

Decodificando códigos de grupo comutativo

Agnaldo J. Ferrari* Grasiele C. Jorge† 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

Um código esférico em um espaço euclidiano n -dimensional é definido como um conjunto finito de pontos sobre a esfera unitária S^{n-1} .

Uma família especial de códigos esféricos é dada pelos códigos de grupo comutativo. Tais códigos são definidos no espaço euclidiano $2n$ -dimensional como a órbita de um vetor $x_0 \in S^{2n-1}$ sob a ação de um grupo comutativo de matrizes ortogonais G [1].

A decodificação em um código esférico, consiste em dado um vetor qualquer no espaço, encontrar o ponto do código esférico mais próximo de tal vetor com relação à distância euclidiana. Em geral, busca-se algoritmos que sejam capazes de decodificar eficientemente certas classes de códigos esféricos.

Para códigos de grupo comutativo existe uma correspondência que associa a cada um desses códigos no espaço euclidiano $2n$ -dimensional um reticulado no espaço euclidiano n -dimensional [1]. A partir dessa correspondência é possível derivar um algoritmo de decodificação para tais códigos, cuja etapa principal consiste na decodificação de um vetor no reticulado associado à metade da dimensão.

Decodificar um reticulado em um espaço euclidiano n -dimensional em geral é um problema difícil e nenhum algoritmo capaz de realizar a decodificação em tempo polinomial é conhecido [2], [3]. Para reticulados que possuem pelo menos um subreticulado ortogonal o processo de decodificação pode ser feito por treliças [4], [5]. Quando decodificamos por treliças fazemos uma partição do reticulado em classes provenientes do quociente do reticulado pelo subreticulado ortogonal. E a decodificação é realizada em cada uma destas classes, o que se torna fácil por tais classes corresponderem a transladados de um subreticulado ortogonal. A complexidade de tal algoritmo está diretamente relacionada com a cardinalidade do quociente do reticulado pelo subreticulado ortogonal. Quanto menor for a cardinalidade maior a eficiência do algoritmo.

Dado um código de grupo comutativo com M pontos, o reticulado Λ associado possui determinante igual a M^{n-1} e possui um sub-reticulado ortogonal gerado pela matriz MI_n . Desta forma, para tais reticulados é possível decodificar por treliças, utilizando M classes.

Como a complexidade do algoritmo de treliças está ligado à cardinalidade do quociente do reticulado pelo sub-reticulado ortogonal, a medida em que reduzimos o quociente, reduzimos a complexidade. Desta forma, é desejável encontrar o sub-reticulado ortogonal Λ' de Λ de forma a minimizar o índice $(\Lambda : \Lambda')$.

Tendo em vista a redução da complexidade, implementamos um algoritmo que através de uma busca exaustiva procura pelo menor subreticulado ortogonal de um dado reticulado.

Sabendo que estes reticulados possuem um subreticulado ortogonal cujo índice é M , devemos encontrar subreticulados ortogonais cujo índice seja menor do que ou igual a M .

*bolsista de Doutorado CNPq - Processo 143269/2008-9

†bolsista de Doutorado CNPq - Processo 140239/2009-0

‡Projeto temático FAPESP - Processo 07/56052-8

Como $\det(\Lambda) = M^{n-1}$, devemos encontrar um subreticulado ortogonal Λ' cujo determinante seja menor do que ou igual a M^n .

Assim, dada $\{v_1, \dots, v_n\}$ uma base de Λ' , como o determinante de um reticulado ortogonal é dado pelo produto das normas dos vetores da base, segue que $\prod_{j=1}^n \|v_j\| \leq M^n$. Sem perda de generalidade, podemos considerar $\|v_1\| \leq \|v_2\| \leq \dots \leq \|v_n\|$, assim $\|v_n\| \leq M^n / \lambda^{n-1}$, onde λ é a norma mínima do reticulado.

Portanto, o algoritmo realiza uma busca exaustiva por n vetores mutuamente ortogonais, tal que o produto das normas destes vetores seja a menor possível, no conjunto de vetores do reticulado cujas normas são menores do que ou iguais a M^n / λ^{n-1} . No entanto, não é necessário verificar a ortogonalidade entre todos estes vetores, pois se w_1, \dots, w_n são mutuamente ortogonais, então para $i \neq j$, w_i e kw_j para $k \in \mathbb{Z}$, $k > 1$ não precisam ser testados.

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

Referências

- [1] A.J. Ferrari, C. Torrezan, G. C. Jorge, S. I. R. Costa, “Um algoritmo de treliça para decodificação de códigos de grupo comutativo”, *XXVII Simpósio Brasileiro de Telecomunicações, Blumenau-SC*, (2009).
- [2] 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).
- [3] M. Ajtai, “The shortest vector problem in L_2 is NP-hard for randomized reductions”, *Proc. 30th Annu ACM Symp. Theory of Computing, Dallas*, pp.193-203, (1998).
- [4] A. H. Banihashemi, “Decoding Complexity and Trellis Structure of Lattices”, *PHD Thesis, Waterloo, Canada*, (1997).
- [5] A. H. Banihashemi, “Minimal Trellis Diagrams of Lattices”, *IEEE International Symposium on Information Theory, Ulm, Germany*, (1997).
- [6] J.H. Conway, N. J. Sloane, “Sphere Packings, Lattices and Groups”, *Springer-Verlag, New York*, (1999).