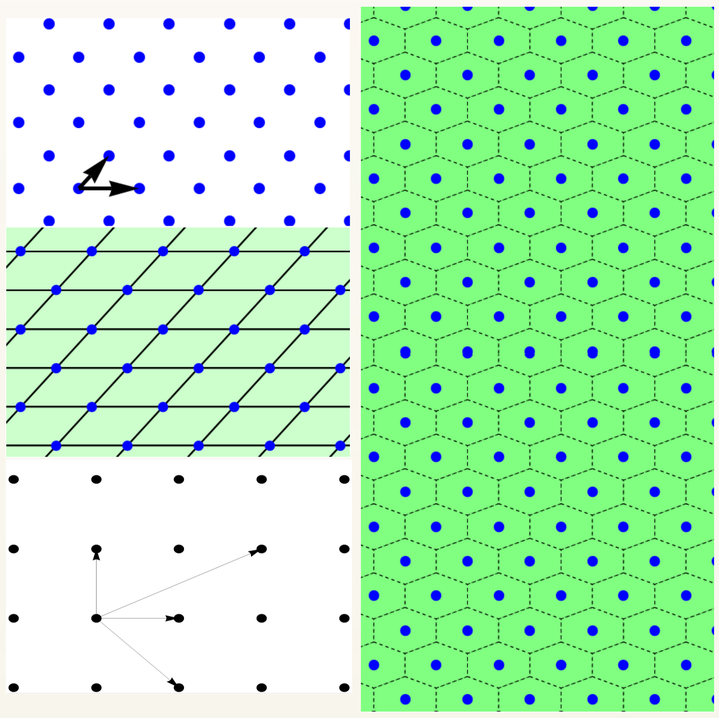
O PROBLEMA DO VETOR MAIS PRÓXIMO NOS RETICULADOS RAÍZES: UMA ABORDAGEM COMPUTACIONAL

Autor: Alan Bondesan De Maria – alan.maria@fca.unicamp.br - Faculdade de Ciências Aplicadas da Unicamp – Limeira
Orientador: Cristiano Torezzan – cristiano.torezzan@fca.unicamp.br - Faculdade de Ciências Aplicadas da Unicamp – Limeira
Agência financiadora: CNPq
Palavras-chave: Reticulados – Teoria de Códigos – Criptografia Pós-Quântica

O que são reticulados?



Qual a importância?

Devido a sua estrutura simétrica, os reticulados surgem em diversos ramos da matemática pura e aplicada. Nesta última, as aplicações na área de códigos e criptografia têm se mostrado promissoras .

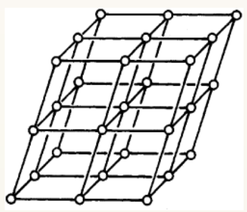
Como assim?

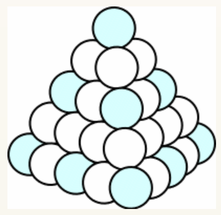
Bons sistemas de criptografia, tais como os de chave pública RSA e ECC, dependem fortemente de problemas matemáticos difíceis para garantir sua segurança. **Os reticulados possuem problemas muito difíceis de se resolver**, o que permite sua utilização no desenvolvimento de criptossistemas baseados em reticulados.

Quais são estes problemas?

Os principais são o ***problema do vetor mais próximo*** e o *problema do vetor mais curto*. **O trabalho desta iniciação científica foi investigar o comportamento computacional do problema do vetor mais próximo em reticulados especiais, chamados reticulados raízes.**

Reticulados Raízes:





Cúbico n-dimensional:

$Z^n = \{(x_1, \dots, x_n), tal\ que\ x_i \in Z\}$

Reticulado D_n:

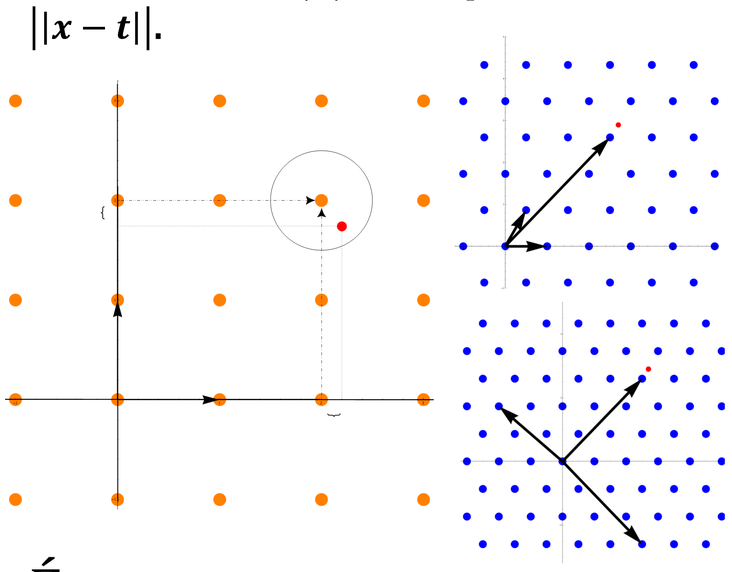
$D_n = \{(x_1, \dots, x_n) \in Z^n\ tal\ que\ \sum x_i\ mod\ 2 = 0\}$

Reticulado A_n:

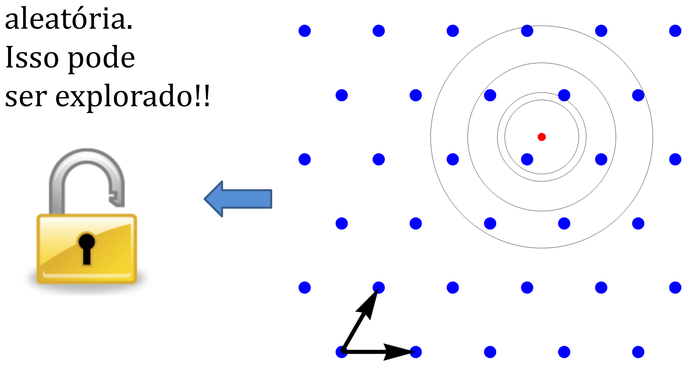
$A_n = \{(x_0, \dots, x_n) \in Z^{n+1}\ tal\ que\ \sum x_i = 0\}$

O Problema do Vetor Mais Próximo

Seja L(**B**) um reticulado e $\boldsymbol{t} \in R^n$ um ponto qualquer do espaço. O problema é encontrar $\boldsymbol{x} \in L(\boldsymbol{B})$ tal que minimize $||\boldsymbol{x} - \boldsymbol{t}||$.



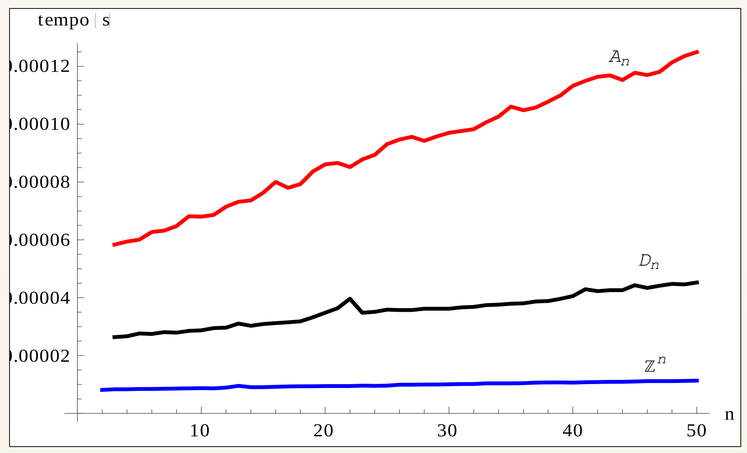
É muito difícil resolver o problema do vetor mais próximo para uma base qualquer, aleatória.
Isso pode ser explorado!!



Principais referências:

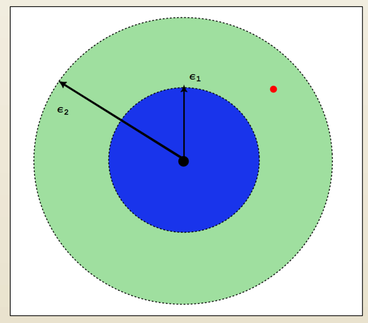
J.H. Conway, N.J.A. Sloane, “Sphere Packings, Lattices and Groups”;
E. Agrell, T. Eriksson, A. Vardy, K. Zegger, "Closest Point Search in Lattices"

Algoritmos



Criptografia

Chave Privada: Matriz geradora $\boldsymbol{B}$; matriz unimodular $\boldsymbol{U}$ ($\boldsymbol{G} = \boldsymbol{UB}$); vetor mais curto $\boldsymbol{u}$ de $L(\boldsymbol{B})$ e algoritmo de decodificação.
Chave pública: **G**, ϵ_1 *e* ϵ_2 (escalares).



A distribuição dos pontos criptografados na malha é aleatória. Assim, diferentes pontos do reticulado estão relacionados com o mesmo bit.

Exemplo: criptografia da string: “000”