TEMA Tend. Mat. Apl. Comput., **11**, No. 1 (2010), 1-8.

Construção de Códigos Esféricos através do Reticulado Hexagonal

C. ALVES[1], Departamento de Matemática, Instituto de Geociências e Ciências Exatas, UNESP - Universidade Estadual Paulista, 13506-900 Rio Claro, SP, Brasil

A.A. de ANDRADE[2], Departamento de Matemática, Instituto de Biociências, Letras e Ciências Exatas, UNESP - Universidade Estadual Paulista, 15054-000 São José do Rio Preto, SP, Brasil

S.I.R. COSTA[3], Departamento de Matemática, Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas, 13083-859 Campinas, SP, Brasil.

Resumo. Códigos esféricos n-dimensionais gerados por grupos comutativos em dimensão par, $n = 2m$, podem ser determinados pelo quociente de reticulados m-dimensionais, quando os vetores que geram o sub-reticulado são mutuamente ortogonais [4]. Apresentamos a construção de sub-reticulados nestas condições, a partir do reticulado hexagonal, A_2. Comparamos a distância mínima do código esférico construído através do quociente destes reticulados com o limitante da distância mínima estabelecido em [5].

Palavras-chave. Reticulados, códigos esféricos, distância mínima.

1. Introdução

Para códigos esféricos, características como boa distância mínima, regiões de decisão simétricas e perfil de distâncias homogêneo da constelação de sinais são determinantes para uma baixa probabilidade de erro na transmissão de sinais através de um canal gaussiano.

Nesse sentido, a utilização de códigos de grupo comutativo merece destaque. Para esses códigos, a análise da distância mínima desempenha papel fundamental, visto que sua estrutura algébrica garante as características de simetria desejadas.

Em [6], Slepian estabeleceu, de maneira geral, os conceitos sobre códigos esféricos para o canal gaussiano e apresentou a teoria necessária para a construção dos códigos gerados por grupos de matrizes ortogonais que geram pontos sobre a superfície de uma hiperesfera, de modo uniforme.

[1]carina_matematica@yahoo.com.br
[2]andrade@ibilce.unesp.br
[3]sueli@ime.unicamp.br

Recebido em 04 Setembro 2009; Aceito em 29 Junho 2010.

De maneira geral, dada uma dimensão n e um número de pontos M procura-se por um código de grupo $[M, n]$ com a maior distância mínima. Este código é chamado *ótimo*. Os principais esforços para resolver este problema são:

- Construção de limitantes para o número de pontos $M = M(n, d)$ de um código esférico que envolva a dimensão n e a distância mínima d.
- Construção de códigos que tenham distâncias mínimas próximas da distância limite.
- Determinação do melhor vetor inicial da esfera unitária do $\mathbb{R}^n$ que, para um determinado grupo gerador, maximiza a distância mínima entre dois pontos quaisquer do código.

De acordo com [2], o número de casos que devem ser verificados para encontrar o código ótimo é aproximadamente $\binom{M/2}{n/2}$. Para grupos que geram um grande número de pontos, a busca pelo código ótimo usando técnicas de programação, torna-se um problema computacional de custo muito alto, o que motivou-nos a utilizar ferramentas que gerassem um procedimento possível para, em casos especiais, gerar códigos de grupos comutativos muito bons, onde para calcular a distância mínima calcula-se a distância entre as imagens dos vetores de norma mínima da base que gera o reticulado e o vetor inicial, sem a necessidade de analisar casos.

Códigos esféricos em dimensão par, gerados por grupos comutativos de matrizes ortogonais, podem ser determinados pelo quociente de dois reticulados na metade da dimensão quando o sub-reticulado é "retangular" (isto é, quando os vetores que o geram são mutuamente ortogonais), [2] e [4]. Assim, o objetivo deste trabalho é a construção de códigos esféricos através do quociente de reticulados, com a finalidade de obter códigos esféricos em que a distância mínima se aproxime do limitante da distância mínima estabelecido em [5].

Na bibliografia pesquisada, verifica-se a existência de sub-reticulados "retangulares" a partir do reticulado hexagonal A_2, que é o de maior densidade de empacotamento conhecida em dimensão 2 e compara-se a distância mínima do código esférico construído através do quociente destes reticulados com o limitante.

Este trabalho é organizado como segue. Na Seção 2, apresentamos algumas definições e resultados usados para a construção de códigos esféricos a partir do quociente de reticulados; na Seção 3, descrevemos a expressão para o cálculo da distância mínima; na Seção 4, exibimos o limitante para códigos de grupo comutativo; na Seção 5, apresentamos um resultado que caracteriza a forma geral dos sub-reticulados de A_2 que satisfazem a condição de ortogonalidade exigida juntamente com um exemplo onde a distância mínima encontrada é comparada com o limitante. Finalmente, na Seção 6, conclusões são dadas.

2. Reticulados e Códigos de Grupo

Definição 2.1 ([1]- Reticulado)**.** *Um reticulado Λ_β é o conjunto de todas as combinações lineares com coeficientes inteiros de um conjunto $\beta = \{w_1, \cdots, w_m\}$ de m*

vetores linearmente independentes do espaço vetorial $\mathbb{R}^m$,

$$\Lambda_\beta = \left\{ \mathbf{x} = \sum_{i=1}^{m} a_i w_i \mid a_i \in \mathbb{Z}, \forall\, i \right\}.$$

O conjunto β *é denominado uma base de* Λ_β.

O reticulado $A_n = \{(x_1, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1} \mid x_1 + \cdots + x_{n+1} = 0\}$ é chamado de reticulado *hexagonal* para $n = 2$. Sua matriz geradora é $\left\{(1,0), (\frac{1}{2}, \frac{\sqrt{3}}{2})\right\}$.

Definição 2.2 ([1] - Sub-reticulado)**.** *Seja* B *uma matriz* $n \times n$ *com entradas inteiras. Um sub-reticulado de* Λ_β *é dado por* $\Lambda_\alpha = \{\mathbf{x} = \lambda BM \mid \lambda \in \mathbb{Z}^n$, *onde* M *é a matriz geradora do reticulado* Λ_β.

O índice do sub-reticulado Λ_α é a cardinalidade do grupo quociente $\Lambda_\beta/\Lambda_\alpha$ e

$$|\Lambda_\beta/\Lambda_\alpha| = \frac{vol(\Lambda_\alpha)}{vol(\Lambda_\beta)} = \frac{\sqrt{\det(\Lambda_\alpha)}}{\sqrt{\det(\Lambda_\beta)}} = |det(B)|.$$

Dado um empacotamento no $\mathbb{R}^n$, associado ao reticulado Λ_β, definimos a sua densidade de empacotamento de esferas de raio r como sendo a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas.

Um código esférico é um subconjunto finito da esfera unitária euclidiana S^n, contida em $\mathbb{R}^{n+1}$. A *distândia mínima* de um código esférico n-dimensional $\mathcal{C} \subset S^n$ é definida como

$$d = \min_{\substack{x, y \in \mathcal{C} \\ x \neq y}} ||x - y||,$$

onde $||x - y||$ é a distância euclidiana em $\mathbb{R}^{n+1}$ entre os pontos do código x e y.

Definição 2.3 ([1]- Órbita)**.** *Seja* $x_0 \in \mathbb{R}^n$ *e* G *um grupo de matrizes* $n \times n$. *Chamamos de órbita de* x_0 *por* G *ao conjunto*

$$G(x_0) = \{g(x_0) \mid g \in G\}.$$

Definição 2.4 ([1]- Código de Grupo)**.** *Um código de grupo* $\mathcal{C}$ *é a órbita de um vetor* v *na esfera unitária* S^{n-1} *por um subgrupo* $G = \{O_i\}_{i=1}^M$ *do grupo das matrizes ortogonais* $n \times n$, $\mathbf{O}(n)$, *tal que o código* $\mathcal{C} = \{O_i v\}_{i=1}^M$ *é substancial em* $\mathbb{R}^n$ *(não está contido em um hiperespaço, isto é, subespaço vetorial de codimensão 1).*

Quando o subgrupo de $\mathbf{O}(n)$ *for comutativo, teremos um código de grupo comutativo.*

A alocação de pontos em uma hiperesfera com a maior distância euclidiana mínima depende da estrutura do grupo que é admitido no processo.

Teorema 2.1 ([1])**.** *Sejam* $\alpha = \{v_1, \cdots, v_m\}$ *e* $\beta = \{w_1, \cdots, w_m\}$ *duas bases de* $\mathbb{R}^m$, Λ_α *e* Λ_β *os reticulados gerados por* α *e* β, *respectivamente, e* $\Lambda_\alpha \subset \Lambda_\beta$. *Se* $A = (a_{ij})$, $a_{i,j} \in \mathbb{Z}$ *é a matriz da base* α *escrita em relação à base* β, *então a classificação e o conjunto de geradores do grupo* $\Lambda_\beta/\Lambda_\alpha$ *são obtidos da forma normal de Smith de* A.

Definição 2.5 ([1]- Forma Normal de Smith)**.** *Dizemos que uma matriz $A = (a_{i,j})$ de ordem $n \times n$ esta na forma normal de Smith se A é uma matriz diagonal com coeficientes inteiros não negativos tal que $a_{i,i}|a_{i+1,i+1}$ para todo $i < n$.*

3. Expressão para a Distância na Imagem por ψ

Seja

$$\begin{aligned} \psi \quad : \quad & \mathbb{R}^m \longrightarrow \mathbb{R}^{2m} \\ & y \longmapsto \psi(y) = \left(\delta_1 \cos(\frac{y_1}{\delta_1}), \delta_1 sen(\frac{y_1}{\delta_1}), \cdots, \delta_m \cos(\frac{y_m}{\delta_m}), \delta_m sen(\frac{y_m}{\delta_m})\right) \end{aligned} \quad (3.1)$$

onde $y = (y_1, \cdots, y_m)$ são coordenadas em relação a uma base ortogonal.

A parametrização ψ induz uma relação de equivalência em $\mathbb{R}^m$ cujas classes formam um conjunto chamado toro planar abstrato. Um conjunto de representantes para essa relação é o paralelepípedo $\prod_{i=1}^{m}[0, 2\pi\delta_i)$. Este conjunto de representantes pode ser visto como um espaço quociente onde os lados paralelos do paralelepípedo são identificados.

Assim, considerando um toro $T_{\delta=(\delta_1,\cdots,\delta_m)}$ na esfera unitária contida em $\mathbb{R}^{2m}$ e a aplicação (3.1), com $\delta_i = \frac{||v_i||}{2\pi}$, definimos a distância euclidiana ao quadrado entre $\psi(x)$ e $\psi(y)$ na esfera de $\mathbb{R}^{2m}$ por

$$\begin{aligned} d^2(\psi(x), \psi(y)) &= ||\psi(x) - \psi(y)||^2 \\ &= 4\sum_{i=1}^{m}\left(\frac{||v_i||}{||v_1|| + \cdots + ||v_m||}\right)^2 sen^2\left(\frac{\pi(x_i - y_i)}{||v_i||}\right) \\ &= 4\sum_{i=1}^{m}\delta_i^2 sen^2\left(\frac{x_i - y_i}{2\delta_i}\right). \end{aligned}$$

Um caso particular que utilizaremos no caso de grupos comutativos é $y = \mathbf{0} = (0, \cdots, 0)$, pois sendo estes geometricamente uniformes, o perfil de distâncias a um ponto é igual para todos os pontos, portanto podemos escolher $\psi(\mathbf{0})$ para estes cálculos.

$$\begin{aligned} d^2(\psi(x), \psi(\mathbf{0})) &= ||\psi(x) - \psi(\mathbf{0})||^2 \\ &= 4\sum_{i=1}^{m}\left(\frac{||v_i||}{||v_1|| + \cdots + ||v_m||}\right)^2 sen^2\left(\frac{\pi x_i}{||v_i||}\right). \end{aligned} \quad (3.2)$$

4. Limitantes para Códigos de Grupo Comutativo

Consideremos um código em T_δ com M pontos e distância mínima d. Isto equivale a um empacotamento de M chapéus esféricos sobre T_δ de maneira que seus centros distem entre si no mínimo d. Como a área $\frac{n}{2}$-dimensional ocupada por estes chapéus é no máximo a área do próprio toro T_δ, o número de chapéus também é limitado. Vamos apresentar um limitante para M estabelecido em [5], supondo que a distância mínima d é fixa.

Definição 4.1 ([1]- Chapéu esférico)**.** *Um chapéu esférico sobre o toro T_δ centrado em x_0 e de raio $\rho = \dfrac{d}{2}$ é definido por*

$$B^{T_\delta}(x_0, \rho) = \{x \in T_\delta; \langle x_0 - x,\, x_0 - x\rangle^{1/2} \leq \rho\}.$$

Proposição 4.1 ([5])**.** *Todo código de grupo comutativo $G(u) = \{O(u),\, O \in G\}$, $u \in S^{n-1}$ de ordem M em $\mathbb{R}^{2m}$ livre de blocos de reflexão 2×2 com distância mínima d e vetor inicial $u = (u_1, \cdots, u_{2m})$ satisfaz*

$$d \leq 4sen\left(\pi\left(\frac{m^{-1/2}.\Lambda_m^{1/m}}{M^{1/m}}\right)\right),$$

onde Λ_m é a densidade de centro máxima de um reticulado em $\mathbb{R}^m$.

Para M grande, d será pequeno e a imagem inversa do chapéu esférico estará arbitrariamente mais próxima do empacotamento reticulado em $\mathbb{R}^m$ e portanto estarão próximos do limitante estabelecido aqui.

Para fins comparativos, este resultado será de grande importância pois construímos códigos esféricos com o objetivo de obter distâncias mínimas mais próximas do limitante da Proposição 4.1.

5. Construção de Sub-reticulados

Considere o reticulado $\Lambda_\beta = A_2$, com $\beta = \{w_1 = (1,0),\, w_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})\}$, uma base de A_2. Nosso interesse é encontrar um sub-reticulado Λ_α de Λ_β, tal que $\alpha = \{v_1, v_2\}$ seja uma base ortogonal de Λ_β, isto é, $< v_1, v_2 >= 0$.

Teorema 5.1 ([1])**.** *Os sub-reticulados de A_2 que admitem uma base $\alpha = \{v_1, v_2\}$ ortogonal são da forma $\Lambda_\alpha =< v_1, v_2 >$, com*

$$v_1 = l_1 v_1^* \text{ e } v_2 = l_2 v_2^*, \quad l_1,\, l_2 \in \mathbb{Z}^*,$$

onde v_1^* e v_2^* podem ser das formas

i) $v_1^* = aw_1 + bw_2$, *com* $mdc(a,b) = 1$ *e*

$$\begin{cases} v_2^* = -(a+2b)w_1 + (2a+b)w_2, \\ ou \\ v_2^* = -\dfrac{(a+2b)}{3}w_1 + \dfrac{(2a+b)}{3}w_2, \text{ caso } 3|(-(a+2b)) \text{ e } 3|(2a+b). \end{cases}$$

ii) $v_1^* = w_1$ *e* $v_2^* = -w_1 + 2w_2$

iii) $v_1^* = w_2$ *e* $v_2^* = -2w_1 + w_2$

Chamaremos de *geradores primitivos* os vetores v_1^* e v_2^* do teorema acima.

Aqui consideramos os sub-reticulados do tipo (i) do Teorema (5.1), com

$$v_1^* = aw_1 + bw_2 \text{ e } v_2^* = -(a+2b)w_1 + (2a+b)w_2.$$

Estes sub-reticulados apresentam melhor desempenho quando mergulhados nos toros planares de esferas no $\mathbb{R}^4$ quando satisfazem:

1. $||v_1^*|| \approx ||v_2^*||$, **ou seja, a "caixa" que define o toro está mais próxima de ser "quadrada".**

   Os bons tamanhos ocorrerão quando tomarmos $v_1 = l_1 v_1^*$ e $v_2 = l_2 v_2^*$ com $\dfrac{|l_1|}{|l_2|} \approx \sqrt{3} \approx 1,73205$. Ou seja, o sub-reticulado estará mais próximo de ser "quadrado" se satisfizer esta condição.

2. **Maior ângulo mínimo entre os vetores de A_2 e os vetores v_1 e v_2.**

   Considerando que a "caixa" seja "quadrada", temos que devido à simetria no eixo x basta considerar $a > b > 0$ e assim o ângulo entre v_1 e w_1 é menor do que 30^o. A situação ótima ocorre quando $\theta = 15^o$ (maior ângulo mínimo - ângulos iguais entre v_1 e w_1 e entre v_2 e w_2) e isto ocorre quando $\dfrac{a}{b} = 1 + \sqrt{3}$.

Exemplo 5.1. *Considere $a = 273, b = 100$. Logo, $c = -(a + 2b) = -473$ e $d = 2a + b = 646$. Observe que $mdc(a, b) = 1 = mdc(c, d)$. Portanto, estes são geradores primitivos do reticulado Λ_α. Assim temos,*

$$\begin{aligned} v_1^* &= 273w_1 + 100w_2 \\ v_2^* &= -473w_1 + 646w_2, \end{aligned}$$

e $M = |det(A)| = \left| det \begin{pmatrix} 273 & -473 \\ 100 & 646 \end{pmatrix} \right| = 223658$ *pontos.*

Pelo Teorema (2.1)*, $G \simeq \mathbb{Z}_{223658}$ e o elemento $\overline{101w_1 + 37w_2}$ é um elemento de ordem 223658.*

Agora, para este sub-reticulado de A_2 ter um melhor desempenho, procuramos

1. $k = \dfrac{a}{b} \approx 2,73205.$

2. $v_1 = l_1 v_1^*,\ v_2 = l_2 v_2^*$ *com* $\dfrac{|l_1|}{|l_2|} = \sqrt{3} \approx 1,73205.$

Vemos que a primeira condição é satisfeita, pois $\frac{273}{100} \approx 2,73205$. Agora, para a segunda condição tomando, por exemplo, $l_1 = 7$ e $l_2 = 4$, temos que $\dfrac{7}{4} = 1,75 \approx \sqrt{3}$.

Assim, para que o desempenho do sub-reticulado seja bom, vamos considerar

$$\begin{aligned} v_1 &= 7v_1^* \\ v_2 &= 4v_2^*. \end{aligned}$$

Agora, $a = 1911$, $b = 700$, $c = -1892$ e $d = 2584$.

Assim, $M = |det(A)| = 6262424$. Pelo Teorema (2.1)*, $G \cong \mathbb{Z}_{6262424}$ e o elemento $\overline{81w_1 + 299w_2}$ é um elemento de ordem 6262424. Portanto, $\overline{81w_1 + 299w_2}$ gera o grupo G.*

Escrevendo os vetores de norma mínima em relação à base de Λ_α, *temos que*

$$\begin{cases} w_1 = \dfrac{646.v_1 - 175.v_2}{1565606} \\ w_2 = \dfrac{1892.v_1 + 1911.v_2}{6262424} \\ w_3 = \dfrac{-692.v_1 + 2611.v_2}{6262424} \end{cases} .$$

Logo, por (3.2),

$$d_{min} = \min\{0.00190773, 0.00190773, 0.00190773\} = 0.00190773.$$

Calculando o limitante da Proposição (4.1), *obtemos que* $d_{min} \leq 0.00190778$, *uma diferença de apenas* 0.00000005. *Logo, este código está próximo do limitante, para* 6262424 *pontos. Segundo* [2], *seria necessário analisar aproximadamente* 4902242728866 *casos para encontrar o código ótimo.*

Observamos que se tivéssemos calculado a distância mínima sem a exigência do ângulo e da norma obteríamos $d_{min} = 0.00939436$ *e pela Proposição* (4.1) $d_{min} \leq 0.010095$ *para* 223658 *pontos, uma diferença de* 0.000700655.

6. Conclusões

A medida que o número de pontos aumenta, o número de operações envolvidas inviabiliza o cálculo, assim, para um número muito grande de pontos ou em dimensões mais altas, ainda não se sabe qual é o código ótimo.

O método que propomos neste trabalho, permite calcular diretamente um vetor inicial, distância mínima, geradores e grupo para códigos que são ótimos ou estão muito próximos destes, independente de quão grande seja o número de pontos M, sem a necessidade de analisar casos em uma busca exaustiva.

Abstract. Spherical codes generated by commutative group codes of orthogonal matrices in even dimensions, $2m$, can be determined by a quotient of m-dimensional lattices, where the sublattice has an orthogonal basis [4]. We characterize the construction of sub-lattices in these conditions, from the hexagonal lattice, A_2 and compared the minimum distance of spherical code constructed with the limiting of the minimum distance established in [5].

Referências

[1] C. Alves, "Reticulados e Códigos", Tese de Doutorado, IMECC-Unicamp, 2008.

[2] E. Biglieri, M. Elia, Cyclic-group codes for the Gaussian channel, *IEEE Transactions on Information Theory*, **22** (1976), 624-629.

[3] H.C. Cohen, "A Course in Computational Algebraic Number Theory", Springer-Verlag, New York, 1993.

[4] S.I.R. Costa, M. Muniz, E. Augustini, R. Palazzo, Graphs, tessellations and perfect codes on flat tori, *IEEE Transactions on Information Theory*, **50** (2004), 2363–2377.

[5] R.M. Siqueira, S.I.R. Costa, Flat tori, lattices and bounds for commutative group codes, *Designs, Codes and Cryptography*, **49** (2008), 307–321.

[6] D. Slepian, Group codes for the Gaussian channel, *Bell Syst. Tech. Journal*, **47** (1968), 575–602.