TEORIA DE RETICULADOS – UNIVERSIDADE ESTADUAL DE CAMPINAS

Orientado: Paulo Henrique Perin Facini; Orientador: João Eloir Strapasson
Email: paulohpfacini@hotmail.com; joao.strapasson@fca.unicamp.br
Conselho Nacional de Desenvolvimento Cientifico e Tecnológico – CNPq
Palavras-chave: reticulados-códigos-criptografia

Introdução

A teoria de reticulados tem inúmeras aplicações, em especial na teoria de códigos e da criptografia. Entretanto estaremos interessados em outra aplicação desta teoria, dada pela sua relação com o problema do empacotamento esférico.

O trabalho tem como objetivo ilustrar a teoria de reticulados, já que ela está sendo bem explorada em outros países, no entanto, a literatura em português sobre a teoria é restrita as dissertações de mestrado e teses de doutorado.

Metodologia

A metodologia utilizada neste trabalho consistiu em leituras de textos e apresentação de seminários que contemplavam a discussão sobre os temas descritos na próxima seção. Por fim, utilizamos o programa *Mathematica*, no qual foram feitos os esboços de reticulados, regiões fundamentais, entre outros.

Resultados e Discussões

Na sequência vamos definir e ilustrar os conceitos introdutórios e básicos da teoria de reticulados:

Definição de Reticulado: Seja R^m um espaço euclidiano m-dimensional, e $\beta = \{u_1, u_{2,\dots,} u_n\}$ um conjunto de n-vetores linearmente independentes que gera um espaço vetorial suporte V, chamaremos de ***reticulado*** *(Λ)* ao seguinte conjunto:

$\Lambda = \{\alpha_1 u_1 + \alpha_2 u_2 + \dots + \alpha_n u_n; \alpha_i \in Z, 1 \leq i \leq n\}$, *onde* o conjunto $\beta = \{u_1, u_2, \dots, u_n\}$ é dito ***base*** do reticulado.

Definição de Matriz Geradora: A **Matriz geradora** *(K)* é aquela que possui os vetores da base em colunas:

$$K = (u_{1,\dots,} u_n)$$

Teorema de mudança de base: Dado um reticulado Λ gerado por uma base β, uma base θ será base deste reticulado se, e somente se, a respectiva matriz mudança de base possui entradas inteiras e determinante ± 1.

Definição de Matriz de Gram: Se K é uma matriz geradora do reticulado Λ, a matriz definida por $G = K^T \cdot K$, onde T denota a transposta de B, é chamada ***matriz de Gram*** *(G)* associada ao reticulado Λ.

Definição de Região de Voronoi: Fixado um vetor $w \in \Lambda$, definimos a **Região de Voronoi** *(Vor)* de w como sendo a região que contém todos os pontos de R^n que estão mais próximos de w do que qualquer outro ponto u do reticulado, ou seja:

$$Vor(w)_\Lambda = \{x \in R^n : ||w-x|| \leq ||u-x||; u \in \Lambda\}$$

Definição de Região Fundamental: Seja $\beta = \{u_1, u_{2,\dots,} u_n\}$ uma base do reticulado, a **Região Fundamental** *(F)* associada é o conjunto:

$$F_{\beta,\Lambda}(V) = \{ V+u; u \; \Sigma \alpha_i u_i \; \alpha \in [0,1)\}$$

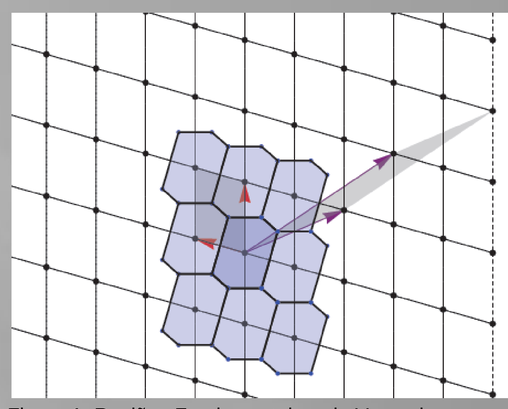


Figura 1: Regiões Fundamentais e de Voronoi em um reticulado aleatório

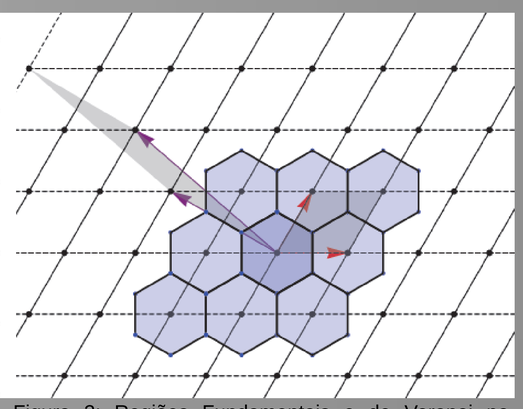


Figura 2: Regiões Fundamentais e de Voronoi no reticulado hexagonal

Definição de Empacotamento Reticulado: Denomina-se empacotamento reticulado quando o centro das bolas são os pontos de um reticulado. A todo reticulado Λ tem-se um empacotamento esférico associado, que é dado por bolas cujo raio é igual a metade da distância mínima os entre pontos de Λ.

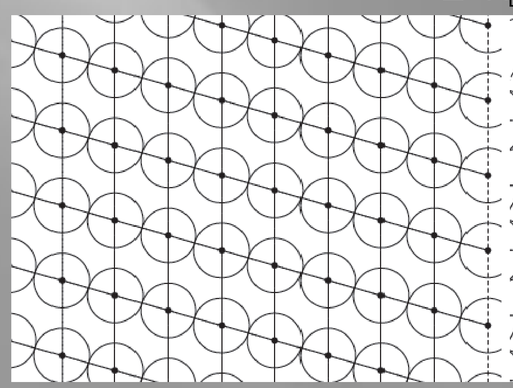
Definição de Raio de Empacotamento: é o maior raio *ρ* tal que $B_\rho(u) \cap B_\rho(v) = \emptyset$ para quaisquer *u* e $v \in \Lambda$ e $u \neq v$.

Definição de Norma Mínima: A norma mínima *(η) de um reticulado Λ é a menor norma dentre os elementos não nulos de Λ:*

$$\eta = \min \{||x||; x \in \Lambda, x \neq 0\}$$

Definição de Densidade de Empacotamento: A densidade do empacotamento (Δ) de um reticulado $\Lambda \in R^2$, é a razão entre a área do disco de empacotamento (A_d) e a e a área da região de Voronoi *(A_{vor}).*

$$\Delta = A_D / A_{vor}$$



Figuras 3: Empacotamento reticulado em reticulado aleatório

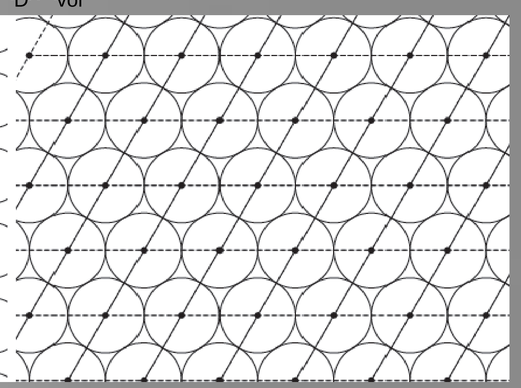


Figura 4: Empacotamento reticulado em reticulado hexagonal

Conclusão

Até o momento foi feito apenas uma introdução a teoria de reticulados e conseguimos notar que cada um possui a sua particularidade. Enfim, agora com a noção básica e essencial desta teoria, iremos trabalhar em aplicações da teoria, em especial a sua relação com a teoria de códigos.

Referências bibliográficas

- Naves, Lígia Rodrigues Bernabé. “A densidade de empacotamentos esféricos em reticulados”

- Gouvêa, Drielson Davison Silva. “Um problema sobre o vetor mais próximo nos reticulados raízes Z^n, A_n e D_n: Algoritmos e simulação numerica”