TEMA Tend. Mat. Apl. Comput., **14**, No. 1 (2013), 13-22.
doi: 10.5540/tema.2013.014.01.0013

Construção e análise de códigos esféricos com boas taxas binárias[1]

L.R.B. NAVES[2], IFRJ - Instituto Federal do Rio de Janeiro, Campus Volta Redonda, 27213-100 Volta Redonda, RJ, Brasil

C. TOREZZAN[3], Faculdade de Ciências Aplicadas, UNICAMP - Universidade Estadual de Campinas, 13484-350 Limeira, SP, Brasil

S.I.R. COSTA[4], Departamento de Matemática, UNICAMP - Universidade Estadual de Campinas 13081-970 Campinas, SP, Brasil

Resumo. Neste trabalho consideramos a distribuição de um conjunto discreto de pontos sobre a superfície de uma esfera euclidiana unitária, com o propósito de construir códigos esféricos para o canal Gaussiano. Apresentamos famílias de códigos esféricos estruturados, que podem ser construídas em tempo linear para dimensões pares e superam, para alguns parâmetros, o limitante inferior de Shannon para a taxa binária de informação.

Palavras-chave. Matemática discreta, Códigos esféricos, taxa binária.

1. Introdução

Um código esférico é um conjunto finito de pontos sobre a esfera unitária do $\mathbb{R}^n$. Vamos denotar por $\mathcal{C}(M, n, \rho)$ um código sobre a esfera unitária $S^{n-1} \subset \mathbb{R}^n$, com M pontos, os quais possuem distância euclidiana mínima ao quadrado igual a ρ.

O problema de alocar pontos sobre a superfície de uma esfera euclidiana tem atraído a atenção de matemáticos, engenheiros e cientistas em geral, devido sua ampla gama de aplicações em diversas áreas [8].

De modo geral, a construção de códigos esféricos envolve a busca por uma configuração de M pontos sobre S^{n-1} que otimiza certos parâmetros de interesse, que podem ser: distância mínima entre pontos, raio de cobertura, kissing number, energia média, coeficiente de quantização, dentre outros. A escolha do parâmetro a ser otimizado vai depender de sua aplicação.

[1] Trabalho apresentado no Congresso de Matemática Aplicada e Computacional - Sudeste - 2011.

[2] ligia.naves@ifrj.edu.br - Bolsista do CNPQ.
[3] cristiano.torezzan@fca.unicamp.br.
[4] sueli@ime.unicamp.br.

Recebido em 21 Outubro 2011; Aceito em 10 Janeiro 2013.

Em telecomunicações, pontos alocados sobre a superfície de uma esfera unitária são utilizados para a comunicação através de um canal Gaussiano e são a generalização natural para a conhecida modulação *phase shift keying (PSK)*, que utiliza os vértices de um polígono regular inscrito na circunferência unitária do $\mathbb{R}^2$.

Para este propósito é desejável maximizar o número de pontos sobre a esfera, além de construir códigos que tenham alguma estrutura adicional que permita lidar com a complexidade de codificação e decodificação. Neste sentido, construções estruturadas são priorizadas em relação à soluções obtidas via métodos de otimização numérica.

O problema de maximizar o número de pontos sobre uma superfície esférica sujeito a estarem afastados de uma distância d é equivalente ao problema de empacotar o maior número de chapéus esféricos com ângulo de abertura central igual a $2arcsen(d/2)$ (Figura 1).

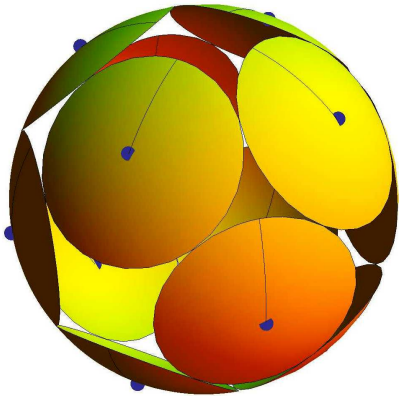

Figura 1: Doze chapéus esféricos relacionados ao código $\mathcal{C}(12, 3, 2 - 2/\sqrt{5})$.

Quando a distancia ρ decresce e/ou a dimensão n aumenta, o número de pontos M pode tornar-se arbitrariamente grande. Quando necessário, a comparação entre códigos esféricos distintos é feita através de medidas que relacionam os parâmetros (M, n, ρ). A densidade de empacotamento do código é uma dessas medidas e expressa a fração da área da superfície esférica que é ocupada pelos chapéus. Outra medida usual é taxa de informação binária (ou taxa de informação), que é definida por:

$$R := \limsup \frac{\log_2(M)}{n}.$$

Como o desafio de encontrar códigos esféricos ótimos é ainda um problema em aberto [8], a descoberta de limitantes para funções que relacionam os parâmetros (M, n, ρ), ou de construções explícitas para os mesmos parâmetros, constituem-se em importantes contribuições para esta área.

Chabauty em 1953 [2] e Shannon em 1959 [7] apresentaram de forma independente um limitante inferior para R como função de ρ dado por:

$$R(\rho) \geq R_{CS}(\rho) := 1 - (1/2)\log_2(\rho(4 - \rho)).$$

Embora este seja o melhor limitante inferior conhecido até o momento para a taxa de informação de códigos esféricos, sua dedução é baseada em argumentos existenciais que não auxiliam na construção efetiva de códigos.

Uma abordagem construtiva foi apresentada em [6], considerando códigos esféricos construídos em tempo polinomial, cuja taxa de informação $R_{pol}(\rho)$ obedece

$$R_{pol}(\rho) \geq 0.5 R_{CS}(\rho).$$

P. Solé e J.C. Belfiore [10], baseados na existência de alguns empacotamentos reticulados, apresentaram a construção de códigos esféricos em tempo polinomial que atingem a taxa $R_L := -0.5\log_2(\rho)$ e mostraram que, para valores de ρ suficientemente pequenos, $R_{CS}(\rho) - R_L(\rho) = O(\rho^2)$.

Neste trabalho apresentamos uma família de códigos esféricos que pode ser construída em tempo linear e tem, para valores de ρ não assintoticamente pequenos, taxa de informação binária acima do limitante inferior de Shannon. A construção utiliza uma folheação da esfera unitária em toros planares baseada em [9].

Este trabalho está dividido da seguinte forma: na seção 2, apresentamos uma rápida revisão sobre a construção de códigos esféricos em camadas de toros, baseados em [8] e [9] ; na seção 3, apresentamos uma maneira de escolher os toros e também de preenchê-los que possibilita a construção em tempo linear; na seção 4, apresentamos um comparativo entre nossa construção e os limitantes mencionados anteriormente.

2. Códigos esféricos em camadas de toros

Dada uma dimensão $k \geq 2$ e $\rho \in (0, 2]$, $\rho = d^2$, seja $\mathcal{C}(k, \rho)$ um código esférico k-dimensional qualquer, com distância mínima ao quadrado maior ou igual a ρ. O código esférico em camadas de toros denotado por $\mathcal{C}_T(2k, \rho)$ é construído em 2 etapas, como segue [9] e [8]:

- Etapa 1- Selecionamos os pontos em $\mathcal{C}(k, \rho)$ que possuem somente coordenadas não negativas. Vamos denotar este subcódigo por $\mathcal{C}(k, \rho)_+$. Cada ponto $c = (c_1, \ldots, c_k) \in \mathcal{C}(k, \rho)_+$ define um toro planar T_c na esfera unitária S^{2k-1}. É interessante que $\mathcal{C}(k, \rho)_+$ tenha boa densidade em S^{k-1} e, se possível, alguma propriedade algébrica ou geométrica. Para este propósito, podemos considerar um $\mathcal{C}_T(k, \rho)$ ou qualquer código esférico k-dimensional conhecido.

- Etapa 2- Para cada toro T_c definido por $\mathcal{C}(k, \rho)_+$, determinamos um conjunto finito de pontos Y_{T_c} com $Y_{T_c} \subset P_c$, para $P_c = \{x \in \mathbb{R}^k : 0 \leq x_i \leq 2\pi c_i\}$, tal que $\|\Phi_c(y) - \Phi_c(x)\| \geq d$, $\forall x, y \in Y_{T_c}$. Onde

  $$\Phi_c(y) = (c_1(cos(\frac{y_1}{c_1}), sen(\frac{y_1}{c_1})), \ldots, c_k(cos(\frac{y_k}{c_k}), sen(\frac{y_k}{c_k}))).$$

  Uma boa opção para Y_{T_c} consiste em considerar pontos de algum reticulado $k-$ dimensional conhecido.

Pode-se demonstrar que, sejam T_b e T_c dois toros planares, para b e c vetores unitários com coordenadas não negativas a distância mínima entre estes toros é

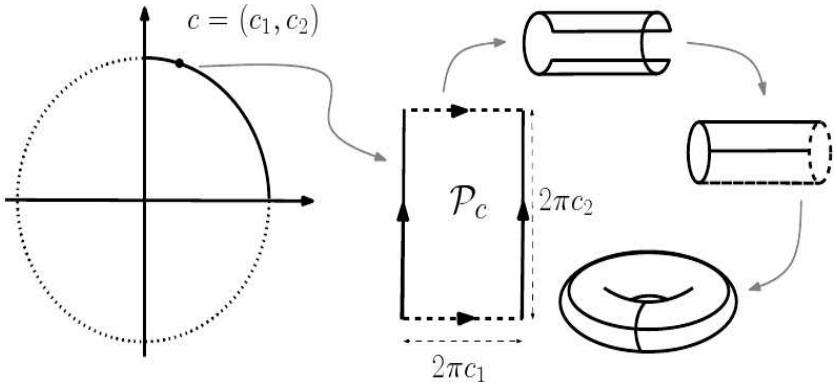

Figura 2: Construção de toro planar em dimensão 4.

dada por [9]:

$$d(T_b, T_c) = \|c - b\| = (\sum_{i=1}^{k}(c_i - b_i)^2)^{1/2}.$$

A distância entre dois pontos no mesmo toro T_c é dada por:

$$d(\Phi_c(u), \Phi_c(v)) = 2(\sum_{i=1}^{k} c_i^2 sen^2(\frac{u_i - v_i}{2c_i}))^{1/2}$$

e é limitada em termos de $\|u - v\|$.

Seja $c = (c_1, c_2, \ldots, c_k)$, $\|c\| = 1$, e sejam $u, v \in P_c$. Seja $d_k = \|u - v\|$ e $d_{2k} = \|\Phi_c(u) - \Phi_c(v)\|$. Então

$$\frac{2}{\pi} d_k \leq \frac{sen\frac{d_k}{2c_\xi}}{\frac{d_k}{2c_\xi}} d_k \leq d_{2k} \leq \frac{sen\frac{d_k}{2}}{\frac{d_k}{2}} d_k \leq d_k$$

onde $\xi = argmin_i(c_i)$ [9].

Existe, portanto, uma deformação na distância quando saímos do $P_c \subset \mathbb{R}^k$ para o $T_c \subset \mathbb{R}^{2k}$.

3. Construção e análise de códigos esféricos

Considerando as duas etapas para a construção de códigos esféricos em camadas de toros explicitadas na seção anterior, analisaremos nessa seção diferentes possibilidades para a escolha do subcódigo na primeira etapa. Manteremos a segunda etapa conforme foi descrita, escolhendo para Y_{T_c} o reticulado D_k reescalado de modo a atingir a distância desejada no código.

As possibilidades de construção analisadas para primeira etapa estão divididas nas subseções a seguir.

3.1. Análise de subcódigo com k elementos

Podemos considerar para a primeira etapa, o subcódigo construído a partir das k permutações do vetor $c_i(t) = \frac{e_i+te}{\|e_i+te\|}$, em que $e = (1, 1, \ldots, 1) \in \mathbb{R}^k$, $t > 0$ e e_i é o i-ésimo vetor canônico do $\mathbb{R}^k$. Cada vetor $c_i(t)$ define um toro planar sobre S^{2k-1}. Podemos estabelecer então o seguinte resultado.

Proposição 3.1. *Para cada ρ, $0 < \rho < 2$, há ao menos k vetores unitários em S^{k-1}, com coordenadas positivas, tais que o quadrado da distância entre dois destes vetores é maior que ρ.*

Demonstração. Pela definição acima, há k vetores $c_i(t) \in \mathbb{R}^k$. A distância ao quadrado entre vetores do tipo $c_i(t)$ supracitado é dada por:

$$\|c_i(t) - c_j(t)\|^2 = \frac{2}{kt^2 + 2t + 1}$$

onde a equação $\frac{2}{kt^2+2t+1} = \rho$ tem sempre uma solução real positiva dada por

$$\bar{t}(\rho) = \frac{-\rho + \sqrt{\rho(k(2-\rho)+\rho)}}{k\rho}$$

. □

Seja c_{min} a menor coordenada de $c_i(\bar{t})$, a imagem da aplicação Φ de qualquer conjunto discreto no interior da caixa $P_{c_i(\bar{t})}$ com distância mínima

$$d_k \geq 2c_{min} arcsen \frac{\sqrt{\rho}}{2c_{min}} \tag{3.1}$$

será um código esférico em S^{2k-1} com distância mínima ao quadrado ρ.

Assim, na segunda etapa de construção, para cada um dos k toros definidos por $c_i(\bar{t})$ consideramos os pontos do reticulado obtido reescalando o reticulado D_k por um fator $\frac{d_k}{\sqrt{2}}$, onde d_k é dado por (3.1).

Como todos os vetores c_i são simétricos por permutações cíclicas de suas coordenadas, é suficiente construir uma camada do código e tomar as permutações cíclicas das coordenadas dos pontos encontrados para obter todo o código.

Como um exemplo desta construção considere $k = 3$ e $\rho = (0, 3)^2$. Neste caso teremos $\bar{t} = 2.34719$ e três toros definidos pelos vetores $c_1(\bar{t}) = (0.710045, 0.497913, 0.497913)$, $c_2(\bar{t}) = (0.497913, 0.710045, 0.497913)$ e $c_3(\bar{t}) = (0.497913, 0.497913, 0.710045)$. Temos $d_k = 0.304734$ e podemos considerar um reticulado reescalado de D_3 pelo fator $d_k/\sqrt{2}$.

As palavras código em cada um dos três toros serão a imagem dos pontos do reticulado $\frac{d_k}{\sqrt{2}} D_3$ na caixa $P_{c_i(\bar{t})}$ pela função Φ_{c_i}. Neste caso, cada toro terá 1605 pontos e teremos $M = 4815$ pontos no código esférico. A taxa de informação deste código é $R = 2.03889$. Para estes parâmetros, os limitantes de Shannon e de Solé & Belfiore são ligeiramente inferiores, 1.75338 e 1.73697, respectivamente.

3.2. Construção de subcódigos com $k!$ elementos

Uma possibilidade de melhorar o número de pontos no subcódigo sem aumentar a complexidade de codificação é tomando as $k!$ permutações do vetor

$$c_i(t) = \frac{p + te}{\|p + te\|},$$

onde $e = (1, 1, \ldots, 1) \in \mathbb{R}^k$, $t > 0$ e p é o vetor $(0, 1, 2, ..., k-1)$ do $\mathbb{R}^k$.

Entretanto, neste caso, a medida que aumenta-se consideravelmente o número de pontos no subcódigo, diminuem-se os valores possíveis a se considerar para distância mínima em dimensões maiores. Por exemplo, para um subcódigo obtido a partir de $c_i(t)$ na dimensão $k = 6$ teremos $k! = 720$ toros mas, para gerar códigos com estes toros, devemos limitar a valores de $\rho < 0.19^2$.

Como um exemplo desta construção, tomemos $k = 3$ e $\rho = (0.3)^2$. Teremos $\bar{t} = 1.59629$, em que $\bar{t}$ é solução positiva da equação

$$\rho = \frac{2}{kt^2 + (k^2 - k)t + \dfrac{k^3}{3} - \dfrac{k^2}{2} + \dfrac{k}{6}}.$$

Os pontos do subcódigo serão as $3! = 6$ permutações do vetor

$$c_i(\bar{t}) = (0.33863, 0.55076, 0.76289).$$

Teremos $d_k = 0.31079$ e novamente na segunda etapa consideraremos na caixa $Pc_i(\bar{t})$ de arestas com medidas $2\pi c_i(\bar{t})$ um reticulado reescalado de D_3 por um fator $\dfrac{d_k}{\sqrt{2}}$.

As palavras código em cada um dos seis toros serão dadas pela imagem de Φ_{c_i} do reticulado $\dfrac{d_k}{\sqrt{2}} D_3$ na caixa $P_{c_i(\bar{t})}$. Cada toro terá 1120 pontos e teremos $M = 6720$ pontos no código esférico. A taxa de informação será $R = 2.11904$, que é superior à taxa obtida no exemplo da subseção anterior para os mesmos valores de ρ e n.

As duas possibilidades analisadas nas subseções anteriores resultam em códigos que podem ser facilmente construídos, além de terem boa taxa de informação binária para alguns parâmetros e terem baixa complexidade de codificação e decodificação. Entretanto é possível ainda aumentar o número máximo de pontos repetindo de forma iterativa a construção anterior baseada na seguinte observação.

É fácil perceber que os vetores c_i obtidos pelo método descrito nas subseções anteriores pertencem, respectivamente, aos hiperplanos

$$x_1 + x_2 + ... + x_k = \frac{1 + kt}{\sqrt{kt^2 + 2t + 1}}$$

e

$$x_1 + x_2 + ... + x_k = \frac{(k-1)k + 2kt}{2\sqrt{kt^2 + (k^2 - k)t + \dfrac{k^3}{3} - \dfrac{k^2}{2} + \dfrac{k}{6}}}.$$

Partindo da ideia de que em qualquer dos dois métodos temos pontos em um único hiperplano, pode haver mais de um hiperplano que, ao interceptar a esfera do $\mathbb{R}^k$, forneça vetores unitários com coordenadas positivas.

Na tentativa de obtermos resultados ainda melhores, propomos uma construção que toma sucessivos hiperplanos paralelos com vetores unitários no $\mathbb{R}^k$ para definir os toros, ao invés de um único hiperplano como foi feito até agora. Isso permite, em geral, aumentar o número de pontos no código para um valor fixado de ρ sem comprometer demasiadamente a complexidade de construção. Essa construção será detalhada na próxima seção.

4. Construção de códigos esféricos por vetores unitários em hiperplanos paralelos

Para realizar essa construção consideraremos, como o primeiro hiperplano Π_1, aquele obtido pelo método descrito na subseção 3.1., em que temos vetores unitários

$$c_i(t) = \frac{e_i + te}{\|e_i + te\|},$$

satisfazendo

$$x_1 + x_2 + ... + x_k = \frac{1 + kt}{\sqrt{kt^2 + 2t + 1}} = \alpha_1.$$

A partir deste hiperplano Π_1, e de acordo com a distância $d = \sqrt{\rho}$ estabelecida é possível obter um novo hiperplano Π_2 paralelo a Π_1 e distante deste o valor x. O valor x é fácil de ser obtido bastando para isso observar que vetores unitários de diferentes hiperplanos devem no mínimo estar distantes o valor d.

Para o caso em que $k = 3$, uma ilustração deste processo é apresentada na figura 3. Cada hiperplano (que neste caso é um plano) corta o primeiro octante em círculos para obter vetores unitários de coordenadas positivas.

A distância x entre os (hiper)planos é obtida por relações trigonométricas simples e pode ser expressa por $x = d \ \ sen(\frac{\theta}{2} + arccos(1 - y))$, em que d é a distância mínima do código e y é a distância entre os pontos $P_0 = \frac{1}{\sqrt{k}}(1, 1, \cdots, 1) \in \mathbb{R}^k$ e $P_i = \frac{\alpha_i}{\sqrt{k}}(1, 1, \cdots, 1) \in \mathbb{R}^k$ (P_i é o ponto do hiperplano Π_i que possui todas as coordenadas iguais e positivas).

Obtido o valor x, o novo plano Π_2 será definido por

$$\Pi_2 : x_1 + x_2 + \ldots + x_k = \alpha_1 - x\sqrt{k}.$$

Neste novo plano tomaremos, sempre que possível, vetores unitários com coordenadas positivas, os quais distem entre si $d = \sqrt{\rho}$. Prosseguimos assim sucessivamente enquanto houverem planos paralelos a Π_i, distantes de Π_i o valor x, que forneçam vetores unitários com coordenadas positivas. Teremos assim mais pontos no subcódigo e, consequentemente, mais toros e um número maior de pontos no $\mathcal{C}_T(2k, \rho)$.

Utilizando este método foram construídos alguns códigos esféricos para diferentes valores de ρ, partindo de vetores no $\mathbb{R}^3$, todos com coordenadas positivas e

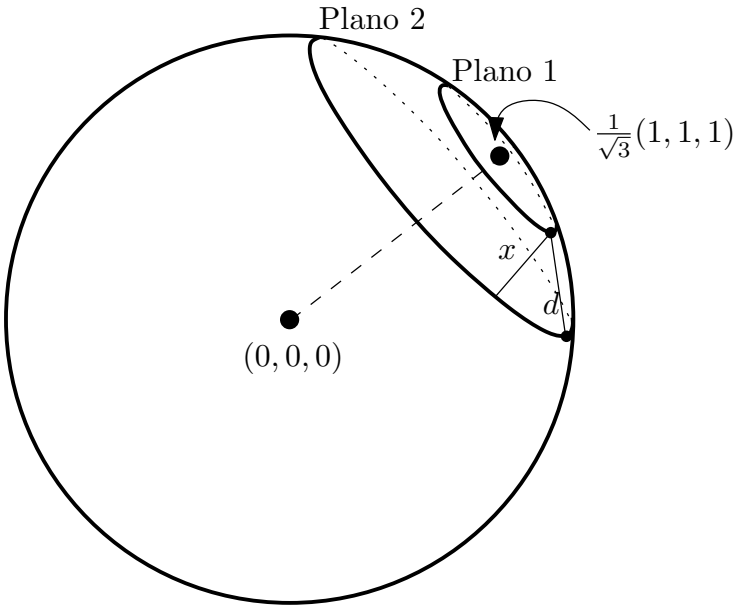

Figura 3: Esfera S^2 interceptada por dois planos. A intersecção são círculos no quadrante positivo.

provenientes de diferentes planos. Cada vetor gerou um toro e depois, cada toro plano tri-dimensional foi preenchido com pontos do reticulado D_3. O resultado foi a obtenção de códigos esféricos no $\mathbb{R}^6$ com boas taxas binária conforme os dados apresentados na tabela 1.

Tabela 1: Comparação entre as taxas binárias de códigos esféricos no $\mathbb{R}^6$ com limitantes inferiores para várias distâncias mínimas.

d	M	Taxa	Shannon	Patric
0.5	194.	1.26665	1.04655	1.
0.4	997.	1.66024	1.35137	1.32193
0.3	7357.	2.14082	1.75338	1.73697
0.2	81095.	2.71789	2.32918	2.32193
0.1	3.50004×10^6	3.62316	3.32373	3.32193
0.01	4.30642×10^{11}	6.44128	6.64387	6.64386

O mesmo método de construção foi usado para se obter códigos $C_T(2k, \rho)$ para $k = 4, 5$ e 6. Na figura 4, apresentamos resultados obtidos para a taxa de informação binária considerando-se diferentes valores de ρ em forma de gráfico. Podemos verificar que vários códigos construídos superam o limitante inferior de Shannon.

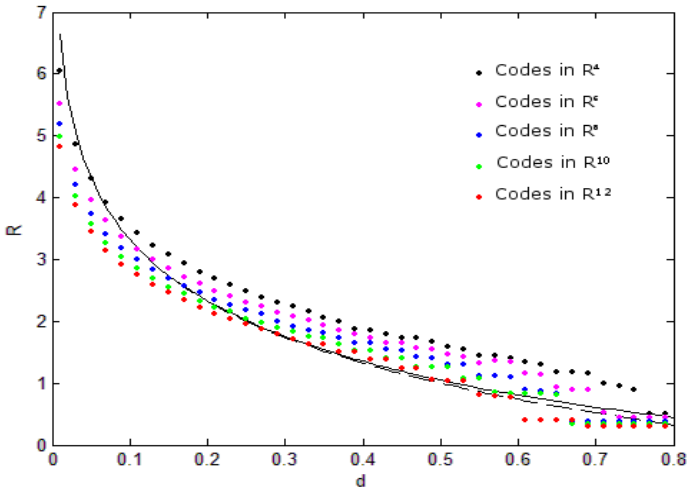

Figura 4: Comparação entre alguns códigos esféricos construídos (pontos isolados) e os limitantes para taxa de informação binária (Shannon: curva contínua. Solé: curva pontilhada) em função de ρ.

5. Conclusão

Neste trabalho consideramos a distribuição de um conjunto de pontos sobre a superfície de uma esfera euclidiana unitária, com o propósito de construir códigos esféricos para o Canal Gaussiano. Apresentamos familias de códigos esféricos estruturados, que podem ser construídos em tempo linear para dimensões pares e superam, em algumas dimensões e para distância mínima não muito pequenas, o limitante inferior de Shannon para a taxa de informação binária. Essa construção é baseada na folheação da esfera unitária por toros planares, proposta em [8] e as contribuições principais deste trabalho referem-se à maneira de obter os toros utilizando vetores de permutação unitários $\mathbb{R}^k$.

Abstract. In this paper we deals with the construction of spherical codes for the Gaussian channel. We present families of structured spherical codes, designed in layers of flat tori, that can be constructed in linear time for even dimensions and improves, for certain parameters, the lower bound for the binary rate given by Shannon.

Keywords. Discrete mathematics, spherical codes, binary rate.

Referências

[1] M. Berger, B. Gostiaux, "Differential Geometry: Manifolds, Curves and Surfaces", Springer-Verlag, Berlin, 1988.

[2] C. Chabauty,"Résultats sur l'empilement de calottes égales sur une périsphère de $\mathbb{R}^n$ et correction à un travail antérieur", C.R. Acad. Sci. Ser. A, **236**, 1953, 1462-1464.

[3] J.H. Conway, N.J.A. Sloane, "Sphere packings, lattices and groups", Springer Verlag, GMW 290, 2003.

[4] S.I.R. Costa, M.M. Alves, E. Agustini, R. Palazzo, "Graphs, tesselations and perfect codes on flat tori", IEEE Transactions on Information Theory, **50**, Oct. 2004, 2363-2377.

[5] T. Ericson, V. Zinoviev, "Codes on Euclidean spheres", North-Holland, Amsterdam, 2001.

[6] G. Lachaud, J. Stern, "Polynomial-time construction of codes. II Spherical codes and the kissing number of spheres", *IEEE Trans. Inform. Theory*, **40**, No.4, 1994, 1140 - 1146.

[7] C.E. Shannon, "Probability of error for optimal codes in a Gaussian channel", Bell Syst. Tech. J., 38, 1959, 611 - 656.

[8] C. Torezzan, "Códigos esféricos em toros planares", Tese de doutorado, IMECC-Unicamp, 2009.

[9] C. Torezzan, S.I.R. Costa, & V.A. Vaishampayan, "Spherical codes on torus layers", International Symposium on Information Theory, Seul, Coreia, 2009.

[10] P. Solé, J.C. Belfiore, "Constructive spherical codes near the Shannon bound", The Seventh International Workshop on Coding and Cryptography, Paris, França, 2011.