 ISSN 1984-820X

Conexões entre códigos corretores de erros e reticulados

Antonio Carlos de Andrade Campello Junior*
Depto. de Matemática Aplicada, IMECC, Universidade Estadual de Campinas
13083-859, R. Sérgio Buarque de Holanda, Campinas-SP
E-mail: campello@ime.unicamp.br

Profa. Dra. Sueli Irene Rodrigues Costa
Depto. de Matemática, IMECC, Universidade Estadual de Campinas
13083-859, R. Sérgio Buarque de Holanda, Campinas-SP
E-mail: sueli@ime.unicamp.br

RESUMO

Estudamos, neste projeto, conexões entre códigos corretores de erros e empacotamentos, através da análise de propriedades de códigos específicos (limitantes envolvendo seus parâmetros, distância mínima para correção de erros, etc.) e da construção explícita de empacotamentos reticulados a partir de códigos lineares binários. Este trabalho insere-se no projeto de iniciação científica "Códigos Corretores de Erros e Matemática Discreta - Uma introdução" e está ligado ao projeto temático "Teoria de Informação e Códigos" ambos com suporte da FAPESP. Uma abordagem inicial dos tópicos aqui tratados foi apresentada em [1].

Códigos lineares são, *grosso modo*, códigos obtidos pela adição de redundância (com propriedades lineares) em um conjunto de "palavras" de um certo tamanho em um alfabeto. De maneira mais precisa, são códigos gerados por transformações lineares injetivas entre dois espaços vetoriais sobre corpos finitos. São fortemente utilizados na prática por herdarem todas as propriedades de espaços vetoriais, o que facilita a busca por códigos "bons" (que corrigem/detectam o maior número de erros com a menor redundância) e o desenvolvimento de algoritmos de codificação/decodificação. Dentre os códigos lineares de largo uso, destacam-se o Código de Hamming, Golay e Reed-Solomon [3].

Reticulados, por sua vez, constituem uma rica estrutura em Geometria Discreta que é associada, por exemplo, ao problema de empacotar esferas de maneira ótima em $\mathbb{R}^n$, o qual possui aplicações em diversas áreas. Existem, além disso, algumas técnicas de construção [2] que relacionam reticulados a códigos binários e permitem a utilização da estrutura dos códigos para a inferência de propriedades dos reticulados, e vice-versa.

É nesse contexto de conexão entre Códigos Corretores de Erro e Reticulados que desenvolvemos este projeto. Na primeira parte, procuramos discutir em profunidade o que acontece na codificação dos pontos de $\mathbb{Z}_2^2$,ou seja, códigos binários de dimensão dois, quando aumentamos o comprimento dos códigos afim de corrigir mais erros. São analisados o comprimento mínimo para a correção de t erros, o número de todas as soluções neste comprimento (ponto de vista combinatório), e o número de toda as soluções isometricamente distintas (ponto de vista geométrico), e discutidas as taxas de informação e correção de erros de tais códigos.

Em particular, analisamos todas as características de melhores códigos do tipo $(n, 2, d)$ que podem ser obtidos e mostramos que códigos corretores de t erros têm comprimento mínimo $3t+2$ e são todos isométricos. Além disso, subindo em 1 o comprimento destes códigos, os estendemos

*bolsista de Iniciação Científica FAPESP proc. 2007/58294-9

para um código que detecta um erro a mais. A taxa de detecção de erros destes códigos está ilustrada na Figura 1, onde D_0 e D_1 são, respectivamente, as taxas dos melhores códigos de comprimento $3t+2$ e $3t+3$.

Partindo de tais códigos, foram construídos reticulados "via Construção A", descrita em [2], cuja densidade de empacotamento supera a do reticulado $\mathbb{Z}^n$ em todas as dimensões. De fato, a densidade de centro dos reticulados obtidos é pelo menos $(1/2)^{n-2}$ (Figura 2), quatro vezes maior que a de $\mathbb{Z}^n$. Fizemos também uma comparação com as densidades dos melhores reticulados conhecidos em dimensões baixas. Em $\mathbb{R}^3$, o reticulado obtido é equivalente ao reticulado D_3, cúbico de face centrada, o de maior densidade neste espaço.

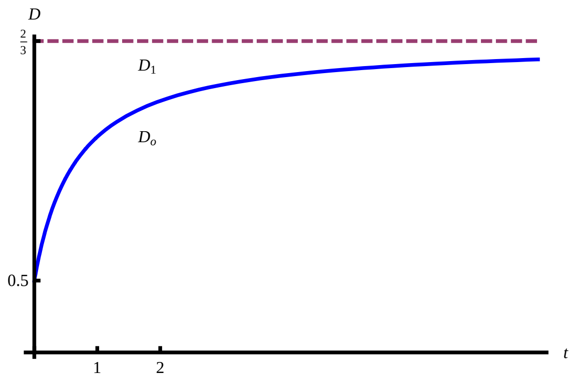

Figura 1: Gráfico da taxa de correção em função do número de erros a serem corrigidos

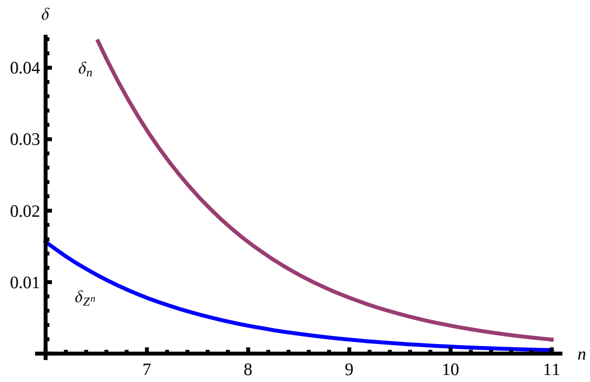

Figura 2: Taxa da densidade de centro pela dimensão n, aqui tratada como variável real para uma análise gráfica.

Por fim, estudamos alguns dos limitantes conhecidos para códigos corretores de erros (por exemplo o limitante do empacotamento esférico e a cota de singleton, [5]) e vimos como estes limitantes se relacionam com limitantes para a densidade de reticulados, partindo também da Construção A.

Palavras-chave: *Códigos Corretores de Erros, Reticulados, Empacotamentos Esféricos, Teoria da Informação*

Referências

[1] Campello A.C. de A. e Costa S.I.R, "Códigos do robô e seus reticulados", IV Simpósio Nacional/Jornadas de Iniciação Científica, Rio de Janeiro, IMPA 2008

[2] Conway J.H. and Sloane N.J.A. "Sphere packings, lattices and groups". Springer-Verlag, New York, 3rd Ed.1998.

[3] Hefez A., Villela M.L.T, "Códigos Corretores de Erros", Rio de Janeiro, IMPA 2002

[4] Lavor C. C., Alves M. M. S, Siqueira R. M e Costa S. I. R, "Uma Introdução à Teoria de Códigos", Notas em Matemática Aplicada SBMAC vol. 21 2006

[5] Pless, V.S, Huffman, W.C. et al, "Handbook of Coding Theory", Elsevier Science B.V. 1998, Vol. 1

[6] Shannon, C. E., "A Mathematical Theory of Communications, Bell Systems", Tech. J., 27 (1948), 379-423, 623-656.