# Códigos de grupo comutativo para o canal gaussiano: Aproximando-se do limitante.

Cristiano Torezzan, João E. Strapasson e Sueli I. R. Costa.
*[cristiano, jes, sueli]@ime.unicamp.br*

***Resumo*— Consideramos a construção de códigos de grupo comutativo ótimos para o canal gaussiano. Tabelas para códigos ótimos em $R^4$ e $R^6$ são apresentadas, incluindo alguns exemplos onde códigos de grupo comutativo não cíclico tem melhor performance de distância mínima do que os gerados por grupos cíclicos de mesma ordem. Os resultados mostram que quando a número de pontos cresce, a distância mínima desses códigos aproxima-se assintoticamente do limitante superior específico.**

***Palavras-Chave*— Códigos de grupo comutativo ótimos, códigos esféricos, limitante para distâncias mínimas.**

***Abstract*— The construction of optimal commutative group codes for the gaussian channel is considered. Table for codes in $R^4$ e $R^6$ are presented, including some examples where non-cyclic codes have better performance than cyclic ones. The results show when the cardinality increase, the specific upper bound for commutative group codes can be arbitrarily aproached.**

***Keywords*— Commutative group codes, spherical codes, bound for minimum distance.**

## I. 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 e em boas taxas de $Eb/No$ na transmissão de sinais através de um canal Gaussiano [3], [4] e [5].

Nesse sentido, a utilização de códigos geometricamente uniformes [2] e, em particular, códigos de grupo comutativo merecem destaque. Para esses códigos, a análise da distância mínima desempenha papel fundamental, visto que sua estrutura algébrica garante as características de simetria desejadas.

Apresentamos aqui alguns resultados de nossa pesquisa que, baseados em [6] exploram a relação entre códigos de grupo comutativo em dimensões pares e reticulados na dimensão metade, para obter um procedimento que determina o melhor código de grupo comutativo para qualquer cardinalidade $M$ e dimensão $n$. Descrevemos aspectos gerais da técnica e apresentamos tabelas com códigos de grupo comutativo ótimos em $R^4$ e $R^6$ destacando a aproximação, quando $M$ cresce, ao limitante superior para distância mínima específico para esses códigos.

Um código de grupo comutativo $\mathcal{C}(M,n)$ é um conjunto $\mathcal{C}=\{x_i\}_{i=1}^{M}$ de vetores unitários, que geram o espaço $R^n$, e é órbita do vetor inicial $x_0$, da esfera unitária $S^{n-1}\subset R^n$, sob a ação do grupo comutativo $G$, de ordem $M$, de matrizes ortogonais, $G=\{G_i\}_{i=1}^{M}$

$$\mathcal{C}=\{G_1x_0, G_2x_0, ..., G_Mx_0\}$$

A distância mínima no código $\mathcal{C}$ é definida por:

$$d_{min}=\min_{x,y\in\mathcal{C}}||x-y||$$

Onde $||x||$, denota a norma euclidiana de $x$.

Um problema fundamental em códigos de grupo, conhecido como *problema do vetor inicial*, abordado por D. Slepian já em seu trabalho pioneiro [7], consiste em determinar o vetor $x_0$, da esfera unitária do $\mathbb{R}^n$, que maximiza a distância mínima entre dois pontos quaisquer do código.

O problema do vetor inicial foi estudado para códigos de grupo cíclico em [1], onde os autores mostram sua equivalência a um problema de programação linear (PL) cujas restrições dependem do grupo de matrizes que gera o código.

Em [9], mostramos que para códigos de grupo comutativo temos um problema de *mini-max* de funções lineares que pode ser transformado em um PL, equivalente ao obtido em [1] para códigos de grupo cíclico.

Um problema mais geral que o problema do vetor inicial é, fixado o número de pontos $M$ e a dimensão $n$, determinar qual é o código de grupo com esses parâmetros que apresenta maior distância mínima (código ótimo).

Dois esforços são fundamentais na obtenção de códigos ótimos. Um é a determinação de limitantes para a distância mínima em função dos parâmetros $M$ e $n$. Outro é a construção de códigos que tenham distâncias mínimas melhores que as conhecidas ou que atinjam o limitante.

Em [6] é estabelecido um limitante específico para distância mínima em códigos de grupo comutativos:

**Limitante do Toro:** Todo código de grupo comutativo em $R^{2k}$ de ordem $M$ com distância mínima $\rho$ e vetor inicial $(u_1,u_2,\ldots,u_{2k})$ satisfaz

$$M\leq\frac{\pi^k\sqrt{\Pi_{i=1}^{k}(u_{2i-1}^2+u_{2i}^2)}\Lambda_k}{(\arcsin\frac{\rho}{4})^k}\leq\frac{\pi^k\Lambda_k}{(\arcsin\frac{\rho}{4})^k k^{k/2}},$$

onde $\Lambda_k$ é a máxima densidade de centro de um empacotamento esférico em $R^k$.

Além deste limitante, outros resultados sobre códigos de grupo comutativo apresentados em [6] são fundamentais na realização do trabalho que desenvolvemos visando a determinação de códigos de grupo comutativo ótimos. Dentre estes destacamos que todo código de grupo comutativo é equivalente ao código

Este trabalho tem o financiamento da FAPESP, através dos processos: 05/58102-7, 07/00514-3 e 02/07473-7 e também do CNPq: 304573/2002

$$\mathcal{C} = \{(R_1(i)\begin{pmatrix} u_1 \\ u_2 \end{pmatrix}, \ldots, R_q(i)\begin{pmatrix} u_{2q-1} \\ u_{2q} \end{pmatrix}, \pm u_{2q+1}, \ldots, \pm u_n)\}_{i=1}^{M},$$

Onde:

$$R_j(i) = \begin{pmatrix} \cos(\frac{2\pi b_{ij}}{M}) & -\sin(\frac{2\pi b_{ij}}{M}) \\ \sin(\frac{2\pi b_{ij}}{M}) & \cos(\frac{2\pi b_{ij}}{M}) \end{pmatrix}, b_{ij} \in Z.$$

Além disso, para $n = 2k$, se o grupo é composto por matrizes livres de blocos de reflexão $(q = k)$ então existe um quociente de reticulados em dimensão $k$ associado ao código.

Nesse trabalho nossa abordagem vai na direção do segundo esforço (supra-citado). Estamos interessados aqui na obtenção de códigos de grupo comutativo que se aproximem da distância limite. Essa abordagem é fundamentalmente distinta da apresentada em [6]. Naquele trabalho estudou-se aspectos gerais relacionados ao comportamento de tais códigos, enquanto nesse, apresentamos de maneira explicita quais são e como são construídos os melhores códigos de grupo comutativo para várias cardinalidades e dimensões 4 e 6.

## II. Determinando códigos de grupo comutativo ótimos

A obtenção de um código de grupo comutativo ótimo com $M$ pontos em $\mathbb{R}^n$ pode ser dividida em duas etapas. A primeira consiste em determinar os sub-grupos comutativos $G$, de ordem $M$, no grupo das matrizes ortogonais $n \times n$. A segunda consiste em resolver o problema do vetor inicial para cada um dos sub-grupos encontrados na primeira etapa. O código ótimo será o que obtiver maior distância mínima entre todos os testados.

O problema é que podem existir um número arbitrariamente grande de sub-grupos (representações matriciais para o grupo comutativo finito de ordem $M$) de matrizes ortogonais $n \times n$. Este número depende da dimensão $n$ e do número de divisores (número de Euler) de $M$.

*Exemplo:*

Para $n = 4$ e $M = 128$, podemos ter vários grupos comutativos: $\{\mathbb{Z}_{128}; \mathbb{Z}_2 \times \mathbb{Z}_{64}; \mathbb{Z}_4 \times \mathbb{Z}_{32}; \mathbb{Z}_8 \times \mathbb{Z}_{16}\}$.

Para cada grupo listado acima, devemos considerar todas as possíveis representações como grupo de matrizes ortogonais de ordem $128$ e resolver o problema do vetor inicial correspondente. Observamos que diferentes representações para o mesmo grupo podem resultar em códigos esféricos distintos (não isométricos) mesmo considerando o melhor vetor inicial para cada caso.

Para ilustrar, o grupo cíclico $\mathbb{Z}_{128}$ pode representado, no conjunto das matrizes ortogonais reais de ordem $4 \times 4$, por qualquer grupo finito de matrizes gerado pela matriz diagonal por blocos $2 \times 2$

$$G_{(a,b)} = diag\left(R\left(\frac{a*2\pi}{128}\right), R\left(\frac{b*2\pi}{128}\right)\right)$$

com $a$ e $b$ são inteiros positivos menores que $128$ com $\gcd(a, b) = 1$ e $R(\alpha)$ é a matriz de rotação no plano:

$$R(\alpha) = \begin{pmatrix} Cos(\alpha) & -Sen(\alpha) \\ Sen(\alpha) & Cos(\alpha) \end{pmatrix}$$

Se considerarmos todas as representações possíveis de grupos comutativos de ordem $128$, teremos um total de $20.092$ (Tabela I). Isto ilustra que o tempo computacional de busca pode se tornar intolerável mesmo para dimensões baixas e pequenos valores de $M$.

### A. Códigos de grupo comutativo em dimensões pares

Com base na relação entre códigos de grupo comutativo em dimensões pares, reticulados e toros planares apresentada em [6] conseguimos caracterizar o conjunto de casos relevantes e reduzir significativamente o número de grupos de matrizes a serem testados, classificando o conjunto de geradores dos reticulados associados.

O procedimento adotado parte do fato fundamental que os códigos de grupo em dimensão $n = 2k$ considerados estão associados a quocientes de reticulados em dimensão $k$. Aperfeiçoando as idéias apresentadas em [8] pudemos provar que, para análise dos códigos esféricos realmente distintos (não isométricos) é suficiente considerar as matrizes geradoras dos reticulados na forma normal de Hermite.

Essa idéia tornou viável a implementação de um algoritmo que resolve o problema do vetor inicial para cada grupo de matrizes associado a um reticulado gerado por uma dessas formas.

A Tabela I apresenta uma comparação entre o número de casos e tempo gasto na procura de do melhor código de grupo comutativo em $\mathbb{R}^4$ com $M$ pontos antes e depois da seleção dos grupos relevantes.

TABELA I

Tempo gasto na procura do melhor código de grupo comutativo em $\mathbb{R}^4$, antes e depois da classificação dos grupos relevantes.

| $M$ | Nº antes | T antes | Nº rel. | T rel. |
|---|---|---|---|---|
| 32 | 975 | 10 minutos | 18 | 0.02s |
| 128 | 20.092 | 4 horas | 67 | 0.06s |
| 1024 | 1.825.158 | 5 dias | 516 | 0.42s |

Utilizando essa redução, foi possível a obtenção de códigos de grupo ótimos para diversas cardinalidades $M$ em várias dimensões. Nas Tabelas II e III apresentamos alguns desses códigos em $R^4$ e $R^6$, respectivamente.

Cada linha da Tabela II apresenta o melhor código de grupo comutativo para $M$ pontos, o qual tem distância mínima igual a $d_{min}$. Quando o grupo de matrizes é cíclico o gerador é a matriz

$$G_{(a,b)} = diag\left(R\left(\frac{a*2\pi}{M}\right), R\left(\frac{b*2\pi}{M}\right)\right)$$

com $(a, b)$ dados na coluna `Gen.` $(a, b)$. Quando o grupo é não-cíclico temos duas matrizes geradoras para o grupo, cada uma determinada por um dos pares $(a, b)$ apresentados na tabela. O vetor inicial ótimo, determinado através da resolução de um PL, tem coordenadas $(\delta_1, 0, \delta_2, 0)$. A última coluna apresenta o limitante para a distância mínima em códigos de grupo comutativo com $M$ pontos.

É possível observar que quando $M$ cresce a distância mínima dos códigos encontrados tende assintoticamente para

TABELA II

MELHORES CÓDIGOS DE GRUPO COMUTATIVO EM $R^4$ COM $M$ PONTOS.

| $M$ | $d_{min}$ | $\delta_1$ | $\delta_2$ | Grupo | Ger. $(a,b)$ | Lim |
|---|---|---|---|---|---|---|
| 10 | 1.224 | 0.707 | 0.707 | $\mathbb{Z}_{10}$ | (1 3) | 1.474 |
| 20 | 0.959 | 0.678 | 0.734 | $\mathbb{Z}_{20}$ | (3 4) | 1.054 |
| 30 | 0.831 | 0.707 | 0.707 | $\mathbb{Z}_{30}$ | (3,5) | 0.864 |
| 40 | 0.714 | 0.607 | 0.794 | $\mathbb{Z}_{40}$ | (4 5) | 0.750 |
| 50 | 0.628 | 0.707 | 0.706 | $\mathbb{Z}_{50}$ | (7 2) | 0.672 |
| 100 | 0.468 | 0.757 | 0.653 | $\mathbb{Z}_5 \otimes \mathbb{Z}_{20}$ | (0 20), (5 10) | 0.476 |
| 200 | 0.330 | 0.750 | 0.660 | $\mathbb{Z}_{200}$ | (93 1) | 0.337 |
| 300 | 0.273 | 0.656 | 0.754 | $\mathbb{Z}_5 \otimes \mathbb{Z}_{60}$ | (60 120), (10 15) | 0.275 |
| 400 | 0.237 | 0.686 | 0.727 | $\mathbb{Z}_{400}$ | (189 1) | 0.238 |
| 500 | 0.211 | 0.674 | 0.738 | $\mathbb{Z}_{500}$ | (13 20) | 0.213 |
| 600 | 0.193 | 0.676 | 0.736 | $\mathbb{Z}_{600}$ | (191 198) | 0.194 |
| 700 | 0.180 | 0.718 | 0.695 | $\mathbb{Z}_{700}$ | (14 25) | 0.180 |
| 800 | 0.168 | 0.670 | 0.742 | $\mathbb{Z}_{800}$ | (16 25) | 0.168 |
| 900 | 0.158 | 0.704 | 0.709 | $\mathbb{Z}_{900}$ | (197 2) | 0.159 |
| 1000 | 0.149 | 0.716 | 0.697 | $\mathbb{Z}_{1000}$ | (33 4) | 0.150 |

o limitante específico para esses códigos. A Figura 1 ilustra esse fato para códigos em $R^4$.

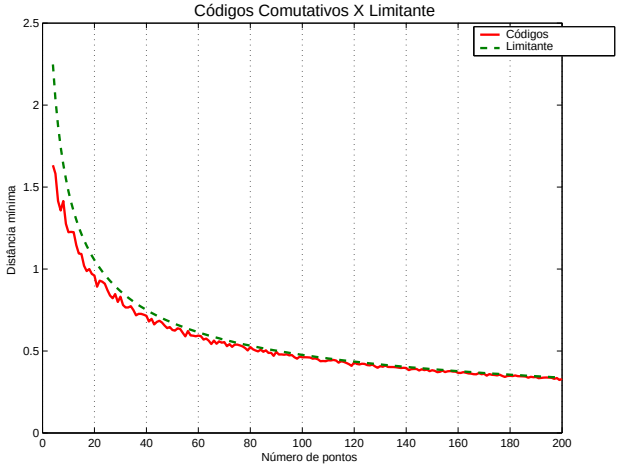


Fig. 1. Comparação entre distância mínima dos melhores códigos de grupo comutativo em $R^4$ e o limitante para esta distância

Outro fato a ser destacado é que em alguns casos o melhor código de grupo comutativo está associado a um grupo não cíclico, como por exemplo para $M = 100$ pontos em $\mathbb{R}^4$ e $M = 40$ ou $M = 900$ pontos em $\mathbb{R}^6$. No entanto, os testes numéricos realizados até agora mostram que esses casos representam menos de 20% do total e, além disso, a distância limite é atingida assintoticamente mesmo considerando apenas códigos de grupo cíclico.

### *B. Códigos de grupo comutativo em dimensões ímpares*

A procura pelos melhores códigos de grupo comutativo em dimensões ímpares $(n = 2k + 1)$ pode ser reduzida a busca pelos melhores códigos na dimensão par imediatamente anterior $(n = 2k)$. A prova dessa afirmação [6] baseia-se no fato de que, o melhor código em dimensão $(n = 2k+1)$, com $M$ pontos pode ser visto como duas cópias do melhor código na dimensão $n = 2k$, com $\frac{M}{2}$, dispostas na esfera do $R^{2k+1}$ na forma de um anti-prisma, conforme ilustra a Figura 2 para $M = 8$ pontos em dimensão 3.

O ajuste da distância entre os hiper-planos que contém as "cópias "do melhor código da dimensão anterior e a "rotação "de uma "cópia "em relação a outra levam a um outro problema de otimização.

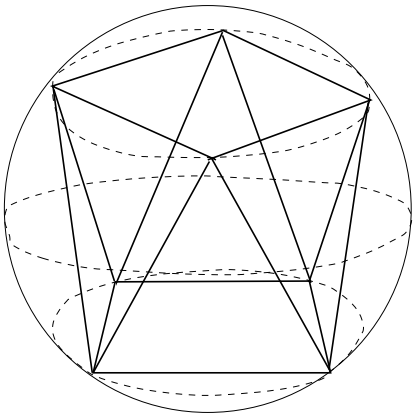

Fig. 2. Ilustração do melhor código de grupo comutativo em $R^3$, com $M = 8$ pontos, visto como duas cópias do melhor código de grupo comutativo com $M = 4$ pontos em $R^2$, dispostas na forma de um anti-prisma.

## III. CONCLUSÕES

A obtenção de códigos de grupo comutativo ótimos pode ser feita de forma eficiente selecionando o conjunto de casos relevantes a serem testados. A associação desses códigos a quocientes de reticulados e a caracterização de que, a menos de isometria, basta considerar matrizes geradoras num formato especial (forma normal de hermite) possibilitou uma redução que tornou viável a determinação de códigos ótimos para um grande número de pontos. Esse método foi implementado num algoritmo computacional que, em cada iteração, resolve um problema de programação linear para encontrar o vetor inicial ótimo associado a cada grupo finito de matrizes ortogonais do conjunto de casos relevantes. Tabelas com códigos ótimos em $R^4$ e $R^6$ foram apresentadas, mostrando que a distância mínima para esses códigos atinge assintoticamente o limitante superior específico quando o número de pontos cresce. Em alguns casos códigos de grupo comutativo não cíclico apresentam distância mínima melhor que os códigos de grupo cíclico de mesma cardinalidade, no entanto, a distância limite é atingida assintoticamente mesmo considerando apenas os códigos de grupo cíclico.

## REFERÊNCIAS

[1] E. Biglieri and M. Elia, "Cyclic-Group Codes for the Gaussian Channel", IEEE Transaction on Information Theory, IT-22, pp 624–629, 1976.
[2] G.D. Forney. Geometrically uniform codes. IEEE Trans. Inform. Theory, vol 37, No. 6, pp. 1241-1259, September 1991.
[3] I. Ingemarsson, "Group Codes for the Gaussian Channel", Lecture Notes in Control and Information Sciences, vol 128, Springer Verlag, pp 73-108,1989.
[4] H. Loeliger "Signals Sets Matched to Groups", IEEE Transaction on Information Theory, vol 37, pp 1675-1682, 1991.
[5] Pellenz, M. E. ; Portugheis, J., " New commutative group codes". Proceedings of ISIT - IEEE International Symposium on Information Theory,Ulm., 1997.
[6] R. M. Siqueira and S. I. R. Costa. Flat Tori, Lattices and Bounds for Commutative Group Codes. *( Aceito para publicação). Designs, Codes and Cryptography, 2008.*.
[7] D. Slepian,"Group codes for the Gaussian Channel", The Bell System Technical Journal, vol 47, pp. 575-602, 1968.
[8] C. Torezzan, R. M. Siqueira, S. I. R. Costa, J. E. Strapasson, "Determinando os melhores códigos esféricos associados a grupos comutativos´´, Proceedings of CNMAC 2007.

TABELA III

MELHORES CÓDIGOS DE GRUPO COMUTATIVO EM $R^6$ COM $M$ PONTOS.

| $M$ | $d_{min}$ | $\delta_1$ | $\delta_2$ | $\delta_3$ | Grupo | Gen (a,b,c) | Limitante |
|---|---|---|---|---|---|---|---|
| 10 | 1.414 | 0.632 | 0.632 | 0.447 | $\mathbb{Z}_{10}$ | (3,1,5) | 1.820 |
| 20 | 1.240 | 0.554 | 0.620 | 0.554 | $\mathbb{Z}_{20}$ | (2,5,6) | 1.465 |
| 30 | 1.133 | 0.534 | 0.654 | 0.534 | $\mathbb{Z}_{30}$ | (3,5, 9) | 1.287 |
| 40 | 1.044 | 0.603 | 0.522 | 0.603 | $\mathbb{Z}_2 \otimes \mathbb{Z}_{20}$ | (20,0,20), (32,10,4) | 1.173 |
| 50 | 0.976 | 0.604 | 0.506 | 0.615 | $\mathbb{Z}_{50}$ | (7,6, 34) | 1.091 |
| 100 | 0.804 | 0.515 | 0.684 | 0.515 | $\mathbb{Z}_{10} \otimes \mathbb{Z}_{10}$ | (50, 10, 0), (30, 0, 10) | 0.870 |
| 200 | 0.673 | 0.555 | 0.619 | 0.555 | $\mathbb{Z}_{200}$ | (28, 25, 4) | 0.692 |
| 300 | 0.585 | 0.585 | 0.498 | 0.639 | $\mathbb{Z}_5 \otimes Z_{60}$ | (0, 0, 60), (25, 30, 30) | 0.605 |
| 400 | 0.540 | 0.562 | 0.605 | 0.562 | $Z_{20} \otimes Z_{20}$ | (300, 40, 0), (60, 0, 20) | 0.550 |
| 500 | 0.504 | 0.577 | 0.577 | 0.577 | $Z_5 \otimes Z_{10}, \otimes Z10$ | (100, 0, 0), (50, 50, 0), (50, 0, 50) | 0.511 |
| 600 | 0.472 | 0.549 | 0.630 | 0.549 | $Z_2 \otimes Z_{300}$ | (300, 0, 300), (384, 50, 12) | 0.481 |
| 700 | 0.445 | 0.531 | 0.612 | 0.585 | $Z_{700}$ | (457, 664, 298) | 0.457 |
| 800 | 0.427 | 0.617 | 0.486 | 0.617 | $\mathbb{Z}_{20} \otimes \mathbb{Z}_{40}$ | (80,0,40),(20,80,60) | 0.437 |
| 900 | 0.413 | 0.592 | 0.591 | 0.547 | $\mathbb{Z}_3 \otimes Z_{300}$ | (0,300,0),(759,36,3) | 0.420 |
| 1000 | 0.397 | 0.560 | 0.632 | 0.535 | $\mathbb{Z}_{1000}$ | (319,694,45) | 0.406 |

[9] C. Torezzan, S. I. R. Costa, R. M. Siqueira and J. Strapasson, "Searching for Optimal Commutative Group Codes", Forthcoming paper