

# Construção de códigos esféricos através do reticulado hexagonal

**Carina Alves**

UFU - Faculdade de Matemática

Campus Santa Mônica

38408-100, Uberlândia, MG

E-mail: carina\_matematica@yahoo.com.br

**Sueli I. Rodrigues Costa**

UNICAMP - IMECC- Instituto de Matemática

13083-859, Campinas, SP

E-mail: sueli@ime.unicamp.br

**Antonio Aparecido de Andrade**

UNESP - Ibilce - Departamento de Matemática

15054-000, São José do Rio Preto, SP

E-mail: andrade@ibilce.unesp.br

**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. Neste trabalho, Slepian apresentou a teoria necessária para a construção dos códigos gerados por grupos de matrizes ortogonais que geram pontos sobre a superfície de uma hipersfera, de modo uniforme.

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, isto 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 bastou calcular 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 o objetivo de obter códigos esféricos em que a distância mínima se aproxime do limitante da distância mínima estabelecido em [5].

Pesquisamos 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 comparamos 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, a expressão para o cálculo da distância mínima. Na Seção 4, 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 Preliminares

**Definição 2.1** Um reticulado  $\Lambda_\beta$  é o conjunto de todas as combinações lineares com coeficientes inteiros de um conjunto  $\beta = \{w_1, \dots, w_m\}$  de  $m$  vetores linearmente independentes do espaço vetorial  $\mathbb{R}^m$ ,

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

O conjunto  $\beta$  é denominado uma base de  $\Lambda_\beta$ .

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

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

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

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

Dado um empacotamento no  $\mathbb{R}^n$ , associado ao reticulado  $\Lambda_\beta$ , 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 *distância 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** *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*

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

**Definição 2.4** *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** *Sejam  $\alpha = \{v_1, \dots, v_m\}$  e  $\beta = \{w_1, \dots, w_m\}$  duas bases de  $\mathbb{R}^m$ ,  $\Lambda_\alpha$  e  $\Lambda_\beta$  os reticulados gerados por  $\alpha$  e  $\beta$ , respectivamente, e  $\Lambda_\alpha \subset \Lambda_\beta$ . Se  $A = (a_{ij})$ ,  $a_{i,j} \in \mathbb{Z}$  é a matriz da base  $\alpha$  escrita em relação à base  $\beta$ , 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** *Dizemos que uma matriz  $A$   $n \times n$  esta na forma normal de Smith se  $A$  é uma matriz diagonal com coeficientes inteiros não negativos tal que  $b_{i,i} | b_{i+1,i+1}$  para todo  $i < n$ .*

### 3 Expressão para a distância na imagem por $\psi$

Seja

$$\begin{aligned} \psi &: \mathbb{R}^m \longrightarrow \mathbb{R}^{2m} \\ y &\longmapsto \psi(y) = \left( \delta_1 \cos\left(\frac{y_1}{\delta_1}\right), \delta_1 \operatorname{sen}\left(\frac{y_1}{\delta_1}\right), \dots, \delta_m \cos\left(\frac{y_m}{\delta_m}\right), \delta_m \operatorname{sen}\left(\frac{y_m}{\delta_m}\right) \right), \end{aligned} \quad (1)$$

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

A parametrização  $\psi$  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  $T_{\delta=(\delta_1, \dots, \delta_m)}$  na esfera unitária contida em  $\mathbb{R}^{2m}$  e a aplicação (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

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

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

$$d^2(\psi(x), \psi(\mathbf{0})) = \|\psi(x) - \psi(\mathbf{0})\|^2 = 4 \sum_{i=1}^m \left( \frac{\|v_i\|}{\|v_1\| + \dots + \|v_m\|} \right)^2 \text{sen}^2 \left( \frac{\pi x_i}{\|v_i\|} \right). \quad (3)$$

## 4 Limitantes para códigos de grupo comutativo

Consideremos um código em  $T_\delta$  com  $M$  pontos e distância mínima  $d$ . Isto equivale a um empacotamento de  $M$  chapéus esféricos sobre  $T_\delta$  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  $T_\delta$ , 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** *Um chapéu esférico sobre o toro  $T_\delta$  centrado em  $x_0$  e de raio  $\rho = \frac{d}{2}$  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  $2 \times 2$  com distância mínima  $d$  e vetor inicial  $u = (u_1, \dots, u_{2m})$  satisfaz*

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

onde  $\Lambda_m$  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  $\Lambda_\alpha$  de  $\Lambda_\beta$ , tal que  $\alpha = \{v_1, v_2\}$  seja uma base ortogonal de  $\Lambda_\beta$ , isto é,  $\langle v_1, v_2 \rangle = 0$ .

**Teorema 5.1** [1] *Os sub-reticulados de  $A_2$  que admitem uma base  $\alpha = \{v_1, v_2\}$  ortogonal são da forma  $\Lambda_\alpha = \langle v_1, v_2 \rangle$ , 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  $\text{mdc}(a, b) = 1$  e

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

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.

Neste trabalho, 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  $v_1 = l_1v_1^*$  e  $v_2 = l_2v_2^*$  com  $\frac{|l_1|}{|l_2|} \approx \sqrt{3} \approx 1,73205$ . 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  $30^\circ$ . A situação ótima ocorre quando  $\theta = 15^\circ$  (maior ângulo mínimo - ângulos iguais entre  $v_1$  e  $w_1$  e entre  $v_2$  e  $w_2$ ) e isto ocorre quando  $\frac{a}{b} = 1 + \sqrt{3}$ .

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

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

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

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

2.  $v_1 = l_1v_1^*$ ,  $v_2 = l_2v_2^*$  com  $\frac{|l_1|}{|l_2|} = \sqrt{3} \approx 1,73205$ .

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  $\frac{7}{4} = 1,75 \approx \sqrt{3}$ .

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  $\Lambda_\alpha$ , temos que

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

Logo, por (3),

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

Calculando o limitante da Proposição (4.1), obtemos que a  $d_{min} \leq 0.00190778$ , 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 o limitante  $\leq 0.010095$  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.

## 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.