-1}n\rceil = 0$$

Além disso, dada a matriz B, pode ser aproximado um valor máximo de $||n||_2$ tal que

$$\lfloor B^{-1}n\rceil = 0.$$

Com esses resultados, nota-se que a base escolhida para a chave privada deve ser o mais ortogonal possível e vetores de norma pequena, além de os reticulados considerados serem de dimensões muito altas (800 ou mais), o que aumenta muito a complexidade computacional no caso de bases não apropriadas. Já a base escolhida para a chave pública deve ter vetores o mais paralelos possível escolhidos de maneira que a norma dos vetores linha da matriz inversa sejam grandes, assim, o vetor de erro terá que ser muito pequeno e a aproximação não coincidirá com a região de Voronoi.

CONCLUSÕES:

Neste trabalho foram selecionados e ilustrados conceitos iniciais da Teoria de Reticulados e aplicação num método de criptografia de chave pública. Essa aplicação possibilita uma introdução na subárea de grande relevância de

criptografia pós-quântica por envolver os problemas computacionais CVP e SVP. Perspectivas de continuidade do projeto incluem estudo de conceitos de machine learning para futuramente, estudar aplicações de reticulados para codificação, inclusive em modelos de “federated learning”.

BIBLIOGRAFIA:

[1]COSTA, S. I. R. et al. **Lattices Applied to Coding for Reliable and Secure Comunications**: Springer, 2017.

[2]MICCIANCIO, D.; REGEV, O. **Lattice-based Cryptography in Post-Quantum Cryptography**: Springer, 2009.

[3]Goldreich, O.; Goldwasser, S.; Halevi, S. (1997). **Public-key cryptosystems from lattice reduction problems**. In: Kaliski, B.S. (eds) Advances in Cryptology — CRYPTO '97. CRYPTO 1997.

[4]Wolfram Research. **Mathematica**. Disponível em:.https://www.wolfram.com/mathematica

[5] NIST(National Institute of Standards and Technology):https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms