ISSN 1984-820X
Anais do CNMAC
v.3
PUBLICAÇÃO DA SBMAC
CNMAC2010
XXXIII CONGRESSO NACIONAL DE MATEMÁTICA APLICADA E COMPUTACIONAL

# Treliça mínima em reticulados bidimensionais

**Grasiele C. Jorge*** **Agnaldo J. Ferrari†** **Sueli I. R. Costa ‡**
Instituto de Matemática, Estatística e Computação Científica, IMECC, UNICAMP,
13083-859, Campinas, SP
E-mail: [ferrari, grajorge, sueli] @ime.unicamp.br

## RESUMO

O processo de decodificação em reticulados consiste em dados um reticulado e um vetor no espaço euclidiano n-dimensional, encontrar o ponto do reticulado mais próximo de tal vetor com respeito a distância euclidiana [7].

Existem alguns algoritmos eficientes para decodificar reticulados conhecidos, como por exemplo os reticulados $A_n$, $D_n$, $E_8$ e o reticulado de Leech [7]. Esses algoritmos decorrem de propriedades especiais destes reticulados. No entanto, não se conhece algoritmo capaz de decodificar reticulados $n$-dimensionais quaisquer em tempo polinomial [1], [2], [5].

Este alto grau de complexidade tem motivado a busca por sistemas criptográficos baseados em reticulados, os quais podem também ser uma alternativa de uso no advento do computador quântico [5].

Para reticulados que possuem sub-reticulado ortogonal podemos utilizar o método de decodificação por treliça, conhecido como algoritmo de Viterbi [8], [3]. A complexidade de tal algoritmo está diretamente ligada com a cardinalidade do grupo quociente do reticulado pelo sub-reticulado ortogonal. Quanto menor for tal cardinalidade maior é a eficiência do algoritmo [3].

Dados um reticulado $\Lambda$ e um sub-reticulado ortogonal $\Lambda^*$, temos uma partição do reticulado $\Lambda$ em $|\Lambda/\Lambda^*|$ classes distintas. Cada uma das classes é obtida por uma translação do sub-reticulado $\Lambda^*$ por vetores do quociente $\Lambda/\Lambda^*$, os gluing vectors.

Devido a simplicidade para decodificar reticulados ortogonais (projeções e arredondamentos), a decodificação por treliças é feita decodificando o vetor recebido em cada uma das classes acima, pois cada classe consiste de uma translação do sub-reticulado ortogonal. A decodificação termina comparando o vetor mais próximo dentre todos os candidatos encontrados em cada classe.

Com o intuito de diminuir a complexidade da decodificação por treliças busca-se um sub-reticulado ortogonal cujo quociente associado tenha cardinalidade mínima. Para alguns reticulados clássicos, como por exemplo, $D_n$, $E_6$, $E_7$ e $E_8$ já é conhecido o menor sub-reticulado ortogonal [3],[4]. Para reticulados gerais é muito difícil encontrar o menor sub-reticulado ortogonal, pois uma busca exaustiva torna-se impraticável a medida em que a dimensão cresce.

Partimos de reticulados que possuem matriz de Gram com números racionais em todas as suas entradas, onde é conhecido pelo menos um sub-reticulado ortogonal. Temos analisado o problema da procura por treliça mínima de reticulados a partir de características da forma de Smith da matriz de Gram [6]. A forma de Smith pode ser aplicada apenas em matrizes com determinante não nulo e cujas entradas pertençam a um domínio de ideais principais. No caso estudado, consideramos reticulados com matriz de Gram racional, mas para cada um destes reticulados sempre existem reticulados equivalentes cuja matriz de Gram possui todas as

*bolsista de Doutorado CNPq - Processo 140239/2009-0
†bolsista de Doutorado CNPq - Processo 143269/2008-9
‡Projeto temático FAPESP - 07/56052-8

entradas inteiras e que são obtidos deste por uma dilatação. Para reticulados bidimensionais foi possível encontrar uma forma fechada para essa caracterização.

Sejam $\Lambda$ um reticulado bidimensional, $\{v_1, v_2\}$ uma base para $\Lambda$ e $G$ a matriz de Gram associada a esta base. A forma de Smith de $G$ resulta em $G = P^{-1}DQ^{-1}$, onde $D$ é uma matriz diagonal com $d_{11}|d_{22}$ e $P, Q$ são matrizes unimodulares. Os sub-reticulados ortogonais de $\Lambda$ que possuem os menores vetores em cada direção são caracterizados pela base $\{w_1, w_2\}$ onde $w_1 = av_1 + bv_2$, $w_2 = cv_1 + dv_2$, com $a, b, c, d$ inteiros satisfazendo:

- $mdc(a, b) = 1$,
- $c = \frac{c^*}{t}$, $d = \frac{d^*}{t}$, onde

$$c^* = -q_{11}w(a\overline{p_{12}} + b\overline{p_{22}}) + q_{12}(a\overline{p_{11}} + b\overline{p_{21}}),$$
$$d^* = -q_{21}w(a\overline{p_{12}} + b\overline{p_{22}}) + q_{22}(a\overline{p_{11}} + b\overline{p_{21}}),$$

com $d_{22} = d_{11}w$, $q_{ij}$ elementos da matriz $Q$, $\overline{p_{ij}}$ elementos da matriz $P^{-1}$ e $t = mdc(c^*, d^*)$.

A partir da forma geral de cada sub-reticulado ortogonal, encontramos uma expressão associada a ele, indicando o número de elementos do quociente do reticulado pelo respectivo sub-reticulado ortogonal. Variando todos os sub-reticulados ortogonais, obtemos uma forma quadrática que apresenta em seus coeficientes expressões dadas por elementos obtidos pela decomposição de Smith da matriz de Gram. Assim, dado um reticulado, quando minimizamos a forma quadrática acima, encontramos o menor subreticulado ortogonal e com isso obtemos a complexidade em decodificar tal reticulado por treliças.

Nosso objeitvo é buscar características de sub-reticulados ortogonais de reticulados em dimensões maiores que permitam reduzir significativamente a busca por treliça mínima. Para isso pretendemos utilizar a forma de Smith da matriz de Gram associada a uma matriz geradora na forma de Hermite.

**Palavras-chave**: *Reticulado, Sub-reticulado ortogonal, Decodificação de reticulado*

## Referências

[1] E. Agrell, T.Eriksson, A. Vardy, K. Zeger, "Closest Point Search in Lattices", *IEEE Transactions on Information Theory,* vol. 48, n.8, pp. 2201-2214, (2002).

[2] M. Ajtai, "The shortest vector problem in $L_2$ is NP-hard for randomized reductions", *Proc. 30th Annu ACMSYmp. Theory of Computing, Dallas,* pp.193-203, (1998).

[3] A. H. Banihashemi, "Decoding Complexity and Trellis Structure of Lattices", *PHD Thesis, Waterloo, Canada*, (1997).

[4] A. H. Banihashemi, "Minimal Trellis Diagrams of Lattices", *IEEE International Symposium on Information Theory, Ulm, Germany*, (1997).

[5] D. J. Bernstein, J. Buckmann, E. Dahem, "Post Quantum Cryptography", *Springer-Verlag,* (2009).

[6] H. Cohen, "A course in Computational Algebraic Number Theory", *Springer-Verlag, Berlin-Heidelberg,* (1993).

[7] J.H. Conway, N. J. Sloane, "Sphere Packings, Lattices and Groups", *Springer-Verlag, New York*, (1999).

[8] A. J. Viterbi, "Error bounds for convolucional codes and an asymptotically optimum decoding algorithm", *IEEE Transactions on Information Theory,* vol. IT-13, pp.260-269, April, (1967).