Códigos Esféricos com Simetrias Cíclicas

Tese de Doutorado

Instituto de Matemática, Estatística e Computação Científica

IMECC, UNICAMP

Maio, 2006

Autor: Rogério Monteiro de Siqueira

Orientadora: Profa. Dra Sueli Irene Rodrigues Costa

Códigos Esféricos com Simetrias Cíclicas

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por Rogério Monteiro de Siqueira e aprovada pela comissão julgadora.

Campinas, 18 de Maio de 2006

.....

Profa. Dra Sueli Irene Rodrigues Costa

Orientador

Banca Examinadora

1. Profa. Dra. Sueli Irene Rodrigues Costa
2. Prof. Dr. Cecílio José Lins Pimentel
3. Prof Dr. Marcelo Muniz Silva Alves
4. Profa. Dra. Maria Aparecida Soares Ruas
5. Prof. Dr. Reginaldo Palazzo Junior

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de Doutor em Matemática.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Júlia Milani Rodrigues – CRB8a / 2116

Siqueira, Rogério Monteiro de
Si75c Códigos esféricos com simetrias cíclicas / Rogério Monteiro de Siqueira -- Campinas, [S.P. :s.n.], 2006.

Orientador : Sueli Irene Rodrigues Costa
Tese (doutorado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Geometria discreta. 2. Empacotamento de esferas. 3. Grupos de simetria. 4. Espaços de curvatura constante. I. Costa, Sueli Irene Rodrigues. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

(mjmr/imecc)

Título em inglês: Spherical codes with cyclic symmetries.

Palavras-chave em inglês (Keywords): 1. Discrete geometry. 2. Sphere packings. 3. Symmetry groups. 4. Spaces of constant curvature.

Área de concentração: Matemática

Titulação: Doutor em Matemática

Banca examinadora: Profa. Dra. Sueli Irene Rodrigues Costa (IMECC/UNICAMP)
Profa. Dra. Maria Aparecida Soares Ruas (ICMC/USP)
Prof. Dr. Cecílio Jose Lins Pimentel (UFPE)
Prof. Dr. Marcelo Muniz Silva Alves (UFPR)
Prof. Dr. Reginaldo Palazzo Junior (FEEC/UNICAMP)

Data da defesa: 18/05/2006

Programa de Pós-Graduação: Doutorado em Matemática

Tese de Doutorado defendida em 18 de maio de 2006e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof. (a). Dr (a). SUELI IRENE RODRIGUES COSTA

Prof. (a). Dr (a). MARIA APARECIDA SOARES RUAS

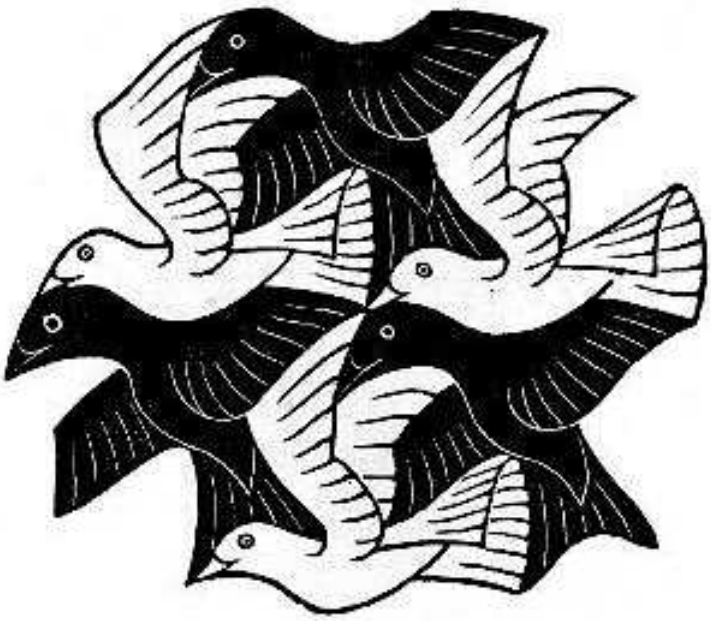
Prof. (a). Dr (a). REGINALDO PALAZZO JÚNIOR

Prof. (a). Dr (a). MARCELO MUNIZ SILVA ALVES

Prof. (a) Dr. (a) CECÍLIO JOSÉ LINS PIMENTEL

Foram girassóis que eu plantei.
Nasceram constelações de brilhantes
nos botões.
Escrevi fórmulas e teoremas,
mas eram bordados de
marias-fumaças, montanhas
verde-oliva e suaves trilhos.
Crianças eram locomotivas
desgovernadas
no céu, como sinais, cometas.

Sei que não planejei nada disso,
minhas mãos são cegas,
minhas lágrimas não sabem.
Eu gritei "aba"e meu sono
seguiu ritmado por tambores.



Agradecimentos

Muitos dos meus amigos não vão entender a matemática que eu estudei, quem trabalha com pesquisa em matemática não pode pretender ser universal. Descobri esta frustração no mestrado. Mas muita gente me entende com aquela acuidade de perceber nos olhos o que eu sinto, quero elencar essas pessoas, além daquelas que viram de perto meu trabalho crescer. Estou elegendo um critério e uma maneira emocional para agradecer, coisa pouco comum na academia, mas não me importo em ficar à margem.

Quando eu entrei no doutorado, queria ser só professor. A pesquisa ia ser um passo para isso. De alguma maneira a Sueli me ajudou a redescobrir o gosto pela pesquisa que eu tenho desde muito cedo. Ela soube dar espaço para essa minha curiosidade, quase selvagem, que eu tenho pela vida. Eu me senti livre para escolher o que estudar, como estudar, no tempo que eu quisesse. Para seres avessos a grade como eu, isto foi um achado. Preciso agradecer também o estímulo constante nos assuntos que eu ia escolhendo e dissertando da maneira mais confusa e peculiar, coisa que a gente faz quando está descobrindo algo. Ela ouvia, às vezes não entendia, mas não raro comentava : "Estou contente que você está progredindo, estas coisas são super interessantes". Eu agradeço a esta força de mulher, eu cresci um bocado por conta disso.

Ao Jaime, devo a pergunta inicial. Aquela que me fez interessar por códigos ótimos, que me levou a estudar limitantes e boa parte das coisas que escrevi aqui.

Agradeço à Cidinha e à Tânia, pelos abacaxis burocráticos que elas descascaram pra mim, e ao povo da biblioteca que procurou revistas, artigos em outras bibliotecas, livros e referências, muito úteis para o meu trabalho.

Tive uns companheiros de viagem imprescindíveis. Com eles eu almocei, tomei café, falei mal dos professores, reclamei que a pesquisa não andava, ri aos borbotões sobre as trapalhadas alheias, ouvi muita piada: João, Andréia e Tatiana são os de trabalho que eu nunca mais

vou esquecer. Devo a eles boas risadas nos momentos de deserto criativo; dos de casa, Gustavo, Lonardo, Tâmara, Daniela, Cadu, Tiago, Marcelle, Marcelo e Verô, não há o que falar. Aguentar o meu eventual mau humor matinal, as minhas cantorias no banheiro, os meus gostos estranhos, faz de vocês gente do meu coração; as cumadres de junho e terças, Carol, Lívia, Débora, Ana e Raquel, obrigado pela torcida e tudo o mais. Vocês são "as" mujeres; aos de longe, de São Carlos e de São Paulo, amigos de conversas longas à beira da mesa, valeu por me refugiar em suas "casas".

Meus pais e minhas irmãs, apesar de sempre encrencar com vocês, quero que saibam que a minha esperança em vocês é enorme, é coisa de quem ama sem explicar. De vocês vem a minha força e a minha paciência.

À Fapesp, agradeço o apoio financeiro desde os tempo de graduação. São simplesmente sete anos financiando a minha pesquisa.

Após defesa, dispontam outros que contribuem muito. Preciso agradecer ao Cristiano pelas ajudas com a "papelada". Também aos membros da banca que sugeriram melhorias ao texto e coletaram os pequenos detalhes que escaparam nas minhas leituras viciadas.

A todos os seres esquecidos, aquelas pessoas que eu conversei aqui e acolá, que jogaram luz nos meus olhos, o meu muito obrigado. Foi muito bom chegar até aqui por conta, em grande parte, da generosidade e felicidade com que fui recebido por todos.

Resumo

Códigos esféricos euclidianos com simetrias são órbitas finitas de grupos de matrizes ortogonais. Tais códigos são também conhecidos como códigos de grupo. Neste trabalho, os códigos de grupo comutativo em dimensão par são caracterizados sobre toros planos, subvariedades da esfera. Em particular, se o grupo de matrizes for cíclico, o código gerado está contido em um nó que se enrola em um toro. Se a dimensão for ímpar, todo código de grupo comutativo mora em anti-primas cujas bases estão contidas em dois toros planos. Tal caracterização permitiu a construção de limitantes para a cardinalidade destas constelações de pontos em termos da distância mínima destes códigos e da densidade de empacotamento de um reticulado associado. Utilizando o método de Biglieri e Elia, que procura o vetor inicial cujo respectivo código de grupo cíclico tem a melhor distância mínima, apresentamos também os melhores códigos de grupo cíclico em dimensão quatro até 100 pontos.

Abstract

Euclidean spherical codes with symmetries are orbits of finite orthogonal matrix groups. These codes are also known as group codes. In this work, the commutative group codes in even dimensions are viewed on flat tori, which are submanifolds of the sphere. Also, if the matrix group is cyclic, the generated code lies on a knot which wraps around a torus. If the dimension is odd, every commutative group code lies on an anti-prism whose bases are contained in two flat tori. This interpretation lead us to build upper bounds for the cardinality of these constelations involving their minimum distance and the packing density of an associated lattice. Using a method by Biglieri and Elia, which searchs the initial vector for a cyclic group in order to achieve the best minimum distance, we also present the best cyclic group codes in dimension four up to 100 points.

Sumário

Lista de Figuras

Lista de Tabelas

Introdução

Um *código esférico* é um subconjunto discreto de uma esfera em um espaço com uma métrica. A razão para um código esférico ser também chamado de constelação de sinais é que todo conjunto de sinais contínuos pode ser representado por um conjunto de pontos na esfera euclidiana. Esta maneira geométrica de ver os sinais possibilitou um avanço importante no manuseio desses conjuntos. Um dos principais ingredientes para que a transmissão de um sinal ocorra com baixa probabilidade de erro é que a distância mínima entre os pontos seja grande. Por isso a análise de desempenho de uma constelação de sinais passa em boa parte dos casos pelo cálculo de sua distância mínima.

De maneira geral, dada uma dimensão n e um número de pontos M, queremos saber qual o código esférico $[M, n]$ com a maior distância mínima. Este código é chamado *ótimo* . Achar um código ótimo é um problema bastante difícil. Na esfera euclidiana $S^2 \subset \mathbb{R}^3$, este problema é conhecido como o problema de Tammes. Segundo Sloane [41], Tammes foi um botânico alemão que estudou o número de poros em um grão de pólen. Seu trabalho de 1930, publicado em uma revista de botânica [44] com o título: "On the origin of number and arrangment of the places of exit on the surface of pollen-grains", procurava relações para a distância mínima entre os poros de um pólen. Configurações ótimas de pontos na esfera $S^2 \subset \mathbb{R}^3$ são conhecidas apenas para $M \leq 12$ e $M = 24$, segundo [17]. Todas as outras são as "melhores conhecidas", sem um prova formal de que são ótimas.

Há dois principais esforços para a solução deste problema. O primeiro é a construção de limitantes para o número de pontos $M = M(n, d)$ de um código esférico que envolvam a dimensão n e a distância mínima d. O segundo é a construção de códigos que tenham distâncias mínimas melhores que as conhecidas para uma determinada dimensão e quantidade de pontos. Quando um código $[M, n]$ alcança a distância mínima limite, estabelecida por um limitante para aquela

dimensão e quantidade de pontos, ele é ótimo.

Mas se o conjunto de pontos é um código de grupo, um código com simetrias, como se comportam esses limitantes? Quem são as melhores configurações de pontos? Estas duas perguntas, dentro da classe dos códigos com simetrias cíclicas, norteiam este trabalho.

Generalizados para qualquer espaço que contenha métrica, os códigos de grupo passaram a se chamar códigos geometricamente uniformes. O estudo dos códigos geometricamente uniformes obteve maior importância e interesse com o trabalho de Forney [18]. Mas a idéia de uniformidade nas regiões de decisão, fundamental nestes trabalhos, remonta ao trabalho seminal de David Slepian:"Group codes for the Gaussian Channel"[40]. Nele, Slepian inicia uma teoria sobre códigos em esferas euclidianas gerados por isometrias.

Evidentemente, por terem uma estrutura algébrica associada, espera-se que esses códigos tenham distância mínima euclidiana menor que aquelas dos códigos ótimos que não apresentam simetrias. Em contra-partida, há outras vantagens nessa abordagem. Dentre elas, talvez a mais importante, é a que os pontos do código tem região de decisão isométricas, o que implica em facilidade na hora da decodificação e cálculo da probabilidade de erro, além de um rotulamento natural, induzido pelo grupo.

O primeiro capítulo deste trabalho mostra os principais resultados e pré-requisitos necessários à leitura dos capítulos subsequentes. Boa parte do que está neste capítulo é de conhecimento corrente na teoria e pode ser encontrada na bibliografia em anexo, salvo alguns fatos que foram esmiuçados de maneira a tornar mais claro alguns conceitos.

O segundo capítulo trata da relação que há entre os códigos de grupo comutativo, especialmente os cíclicos, com os subgrupos de $(\mathbb{Z}_M)^n$. Todo código de grupo cíclico está associado, via um isomorfismo de grupo, a um subgrupo cíclico de $(\mathbb{Z}_M)^n$. Ao gerador deste subgrupo daremos o nome de assinatura do código. Condições necessárias para a existência de um código de grupo cíclico, sua dimensão e se ele mora em um hiperplano do espaço são estabelecidas em termos da sua assinatura. Com intuito de classificar tais códigos, uma série de operações que produzem códigos de grupo cíclico isométricos são listadas.

O terceiro capítulo contém a principal contribuição deste trabalho. Mostramos que todo código de grupo comutativo, em dimensão par, pode se visto sobre toros de curvatura gaussiana nula, os toro planos. Em dimensão ímpar, o código é formado por duas cópias de códigos de grupo comutativo que moram, cada uma, em toros planos. Em particular, códigos de grupo

cíclico em dimensão ímpar são anti-prismas. Tal caracterização permitiu desenvolver limitantes para a cardinalidade de um código de grupo comutativo em termos de sua distância mínima, de seu vetor inicial e da máxima densidade de empacotamento de esferas em $\mathbb{R}^m$, onde m é a dimensão do toro. Até o presente momento, não encontramos na literatura limitantes similares, ou seja, que levam em conta as simetrias do código esférico. Comparados com os limitantes da união e de Rankin para códigos esféricos gerais, os limitantes obtidos são melhores. Além disso, dependem,tal qual o limitante de Böröckzy - Coxeter [9], da dimensão da variedade onde o código mora, o toro plano.

Por fim, o terceiro capítulo, utilizando o algoritmo de Biglieri e Elia [7], mostra os melhores códigos de grupo cíclico em dimensão quatro e analisa uma classe destes que mora no toro plano de área máxima em $\mathbb{R}^4$.

Capítulo 1

Preliminares

"The fundamental problem of communication is that of reproducing at one point either exactly or aproximately a message selected at another point."

C. E. Shannon

Este capítulo introduz os temas estudados nos capítulos subsequentes, mostrando os principais resultados e referências conhecidos. Discute a relação que os sinais contínuos têm com os códigos esféricos e descreve as propriedades que procuramos em uma constelação de sinais. Introduz os códigos de grupo, apresentando uma bibliografia significativa sobre o problema do vetor inicial, e mostra os principais limitantes para os códigos esféricos euclidianos.

1.1 O Problema da Transmissão de Sinais Digitais

O prólogo deste capítulo expressa bem o objetivo crucial da teoria da informação: transmitir mensagens com confiabilidade, sem perdas de informação no decorrer da transmissão. Em geral, a transmissão se dá, seguindo o esquema da figura 1.1, da seguinte maneira: uma informação é relacionada na fonte a um código binário, um conjunto de sequências de "zeros e uns". Aos blocos, esses conjuntos de informação binária são melhorados de maneira a diminuir a probabilidade de erro na transmissão e, então, associados a sinais contínuos. Nesta última forma são transmitidos, via cabo, satélite ou qualquer outro meio de transmissão de sinais, a um receptor, que deverá executar as etapas anteriores na ordem inversa até chegar na informação transmitida.

Estudar códigos esféricos euclidianos diz respeito a um pequeno trecho do processo dentro

da fase de modulação: Os sinais contínuos, associados aos blocos de sequências binárias, podem ser representados como pontos em esferas euclidianas. Procuramos, então, melhorar essas constelações obtidas de forma a aumentar a confiabilidade da trasmissão.

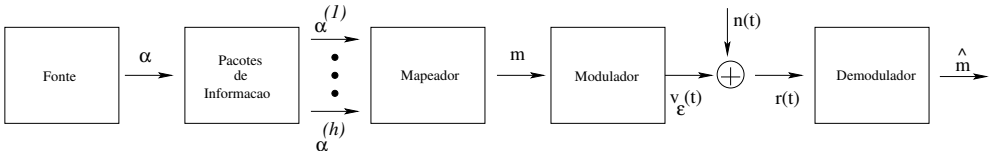


Figura 1.1: Um modelo de canal

1.1.1 A Modulação PSK

PSK é uma sigla, oriunda da língua inglesa, para Phase-Shift Keying, uma modulação intimamente ligada às rotações do espaço euclidiano. Suponhamos que uma informação pode ser representada binariamente, por exemplo, ligar e desligar a luz de um quarto, ou, abrir e fechar uma porta. Ligar é "0"e desligar é "'1". Vamos associar cada uma destas operações a uma fase de um sinal contínuo, conforme a figura 1.2. Ao "zero"associamos a fase zero e ao "um"associamos a fase π. Tais fases, por conseguinte, estão associadas a dois sinais contínuos

$$x_i(t) = \cos[\pi t + (i-1)\pi],\ t \in (0,2),\ i = 1,2.$$

Mas, $x_1(t) = \cos[\pi t]$ e $x_2(t) = -\cos[\pi t]$. Escritas como combinação das funções

$$\{-\sin[\pi t], \cos[\pi t]\},$$

temos $x_1(t) = 0.(-\sin[\pi t]) + 1.(\cos[\pi t])$ e $x_2(t) = 0.(-\sin[\pi t]) - 1.(\cos[\pi t])$.

Assim, representamos "zero" pelo ponto $(0,1)$ e "um" pelo ponto $(0,-1)$, conforme figura 1.3.

Esta construção se generaliza para o conjunto de M sinais

$$x_i(t) = \cos[\pi t + 2(i-1)\pi/M],\ t \in (0,2),\ i = 1,2,\ldots,M,$$

conhecido por M-PSK, cuja representação geométrica é um polígono regular de M vértices. De fato,

$$x_i(t) = cos(\pi t).cos(2(i-1)\pi/M) - sen(\pi t).sen(2(i-1)\pi/M) \text{ e, portanto,}$$

ao sinal i associamos o vetor $(cos(2(i-1)\pi/M), sen(2(i-1)\pi/M))$.

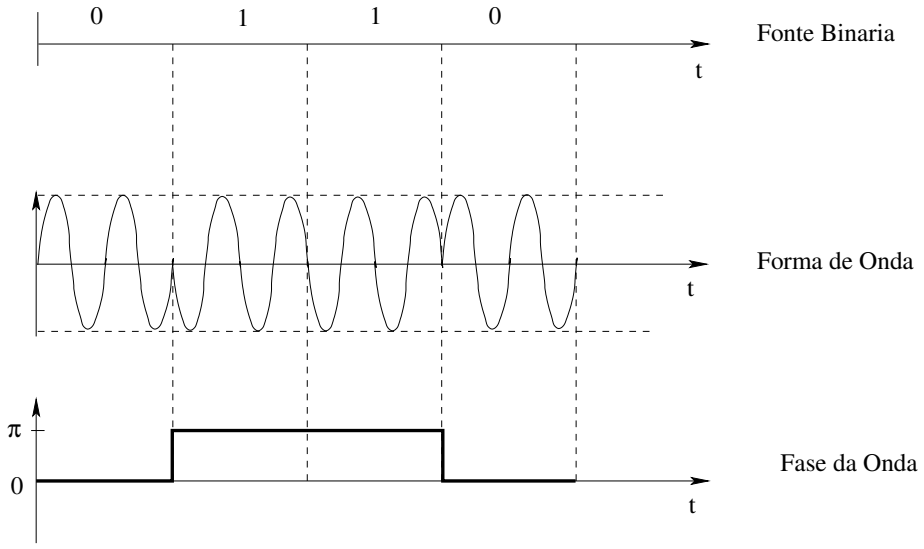


Figura 1.2: A modulação de um 2 PSK

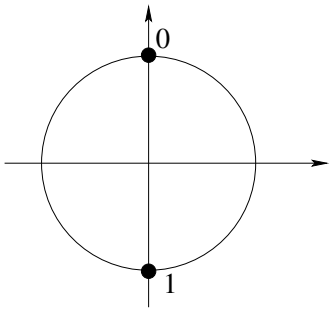


Figura 1.3: Representação Geométrica de um 2 PSK

1.1.2 Representação Geométrica de Sinais

A representação geométrica, apresentada na seção anterior, pode ser usada para um conjunto de sinais qualquer. Seja $\{s_1(t), ..., s_M(t)\}$ um conjunto de sinais. Pelo processo de ortonormalização de Gram-Schmidt, é sempre possível obter uma base $\{\phi_i(t)\}_{i=1}^{N}$ ortonormal de funções de tal maneira que

$$s_j(t) = \sum_{i=1}^{N} s_{ij}\phi_i(t).$$

Assim, para cada sinal $s_i(t)$ associamos um vetor $(s_{1i}, s_{2i}, s_{3i}, \ldots, s_{Ni}) \in \mathbb{R}^N$. Além disso,

o desempenho do erro, quando um dos sinais $s_i(t)$ é transmitido através de um canal AWGN[1], dependerá somente das suas representações no $\mathbb{R}^N$ e da densidade de potência do ruído. Portanto, toda a análise de desempenho de um conjunto de sinais é feita em cima do conjunto de coordenadas $\{(s_{1i}, \ldots, s_{Ni}) \in \mathbb{R}^N; i = 1, \ldots, M\}$. Este conjunto é chamado de constelação de sinais.

1.2 Propriedades importantes de uma constelação de sinais.

Seja $\{\xi_k\}_{k=1}^M \subset \mathbb{R}^N$ uma constelação de sinais. Ao transmitir ξ_k, o canal de transmissão acrescenta um erro r ao sinal ξ_k e receptor recebe $\widehat{\xi_k} = \xi_k + r$. Para recuperar o sinal transmitido, procuramos saber em qual *região de decisão* $R_i = \{x \in \mathbb{R}^N / |x - \xi_i| < |x - \xi_k|,$ para todo $k \neq i\}$ está $\widehat{\xi_k}$. Se $\widehat{\xi_k} \in R_m$, decidimos que o sinal transmitido foi ξ_m. Se $m = k$, a transmissão foi um sucesso, pois o canal tinha transmitido de fato ξ_k. Caso contrário, dizemos que houve um erro na transmissão.

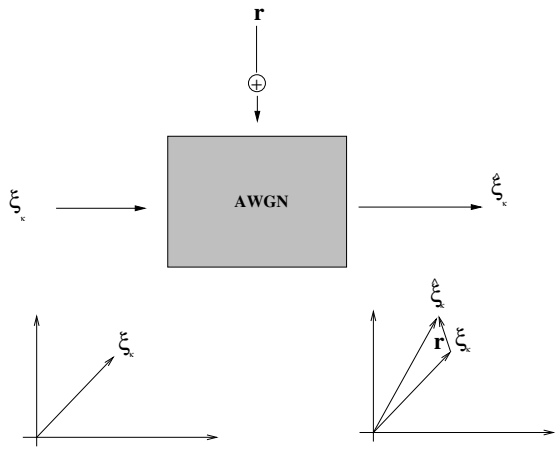


Figura 1.4: Canal com ruído Gaussiano Branco Aditivo.

O desempenho de uma constelação é medido pela probabilidade de erro na transmissão dos sinais $P(e)$.

[1]Additive White Gaussian Noise Channel: Canal com ruído aditivo gaussiano branco. A distribuição de probabilidade do erro é gaussiana e aditiva e a densidade espectral de potência dos sinais é invariante.

É de interesse diminuir o valor de $P(e)$ preservando a energia média da constelação

$$\frac{1}{M}\sum_{j=1}^{M}|\xi_j|^2.$$

Se todos os sinais ξ_j são equiprováveis de transmissão, a *probabilidade de erro* de símbolo pode ser escrita como

$$P(e) = 1 - P(c) = 1 - \frac{1}{M}\sum_{j=1}^{M} P(c \mid \xi_j),$$

onde $P(c \mid \xi_j)$ é probabilidade de decisão correta, dado que ξ_j foi transmitido. Se R_j é a região de decisão de ξ_j, então $P(c \mid \xi_j) = P\{\widehat{\xi}_j \in R_j \mid \xi_j\}$.

Se $\widehat{\xi}_j$ for obtido adicionando a ξ_j um vetor de ruído gaussiano com média zero e variância $N_0/2$, obtemos $P(c \mid \xi_j)$ integrando a função densidade de probabilidade de $\widehat{\xi}_j$, dado ξ_j, na região R_j. Portanto,

$$P(c \mid \xi_j) = \int_{R_j} \frac{1}{(\pi N_0)^{N/2}} e^{\frac{-|r-\xi_j|^2}{N_0}} dr.$$

Qualquer transformação que leva as regiões de decisão em regiões congruentes, não muda a probabilidade de erro da constelação. Se a constelação for órbita de um grupo de isometrias de $\mathbb{R}^N$, então todo sinal poderá ser levado a qualquer outro, bem como as suas respectivas regiões de decisão, isometricamente. Assim, $P(c \mid \xi_j) = P(c \mid \xi_1)$ para todo $j = 1, \ldots, M$, e

$$P(e) = 1 - \int_{R_1} \frac{1}{(\pi N_0)^{N/2}} e^{\frac{-|r-\xi_1|^2}{N_0}} dr.$$

1.2.1 O Limitante de Bhattacharyya

Apesar de ter uma expressão clara, a probabilidade de erro é de difícil cálculo. As regiões de decisão não são fáceis de identificar e a integral da função $f(x) = e^{-x^2}$ é estudada numericamente, uma vez que não possui primitiva. O cálculo de limitantes para essa probabilidade é crucial pois, apesar de não sabermos a probabilidade exata, a temos limitada por uma faixa de segurança.

Um limitante conhecido para a probabilidade de erro é o *limitante de Bhattacharyya* ([1], pp 190-192). Se $d_{ij} = |s_i - s_j|$, então

$$P(e) \leq \frac{1}{M}\sum_{i=1}^{M}\sum_{j\neq i} e^{\frac{-d_{ij}^2}{4N_0}} = \frac{1}{M}\sum_{i=1}^{M}\sum_{j\neq i} e^{\frac{-d_{ij}^2 \log_2(M)\eta_b}{4\varepsilon}},$$

onde $\varepsilon = \frac{1}{M}\sum_{i=1}^{M}||s_i||^2$ é a energia média da constelação e $\eta_b = \frac{\varepsilon_b}{N_0} = \frac{\varepsilon}{\log_2(M)N_0}$ é a relação sinal-ruído (SNR) .

Boas constelações apresentam probabilidade de erro baixa mesmo quando a interferência é grande, ou seja, a variância N_0 do processo estocástico de interferência é grande. Equivalentemente, elas não precisam dispender muita energia média ε para compensar a interferência. Uma maneira para isto acontecer é aumentando a distância entre as palavras da constelação. Segue daí um dos primeiros objetivos na construção de uma constelação de sinais S: maximizar $d_{min}(S) = min\{|s_i - s_j|; s_i, s_j \in S, i \neq j\}$, para um número fixo de pontos e energia média fixada.

Às vezes não basta diminuir a distância mínima, o número de pontos vizinhos também desempenha papel relevante em $P(e)$. Um exemplo deste fato pode ser encontrado no problema 4.17 de [1].

1.2.2 Momento de inércia de uma constelação

Pode-se diminuir a probabilidade de erro de uma constelação aumentando a energia $|s_i|^2$ do sinal s_i. Entretanto, isto implicaria em maiores gastos com energia na hora da transmissão. Assim, além de diminuir a probabilidade de erro $P(e)$, queremos que a energia média da constelação

$$\mathcal{E} = \frac{1}{M}\sum_{j=1}^{M} |s_j|^2$$

seja minimizada.

A energia média de uma constelação pode ser vista como o seu momento de inércia em relação a origem. Em geral, a cada elemento da constelação s_i associa-se uma probabilidade p_i de ocorrência da informação "i", de tal modo que $\sum_{i=1}^{M} p_i = 1$. Define-se então o momento de inércia da constelação em relação a um ponto q como

$$f(q) = \sum_{j=1}^{M} |s_j - q|^2 p_i.$$

Se o canal não fizer predileção entre as palavras, pode-se supor que as probabilidades são todas iguais a $p_i = 1/M$. Portanto, procura-se um ponto $q = (q_1, q_2, \ldots, q_N)$ que minimize a função $f(q) = \frac{1}{M}\sum_{j=1}^{M} |s_j - q|^2$.

Calculando as derivadas parciais de f em relação a q_i, i variando de 1 a N , obtêm-se

$$\frac{\partial f}{\partial q_i} = \frac{\partial}{\partial q_i}(\frac{1}{M}\sum_{j=1}^{M}\langle s_j - q, s_j - q\rangle) = \frac{2}{M}\sum_{j=1}^{M}\langle e_i, s_j - q\rangle,$$

onde $\{e_i\}_{i=1}^N$ é a base canônica de $\mathbb{R}^N$.

Assim, $\frac{\partial f}{\partial q_i} = 0$ se, e somente se, $\sum_{j=i}^M (s_j^i - q_i) = 0$, denotando $s_j = (s_j^1, \ldots, s_j^N)$. Portanto, o único ponto crítico q de f deve satisfazer $Mq_i = \sum_{j=1}^M s_j^i$. Logo,

$$q = \frac{1}{M}(s_1^1 + s_2^1 + \ldots + s_M^1, \ldots, s_1^N + \ldots + s_M^N) = \frac{1}{M}\sum_{j=1}^N s_j.$$

Note que $\frac{\partial^2 f}{\partial q_j \partial q_i} = \frac{2}{M}\sum_{j=1}^N \langle e_i, e_j\rangle = 2\delta_{ij}$, onde δ_{ij} é o delta de Kronecker. Portanto $q = \frac{1}{M}\sum_{j=1}^N s_j$ é mínimo local. Dado as condições do problema, é mínimo global.

Logo, a energia média da constelação é mínima quando o momento de inércia da constelação em relação à origem for mínimo. Isto ocorre somente quando $\frac{1}{M}\sum_{j=1}^N s_j = 0$. Portanto, procuramos constelações cuja distância mínima é a maior possível e $\frac{1}{M}\sum_{j=1}^N s_j = 0$.

Quando estudamos códigos esféricos, tais comentários perdem sentido, uma vez que a enegia média da constelação é constante. Entretanto, Loeliger [30] mostrou que, para os códigos de Slepian, $\frac{1}{M}\sum_{j=1}^N s_j \neq 0$ significa, além de perda de energia, má utilização da dimensão disponível. Isto torna esta última expressão ainda de interesse para códigos esféricos. Enunciaremos este resultado mais a frente, no final da seção sobre códigos de grupo.

A partir deste momento, todas as constelações estudadas serão esféricas, ou seja, todos os pontos terão energia igual e constante.

1.2.3 Matriz de Gram de um Código

A distância ao quadrado entre dois pontos s_1 e s_2 de energia um é

$$d^2(s_1, s_2) = |s_1 - s_2|^2 = 2 - 2\langle s_1, s_2\rangle.$$

Portanto, aumentar a distância entre as palavras de um código esférico é diminuir o produto interno entre as palavras da constelação, $\langle s_i, s_j\rangle$. A matriz formada pelos produtos escalares de uma constelação é chamada matriz de configuração ou matriz de Gram da constelação S. Essa matriz pode ser vista como o produto $M = a^T.a$, onde a é a matriz formada pelos vetores da constelação e satisfaz algumas propriedades conforme proposição a seguir.

Proposição 1.2.1 *[[16],p. 214] Seja $\{x_1, \ldots, x_M\} \subset S^{n-1}$ um conjunto de geradores para $\mathbb{R}^n$, então $G = (g_{ij}) = (x_i x_j) = a^T.a$ é matriz real, simétrica, não negativa e de posto n.*

Demonstração : É claro que G é real e simétrica. Note que se a é matriz de um operador A, a^T é a matriz da transformação linear adjunta A^*. Sendo assim,

$$\langle Gv, v\rangle = \langle a^T av, v\rangle = \langle av, av\rangle \geq 0.$$

Logo, G é definida não negativa e todos os seus auto valores são não negativos.

Quanto ao posto, provemos que o posto de G é o mesmo que o de a, ou seja, que a imagem do operador A^*A tem a mesma dimensão que a do operador A. Para tanto, considere $v \in N(A)$, o núcleo do operador A. É claro que $v \in N(A^*A)$, portanto $N(A) \subset N(A^*A)$.

Reciprocamente, considere $v \in N(A^*A)$, então $A^*A(v) = 0$, logo $Av \in N(A^*)$. Mas $N(A^*)$ é o complemento ortogonal $Im(A)^\perp$ da imagem de A. Logo $Av \in Im(A) \cap Im(A)^\perp$, e $A.v = 0$. Portanto, $v \in N(A)$ e $N(A) = N(A^*A)$.

Assim, $dimIm(A^*A) = M - dim(N(A^*A)) = M - dim(N(A)) = dimIm(A)$. ■

Blake estudou as matrizes de Gram de um código de grupo em [3]. Neste artigo, o autor dá uma condição simples em termos dos auto-valores da matriz de Gram da constelação para que o código gere o espaço.

1.3 As isometrias do espaço euclidiano

Uma isometria é um movimento no espaço que preserva distâncias. Isto é, se ϕ é uma aplicação em $\mathbb{R}^n$, ela será uma isometria se $|\phi(u) - \phi(v)| = |u - v|$ para todo $u, v \in \mathbb{R}^n$. Veremos a seguir que uma *isometria euclidiana* é uma composição de dois operadores: um operador que preserva norma e uma translação, sendo que a matriz do operador que preserva norma é uma concatenação de três tipos de operadores: identidade, reflexões pelos eixos coordenados e rotações.

Proposição 1.3.1 *[[16], p. 192] Toda isometria ϕ do espaço euclidiano $\mathbb{R}^n$ tem a forma $\phi(v) = A.v + b$, onde $A : \mathbb{R}^n \to \mathbb{R}^n$ é um operador linear que preserva norma e $b \in \mathbb{R}^n$ é um vetor constante independente de v.*

Demonstração : Considere $b = \phi(0)$ e $\psi(v) = \phi(v) - v$. O operador ψ é uma isometria que leva a origem na origem satisfazendo $|\psi(v)| = |\psi(v) - \psi(0)| = |v - 0| = |v|$. Como o produto interno em $\mathbb{R}^n$ satisfaz $\langle u, v\rangle = \frac{1}{2}(|u|^2 + |v|^2 - |u - v|^2)$, para todo $u, v \in \mathbb{R}^n$, segue que $\langle \psi(u), \psi(v)\rangle = \frac{1}{2}(|\psi(u)|^2 + |\psi(v)|^2 - |\psi(u) - \psi(v)|^2) = \frac{1}{2}(|u|^2 + |v|^2 - |u - v|^2) = \langle u, v\rangle$.

Portanto, o conjunto $\{u_i = \psi(e_i)\}_{i=1}^n$ é uma base ortonormal em $\mathbb{R}^n$. De fato, $|u_i| = |\psi(e_i)| = |e_i| = 1$, $\langle u_i, u_j\rangle = \langle \psi(e_i), \psi(e_j)\rangle = \langle e_i, e_j\rangle = \delta_{ij}$ e, se existissem números reais λ_i, de tal modo que $\sum_{i=1}^n \lambda_i u_i = 0$, seguiria que $0 = \langle \sum_{i=1}^n \lambda_i u_i, \sum_{i=1}^n \lambda_i u_i\rangle = \sum_{i=1}^n \lambda_i^2$, o que implicaria em $\lambda_i = 0$ para todo $i = 1, \ldots, n$.

Provemos então que, dado $v = \sum_{i=1}^n x_i e_i \in \mathbb{R}^n$, $\psi(v) = \sum_{i=1}^n x_i u_i$, ou seja, que a aplicação ψ é linear. Antes, vê-se que $\langle \psi(v), u_i\rangle = \langle \psi(v), \psi(e_i)\rangle = \langle v, e_i\rangle = x_i$. Portanto,

$$\begin{aligned}\langle \psi(v) - \sum_{i=1}^n x_i u_i, \psi(v) - \sum_{i=1}^n x_i u_i\rangle &= \langle \psi(v), \psi(v)\rangle - 2\langle \psi(v), \sum_{i=1}^n x_i u_i\rangle + \sum_{i=1}^n \langle x_i u_i, x_i u_i\rangle = \\ \langle v, v\rangle - 2\sum_{i=1}^n x_i \langle \psi(v), u_i\rangle + \sum_{i=1}^n x_i^2 &= \sum_{i=1}^n x_i^2 - 2\sum_{i=1}^n x_i x_i + \sum_{i=1}^n x_i^2 = 0.\end{aligned}$$

■

Operadores que preservam norma, como os da proposição, são chamados operadores ortogonais. Usando artifícios análogos aos usados na demonstração anterior, pode-se demonstrar as seguintes equivalências sobre a matriz de um operador ortogonal.

Proposição 1.3.2 *[[16],p 184] As seguintes afirmações são equivalentes:*

1. $A \in O(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}); \langle A(x), A(y)\rangle = \langle x, y\rangle, x, y \in \mathbb{R}^n\}$
2. $\langle A(e_i), A(e_j)\rangle = \delta_{ij}$, *onde* $\{e_i\}$ *é a base ortonormal canônica.*
3. *A leva base ortonormal em base ortonormal.*
4. *As linhas de A formam uma base ortonormal.*
5. *As colunas de A formam uma base ortonormal.*
6. $A^T = A^{-1}$, *onde* A^T *é a matriz transposta de A.*

1.3.1 Uma forma normal para os operadores ortogonais

Considere um operador ortogonal $A : \mathbb{R}^n \to \mathbb{R}^n$. Se λ_k é autovalor de A relativo ao autovetor v_k, então

$$\langle v_k, v_k\rangle = \langle Av_k, Av_k\rangle = \langle \lambda_k v_k, \lambda_k v_k\rangle = \lambda_k \overline{\lambda_k} \langle v_k, v_k\rangle.$$

Logo $\lambda_k\overline{\lambda_k} = 1$, onde $\overline{\lambda_k}$ denota o conjugado complexo de λ_k. Se λ_k é real, $\lambda_k = \pm 1$. Se λ_k é complexo, existe θ_k real, de tal maneira que $\lambda_k = cos(\theta_k) + \imath sen(\theta_k)$. Escrevendo $v_k = \Re(v_k) + \imath\Im(v_k)$, segue que

$$A(\Re(v_k)) + \imath A(\Im(v_k)) = A(\Re(v_k) + \imath\Im(v_k)) = \lambda_k v_k = (cos(\theta_k) + \imath sen(\theta_k))(\Re(v_k) + \imath\Im(v_k)) =$$

$$= cos(\theta_k).\Re(v_k) - sen(\theta_k)\Im(v_k) + \imath(cos(\theta_k).\Im(v_k) + sen(\theta_k)\Re(v_k)).$$

Consequentemente,

$$\begin{cases} A(\Re(v_k)) = cos(\theta_k)\Re(v_k) - sen(\theta_k)\Im(v_k) \\ A(\Im(v_k)) = cos(\theta_k).\Im(v_k) + sen(\theta_k)\Re(v_k) \end{cases}$$

Usando as identidades $\Re(v_k) = \frac{1}{2}(v_k + \overline{v_k})$ e que $\Im(v_k) = \frac{1}{2\imath}(v_k - \overline{v_k})$, demonstra-se que $\{\Re(v_k), \Im(v_k))\}$ é um par de vetores ortogonais. Logo, no subespaço gerado pelo par de vetores, invariante por A, a aplicação A tem a forma de uma rotação de ângulo θ_k.

Como o complemento ortogonal também é invariante por A, é possível construir recursivamente um conjunto de autovetores complexos $\{v_k\}$ de onde retiramos um conjunto de vetores ortogonais $\{\Re(v_k), \Im(v_k)\}$ que, junto com os autovetores reais, formam uma base para o $\mathbb{R}^n$ onde o operador A se escreve

$$\begin{cases} A(\Re(v_k)) = cos(\theta_k)\Re(v_k) - sen(\theta_k)\Im(v_k) & k = 1, \ldots, q \\ A(\Im(v_k)) = cos(\theta_k).\Im(v_k) + sen(\theta_k)\Re(v_k) & k = 1, \ldots, q \\ A(v_l) = \mu_l v_l & l = 2q+1, \ldots, n, \end{cases}$$

com $\mu_l = \pm 1$. Assim, podemos enunciar o teorema:

Teorema 1.3.1 *([19]) Sejam $A : \mathbb{R}^n \to \mathbb{R}^n$ um operador ortogonal, $\{v_k\}_{k=1}^q$ seus autovetores complexos associados aos autovalores λ_k, distintos e não conjugados, e $\{u_l\}_{l=2q+1}^n$, os autovetores reais de A associados aos autovalores $\mu_l = \pm 1$. Denote $x_k = \Re(v_k)$ e $y_k = \Im(v_k)$. Então, a matriz $\mathcal{A}$ de A satisfaz*

$$\mathcal{A} = Q\{\begin{vmatrix} cos(\lambda_1) & -sen(\lambda_1) \\ sen(\lambda_1) & cos(\lambda_1) \end{vmatrix}, \ldots, \begin{vmatrix} cos(\lambda_q) & -sen(\lambda_q) \\ sen(\lambda_q) & cos(\lambda_q) \end{vmatrix}, \pm 1, \ldots, \pm 1\}Q^T,$$

onde a matriz Q escrita na forma de coluna é $(x_1, y_1, \ldots, x_q, y_q, u_{2q+1}, \ldots, u_n)$ e a matriz entre Q e Q^T está descrita na forma diagonal de modo que os elementos fora dela são nulos.

O resultado que se segue, generalização do teorema acima, se baseia no fato de que matrizes que comutam tem os mesmos autoespaços invariantes.

Teorema 1.3.2 *([19],pp 292):*

Para todo conjunto C de matrizes reais, normais[2] *e comutativas existe uma transformação ortogonal Q tal que toda matriz $A \in C$ satisfaz*

$$Q^T AQ = \{ \begin{vmatrix} \mu(A)_1 & -\nu(A)_1 \\ \nu(A)_1 & \mu(A)_1 \end{vmatrix}, \ldots, \begin{vmatrix} \mu(A)_q & -\nu(A)_q \\ \nu(A)_q & \mu(A)_q \end{vmatrix}, \mu_{2q+1}, \ldots, \mu_n \}.$$

Além disso, se os operadores de C forem ortogonais, temos que $\mu(A)_k = cos(\phi_k(A))$,$\nu(A)_k = sen(\phi_k(A))$, onde $k = 1, \ldots, q$, e $\mu_l(A) = \pm 1)$, onde $l = 2q+1, \ldots, n$.

1.4 Códigos de Grupo

Um *código de grupo* (M, n) é um conjunto $\mathcal{X} = \{x_i\}_{i=1}^M$ de vetores unitários, geradores de $\mathbb{R}^n$, que é órbita de um grupo multiplicativo de matrizes ortogonais $G = \{O_i\}_{i=1}^M$ a partir de algum $x \in \mathcal{X}$, ie, $\mathcal{X} = G(x)$. Uma consequência imediata desta definição é que em um código de grupo existe sempre uma isometria que leva uma palavra em uma outra da constelação. Portanto, todas as regiões de decisão são isométricas, o conjunto das distâncias de uma palavra a todas as outras e o número de seus vizinhos é invariante em toda a constelação. Assim, a probabilidade de erro de todas as palavra é a mesma.

Quem introduziu os códigos de grupo pela primeira vez foi David Slepian no trabalho "Group Codes for the Gaussian Channel"[40] em 1968. Há duas questões fundamentais sobre códigos de grupo propostas por Slepian. A primeira diz respeito a sua existência: dada uma dimensão n e um número de pontos M, existe um código de grupo com esses parâmetros para todo grupo abstrato G escolhido? A segunda, conhecida por problema do vetor inicial, procura por um código de grupo $[M, n]$ ótimo. Mais especificamente, dado um grupo abstrato G e um homomorfismo bijetor $\phi : G \to \mathcal{G} \subset \mathcal{O}(n, \mathbb{R})$, chamado *representação fiel* de ordem n de G no grupo das matrizes ortogonais reais de dimensão n, $\mathcal{O}(n, \mathbb{R})$, qual é o vetor inicial $x \in R^n$ que maximiza a distância mínima entre as palavras?

A resposta para a dimensão dois é fácil de ser encontrada. As melhores constelações nesta dimensão são as formadas pelos vértices dos polígonos regulares. Essas constelações podem ser obtidas pelas matrizes de rotação 2×2 e são conhecidas como modulação PSK. Fica claro que, se usamos matrizes de rotação, a escolha independe do vetor inicial e todas as constelações serão

[2]Uma matriz é normal quando ela comuta com sua transposta.

isométricas. Entretanto, se o grupo escolhido for o grupo das reflexões pelos eixos coordenados e as retas $y = \pm x$, veremos que a configuração dos pontos dependerá do vetor inicial (Figura 1.5).

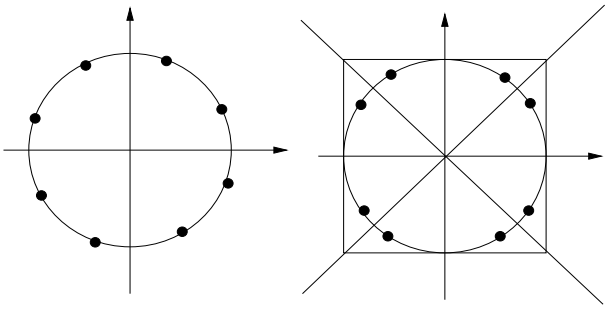


Figura 1.5: Oito pontos gerados por um grupo cíclico e um grupo de reflexões

Os primeiros pesquisadores que consideraram a questão da existência dos códigos de grupo foram Biglieri e Elia em [5]. Neste artigo, utilizando teoria de grupos e suas representações, eles obtiveram o seguinte resultado sobre a existência de códigos de grupo $[M, n]$ não contidos em hiperplanos (não planares):

n par e M primo Existe somente o código não planar gerado pelo grupo cíclico de ordem M.

n par, M não primo, ou, n ímpar e M par Existe pelo menos um código de grupo não planar, gerado pelo grupo cíclico de ordem $g = M$.

n ímpar e M primo Não existem códigos de grupo não planares.

n ímpar e M ímpar Não existem códigos de grupo gerados por um grupo de ordem $g = M$. Se um código de grupo não planar existir, ele precisará ser gerado por um grupo de ordem par.

Em [27], Downey e Karlof explicitaram algumas condições de existência para o caso n ímpar e M ímpar, aprofundando mais na questão do que Biglieri e Elia em [5]. Mais tarde, em [28], Downey e Karlof demonstraram que:

- (Teorema 4) Se $n \neq 3$, um código de grupo $[M, n]$, para algum M ímpar, existe.
- (Teorema 5) Não existem códigos de grupo para $n = 3$ e M ímpar.

É claro que o teorema 4 não garante a existência de um código [M,2n+1] para todo M. Se M é primo, é possível provar que não existem códigos de grupo [M,2n+1].

Nessa mesma época, Djoković e Blake, em [2], trataram do problema do vetor inicial de uma perspectiva mais abstrata. Estudaram-no para alguns G-módulos, onde G é o grupo que se quer representar. Mais tarde, Blake, utilizando as técnicas de [2], estudou o problema para algumas representações do grupo simétrico $\mathcal{S}_n$, o grupo de todas as permutações do conjunto $\{1, 2, 3, \ldots, n\}$, e o grupo de Mathieu em [4]. Mas as técnicas utilizadas nesses artigos não jogaram luz sobre o problema em geral. O que se procura é o melhor código entre todas representações de um determinado grupo. Em 1989 a questão, no caso dos grupos de permutação, é retomada por Karlof em [24].

Em alguns casos, para obter as soluções do problema do vetor inicial, desenvolveu-se programas computacionais sem a preocupação de deduzir expressões gerais para cada caso. Isto aconteceu para os códigos de grupo cíclicos, estudados por Biglieri e Elia em [7]. Neste artigo, os autores reapresentam a questão do vetor inicial na forma de um problema de programação linear que depende da representação do grupo utilizada. Fixada a dimensão da representação, há várias maneiras de representar um grupo cíclico. Entre todas as possíveis representações, qual delas gera um conjunto de pontos com maior distância mínima ? Procedimento análogo foi adotado para os códigos de permutação, analisados por Karlof em [24] e por Karlof e Chang em [25].

Além dos códigos de grupos cíclicos, Biglieri e Elia propuseram uma solução para o problema da modulação de permutação, variante I, em [6]. As palavras da variante I são formadas a partir das permutações das entradas de um vetor inicial. Ingemarsson, em [23], apresentou expressões mais elegantes para a distância mínima ótima da variante I e analisou também a variante II dos códigos de permutação, que incluem, além das permutações das entradas, mudança de sinal nas coordenadas das palavras.

A questão do vetor inicial para representações de grau 3 foi completamente analisada por Downey e Karlof nos artigos [26] e [29]. Neles, os autores estudam todos os possíveis movimentos rígidos em $\mathbb{R}^3$ e calculam o melhor vetor inicial em cada caso.

Mais recentemente, Mittelholzer, em [31], abordou os problema para os grupos de reflexão finitos irredutíveis, seguindo uma classificação de Coxeter através de grafos.

No caso dos códigos de grupo, o fato da constelação não minimizar a energia média tem

um significado interessante. Veremos , no próximo teorema, que $\sum_{s\in\mathcal{X}} s \neq 0$ significa, além de perda de energia, que a constelação mora em um hiperplano afim do espaço, consequentemente não usa todo o espaço desta dimensão. Nesse caso, dizemos que a constelação é não substancial ou planar.

A exigência que Slepian faz para que os códigos de grupo fossem um conjunto de geradores para o espaço não impede que a constelação não seja substancial. A base canônica do $\mathbb{R}^N$ é um código de grupo não substancial que, quando visto no hiperplano que contém os pontos da base, é chamado simplex. Maiores detalhes sobre o código simplex serão descritos no próximo capítulo.

Teorema 1.4.1 *[30] Seja S uma constelação de sinais em $\mathbb{R}^N$, órbita de um grupo de matrizes ortogonais. Denote por $dimS$ a dimensão do espaço gerado por S e $dim\Delta S$ a dimensão do espaço gerado pela constelação $\Delta S = \{s - s^{'}; s, s^{'} \in S\}$. Então*

$$\sum_{s\in S} s = 0 \ \ \textit{se, e somente se,} \ \ dimS = dim\Delta S.$$

Se $\sum_{s\in S} s \neq 0$, então existe uma translação T tal que $\sum_{s\in S} T(s) = 0$ e $dimT(S) = dimS - 1$.

O lema 2.2.1, do capítulo 2, dá uma interpretação nova à expressão $\frac{1}{M}\sum_{j=1}^{N} s_j \neq 0$ para códigos de grupo cíclico.

1.5 Constelações de Sinais Equivalentes

Como já dissemos na seção anterior, isometrias são transformações importantes na construção de constelações de sinais e servem como bom parâmetros para compará-las. Na seção 1.3 vimos que as isometrias do espaço euclidiano são, a menos de uma translação, os operadores ortogonais. Por isso, diremos que dois códigos de grupo $\mathcal{X}_1$ e $\mathcal{X}_2$ são *equivalentes* se existir uma matriz ortogonal O que leva um código no outro, ou seja, $O\mathcal{X}_1 = \mathcal{X}_2$.

Eles serão *fracamente equivalentes* se a matriz de Gram de $\mathcal{X}_1$, $(a_{ij})_{M\times M} = (x_i x_j)$ com $x_i \in \mathcal{X}$, for igual a de $\mathcal{X}_2$. Se a matriz de Gram de um conjunto de pontos for igual a um outro conjunto, as distâncias entre as palavras, por conseguinte as distâncias mínimas dos códigos e o número de pontos próximos, serão iguais. Note que códigos equivalentes são códigos fracamente equivalentes, mas não vale a recíproca. O conceito de fracamente equivalente permite

comparações entre constelações em dimensões diferentes, o que não ocorre com constelações equivalentes.

Biglieri, Karlof e Viterbo, em 1999, mostraram que todo código de grupo é fracamente equivalente a um código de grupo de permutação [8].

1.6 Limitantes Gerais para uma distribuição de pontos na esfera

Dados $x, y \in S^n$, o ângulo entre estes pontos é $\arccos\langle x, y\rangle$. Se d é a distância mínima em um código esférico, então o *ângulo mínimo* entre os pontos é

$$\theta = 2\arcsin(\frac{d}{2}).$$

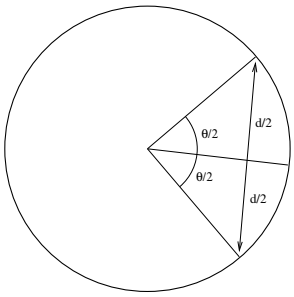


Figura 1.6: Ângulo mínimo e a distância mínima em um código esférico.

O conjunto dos pontos da esfera S^{n-1} cuja separação angular de um ponto $X \in S^{n-1}$ é menor ou igual a ϕ é chamado *chapéu esférico* centrado em X e de ângulo ϕ. Denotaremos esse chapéu por

$$C_X(n, \phi) = \{y \in S^{n-1}; \langle x, y\rangle > \cos(\phi)\}.$$

Se o ponto central do chapéu não for importante denotaremos $C(n, \phi)$. É possível demonstrar ([17]) que a área do chapéu esférico é

$$A(C(n,\phi)) = k_{n-1}\int_0^{\phi}(\sin\alpha)^{n-2}d\alpha, \text{ onde}$$

$$k_n = \begin{cases} \frac{(2\pi)^{n/2}}{(n-2)!!} & n = 2, 4, \ldots \\ \frac{2.(2\pi)^{(n-1)/2}}{(n-2)!!} & n = 3, 5, \ldots \end{cases} \quad e \tag{1.1}$$

$$n!! = \begin{cases} n(n-2)(n-4)\ldots 1 & \text{n ímpar} \\ n(n-2)(n-4)\ldots 2 & \text{n par} \end{cases}.$$

Em particular, a área total da esfera é

$$A(C(n,\pi)) = \begin{cases} \frac{(2\pi)^m}{(2(m-1))!!} & \text{se } n = 2m \\ \frac{2(2\pi)^m}{(2m-1)!!} & \text{se } n = 2m+1 \end{cases}.$$

A densidade $\Delta_{\mathcal{C}}$ de um código esférico $\mathcal{C} \subset S^{n-1}$ com distância mínima $d = 2\sin(\frac{\theta}{2})$ é a razão entre a *área dos* $|\mathcal{C}|$ *chapéus esféricos* disjuntos centrados nas palavras do código com ângulo $\theta/2$ pela área da esfera S^{n-1}. Se $A(C(n,\theta/2))$ é a área de um destes chapéus e $A(C(n,\pi))$ é a *área da esfera* S^{n-1}, então

$$\Delta_{\mathcal{C}} = \frac{|\mathcal{C}|A(C(n,\phi/2))}{A(C(n,\theta))}.$$

1.6.1 O Limitante da União

Dado um ângulo θ, qual seria um limitante para o número de chapéus $A(n,\theta)$ não sobrepostos na esfera S^{n-1} ? Os cálculos feitos acima nos dão um limitante para o número de pontos de um código esférico. Um código com M pontos e distância mínima d implica em M chapéus esféricos disjuntos com ângulo $\theta/2$, onde θ satisfaz $d = 2\sin\theta/2$, sobre a esfera. Logo, a área ocupada por esses chapéus é limitada pela área total da esfera. Segue portanto o teorema abaixo.

Teorema 1.6.1 *Limitante da União*
Seja um código esférico n-dimensional com M pontos e distância mínima $d = 2\sin\theta/2$. *Então, em termos do coeficiente* k_n *definido em 1.1, a seguinte desigualdade deve ser satisfeita:*

$$M \leq \frac{A(C(n,\pi))}{A(C(n,\theta/2))} = \frac{k_n}{k_{n-1}\int_0^{\theta/2}(sen\alpha)^{n-2}d\alpha}.$$

1.6.2 O Limitante de Tóth, Coxeter e Böroöckzy

Um dos primeiros limitantes a aparecer para códigos em $\mathbb{R}^3$ foi o de L. Fejes Tóth, 1943. Este limitante é alcançado por códigos com $M = 4, 6$ e 12 pontos, o tetraedro regular, o octaedro e o icosaedro. Sua construção utiliza estimativas sobre a área de triângulos esféricos.

Teorema 1.6.2 *Limitante de Tóth, [46, 45]*
Em $\mathbb{R}^3$, *todo código esférico com M pontos tem ângulo mínimo* θ *satisfazendo*

$$\theta \leq \arccos\frac{\cot^2\frac{M\pi}{6(M-2)}}{2}.$$

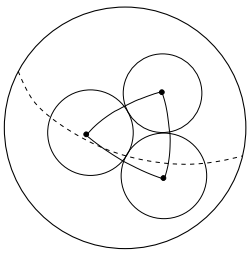


Figura 1.7: Três pontos na esfera S^2 com seus respectivos chapéus esféricos. O limitante de Tóth envolve estimativas para a área não ocupada pelos chapéus, interna ao triângulo formado pelos pontos.

Mais tarde, em 1963, Coxeter, disse ser "intuitivamente óbvio" que n esferas $n-2$-dimensionais são empacotadas o máximo possível quando cada uma toca todas, de maneira que seus centros são os n vértices do simplex regular. Ele se baseava nas idéias que Tóth utilizou para estabelecer o limitante para $n = 3$. Essa conjectura só foi resolvida 25 anos depois, em 1978, por Böröckzy [9]. Coxeter havia obtido como consequência da sua conjectura um limitante para códigos esféricos que, após a prova de Böröckzy, passou a ser chamado de limitante de Böröckzy - Coxeter.

Teorema 1.6.3 *Limitante de Böröckzy - Coxeter*
Todo código esférico em $\mathbb{R}^n$ *tem ângulo mínimo* ϕ *e número de pontos* M *satisfazendo*

$$M \leq \frac{2F_{n-1}(\alpha)}{F_n(\alpha)},$$

onde $\sec 2\alpha = sec\phi + n - 2$ *e* $F_n(\alpha)$ *é a função de Schläfli definida por*

$$F_n(\alpha) = \frac{2^n U}{n.n!V_n}$$

onde U *é a área de um simplexo esférico regular de ângulo* 2α *contido em* S^{n-1} *e* V_n *é o volume da esfera* S^{n-1} .

Infelizmente, o cálculo da área desses simplexos é muito complicado para n maior que três, o que torna o limitante Böröckzy - Coxeter difícil de manipular.

1.6.3 O Limitante de Rankin

Em 1954, Rankin propôs alguns limitantes para códigos esféricos euclidianos que, além de uma fácil manipulação, possibilitaram demonstrar que as classes de códigos simplex e biortogonal são ótimas.

Teorema 1.6.4 *Limitante de Rankin I*

Todo código com M pontos e ângulo mínimo 2ϕ contido na esfera $S^{n-1} = \{x \in \mathbb{R}^n; |x| = 1\}$ satisfaz as seguintes desigualdades:

1. $M \leq [\frac{2\sin(\phi)^2}{2\sin^2(\phi)-1}]$, *para* $\frac{\pi}{4} + \frac{\arcsin(\frac{1}{n})}{2} \leq \phi \leq \frac{\pi}{2}$
2. $M \leq n+1$, *para* $\frac{\pi}{4} < \phi \leq \frac{\pi}{4} + \frac{\arcsin(\frac{1}{n})}{2}$
3. $M \leq 2n$, *para* $\phi = \frac{\pi}{4}$.

É fácil reescrever o teorema acima em termos de distância mínima. Por exemplo, a segunda desigualdade é equivalente às expressões:

$$\frac{\pi}{4} \leq \phi \leq \frac{\pi}{4} + \frac{\arcsin(\frac{1}{n})}{2},$$

$$0 \leq \phi - \frac{\pi}{4} \leq \frac{\arcsin(\frac{1}{n})}{2},$$

$$0 \leq 2\phi - \frac{\pi}{2} \leq \arcsin(\frac{1}{n}),$$

$$0 \leq \sin(2\phi - \frac{\pi}{2}) \leq \frac{1}{n},$$

$$0 \leq 2\sin^2\phi - 1 \leq \frac{1}{n},$$

$$2 \leq 4\sin^2\phi \leq \frac{2(n+1)}{n}.$$

Como o ângulo mínimo é 2ϕ, a distância mínima do código é $d = 2\sin\phi$. Consequentemente, se a distância mínima ao quadrado d^2 de um código esférico com M pontos em $\mathbb{R}^n$ satisfazer a desigualdade

$$2 \leq d^2 \leq \frac{2(n+1)}{n},$$

então $M \leq n+1$. De maneira análoga, pode-se reescrever as outras desigualdades e obter a seguinte versão do teorema 1.6.4:

Teorema 1.6.5 *Limitante de Rankin I*

Todo código com M pontos e distância mínima d contido na esfera $S^{n-1} = \{x \in \mathbb{R}^n; |x| = 1\}$ satisfaz as seguintes desigualdades:

1. $M \leq [\frac{d^2}{d^2-2}]$, *para* $\frac{2(n+1)}{n} \leq d^2 \leq 4$.

2. $M \leq n+1$, *para* $2 \leq d^2 \leq \frac{2(n+1)}{n}$.

3. $M \leq 2n$, *para* $d^2 = 2$.

A seguir, demonstraremos três limitantes equivalentes aos enunciados acima.

Proposição 1.6.1 *Rankin A*

Qualquer código esférico $\mathcal{X}$ *em* $\mathbb{R}^n$ *com distância mínima ao quadrado* ρ *e* M *pontos satisfaz*

$$\rho \leq \frac{2M}{M-1}.$$

Demonstração : É fácil ver que $\rho \leq 2 - 2\langle x_i, x_j\rangle$, para todo x_i, x_j distintos em $\mathcal{X}$. Assim, temos $\langle x_i, x_j\rangle \leq \frac{2-\rho}{2}$ e

$$\sum_{i,j}\langle x_i, x_j\rangle = M + M(M-1)(\frac{2-\rho}{2}).$$

Por outro lado,

$$\sum_{i,j}\langle x_i, x_j\rangle = \sum_{i,j}\sum_{k=1}^{n} x_{ik}.x_{jk} = \sum_{k=1}^{n}\sum_{i,j} x_{ik}.x_{jk} = \sum_{k=1}^{n}\left(\sum_{i}^{M} x_{ik}\right)^2 \geq 0.$$

■

Proposição 1.6.2 *Rankin B*

Qualquer código esférico $\mathcal{X}$ *em* $\mathbb{R}^n$ *com distância mínima ao quadrado* ρ*, satisfazendo* $2 < \rho \leq 4$*, e* M *pontos satisfaz*

$$M \leq n+1.$$

Demonstração : Como $2 < 2 - 2\langle x_i, x_j\rangle \leq 4$, para todos x_i e x_j distintos em $\mathcal{X}$, segue que $-1 \leq \langle x_i, x_j\rangle < 0$. Em particular,

$$\langle x_i, x_M\rangle < 0 \;\; e \;\; -1 < \langle x_i, x_M\rangle, \;\; \text{para} \;\; i = 1, \ldots, M-1.$$

A última desigualdade é estrita pois, se existisse um ponto de $\mathcal{X}$, digamos x_{M-1}, tal que $\langle x_{M-1}, x_M\rangle = -1$, então $x_{M-1} = -x_M$ e $\langle x_i, x_{M-1}\rangle = -\langle x_i, x_M\rangle > 0$, $i = 1, \ldots, M-2$, contrariando as hipóteses.

Assim, defina $\gamma_i = 1 - \langle x_i, x_M\rangle^2 > 0$ e $y_i = \frac{1}{\gamma_i^1/2}(x_i - \langle x_i, x_M\rangle x_M)$, para $i = 1, \ldots, M-1$. Note que

$$\sqrt{\gamma_i\gamma_j}\langle y_i, y_j\rangle = \langle x_i, x_i\rangle - \langle x_i, x_M\rangle\langle x_j, x_M\rangle, \;\; \text{para} \;\; 1 \leq i, j \leq M-1.$$

Logo, $\langle y_i, y_j \rangle < 0$ porque $\langle x_i, x_j \rangle < 0$ para $i \neq j$ distintos. Portanto, temos um novo código $\mathcal{X}_{n-1} = \{y_1, \ldots, y_{M-1}\}$ com $M-1$ pontos e distância mínima ao quadrado maior que dois, contido num hiperplano normal a x_M, consequentemente de dimensão $n-1$.

Recursivamente, contruímos um código $\mathcal{X}_k$ com distância mínima ao quadrado maior que dois e $M-n+k$ pontos que está contido em $\mathbb{R}^k$. Para concluir a demonstração, basta ver que o código $\mathcal{X}_1$, contido em dimensão 1, tem $M-n+1$ pontos. Por ser dimensão 1, $M-n+1 \leq 2$. ■

Proposição 1.6.3 *Rankin C*
Qualquer código esférico em $\mathbb{R}^n$ com distância mínima ao quadrado $\rho \geq 2$ e M pontos satisfaz

$$M \leq 2n.$$

Demonstração : Basta repetir a contrução da família de códigos $\mathcal{X}_k$, da proposição anterior, observando que a distância mínima ao quadrado pode ser 2. Assim, a cardinalidade diminui de um ponto ou dois. Portanto o número de pontos de $\mathcal{X}_k$ é maior ou igual a $M-2(n-k)$. Logo, para $k=1$, segue que $2 \geq M-2(n-1)$. ■

Teorema 1.6.6 *Limitante de Rankin II*
Se $0 < \phi < \frac{\pi}{4}$ e $\beta = \arcsin(\sqrt{2}\sin(\phi))$, então todo código esférico em $\mathbb{R}^n$ com M pontos e ângulo mínimo 2ϕ satisfaz

$$M \leq \frac{\sqrt{2}\Gamma(\frac{n-1}{2})\sin\beta\tan\beta}{2\Gamma(\frac{n}{2})\int_0^\beta(\sin^{n-2}\theta)(\cos\theta-\cos\beta)d\theta},$$

onde $\Gamma(x) = \int_0^x t^{x-1}e^{-t}dt$ é a função gama.

Procurar por códigos esféricos com boa distância mínima e por empacotamentos de chapéus esféricos com melhores densidades são tarefas que nem sempre podem ser confundidas, apesar de suas similaridades. é possível demonstrar, segundo Rankin [33], que se $n+2$ pontos podem ser colocados na esfera S_{n-1}, então $2n$ podem ser colocados com a mesma distância mínima. Isto quer dizer que apesar da densidade do código esférico aumentar, sua distância mínima se mantém constante. Os primeiros a demonstrar esse fato, para $n=3$, foram Schüte e van der Waerden [36] em 1951. O resultado acima, além de estabelecer novos limitantes para códigos esféricos, traz essa sutileza entre densidade e distância mínima.

1.6.4 Empacotamento de Esferas em Espaços de Curvatura Constante

A definição de densidade de um empacotamento de chapéus esféricos é análoga a definição de densidade de empacotamento de esferas em $\mathbb{R}^n$: divide-se a área que os chapéus ocupam pela área total do espaço, seja ele uma esfera, o plano hiperbólico ou um cubo.

Segundo Böröczky, foram L. Fejes Tóth [48, 49] e Coxeter [13] que estenderam os problemas de empacotamento para espaços de curvatura constante. Tóth [48] e Coxeter [13] conjecturaram que a densidade de um empacotamento de esferas em um espaço de curvatura constante n-dimensional não deveria exceder a densidade de empacotamento de $n+1$ esferas tocando-se mutuamente. Rogers [35] demonstrou este fato para empacotamentos em esferas euclidianas e Böröczky o generalizou para todos os espaços de curvatura constante. Estes resultados possibitaram concluir que qualquer conjunto de círculos de igual raio no plano não pode exceder a densidade $\frac{\pi}{\sqrt{12}} = 0.9069...$ e em $\mathbb{R}^3$ esta densidade não pode passar 0.7797...

Este último limitante é maior que o limitante de Kepler $\frac{\pi}{\sqrt{18}} = 0.7404...$ Kepler conjecturou, em 1611, que a melhor maneira de arranjar esferas S^2 é aquela em que cada esfera tem doze outras esferas que a tocam. Quase quatrocentos anos depois, em 2003, uma prova foi apresentada por Hales [21]. Segundo Weisstein [51], a prova de Hales envolveu métodos da otimização global, programação linear e aritmética intervalar, além de códigos computacionais e arquivos de informação ocupando mais de 3 Gb de memória.

Capítulo 2

Assinatura de um Código de Grupo Cíclico

"Numbers measure size, groups measure symmetry."

M.A. Armstrong

Nste capítulo, discutimos a relação que há entre os códigos de grupo cíclico e subgrupos cíclicos de $\mathbb{Z}_M^n$ em $\mathbb{R}^{2n}$. Demonstramos que a dimensão e a cardinalidade destas constelações dependem da escolha do subgrupo a ser mergulhado e apresentamos uma condição necessária e suficiente, em termos destes grupos, para que o código minimize energia, relacionando com os resultados de Loeliger [30] sobre dimensão de códigos rotulados por grupos de matrizes ortogonais. Tais análises permitiram diminuir a quantidade de representações de $\mathbb{Z}_M$ relevantes na construção de códigos esféricos, facilitando a procura do melhor código de grupo cíclico em $\mathbb{R}^{2n}$ com M pontos.

2.1 Representações Matriciais de Grupos Cíclicos

Considere o grupo cíclico $\mathbb{Z}_M = \{0, 1, 2, \ldots, M-1\}$ munido da operação soma módulo M. Conforme dito no capítulo anterior, uma representação matricial de ordem n de $\mathbb{Z}_M$ é um homomorfismo h de $\mathbb{Z}_M$ no grupo das matrizes ortogonais reais de dimensão n, $\mathcal{O}(n, \mathbb{R})$, com a operação produto. Pretende-se construir códigos esféricos gerados por grupos cíclicos, de maneira

que cada ponto da constelação esteja associado a um único elemento do grupo. Esta operação, também chamada de rotulamento, deve ser, portanto, uma bijeção entre $\mathbb{Z}_M$ e a constelação. Isto implica que as representações que realmente nos interessarão são os isomorfismos de grupo entre $\mathbb{Z}_M$ e um subgrupo de $\mathcal{O}(n,\mathbb{R})$. Tais representações são chamadas representações fiéis de $\mathbb{Z}_M$. A teoria de representação de grupos é extensa. O leitor pode encontrar em [34], sob outro enfoque e de maneira mais ampla, um estudo das representações matriciais de grupo. No que concerne aos códigos esféricos, queremos saber quais condições uma representação de $\mathbb{Z}_M$ em $\mathcal{O}(n,\mathbb{R})$ deve satisfazer para ser fiel. Mais ainda, procuramos uma maneira de classificá-las.

Comecemos pelas representações de ordem 1. Há duas possibilidades para representar $\mathbb{Z}_M$ em matrizes ortogonais de ordem 1. Se $h:\mathbb{Z}_M\to\{-1,1\}$ é um homomorfismo, então $h(0)=1$, e $h(1)$ é 1 ou -1. No primeiro caso, segue que $h(m)=h(1)\dots h(1)=1$ e, portanto, h é a representação trivial. No segundo caso, temos $h(m)=h(1)\dots h(1)=h(1)^m=(-1)^m$, logo $1=h(0)=h(M)=(-1)^M$, o que se verifica somente quando M for par. É evidente que o único caso fiel de ordem 1 é $h:\mathbb{Z}_2\to\{-1,1\}$, com $h(1)=-1$.

Já as representações de ordem 2 são as rotações de ângulo $\frac{2\pi k_i}{M}$, com k_i um inteiro menor que M, ou as geradas pelas matrizes da forma

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix},$$

podendo aparecer -1 somente se M for par. As matrizes com ± 1 em suas entradas não dão representações fiéis, a menos que $M=2$. Assim, as representações de ordem 2, para $M\geq 3$, são somente as rotações.

Para as representações matriciais de ordem maior que dois, basta concatenar as representações de ordem 1 e 2 na diagonal da matriz geradora. Estes são todos os casos possíveis, uma vez que todo conjunto comutativo de matrizes ortogonais pode ser sempre reduzido a essa forma, segundo o teorema 1.3.2. Assim sendo, para determinar a forma geral de uma representação h de $\mathbb{Z}_M$ de ordem $N=2n_1+n_2+n_3$, basta saber onde ela leva o elemento $1\in\mathbb{Z}_M$. De fato, se $h(1)$ é a matriz $[R(\frac{2\pi k_1}{M}),\dots,R(\frac{2\pi k_{n_1}}{M}),\underbrace{1,\dots,1}_{n_2},\underbrace{-1,\dots,-1}_{n_3}]=$

$$\begin{pmatrix}
cos(\frac{2\pi k_1}{M}) & -sen(\frac{2\pi k_1}{M}) & & & & & & & & & \\
sen(\frac{2\pi k_1}{M}) & cos(\frac{2\pi k_1}{M}) & & & & & & & & & \\
& & \ddots & & & & & & & & \\
& & & cos(\frac{2\pi k_{n_1}}{M}) & -sen(\frac{2\pi k_{n_1}}{M}) & & & & & & \\
& & & sen(\frac{2\pi k_{n_1}}{M}) & cos(\frac{2\pi k_{n_1}}{M}) & & & & & & \\
& & & & & 1 & & & & & \\
& & & & & & \ddots & & & & \\
& & & & & & & 1 & & & \\
& & & & & & & & -1 & & \\
& & & & & & & & & \ddots & \\
& & & & & & & & & & -1
\end{pmatrix},$$

$h(m) = h(1 + \ldots + 1) = \underbrace{h(1) \ldots h(1)}_{\text{m vezes}} = [R(\frac{2\pi k_1}{M} m), \ldots, R(\frac{2\pi k_{n_1}}{M} m), 1, \ldots, 1, -1^m, \ldots, -1^m]$. A aplicação h pode ser vista como composta de duas aplicações:

$$f : m \in \mathbb{Z}_M \rightarrow m(k_1, \ldots, k_{n_1}) \in {\mathbb{Z}_M}^{n_1} \text{ e}$$

$$g : m(k_1, \ldots, k_{n_1}) \in \langle (k_1, \ldots, k_{n_1}) \rangle \rightarrow [R(\frac{2\pi}{M})^{mk_1}, \ldots, R(\frac{2\pi}{M})^{mk_{n_1}}, 1, \ldots, 1, -1^m, \ldots, -1^m],$$

conforme ilustra o diagrama

$$\begin{array}{ccc}
\mathbb{Z}_M & \xrightarrow{\quad f \quad} & \langle (k_1, \ldots, k_{n_1}) \rangle \\
& \searrow^{h} & \downarrow g \\
& & \left\langle [R(\frac{2\pi k_1}{M}), \ldots, R(\frac{2\pi k_{n_1}}{M}), 1, \ldots, 1, -1, \ldots, -1] \right\rangle,
\end{array}$$

onde $\langle a \rangle$ denota o subgrupo cíclico gerado por a.

Note que h ser uma bijeção é equivalente a f ser também. Mas f ser uma bijeção equivale a $\langle (k_1, \ldots, k_n) \rangle$ ter cardinalidade M. A próxima proposição estabelece as condições necessárias e suficientes para a cardinalidade de $\langle (k_1, \ldots, k_{n_1}) \rangle$ ser M, em função dos índices de rotação k_i. Ela pode ser encontrada na versão unidimensional em [20].

Proposição 2.1.1 *A cardinalidade de $\langle (k_1, \ldots, k_n) \rangle$ é M em $(\mathbb{Z}_M)^n$ se, e somente se, o máximo divisor comum $MDC(k_1, \ldots, k_n, M)$ entre $k_1, \ldots, k_n$ e M é 1.*

Demonstração : Se $MDC(k_1, \ldots, k_n, M) = 1$, do algoritmo de Euclides segue que existem inteiros $h_1, \ldots, h_n$ e h_{n+1} satisfazendo $h_1k_1 + \ldots + h_nk_n + h_{n+1}M = 1$. Além disso, se m é a cardinalidade de $\langle(k_1, \ldots, k_n)\rangle$, existem inteiros g_i´s tais que $mk_i = g_iM$. Assim,

$$m = m(\sum_{i=1}^{n} k_ih_i + h_{n+1}M) = \sum_{i=1}^{n} mk_ih_i + mh_{n+1}M = \sum_{i=1}^{n} g_iMh_i + mh_{n+1}M.$$

Portanto, $m = (\sum_{i=1}^{n} g_ih_i + mh_{n+1})M$ é um múltiplo de M. Mas $M(k_1, \ldots, k_n) = 0$ em $\mathbb{Z}_M^n$, logo $m \leq M$ e $m = M$.

Reciprocamente, considere $m = \frac{M}{MDC(k_1,\ldots,k_n,M)}$. Segue que $mk_i = \frac{Mk_i}{MDC(k_1,\ldots,k_n,M)} = 0\ modM$. Como M é a cardinalidade de $\langle(k_1, \ldots, k_n)\rangle$, temos $M \leq m$. Portanto $m = M$ e, consequentemente, $MDC(k_1, \ldots, k_n, M) = 1$. ■

Como os blocos de ordem um não-alternantes não contam na ordem do grupo de matrizes, resta-nos analisar a ordem das matrizes do tipo $[R(\frac{2\pi k_1}{M}), \ldots, R(\frac{2\pi k_{n_1}}{M}), -1, \ldots, -1]$ em relação aos seus índices de rotação.

Note que, como conjunto, o grupo cíclico $\langle[R(\frac{2\pi k_1}{M}), \ldots, R(\frac{2\pi k_{n_1}}{M}), -1, \ldots, -1]\rangle$ é a união de

$$\mathcal{B} = \{[R^{2k}(\frac{2\pi k_1}{M}), \ldots, R^{2k}(\frac{2\pi k_{n_1}}{M}), 1, \ldots, 1]; k \in \mathbb{Z}\}$$

com

$$\{[R^{2k+1}(\frac{2\pi k_1}{M}), \ldots, R^{2k+1}(\frac{2\pi k_{n_1}}{M}), -1, \ldots, -1]; k \in \mathbb{Z}\}.$$

Sendo que este último é

$$\{[R(\frac{2\pi k_1}{M}), \ldots, R(\frac{2\pi k_{n_1}}{M}), -1, \ldots, -1]\mathcal{B}.$$

Portanto a ordem $[R(\frac{2\pi k_1}{M}), \ldots, R(\frac{2\pi k_{n_1}}{M}), -1, \ldots, -1]$ é duas vezes a cardinalidade de $\mathcal{B}$. Este último, da proposição 2.1.1, tem cardinalidade $M/2$ se, e somente se, $MDC(k_1, \ldots, k_{n_1}, M/2) = 1$. Logo, concluímos:

Corolário 2.1.1 *O homomorfismo*

$$\psi : l \in \mathbb{Z}_M \rightarrow [R(\frac{2\pi k_1}{M}), \ldots, R(\frac{2\pi k_{n_1}}{M}), 1, \ldots, 1]^l$$

é bijetor se, e somente se, $MDC(k_1, \ldots, k_{n_1}, M) = 1$.

Corolário 2.1.2 *O homomorfismo*

$$\phi : l \in \mathbb{Z}_M \rightarrow [R(\frac{2\pi k_1}{M}), \ldots, R(\frac{2\pi k_{n_1}}{M}), 1, \ldots, 1, -1^m, \ldots, -1^m]^l, \quad \textit{para } M \textit{ par,}$$

é bijetor se, e somente se, $MDC(k_1, \ldots, k_{n_1}, M/2) = 1$.

Uma representação do grupo cíclico $\mathbb{Z}_M$ pode se dar também partindo de uma matriz ortogonal A tal que A^M é a matriz identidade e M é o menor inteiro satisfazendo esta propriedade. A representação h de $\mathbb{Z}_M$ de mesma ordem que A é direta, basta tomar $h(1) = A$. Usando o teorema 1.3.2, descobre-se quem são os auto espaços de A e qual é a matriz ortogonal em formato de blocos equivalente a A. Em virtude de sua fácil manipulação e de sua direta conexão com os subgrupos cíclicos sobre $\mathbb{Z}_M$, consideraremos as representações sempre nesta forma. Isto conclui o problema da representação matricial fiel de um grupo cíclico e de uma forma normal para elas.

2.2 Códigos de Grupo Cíclico

Uma vez entendido o problema da representação fiel de um grupo cíclico, estudemos as constelações de sinais com simetrias cíclicas. Dada uma representação matricial h de ordem N do grupo cíclico $\mathbb{Z}_M$ satisfazendo $h(1) = \mathcal{R}$ e um vetor x_0 unitário de $\mathbb{R}^N$, chamaremos de código de grupo cíclico o conjunto

$$\mathcal{X} = \{h(l)x_0\}_{l=0}^{M-1} = \{\mathcal{R}^l x_0\}_{l=0}^{M-1}.$$

A proposição 2.1.1 traz duas consequências importantes na construção de um código de grupo cíclico com M pontos: os índices de rotação k_i devem ter simultaneamente máximo divisor comum com M igual a um, o que exclui algumas representações; todo código de grupo cíclico é completamente determinado por um elemento de $\mathbb{Z}_M^n$, vetor cujas entradas são os índices de rotação dos blocos de ordem dois da matriz geradora, a menos dos blocos de ordem 1, e um vetor inicial. Considere o vetor composto pelos índices de rotação dos blocos de ordem dois e os blocos de ordem 1 de $\mathcal{R}$. A este vetor daremos o nome de *assinatura do código de grupo cíclico* $\mathcal{X}$. Em geral, as assinaturas têm a forma $(k_1, \ldots, k_n)$ ou $(k_1, \ldots, k_n, -1)$, conforme os lemas que seguirão.

Da definição proposta por Slepian, um código de grupo em $\mathbb{R}^N$ deve ser um conjunto de geradores para o espaço. Certas assinaturas, seja qual for o vetor inicial, impedem a construção de um código de grupo pois acabam restringindo o código a um hiperplano do espaço. Os lemas abaixo mostram que algumas assinaturas não geram um código de grupo cíclico.

Sejam $\mathcal{R}$ a matriz $[R(\frac{2\pi k_1}{M}), \ldots, R(\frac{2\pi k_{n_1}}{M}), \underbrace{1, \ldots, 1}_{n_2}, \underbrace{-1, \ldots, -1}_{n_3}]$ e $X_0 \in \mathbb{R}^N$ o vetor inicial $(x_1, \ldots, x_N) \in \mathbb{R}^N$. Seja $\mathcal{X} = \{\mathcal{R}^l X_0\}_{l=1}^M$ a órbita do grupo cíclico de matrizes $\langle \mathcal{R} \rangle$ começando pelo ponto X_0. Denotamos a dimensão do espaço vetorial gerado por $\mathcal{X}$ por $dim(\mathcal{X})$. Valem os seguintes lemas:

Lema 2.2.1 *Se $n_2 \neq 0$, então existe uma translação T tal que $dim(T(\mathcal{X})) \leq N - n_2$. Além disso, $n_2 \neq 0$ se, e somente se $\sum_{x \in \mathcal{X}} x \neq 0$.*

Demonstração : Observe que se $x_i = 0$ para algum $i = 2n_1+1, \ldots, N$, a i-ésima coordenada de todos os pontos do código serão nulas, portanto $dim(\mathcal{X})$ será menor que N. Portanto suporemos, a partir de agora, que $x_i \neq 0$, para $i = 2n_1 + 1, \ldots, N$.

Considere a translação $T : \mathbb{R}^N \to \mathbb{R}^N$ dada por

$$T(y) = y - (\underbrace{0, \ldots, 0}_{2n_1}, x_{2n_1+1}, \ldots, x_{n_2}, \underbrace{0, \ldots, 0}_{n_3}).$$

Como todos os pontos de $\mathcal{X}$ tem da $(2n_1+1)$-ésima coordenada até a $(2n_1+n_2)$-ésima coordenada igual a do vetor inicial, a aplicação T apenas as anula. O conjunto resultante $T(\mathcal{X})$, portanto, está contido em $\mathbb{R}^{2n_1} \times \underbrace{0 \times \ldots \times 0}_{n_2} \times \mathbb{R}^{n_3}$, conjunto cuja dimensão é $N - n_2$. Consequentemente, $dim(T(\mathcal{X})) \leq N - n_2$. Provemos agora que $n_2 \neq 0$ é equivalente, no caso das órbitas de grupo cíclicos, a constelação não minimizar energia. Observe primeiro que se existir algum bloco unidimensional alternante, a cardinalidade M do código é par. Se x_n é a coordenada do vetor inicial relativa a este bloco alternante, vê-se que

$$\sum_{l=1}^{M} (-1)^l x_n = x_n \frac{M}{2}(1 - 1) = 0.$$

Portanto as coordenadas relativas aos blocos alternantes sempre se anulam quando somadas. Quanto às coordenadas relativas aos blocos de rotação, mesmo comportamento se dá. De fato, se R é uma matriz de rotação 2×2 do tipo

$$\begin{pmatrix} cos(\frac{2\pi k}{M}) & -sen(\frac{2\pi k}{M}) \\ sen(\frac{2\pi k}{M}) & cos(\frac{2\pi k}{M}) \end{pmatrix},$$

então $S_M = R + R^2 + \ldots + R^{M-1} + Id$, onde Id é a matriz identidade 2×2, satisfaz $RS_M = S_M$. Então $(R - Id)S_M = 0$ e a imagem do operador linear cuja matriz é S_M está contida no núcleo da transformação $R - Id$. Mas, se x é tal que $(R - Id)x = 0$, então x é ponto fixo da rotação R. Como o único ponto fixo de uma rotação 2-dimensional é a origem, o núcleo de $R - Id$ é somente $\{(0,0)\}$ e o operador cuja matriz é S_M é o nulo. Logo $S_M = 0$ e, consequentemente, as coordenadas dos pontos de $\mathcal{X}$, relativas aos blocos de rotação, se anulam quando somadas. Portanto, concluímos que as únicas coordenadas que cooperam para que o momento de inércia da constelação seja não nulo são aquelas relativas aos blocos unidimensionais não alternantes. Suas somas se anularão se, e somente se, elas forem nulas, o que contradiz as hipóteses assumidas no começo da demonstração. Assim, o problema somente se resolve quando $n_2 = 0$. ■

Em vista do resultado que acabamos de demonstrar,*a partir de agora consideraremos* $n_2 = 0$.

Lema 2.2.2 *Se* $n_3 > 1$, *então* $dim(\mathcal{X}) \leq N - n_3 + 1$.

Demonstração : Assumiremos que todas as coordenadas x_i, do vetor inicial, com $i = 2n_1 + 1, \ldots, N$ são não nulas, do contrário a dimensão de $\mathcal{X}$ será menor que N, diretamente. Se $n_3 \neq 0$ e $Y = (Y_1, \ldots, Y_N) \in \mathbb{R}^N$, é fácil ver que os pontos de $\mathcal{X}$ moram simultaneamente nos planos

$$x_{2n_1+i+1}Y_{2n_1+i} - x_{2n_1+i}Y_{2n_1+i+1} = 0,$$

onde $1 \leq i \leq n_3 - 1$ e x_i são as coordenadas do vetor inicial. Equivalentemente, $\mathcal{X}$ está contido no núcleo da transformação linear $T : Y \in \mathbb{R}^N \to \mathbb{R}^{n_3-1}$ definida por

$$T(Y) = (x_{2n_1+2}Y_{2n_1+1} - x_{2n_1+1}Y_{2n_1+2}, \ldots, x_{2n_1+n_3}Y_{2n_1+n_3-1} - x_{2n_1+n_3-1}Y_{2n_1+n_3}).$$

Veja que a matriz (a_{ij}) de T,

$$\begin{pmatrix} 0 & \ldots & 0 & x_{2n_1+2} & -x_{2n_1+1} & 0 & & \\ & & 0 & 0 & x_{2n_1+3} & -x_{2n_1+2} & 0 & \\ & & & \ddots & \ddots & \ddots & \ddots & \\ & & & 0 & 0 & x_{2n_1+n_3-1} & -x_{2n_1+n_3-2} & 0 \\ & & & & 0 & 0 & x_{2n_1+n_3} & -x_{2n_1+n_3-1} \end{pmatrix}_{(n_3-1)\times N},$$

possui uma submatriz $(n_3-1)\times(n_3-1)$, formada pelas colunas a_{ij_0}, com $j_0 = 2n_1+1, \ldots, N-1$, com determinante igual a $x_{2n_1+2} \ldots . x_{2n_1+n_3}$, que é não nulo. Portanto o posto dessa matriz é

$n_3 - 1$ e a imagem de T tem dimensão $n_3 - 1$. Assim o núcleo de T, onde mora $\mathcal{X}$, tem dimensão $N - n_3 + 1$. Consequentemente, $dim(\mathcal{X}) \leq N - n_3 + 1$. ■

A partir de agora, *consideraremos* $n_3 = 0$ *ou* 1, se a dimensão do espaço for par ou ímpar, respectivamente. Além disso, para facilitar as demonstrações, suporemos o vetor inicial igual a

$$X_0 = (x_1, 0, x_3, 0, \ldots, x_{2n_1-1}, 0) \text{ ou} (x_1, 0, x_3, 0, \ldots, x_{2n_1-1}, 0, x_{2n_1+1}).$$

Na verdade, esta suposição não oferece uma grande mudança no código pois o código obtido será isométrico ao original. De fato, se $\phi_i = Arctang(\frac{x_{2i}}{x_{2i-1}})$ e

$$R(2\pi - \phi) = \begin{pmatrix} cos(2\pi - \phi) & -sen(2\pi - \phi) \\ sen(2\pi - \phi) & cos(2\pi - \phi) \end{pmatrix},$$

considere a matriz ortogonal, cuja diagonal é formada pelas rotações 2-dimensionais acima descritas, $R = [R(2\pi - \phi_1), \ldots, R(2\pi - \phi_{n_1})]$, se N for par, e $R = [R(2\pi - \phi_1), \ldots, R(2\pi - \phi_{n_1}), 1]$, se N for ímpar. Note que $R(2\pi - \phi_i)(x_{2i-1}, x_{2i})^t = ((x_{2i-1}^2 + x_{2i}^2)^{1/2}, 0)$.

Logo,

$$\widetilde{\mathcal{X}} = R(\mathcal{X}) = \{R\mathcal{R}^l X_0\}_{l=1}^M = \{\mathcal{R}^l R X_0\}_{l=1}^M = \{\mathcal{R}^l \widetilde{X_0}\}_{l=1}^M,$$

onde

$$\widetilde{X_0} = ((x_1^2 + x_2^2)^{1/2}, 0, \ldots, (x_{2n_1-1}^2 + x_{2n_1}^2)^{1/2}, 0), \; ou$$

$$((x_1^2 + x_2^2)^{1/2}, 0, \ldots, (x_{2n_1-1}^2 + x_{2n_1}^2)^{1/2}, 0, x_{2n_1+1}).$$

Por R ser uma isometria euclidiana, $\widetilde{\mathcal{X}} = R(\mathcal{X})$ e $\mathcal{X}$ são códigos equivalentes.

Lema 2.2.3 *Se* $k_1 = \ldots = k_m = k$, *então* $dim(\mathcal{X}) \leq N - 2(m-1)$.

Demonstração : Denote $\{e_i\}_{i=1}^N$ a base canônica de $\mathbb{R}^N$. Das observações feitas sobre o vetor inicial, segue que $\mathcal{R}^l X_0$ é

$$\sum_{i=1}^{m} x_{2i-1}(cos(\frac{2\pi kl}{M})e_{2i-1} + sen(\frac{2\pi kl}{M})e_{2i})) + \sum_{i=m+1}^{N/2} x_{2i-1}(cos(\frac{2\pi k_i l}{M})e_{2i-1} + sen(\frac{2\pi k_i l}{M})e_{2i})),$$

mais o termo alternante $(-1)^l x_N e_N$, se a dimensão for ímpar.

Assim, se $Y = (Y_1, \ldots, Y_N) \in \mathcal{X}$ e $1 \leq i \leq m-1$, valem as igualdades:

$$x_{2(i+1)-1}Y_{2i-1} - x_{2i-1}Y_{2(i+1)-1} = 0$$

$$x_{2(i+1)-1}Y_{2i} - x_{2i-1}Y_{2(i+1)} = 0$$

Isto quer dizer que $\mathcal{X}$ está contido no núcleo da transformação linear $T : \mathbb{R}^N \to \mathbb{R}^{2(m-1)}$, onde $T(y_1, \ldots, y_N)$ é

$$(x_3Y_1 - x_1Y_3, x_3Y_2 - x_1Y_4, \ldots, x_{2m-1}Y_{2m-4} - x_{2m-3}Y_{2m-1}, x_{2m-1}Y_{2m-2} - x_{2m-3}Y_{2m}).$$

As $2(m-1)$ primeiras colunas da matriz de T formam uma matriz quadrada triangular superior cuja diagonal é $(x_3, x_3, x_5, x_5, \ldots, x_{2m-1}, x_{2m-1})$. Supondo não nulas as m primeiras entradas ímpares do vetor inicial, do contrário a constelação não estaria em $\mathbb{R}^N$ desde o princípio, tal submatriz tem determinante não nulo e a imagem de T tem dimensão $2(m-1)$. Logo, a dimensão do núcleo de T é $N - 2(m-1)$ e $dim(\mathcal{X}) \leq N - 2(m-1)$. ■

Assim, podemos concluir o seguinte teorema sobre códigos de grupo cíclico:

Teorema 2.2.1 *Seja $\mathcal{X}$ um código de grupo cíclico rotulado por $\mathbb{Z}_M$ em $\mathbb{R}^N$ com assinatura $(k_1, \ldots, k_m)$. Então $m = \frac{N}{2}$, se N for par, ou $m = \lfloor \frac{N}{2} \rfloor + 1$, se N for ímpar. Neste último caso, $k_m = -1$. Além disso, os inteiros $k_1, \ldots, k_{\lfloor \frac{N}{2} \rfloor}$ são positivos e distintos com $mdc(k_1, \ldots, k_{\lfloor \frac{N}{2} \rfloor}, M) = 1$, se N é par, ou, $mdc(k_1, \ldots, k_{\lfloor \frac{N}{2} \rfloor}, M/2) = 1$, se N é ímpar.*

2.3 Códigos de Grupo Cíclico Equivalentes

Sob certas condições, códigos de grupo cíclico com assinaturas diferentes dão o mesmo código ou códigos equivalentes. Esta seção discute alguns destes casos.

Antes de tudo, observe que um mesmo grupo pode possuir vários geradores. Assim, duas assinaturas podem gerar o mesmo grupo cíclico e, portanto, o mesmo grupo de matrizes. Por isso, apresentamos a proposição abaixo sobre geradores e automorfismos de grupos cíclicos. Esta proposição é um apanhado de pequenos resultados conhecidos em álgebra de grupos, mas que, até o momento, não foi encontrada na presente forma.

Proposição 2.3.1 *Seja $a \in \mathbb{Z}_M^n$ com ordem M. Um homomorfismo $\psi : \langle a \rangle \subset \mathbb{Z}_M^n \to \langle a \rangle$ é um automorfismo de $\langle a \rangle$ se, e somente se, $\psi(a) = ma$ para algum inteiro m co-primo com M, ie, a ordem de m em $\mathbb{Z}_M$ é M.*

Demonstração : Suponha ψ um automorfismo de $\langle a \rangle$, e tome d tal que $\psi(a) = da$. Suponha que a ordem de d, $o(d)$, é menor que M. Note que $o(d)d = 0$ em $\mathbb{Z}_M$. Logo, $\psi(o(d)a) =$

$o(d)da = 0$ e a imagem de ψ terá no máximo $o(d)$ elementos, o que é uma contradição, uma vez que ψ é um automorfismo. Assim, d é co-primo com M. Reciprocamente, é claro que ψ é um homomorfismo de $\langle a \rangle$. Suponha que, para algum k, $\psi(ka) = kma = 0$. Como a ordem de a é M, $km = 0\ mod\ M$, o que implica k ser também um mútiplo de M, pois m é co-primo com M. Assim, ψ é homomorfismo injetor em $\langle a \rangle$. ■

Isto implica que duas assinaturas que diferem por um inteiro m, co-primo com a ordem do grupo, geram o mesmo grupo cíclico e, por conseguinte, o mesmo grupo de matrizes geradoras do código. Portanto os códigos são iguais, se escolhidos os mesmos vetores iniciais. Esta observação bem como outras equivalências estão condensadas na proposição abaixo.

Proposição 2.3.2 *1. Se $k_i = m_i(modM)$, então os códigos de grupo cíclico cujas assinaturas são $(k_1, \ldots, k_i, \ldots, k_\nu)$ e $(k_1, \ldots, m_i, \ldots, k_\nu)$ serão os mesmos se os vetores iniciais também forem.*

2. Se $k_i = -m_i(modM)$, então os códigos de grupos cíclicos com M pontos e assinaturas $(k_1, \ldots, k_i, \ldots, k_\nu)$ e $(k_1, \ldots, m_i, \ldots, k_\nu)$ são equivalentes para o mesmo vetor inicial.

3. Se m é co-primo com M, então os códigos de grupo cíclico com assinaturas $(k_1, \ldots, k_\nu)$ e $m(k_1, \ldots, k_\nu)$, vistas como elementos de $\mathbb{Z}_M^\nu$, são os mesmos, considerando o mesmo vetor inicial.

4. Se para duas matrizes ortogonais A e B existir uma outra matriz ortogonal Q tal que $A = QBQ^T$, então os códigos gerados por A e B, juntamente com os vetores iniciais x_0 e $Q^T x_0$, respectivamente, são equivalentes.

Demonstração : Se $k_i = m_i(modM)$, então $cos(\frac{2\pi k_i}{M}) = cos(\frac{2\pi m_i}{M})$ e $sen(\frac{2\pi k_i}{M}) = sen(\frac{2\pi m_i}{M})$. Portanto, as matrizes geradoras dos códigos são iguais e também suas órbitas, o que conclui o primeiro item .

Para demonstrar o segundo item, considere primeiro o caso em dimensão dois. Se $q = (q_1, 0)$ é o vetor inicial e $R(\frac{2\pi k_i}{M})$ a rotação horária de ângulo $\frac{2\pi k_i}{M}$, temos que $R(\frac{2\pi k_i}{M})q = R(\frac{-m_i 2\pi}{M})q = (cos(\frac{-m_i 2\pi}{M}), sen(\frac{-m_i 2\pi}{M})) = (cos(\frac{m_i 2\pi}{M}), -sen(\frac{m_i 2\pi}{M}))$. Considere então $\mathcal{R}_x$ a matriz da reflexão pelo eixo x, então $\mathcal{R}_x(a, b) = (a, -b)$ e

$$\mathcal{R}_x R(\frac{2\pi l k_i}{M})q = \mathcal{R}_x(cos(\frac{m_i l 2\pi}{M}), -sen(\frac{m_i l 2\pi}{M})) = (cos(\frac{m_i l 2\pi}{M}), sen(\frac{m_i l 2\pi}{M})),$$

onde $1 \leq l \leq M$. Logo, os dois códigos são equivalentes.

Para fazer o caso geral, basta fazer o processo análogo ao 2-dimensional utilizando a matriz diagonal

$$[1, \ldots, 1, \mathcal{R}_x, 1, \ldots, 1],$$

de maneira que a reflexão planar $\mathcal{R}_x$ esteja na posição $2i-1$ e $2i$ e a ordem da matriz seja a mesma que a da matriz que gera o código.

O terceiro caso segue das considerações prévias a proposição e o quarto caso é consequência direta da definição de matrizes equivalentes. ■

Matrizes que satisfazem a condição 3 do lema anterior são chamadas ortogonalmente similares. Dois códigos equivalentes não possuem necessariamente matrizes geradoras ortogonalmente similares, os códigos do ítem 2 do lema estão entre estes.

Uma consequência importante do item 2, do lema anterior, é que para estudar os códigos de grupo cíclico com M pontos, basta considerar assinaturas $(k_1, \ldots, k_m)$ com $k_i \leq \lfloor \frac{M}{2} \rfloor$, onde $\lfloor x \rfloor$ denota o maior inteiro menor que x, além das restrições feitas no teorema 2.3.2.

2.3.1 Os códigos de grupo cíclico em $\mathbb{R}^4$ com 13 pontos: um exemplo

Mostraremos, usando os resultados anteriores, que as únicas assinaturas relevantes para códigos de grupo cíclico são $(1,2)$, $(1,3)$ e $(1,5)$. Note primeiro que, por 13 ser primo, todos os elementos não nulos de $\mathbb{Z}_{13}$ são invertíveis. Assim, toda assinatura (a,b) é igual a $a(1,a^{-1}b)$, com a invertível. Logo, podemos trocar (a,b) por $(1,a^{-1}b)$ pois os códigos gerados serão iguais. Portanto, nos restringimos às assinaturas $(1,2)$, $(1,3)$, $(1,4)$, $(1,5)$, $(1,6)$, $(1,7)$, $(1,8)$, $(1,9)$, $(1,10)$, $(1,11)$ e $(1,12)$.

Mas $2 = -11 \ mod\ 13$, $3 = -10 \ mod\ 13$, $4 = -9 \ mod\ 13$, $5 = -8 \ mod\ 13$ e $6 = -7 \ mod\ 13$. Logo, retirando as assinaturas que dão códigos isométricos, nos restam $(1,2)$, $(1,3)$, $(1,4)$, $(1,5)$ e $(1,6)$.

Entretanto, $2(1,6) = (2,12)$ e $(2,12)$ é isométrico a $(2,1)$ que, por sua vez, é isométrico a $(1,2)$. Da mesma maneira, $3(1,4) = (3,12)$ é isométrico a $(3,1)$ e $(1,3)$, restando, portanto, as assinaturas $(1,2)$, $(1,3)$ e $(1,5)$.

Cálculos computacionais mostram que tais assinaturas e seus vetores iniciais ótimos são

$$(1,2) \ \text{ e } \ (\sqrt{0.1460}, 0, \sqrt{0.8540}, 0);$$

$$(1,3) \text{ e } (\sqrt{0.3815}, 0, \sqrt{0.6185}, 0);$$

$$(1,5) \text{ e } (\sqrt{0.5}, 0, \sqrt{0.5}, 0);$$

Suas distâncias mínimas ótimas são 0.878173, 1.0841 e 1.14516, respectivamente. Portanto, o melhor código cíclico em dimensão 4 com 13 pontos é aquele com assinatura $(1,5)$ e vetor inicial $(\sqrt{0.5}, 0, \sqrt{0.5}, 0)$.

Retornaremos a esta questão, discutindo também alguns algoritmos que procuram o vetor inicial ótimo para outras quantidades de pontos, no último capítulo.

2.4 Os códigos Simplex e Biortogonal

Duas classes de códigos geradas por matrizes cíclicas são amplamente conhecidas: os códigos simplex e biortogonal. Esses códigos possuem matrizes geradoras bastante simples e distância mínima ótima. Mostraremos este último fato e apresentaremos as suas assinaturas, como aplicação da seção anterior.

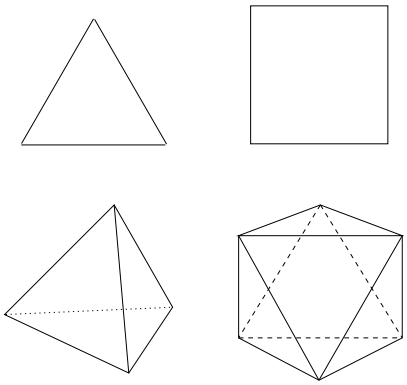


Figura 2.1: Os códigos simplex e biortogonal em dimensão dois e três.

2.4.1 O Código Simplex

Considere $\mathcal{S}_n$ o conjunto dos pontos $(1, \ldots, 1, -n)$ em $\mathbb{R}^{n+1}$ e seus deslocamentos cíclicos, ou melhor, a órbita de $(1, \ldots, 1, -n)$ pelo grupo gerado pela matriz

$$S = \begin{pmatrix} 0 & \dots & 0 & 1 \\ & & & 0 \\ & Id_n & & \vdots \\ & & & 0 \end{pmatrix},$$

onde Id_n é a matriz identidade $n \times n$. Chamaremos $\mathcal{S}_n$ de *código simplex*. Da sua definição segue que, se $x = (x_1, \dots, x_{n+1}) \in \{R^l(1, \dots, 1, -n)\}_{l=1}^{n+1}$, então $x_1 + \dots + x_{n+1} = 0$ e $x_1^2 + \dots + x_{n+1}^2 = n + n^2$. Logo, $\mathcal{S}_n$ é um código esférico que mora em um hiperplano de $\mathbb{R}^{n+1}$, portanto em $\mathbb{R}^n$. É de fácil demonstração que $\mathcal{S}_n$ é um conjunto de geradores para $\mathbb{R}^n$, assim o simplex é um código com $M = n+1$ pontos em $\mathbb{R}^n$ com distância mínima ao quadrado $\frac{2(1+n)^2}{n^2+n} = \frac{2(1+n)}{n}$. O limitante de Rankin, teorema 1.6.5, assegura que, na esfera S^{n-1} em $\mathbb{R}^n$, o máximo que se consegue com distância mínima ao quadrado $\frac{2(1+n)}{n}$ é colocar $n+1$ pontos. Portanto, o código simplex é o melhor código esférico em $\mathbb{R}^n$ com $n+1$ pontos e distância mínima ao quadrado $\frac{2(1+n)}{n}$.

A assinatura do código Simplex

Seja $det(S - \lambda Id_{n+1})$ o polinômio característico de S. Usando o método de Laplace, vê-se que $det(S - \lambda Id_{n+1})$ é igual a

$$-\lambda \begin{vmatrix} -\lambda & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & -\lambda \end{vmatrix} + (-1)^{n+2} \begin{vmatrix} 1 & \lambda & & 0 \\ & \ddots & \ddots & \\ & & \ddots & \lambda \\ 0 & & & 1 \end{vmatrix} = (-1)^{n+1}(\lambda^{n+1} - 1).$$

Assim, os auto-valores de S são as $(n+1)$-raízes da unidade, ie, $\lambda_k = cos(\frac{2k\pi}{n+1}) + isen(\frac{2k\pi}{n+1})$, onde $k = 0, \dots, n$. Da demonstração do teorema 1.3.2, S é equivalente a uma matriz ortogonal diagonal $\mathcal{R}$. Observe que $\lambda_0 = 1$ indica a existência de um bloco unidimensional em $\mathcal{R}$ não alternante. Ainda, se n é ímpar, $\lambda_{\frac{n+1}{2}} = -1$ indica um outro bloco unidimensional, mas alternante. Note ainda que, para a construção de $\mathcal{R}$, é preciso considerar apenas a primeira metade dos auto-valores, uma vez que os outros são conjugados e devem gerar blocos de rotação similares. Então temos os blocos $R(\lambda_1), \dots, R(\lambda_{\frac{n}{2}} - 1), R(\lambda_{\frac{n}{2}})$ e 1, se n é par, ou $R(\lambda_1), \dots, R(\lambda_{\lfloor \frac{n}{2} \rfloor}), -1$ e 1, se n é ímpar, onde $R(\lambda)$ é a rotação horária de ângulo λ.

Para obter qual é o novo vetor inicial, devemos construir a matriz de mudança de base formada pelos auto-vetores de S. O auto-vetor X_k, associado a λ_k, é definido pela expressão

$SX_k = \lambda_k X_k$. Se $X_k = (X_k^1, \ldots, X_k^{n+1})$, essa expressão fica

$$\begin{cases} X_k^{n+1} &= \lambda_k X_k^1 \\ X_k^1 &= \lambda_k X_k^2 \\ & \vdots \\ X_k^n &= \lambda_k X_k^{n+1} \end{cases}.$$

Assim $X_k^{n+1} = \lambda_k X_k^1 = \lambda_k^2 X_k^2 = \ldots = \lambda_k^{n+1} X_k^{n+1}$ e

$$X_k = X_k^{n+1}(\lambda_k^n, \lambda_k^{n-1}, \ldots, \lambda_k^2, \lambda_k, 1).$$

Assumindo que $|X_k| = 1$, temos $|X_k^{n+1}| = \frac{1}{\sqrt{n+1}}$. Logo $X_k = \frac{1}{\sqrt{n+1}}(\lambda_k^n, \lambda_k^{n-1}, \ldots, \lambda_k, 1)$. Se $\mathcal{R}$ é a matriz de blocos equivalente a S, então Q, cujas colunas são as partes real e imaginária dos auto-vetores intercaladas, satisfaz $S = Q\mathcal{R}Q^T$. Assim, se n é par, o novo vetor inicial $Q^T(1, \ldots, 1, -n)^T$ é

$$\frac{1}{\sqrt{n+1}}(\sum_{j=1}^{n} Re(\lambda_1^j) - nRe(\lambda_k^{n+1}), \sum_{j=1}^{n} Im(\lambda_1^j) - nIm(\lambda_k^{n+1}), \ldots$$

$$\ldots, \sum_{j=1}^{n} Re(\lambda_{n/2}^j) - nRe(\lambda_k^{n+1}), \sum_{j=1}^{n} Im(\lambda_{n/2}^j) - nIm(\lambda_k^{n+1}), \sum_{j=1}^{n} 1 - n).$$

Como $Re(\lambda_k^{n+1}) + iIm(\lambda_k^{n+1}) = 1$ e $\lambda_k = e^{(\frac{2\pi k}{n+1})i} = cos(\frac{2\pi k}{n+1}) + isen(\frac{2\pi k}{n+1})$,

$$\sum_{j=1}^{n+1} \lambda_k^j = \sum_{j=1}^{n+1} [Re(\lambda_k^j) + iIm(\lambda_k^j)] = \sum_{j=1}^{n+1} Re(\lambda_k^j) + i \sum_{j=1}^{n+1} Im(\lambda_k^j) = 0,$$

segue que $\sum_{j=1}^{n} Re(\lambda_k^j) - 1 = 0$ *e* $\sum_{j=1}^{n} Im(\lambda_k^j) = 0$. Portanto, $Q^T(1, \ldots, 1, -n)^T = -(n+1)^{1/2}(1, 0, 1, 0, \ldots, 1, 0, 0)$.

Se n é ímpar, o auto-vetor correspondente ao auto-valor -1 é $(-1, 1, \ldots, -1, 1) \in \mathbb{R}^{n+1}$. Assim, a entrada do vetor inicial corresponde a multiplicação da $(\lfloor \frac{n}{2} \rfloor + 1)$-ésima linha de Q^T com $(1, \ldots, 1, -n)$ dá $(-1-n)$ dividido por $(1+n)^{1/2}$, ou seja, $-(1+n)^{1/2}$, o mesmo valor que no caso par.

Note que a última coordenada do vetor inicial, correspondente ao bloco unidimensional não alternante, é nula. Então, após alterar o tamanho do vetor inicial para torná-lo unitário, obtemos uma nova representação da família Simplex, conforme teorema abaixo.

Teorema 2.4.1 *Considere $\mathcal{X}$ o código de grupo cíclico com $n+1$ pontos em $\mathbb{R}^n$ com assinatura $(1, 2, \ldots, \frac{n}{2})$ e vetor inicial $\sqrt{\frac{2}{n}}(1, 0, 1, 0, \ldots, 1, 0)$, se n for par, e $(1, 2, \ldots, \lfloor \frac{n}{2} \rfloor, -1)$ e vetor inicial $\sqrt{\frac{2}{n+1}}(1, 0, 1, 0, \ldots, 1, 0, 1)$, se n for ímpar. Então $\mathcal{X}$ é o código Simplex em $\mathbb{R}^n$.*

2.4.2 O Código Biortogonal

Considere $\mathcal{B}_n$ o conjunto formado por $(0, \ldots, 0, \pm 1)$ e seus deslocamentos cíclicos em $\mathbb{R}^n$. É fácil ver que $\mathcal{B}_n$ é a órbita de $(1, 0, \ldots, 0)$ pelo grupo gerado pela matriz

$$B = \begin{pmatrix} 0 & \ldots & 0 & -1 \\ & & & 0 \\ & Id_{n-1} & & \vdots \\ & & & 0 \end{pmatrix},$$

onde Id_{n-1} é a matriz identidade $(n-1) \times (n-1)$. Chamaremos esse conjunto com $2n$ pontos de *código biortogonal*. Note que há duas distâncias ao quadrado d^2 possíveis entre os pontos de $\mathcal{B}_n$: $2 = |(1, 0, \ldots, 0) - (0, \ldots, 0, 1)|^2$ e $4 = |(1, 0, \ldots, 0) - (-1, 0, \ldots, 0)|^2$. Assim $\mathcal{B}_n$ é um código em $\mathbb{R}^n$ com $2n$ pontos e distância mínima ao quadrado 2. Portanto, o código biortogonal satisfaz o limitante de Rankin, teorema 1.6.5, o que o faz um código ótimo.

A assinatura do código Biortogonal

Seja $det(B - \lambda Id_n)$ o polinômio característico de B. Usando o método de Laplace, vê-se que $det(B - \lambda Id_n)$ é igual a

$$-\lambda \begin{vmatrix} -\lambda & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & -\lambda \end{vmatrix} + (-1)^{n+1}.(-1) \begin{vmatrix} 1 & \lambda & & 0 \\ & \ddots & \ddots & \\ & & \ddots & \lambda \\ 0 & & & 1 \end{vmatrix} = (-1)^n(\lambda^n + (-1)^2).$$

Assim, os auto-valores de R são $\lambda_k = cos(\frac{(2k+1)\pi}{n}) + isen(\frac{(2k+1)\pi}{n})$, onde $k = 0, \ldots, n-1$. O único auto-valor real λ_k aparece para $k = \frac{n-1}{2}$, quando n é ímpar. Analogamente ao caso do código simplex, os auto-vetores associados aos auto-valores λ_k são $X_k = \frac{1}{\sqrt{n}}(\lambda_k^{n-1}, \ldots, \lambda_k, 1)$. O novo vetor inicial, relativo à matriz de blocos, é $Q^T(1, 0, \ldots, 0)$, onde Q^T é a matriz cujas linhas são formadas pelas partes real e imaginária dos auto-vetores X_k alternadamente. Portanto, para

n par,

$$Q^T(1,0,\ldots,0) = \frac{1}{\sqrt{n}}(Re(\lambda_0^{n-1}), Im(\lambda_0^{n-1}), \ldots, Re(\lambda_{n/2-1}^{n-1}), Re(\lambda_{n/2-1}^{n-1})).$$

Como $\lambda_k^{n-1} = -cos(\frac{(2k+1)\pi}{n}) + isen(\frac{(2k+1)\pi}{n})$,

$$Q^T(1,0,\ldots,0) = \frac{1}{\sqrt{n}}(-cos\frac{\pi}{n}, sen\frac{\pi}{n}, \ldots, -cos\frac{(n-1)\pi}{n}, sen\frac{(n-1)\pi}{n}).$$

Este vetor pode ser mudado, via uma isometria, para $\frac{1}{\sqrt{n}}(1,0,1,0,\ldots,1,0)$. Como a nova matriz geradora é a matriz de blocos

$$\mathcal{R} = [R(\frac{\pi}{n}), R(\frac{3\pi}{n}), \ldots, R(\frac{(n-1)\pi}{n})] = [R(\frac{2\pi}{2n}), R(\frac{2\pi 3}{2n}), \ldots, R(\frac{(n-1)2\pi}{2n})],$$

temos que a assinatura do biortogonal em dimensão par é $(1,3,5,\ldots,n-1)$.

Se a dimensão é ímpar, temos mais um auto valor $\lambda_{\frac{n-1}{2}}$ real e igual a -1 cujo auto-vetor associado é $\frac{1}{\sqrt{n}}(1,-1,1,-1,\ldots,1,-1,1)$. Então à última coordenada do vetor inicial e à última coordenada da assinatura deve ser acrescentado $\frac{1}{\sqrt{n}}$ e -1, respectivamente. O teorema a seguir resume todos estes fatos.

Teorema 2.4.2 *Seja $\mathcal{X}$ o código de grupo cíclico com $2n$ pontos em $\mathbb{R}^n$ com assinatura*

$$(1,3,5,\ldots,n-1) \text{ e vetor inicial } \sqrt{\frac{2}{n}}(1,0,1,0,\ldots,1,0), \text{ para } n \text{ par, ou, assinatura}$$

$$(1,3,5,\ldots,n-1,-1) \text{ e vetor inicial } \sqrt{\frac{2}{n+1}}(1,0,1,0,\ldots,1,0,1), \text{ para } n \text{ ímpar.}$$

Então $\mathcal{X}$ é o código Biortogonal em $\mathbb{R}^n$.

Observação 2.4.1 *Ingermasson, em um resultado similar de [22], mostrou que, partindo de um grupo de matrizes desta forma, o vetor inicial $\frac{1}{\sqrt{n}}(1,1,\ldots,1)$ minimiza a probabilidade de erro da constelação e origina também os códigos simplex e biortogonal. Aqui, o caminho foi inverso: partimos dos códigos para obter as representações, via isometrias do espaço.*

Uma outra diferença é que, apesar de [22] utilizar também da classificação dos operadores ortogonais feita em [19], as relações descritas em [22] entre os códigos de grupo cíclico e o grupo de índices de rotação não desembocam na geometria dos toros que nós apresentamos no próximo capítulo, nem pretendem saber se estes códigos são planares ou não. Ingemarsson faz um estudo da dimensão destes códigos e sua probabilidade de erro.

Códigos de grupo cíclico podem ser vistos como grafos circulantes mergulhados em toros planos. O conjunto de vértices, neste caso, é formado pelo grupo cíclico gerado pela assinatura em $(\mathbb{Z}_M)^n$*. Esta conexão aparece no artigo [38], trabalho que o autor desta tese contribuiu.*

Capítulo 3

Limitantes para Códigos de Grupo Comutativo

Neste capítulo é apresentada uma caracterização para o local geométrico dos códigos de grupo cíclico. Em dimensão par, os códigos de grupo cíclico estão contidos em nós que se enrolam em toros planos e, em dimensão ímpar, em anti-primas cujas bases são toros planos. Este resultado vale também para códigos de grupo comutativo. Tais interpretações permitiram desenvolver um limitante superior para a quantidade de pontos de um código de grupo comutativo, em termos de suas distâncias mínimas. Os resultados sobre limitantes aqui apresentados foram publicados parcialmente em [37]. Aplicações da geometria dos toros planos a codificação contínua e discreta podem ser encontrados nos artigos [50, 11], de autoria de Costa e outros.

3.1 Variedades Euclidianas e suas Isometrias

Uma variedade diferenciável (C^∞) é um subconjunto S de $\mathbb{R}^n$ tal que para todo $p \in S$ existe uma vizinhança V de p em $\mathbb{R}^n$ e uma aplicação $\mathcal{F} : U \to V \cap S$ de um aberto $U \subset \mathbb{R}^m$ sobre $V \cap S \subset \mathbb{R}^n$ de tal maneira que

1. a aplicação $\mathcal{F}$ é diferenciável, isto é, tem todas as derivadas parciais contínuas de todas as ordens em U;

2. $\mathcal{F}$ também é um homeomorfismo entre U e $V \cap S$;

3. O operador linear $d\mathcal{F}_q : \mathbb{R}^m \to \mathbb{R}^n$, cuja matriz é a matriz jacobiana de $\mathcal{F}$ em q, é injetor para todo q em U.

A aplicação $\mathcal{F}$, descrita acima, é chamada de carta ou parametrização local da variedade S. Se F é uma parametrização local para uma variedade S, a imagem da aplicação linear dF_p é chamada de espaço tangente a S em $F(p)$ e denotada $T_{F(p)}S$. O espaço tangente $T_{F(p)}S$ pode ser visto como o conjunto dos vetores tangentes às curvas diferenciáveis contidas em S que passam por $F(p)$. A dimensão de uma variedade é definida como a dimensão de seu espaço tangente.

Sejam duas variedades diferenciáveis parametrizadas S_1 e S_2. Uma aplicação $\phi : U \subset S_1 \to S_2$ é um difeomorfismo local em $p \in U$ se existir uma vizinhança $V \subset U$ de p de tal maneira que ϕ restrita a V é um difeomorfismo sobre $\phi(V) \subset S_2$. A interpretação do espaço tangente como o conjunto dos vetores tangentes permite definir o diferencial $d\phi_p : T_pS_1 \to T_qS_2$ da aplicação ϕ, onde $q = \phi(p)$. Se $v \in T_pS_1$, existe $\beta : I \subset \mathbb{R} \to S_1 \subset \mathbb{R}^m$ com $\beta(t_0) = p$ e vetor tangente $\beta'(t_0) = v$. Então $\phi \circ \beta : I \subset \mathbb{R} \to S_2 \subset \mathbb{R}^n$ é uma curva em S_2 que passa por q. Definimos então $d\phi_p(v) = \frac{d\phi \circ \beta}{dt}(t_0)$.

É possível demonstrar que esta aplicação é linear e não depende da curva β tomada. Assim podemos definir isometrias entre variedades. Um difeomorfismo $\phi : S_1 \to S_2$ é uma isometria se, para todo $p \in S_1$ e $w_1, w_2 \in T_pS_1$, temos

$$\langle w_1, w_2 \rangle_p = \langle d\phi_p(w_1), d\phi_p(w_2) \rangle_{\phi(p)}, \tag{3.1}$$

onde $\langle , \rangle_p$ e $\langle , \rangle_{\phi(p)}$ são os produtos internos euclidianos restritos a T_pS_1 e $T_{\phi(p)}S_2$, respectivamente. Duas variedades S_1 e S_2 são localmente isométricas se para todo ponto $p \in S_1$ existir uma vizinhança $V_1 \subset S_1$ de p, onde uma isometria $\phi_p : V_1 \subset S_1 \to \phi_p(V_1) \subset S_2$ pode ser estabelecida. Neste caso, ϕ_p é chamada *isometria local* . Tal propriedade deve também valer para todo ponto de S_2.

Todas propriedades que dependem do produto interno, tais como área de regiões, comprimentos de curvas e a curvatura Gaussiana, são preservadas entre *variedades isométricas.*

3.2 Os Toros Planos

O *toro plano* $T_{(\delta_1,\ldots,\delta_m)}$ pode ser definido como o seguinte subconjunto da esfera S^{2m-1}:

$$T_\delta = T_{(\delta_1,\ldots,\delta_m)} = \{(x_1, x_2, \ldots, x_{2m}) \in \mathbb{R}^{2m}; \delta_i^2 = x_{2i-1}^2 + x_{2i}^2 \; e \; \sum_i^m \delta_i^2 = 1\}.$$

A cada $\delta = (\delta_1, \ldots, \delta_m) \in S^{m-1}$, associamos um toro de maneira que $\bigcup_{\delta \in S^{m-1}} T_\delta = S^{2m-1}$, ou seja, o conjunto $\{T_\delta\}_{\delta \in S^{m-1}}$ é uma folheação de S^{2m-1}. Seja $\psi : \mathbb{R}^m \to \mathbb{R}^{2m}$ definida por

$$\psi(y) = (\delta_1 cos(\frac{y_1}{\delta_1}), \delta_1 sen(\frac{y_1}{\delta_1}), \ldots, \delta_m cos(\frac{y_m}{\delta_m}), \delta_m sen(\frac{y_m}{\delta_m})), \tag{3.2}$$

onde $y = (y_1, \ldots, y_m)$ e $\sum_{i=1}^{m} \delta_i^2 = 1$.

A aplicação ψ é claramente diferenciável, tem imagem igual ao toro T_δ e

$$\frac{\partial \psi}{\partial y_i} = d\psi_y(e_i) = -sen(\frac{y_i}{\delta_i})e_{2i-1} + cos(\frac{y_i}{\delta_i})e_{2i}$$

satisfaz a condição 3.1, ie, $\langle d\psi_y(e_i), d\psi_y(e_j)\rangle = \langle \frac{\partial \psi}{\partial y_i}, \frac{\partial \psi}{\partial y_j}\rangle = \langle e_i, e_j\rangle$. Portanto ψ é uma parametrização para T_δ e uma isometria local entre $\mathbb{R}^m$ e o toro T_δ.

A parametrização ψ induz uma relação de equivalência em $\mathbb{R}^m$ cujas classes formam um conjunto chamado toro plano abstrato.

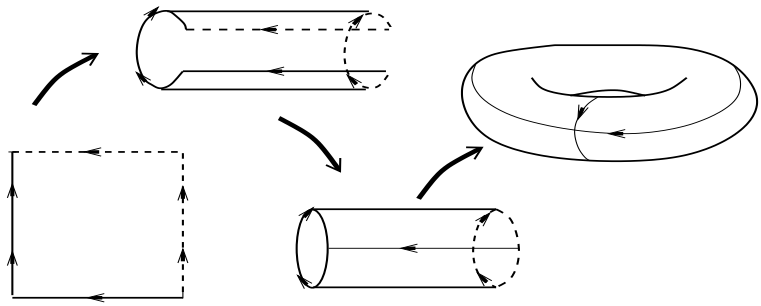


Figura 3.1: A construção do Toro Plano

Dizemos que x e y em $\mathbb{R}^m$ são equivalentes se $\psi(x) = \psi(y)$. Um conjunto de representantes para essa relação é o paralelepípedo $\Pi_{i=1}^{m}[0, 2\pi\delta_i)$. Este conjunto de representantes pode ser visto como um espaço quociente onde os lados paralelos do paralelepípedo são identificados.

O espaço quociente é definido do seguinte modo: Seja Λ o reticulado gerado pelos vetores $u_i = 2\pi\delta_i e_i$, onde $\{e_i\}$ é a base canônica do $\mathbb{R}^m$. Dizemos que $x = (x_1, \ldots, x_m)$ e $y = (y_1, \ldots, y_m)$ são equivalentes se $x_i = y_i \ mod\ 2\pi\delta_i$, ou seja, $x - y \in \Lambda$. Neste caso, denotamos $x = y \ mod\ \Lambda$ e o espaço quociente $\frac{\mathbb{R}^m}{\Lambda}$.

A noção de aberto nestes conjuntos quocientes é oriunda da métrica usual de $\mathbb{R}^m$, considerando as devidas identificações feitas pelo quociente. Ou seja, um aberto de $\frac{\mathbb{R}^m}{\Lambda}$ é dado

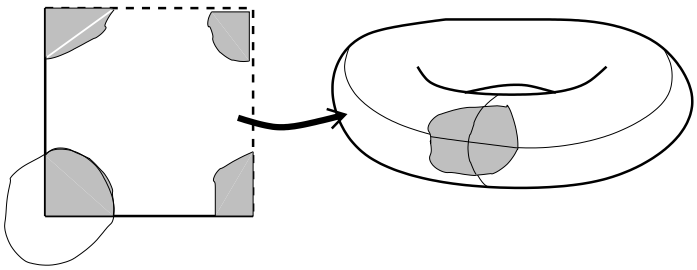


Figura 3.2: A topologia da identificação em um toro plano.

pela imagem de um aberto de $\mathbb{R}^m$ pela aplicação projeção $\Pi : x \in \mathbb{R}^m \to \overline{x} \in \frac{\mathbb{R}^m}{\Lambda}$, onde $\overline{x}$ é a classe de equivalência de x. Esta topologia (conjunto de abertos do toro) é chamada topologia da identificação.

Como a imagem de ψ é $T_{(\delta_1,\ldots,\delta_m)}$ e ψ está bem definida no quociente $\frac{\mathbb{R}^m}{\Lambda}$, ou seja, $\psi(x) = \psi(y)$ se, e somente se, $x = y \ mod \ \Lambda$, o quociente $\frac{\mathbb{R}^m}{\Lambda}$ é identificado com o domínio da aplicação ψ e, por conseguinte, $\frac{\mathbb{R}^m}{\Lambda}$ com T_δ.

O teorema Egregium de Gauss diz que a curvatura Gaussiana de uma superfície é preservada por isometrias locais. Como a curvatura Gaussiana de $\mathbb{R}^m$ é nula, segue que os toros T_δ tem curvatura Gaussiana nula. O nome "toro plano" reflete, portanto, duas propriedades de T_δ: a identificação dos lados do quadrado, sugerindo a forma do toro contido em $\mathbb{R}^3$, e a curvatura nula, tal como o plano euclidiano.

Uma outra propriedade satisfeita pelos toros planos é a homogeneidade. Dizemos que uma *variedade M é homogênea* se para qualquer par de pontos $\widetilde{p}$ e $\widetilde{q}$ em M existir uma isometria de M que leva $\widetilde{p}$ em $\widetilde{q}$.

Construir uma isometria entre dois pontos de um toro plano é equivalente a construir uma translação entre a pré-imagem destes pontos no cubo localmente isométrico ao toro. De fato, se $\psi : \Pi_{i=1}^m [0, 2\pi\delta_i) \to T_\delta$ é a isometria local (3.2) e $\widetilde{p}$ e $\widetilde{q}$, pontos de T_δ, considere a translação $\mathcal{T}$ que leva $p = \psi^{-1}(\widetilde{p})$ a $q = \psi^{-1}(\widetilde{q})$, ambos em $\Pi_{i=1}^m [0, 2\pi\delta_i)$. Tal translação é definida por $\mathcal{T}(y) = y + q - p$, onde $q = (q_1, \ldots, q_m)$ e $p = (p_1, \ldots, p_m)$.

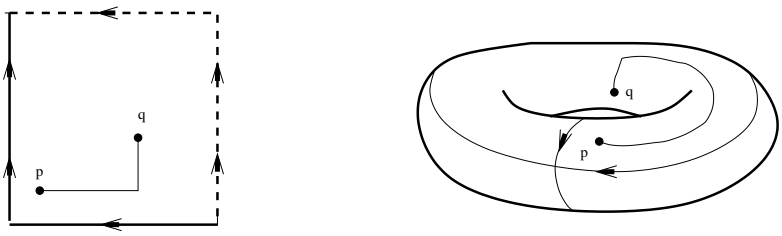


Figura 3.3: Construção de uma isometria entre dois pontos do toro plano.

$$\text{Então } \psi \circ T(y) = \sum_{i=1}^{m} \delta_i (cos(\frac{y_i + q_i - p_i}{\delta_i}) e_{2i-1} + sen(\frac{y_i + q_i - p_i}{\delta_i}) e_{2i}) =$$

$$\mathcal{R}(\delta_1 cos(\frac{y_1}{\delta_1}), \delta_1 sen(\frac{y_1}{\delta_1}), \ldots, \delta_m cos(\frac{y_m}{\delta_m}), \delta_m sen(\frac{y_m}{\delta_m})),$$

onde $\mathcal{R}$ é a matriz ortogonal cujos blocos são as rotações 2-dimensionais de ângulo $\frac{q_i - p_i}{\delta_i}$. Logo $\psi \circ \mathcal{T}(y) = \mathcal{R}\psi(y)$, de onde segue que $\widetilde{q} = \psi(q) = \psi \circ T(p) = \mathcal{R}\psi(p) = \mathcal{R}\widetilde{p}$. Note que $\mathcal{R}$ é uma isometria euclidiana que preserva T_δ. Assim, podemos concluir a seguinte proposição:

Proposição 3.2.1 *Os toros planos T_δ são superfícies homogêneas. Além disso, se*

$$\psi : \Pi_{i=1}^{m}[0, 2\pi\delta_i) \to T_\delta$$

é a isometria (3.2) e $a \in \Pi_{i=1}^{m}[0, 2\pi\delta_i)$, vale a igualdade

$$||\psi(x + a) - \psi(a)|| = ||\psi(x) - \psi(0)||.$$

Um referência com maiores detalhes sobre curvatura e isometrias entre variedades é o livro [10].

3.3 Códigos de Grupo Comutativo e Toros Planos

Considere o código de grupo cíclico com M pontos, vetor inicial $(x_1, 0, x_3, 0, \ldots, x_{2m-1}, 0)$ e assinatura $(k_1, \ldots, k_m)$. As palavras deste código são, para $1 \leq l \leq M - 1$,

$$P(l) = (x_1 cos(\frac{2\pi k_1 l}{M}), x_1 sen(\frac{2\pi k_1 l}{M}), \ldots, x_{2m-1} cos(\frac{2\pi k_m l}{M}), x_{2m-1} sen(\frac{2\pi k_m l}{M})).$$

Se ψ é a isometria local (3.2) entre $\mathbb{R}^m$ e T_δ, $\psi(y) = P(l)$ se

$$\delta_i = x_{2i-1} \quad \text{e} \quad \frac{y_i}{x_{2i-1} k_i} = \frac{2\pi l}{M}.$$

O conjunto $\{(y_1, \ldots, y_m) \in \mathbb{R}^m; \frac{y_1}{x_1 k_1} = \ldots = \frac{y_m}{x_{2m-1} k_m}\}$ é uma reta cuja parametrização é $r : \mathbb{R} \to \mathbb{R}^m$ onde $r(t) = (x_1 k_1, x_3 k_3, \ldots, x_{2m-1} k_m)t$. Então

$$\{P(l)\}_{l=1}^{M} \subset \Gamma = \{\psi(r(t)); t \in \mathbb{R}\}.$$

Geometricamente, Γ é uma curva fechada sobre T_δ chamada nó. Identificando os lados do cubo $\Pi_{i=1}^{m}[0, 2\pi\delta_i)$ perpendiculares ao lado correspondente à coordenada y_i, obtemos um cilindro onde Γ se enrola k_i vezes, conforme mostra a figura 3.4. A constelação cíclica é formada pelos pontos do nó onde $t = \frac{2\pi l}{M}$, para $l = 1, \ldots, M-1$.

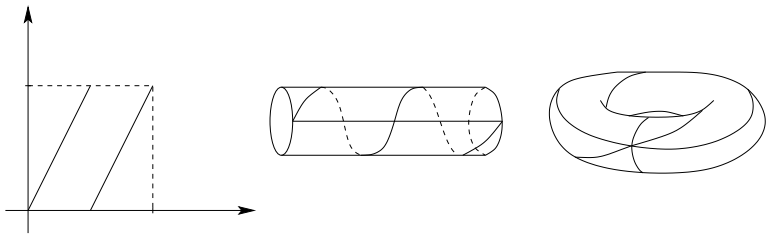


Figura 3.4: Um nó no toro plano.

Mais ainda, ladrilhando o cubo $\Pi_{i=1}^{m}[0, 2\pi\delta_i)$ com cópias do paralelepípedo $[0, \frac{2\pi x_1}{M}] \times \ldots \times [0, \frac{2\pi x_{2m-1}}{M}]$, obtemos uma malha retangular, deformada a partir de $\frac{\mathbb{Z}^m}{M\mathbb{Z}^m}$ pela homotetia de $\mathbb{R}^m$

$$H(y_1, \ldots, y_m) = 2\pi(x_1 y_1, x_3 y_2, \ldots, x_{2m-1} y_m).$$

A intersecção da reta, que gera o nó, com os vértices da malha dá a pré-imagem da constelação pela isometria.

Assim, concluímos: O vetor inicial indica a deformação desejada da malha quadrada. Em outras palavras, implica na escolha de um toro plano. Enquanto que a assinatura indica qual o nó onde mora a constelação, por conseguinte quantas vezes o nó se enrolará no toro. A diferença entre um código cíclico e um comutativo em dimensão par não é grande quando os vemos sobre um toro. O teorema 1.3.2 diz que todo grupo de matrizes comutativo pode ser visto, a menos de uma similaridade ortogonal, como um conjunto de matrizes de rotação. Uma vez fixado o vetor inicial, tanto o código comutativo, quanto o cíclico deve morar no mesmo toro plano da esfera. A diferença é que no cíclico as palavras moram em apenas um nó que se enrola no toro, o que não acontece com o comutativo. Estes terá tantos nós quantos forem seus subgrupos cíclicos.

Para colocar um vetor inicial qualquer no formato $(x_1, 0, x_3, 0, \ldots, x_{2m-1}, 0)$ tal qual assumimos no começo da seção, aplicamos à constelação uma rotação de $\mathbb{R}^{2m}$ que preserva o peso dos pares formados pelas coordenadas $2i-1$ e $2i$, com $1 \leq i \leq m$ e, portanto, deixam os toros invariantes. Assim, de maneira concisa, podemos enunciar o seguinte teorema:

Teorema 3.3.1 *Todo código comutativo, com vetor inicial* $(x_1, x_2, \ldots, x_{2m-1}, x_{2m})$*, mora no toro* $T_{(\delta_1,\ldots,\delta_m)}$ *onde* $\delta_i^2 = x_{2i-1}^2 + x_{2i}^2$*. Em particular, se o código de grupo for cíclico com assinatura* $(k_1, \ldots, k_m)$*, ele mora sobre o nó* $\Gamma = \{\psi(r(t)); t \in \mathbb{R}\} \subset T_\delta$*, onde*

$$r(t) = (x_1k_1, x_3k_3, \ldots, x_{2m-1}k_m)t$$

e ψ *é a isometria (3.2).*

3.4 Os Anti-prismas

Uma glisso-reflexão no plano é a composição de uma translação T ao longo de uma reta m com uma reflexão R por m. Aplicando sucessivamente RT em um ponto do plano, obtém-se um polígono chamado zigzag regular. O mesmo procedimento na esfera é produzido pela composição de uma rotação em torno de uma reta m e uma reflexão por um plano ortogonal a m. O polígono obtido é um zigzag esférico que mora alternadamente em dois círculos de mesmo raio e paralelos ao plano tomado.

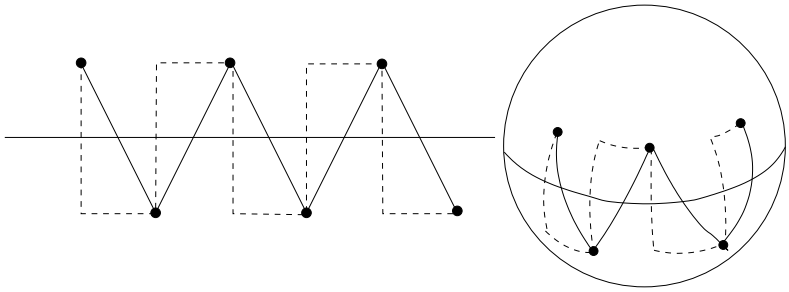


Figura 3.5: Órbitas de uma glisso reflexão planar e esférica

Se a rotação for de ângulo $\frac{d\pi}{p}$, com d e p co-primos, o poliedro obtido possui $2p$ vértices, divididos igualmente em dois meridianos de mesmo raio formando um polígono regular com p vértices. Isto segue diretamente do corolário 2.1.2. Cada um desses polígonos pode ser obtido a

partir do outro pela glisso-reflexão que os definiram, o que faz com que o poliedro seja um prisma com uma das base rotacionadas. Por esta razão, esses poliedros são chamados *anti-prismas*. Por serem constituídos por duas cópias de um mesmo polígono, os anti-prismas sempre tem um número par de vértices (veja fig3.6).

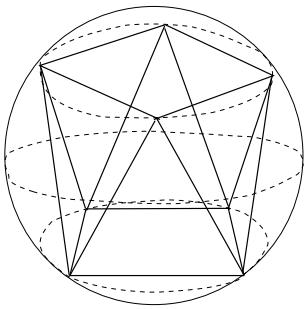


Figura 3.6: O anti-prisma de oito pontos

Códigos de grupo cíclico em dimensão ímpar também são anti-prismas. De fato, a matriz geradora é sempre da forma

$$[R(k_1), R(k_2), \ldots, R(k_q), -1] = [R(k_1), R(k_2), \ldots, R(k_q), 1].[1, \ldots, 1, -1],$$

que claramente é o produto de uma rotação em $\mathbb{R}^{2q+1}$ em torno do eixo gerado por e_{2q+1} e uma reflexão pelo hiperplano normal a e_{2q+1}. Se a dimensão onde o código mora for $2\nu+1$, as bases do anti-prisma moram em toros planos em dimensão 2ν.

Teorema 3.4.1 *Em dimensão ímpar $2m+1$, todo código cíclico com M pontos, assinatura $(k_1, \ldots, k_m, -1)$ e vetor inicial $X_0 = (x_1, x_2, \ldots, x_{2m+1})$ é, a menos de uma homotetia e uma translação, formado por duas cópias do código cíclico em $\mathbb{R}^{2m}$ com $M/2$ pontos, assinatura $(k_1, \ldots, k_m)$ e vetor inicial $\frac{1}{(\sum_{i=1}^{2m} x_i^2)^{1/2}}(x_1, \ldots, x_m)$.*

Demonstração : Se $\mathcal{R}$ é matriz ortogonal de blocos $[R(\frac{2\pi k_1}{M}), \ldots, R(\frac{2\pi k_m}{M}), -1]$, então o código cíclico com assinatura $(k_1, \ldots, k_m, -1)$ e vetor inicial X_0 é $\mathcal{X} = \{\mathcal{R}^l X_0\}_{l=1}^{M} = \{\mathcal{R}^{2l} X_0\}_{l=1}^{M/2} \cup \{\mathcal{R}^{2l+1} X_0\}_{l=0}^{M/2-1}$. Mas

$$\mathcal{X}_1 = \{\mathcal{R}^{2l} X_0\}_{l=1}^{M/2} = \{[R(\frac{2\pi k_1 l}{M/2}), \ldots, R(\frac{2\pi k_m l}{M/2}), 1] X_0\}_{l=1}^{M/2} \; e$$

$$\mathcal{X}_2 = \{\mathcal{R}^{2l+1} X_0\}_{l=0}^{M/2-1} = \{[R(\frac{2\pi k_1 l}{M/2} + \frac{2\pi k_1}{M}), \ldots, R(\frac{2\pi k_m l}{M/2} + \frac{2\pi k_m}{M}), -1] X_0\}_{l=1}^{M/2} =$$

$$\{[R(\frac{2\pi k_1 l}{M/2})R(\frac{2\pi k_1}{M}),\ldots,R(\frac{2\pi k_m l}{M/2})R(\frac{2\pi k_m}{M}),-1]X_0\}_{l=1}^{M/2}.$$

Logo $\mathcal{X}_2 = [R(\frac{2\pi k_1}{M}),\ldots,R(\frac{2\pi k_1}{M}),-1]\mathcal{X}_1$. Ou seja, $\mathcal{X}_1$ e $\mathcal{X}_2$ são códigos isométricos que formam $\mathcal{X}$. Mais ainda, eles moram em $\mathbb{R}^{2m}$ numa esfera de raio $(\sum_{i=1}^{2m} x_i^2)^{1/2} < 1$.

Colocamos $\mathcal{X}_1$ na esfera S^{2m-1} através da composição da translação $T : \mathbb{R}^{2m+1} \to \mathbb{R}^{2m+1}$, $T(y) = y - (0,\ldots,0,x_{2m+1})$, e a homotetia $H : \mathbb{R}^{2m} \to \mathbb{R}^{2m}$, $H(y) = \frac{y}{(\sum_{i=1}^{2m} x_i^2)^{1/2}}$. Em S^{2m-1}, a nova constelação $H\circ T(\mathcal{X}_1)$ é a constelação cíclica cuja assinatura e o vetor inicial são $(k_1,\ldots,k_m)$ e $\frac{1}{(\sum_{i=1}^{2m} x_i^2)^{1/2}}(x_1,\ldots,x_m)$, respectivamente. ■

3.5 Um Limitante da União para Toros Planos

Para cada parâmetro $\delta = (\delta_1,\ldots,\delta_m)$, pode-se calcular a área $A(\delta)$ do toro T_δ. Como todo código de grupo comutativo com vetor de pesos δ mora em T_δ , $A(\delta)$ certamente traz restrições sobre a distância mínima deste código. O objetivo desta seção é construir um limitante que expresse tal restrição. Ele será feito nos moldes do limitante da união, apresentado no primeiro capítulo. Primeiro mostraremos que o *toro de maior área* é aquele com pesos iguais.

Proposição 3.5.1 *O toro $T_{\delta_1,\ldots,\delta_{2m-1}}$ de maior área na esfera S^{2m-1} tem índices satisfazendo a igualdade $\delta_1 = \ldots = \delta_{2m-1} = \frac{1}{\sqrt{m}}$ e área igual a $(\frac{2\pi}{\sqrt{m}})^m$.*

Demonstração : Dado que ψ, tal como em (3.2), é uma isometria local entre o paralelepípedo $\Pi_{i=1}^m[0,2\pi\delta_i)$ e T_δ, segue que a área desses objetos é a mesma. Ou seja, $A(\delta) = (2\pi)^m\Pi_{i=1}^m\delta_i$.

Para maximizar $A(\delta)$ restrita a $G(\delta) = |\delta|^2 - 1 = 0$, usaremos o método multiplicadores de Lagrange. Note que

$$\nabla A = (2\pi)^m \sum_{i=1}^{m}(\delta_1\ldots\widehat{\delta_i}\ldots\delta_m)e_i,$$

onde $\widehat{\delta_j}$ denota a ausência de δ_j no produto $\delta_1\ldots\delta_m$ e

$$\nabla G = 2(\delta_1,\ldots,\delta_m).$$

Assim, o problema se resume a encontrar as soluções do sistema

$$\begin{cases} (2\pi)^m(\delta_1\ldots\widehat{\delta_j}\ldots\delta_m) = \lambda 2\delta_j \qquad 1 \le j \le m \\ |\delta|^2 = 1 \end{cases}.$$

Multiplicando a primeira equação por δ_j, obtemos que todos os pesos devem ser iguais. Usando este fato na segunda equação, segue que

$$m\delta_1^2 = \sum_{i=1}^{m} \delta_1^2 = \sum_{i=1}^{m} \delta_i^2 = 1.$$

Logo, $\delta_i = \frac{1}{\sqrt{m}}$. Portanto a maior área que um toro plano T_δ pode ter é $A(\frac{1}{\sqrt{m}}, \ldots, \frac{1}{\sqrt{m}}) = (\frac{2\pi}{\sqrt{m}})^m$. ■

3.5.1 Empacotamentos de chapéus esféricos em T_δ

Considere um código em T_δ com M pontos e distância mínima ρ. Isto equivale a um empacotamento de M chapéus esféricos sobre T_δ de maneira que seus centros distem entre si no mínimo ρ. Como a área ocupada por estes chapéus é no máximo a área do próprio toro T_δ, o número de chapéus também é limitado. Vamos dar uma estimativa para a área destes chapéus e depois apresentar um limitante para M, supondo que a distância mínima ρ é fixa.

Um chapéu esférico sobre o toro T_δ centrado em x_0 e de raio ρ é definido por

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

Como a área de $B^{T_\delta}(x_0, \rho)$ é a mesma que a de $S_\rho = \psi^{-1}(B^{T_\delta}(x_0, \rho))$, procuramos uma estimativa para esta última. A figura 3.7 mostra S_ρ para diferentes valores de ρ. Segundo a proposição 3.2.1, os toros planos são homogêneos, portanto a área de S_ρ independe do ponto central x_0 escolhido, depende apenas de ρ e do peso δ da isometria. Assim, o problema se restringe a obter uma estimativa da área do conjunto

$$S_\rho = \{y \in \mathbb{R}^m \ ; \ D(y) \leq \rho^2\}, \text{ onde } D(y) = ||\psi(y) - \psi(0)||^2 = 4\sum_{i=1}^{m} \delta_i^2 sen^2(\frac{y_i}{2\delta_i}).$$

Em [50], Vaishampayan e Costa, mostraram que, para pesos iguais, o bordo de S_ρ é limitado por duas esferas centradas na origem de $\mathbb{R}^m$ com raios $\frac{2}{\sqrt{m}} arcsen(\frac{\rho\sqrt{m}}{2})$ e $2arcsen(\frac{k}{2})$. A proposição a seguir generaliza este resultado para toros com qualquer peso.

Proposição 3.5.2 *O máximo e o mínimo de $G(u_1, \ldots, u_m) = \sum_{i=1}^{m} u_i^2$ restrita ao bordo de S_k, ou seja, ao conjunto $\{u \in \mathbb{R}^m \ ; \ D(u) = \rho^2\}$, onde $D(u) = 4\sum_{i=1}^{m} \delta_i^2 sen^2(\frac{u_i}{2\delta_i})$, são $4\mu^2 arcsen^2(\frac{\rho}{2\mu})$ e $4arcsen^2(\frac{\rho}{2})$, respectivamente, onde μ é o menor dos pesos δ_i.*

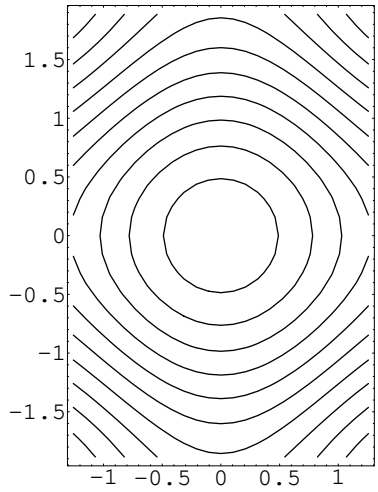


Figura 3.7: Imagem inversa de um chapéu esférico em um toro plano em dimensão 4 com pesos diferentes.

Demonstração : Observe que o bordo do conjunto S_ρ é um compacto, portanto a função G restrita a ele assume máximo e mínimo. Usando o método dos multiplicadores de Lagrange, vê-se que estes pontos u devem satisfazer o sistema de equações

$$\nabla D(u) = \lambda \nabla G(u) = 2\lambda u \quad \text{e} \quad D(u) = \rho^2.$$

Como $\frac{\partial D}{\partial u_i}(u) = 4\delta_i sen\left(\frac{u_i}{2\delta_i}\right) cos\left(\frac{u_i}{2\delta_i}\right) = 2\delta_i sen(\frac{u_i}{\delta_i})$, o sistema fica

$$\lambda u_i = \delta_i sen(\frac{u_i}{\delta_i}) \quad \text{e} \quad 4\sum_{i=1}^{m} \delta_i^2 sen^2(\frac{u_i}{2\delta_i}) = \rho^2.$$

Se I é o conjunto de índices i tais que $u_i \neq 0$, segue que os quocientes

$$\frac{sen(\frac{u_i}{\delta_i})}{\frac{u_i}{\delta_i}}, \text{ para } i \in I \ e \ -\pi \leq \frac{u_i}{\delta_i} \leq \pi,$$

são todos iguais. Mas $\frac{sen(x)}{x}$ é função par e injetora em $[0, \pi]$, logo $\frac{u_i}{\delta_i} = \frac{u_l}{\delta_l}$ para todo i e l em I. Estamos supondo u_i positivo pois as funções D e G são pares, o que acontece para u_i positivo se repete para u_i negativo. Então, da segunda equação, para qualquer $l \in I$, segue que

$$4\sum_{i \in I} \delta_i^2 sen^2(\frac{u_l}{2\delta_l}) = \rho^2.$$

Portanto, u que minimiza e maximiza G deve ter as coordenadas não nulas iguais a

$$u_l = 2\delta_l arcsen\left(\frac{\rho}{2(\sum_{i\in I}\delta_i^2)^{1/2}}\right).$$

Logo, a distância máxima e mínima de G quando restrita ao bordo de S_ρ deve ser

$$4\sum_{i\in I}\delta_i^2\left[arcsen^2\left(\frac{\rho}{2(\sum_{i\in I}\delta_i^2)^{1/2}}\right)\right],$$

para algum conjunto de índices I.

Para que a prova se complete, usaremos o fato (com prova posterior) de que a função $f(x) = 4x\left[arcsen^2\left(\frac{\rho}{2x^{1/2}}\right)\right]$ é decrescente em $[(\frac{\rho}{2})^2, 1]$. Tal fato implica que o mínimo de G se dá quando todas coordenadas de u são não nulas e o máximo na coordenada cujo respectivo peso δ_i é o menor possível. Isto conclui o lema. ■

Observação 3.5.1 *A função f não é definida para $x \leq \left(\frac{\rho}{2}\right)^{1/2}$. Isto quer dizer que para obter códigos de grupo comutativo com distância mínima ρ, o menor dos pesos deve ser maior que $\left(\frac{\rho}{2}\right)^{1/2}$. Tal restrição, na verdade, é geométrica. O menor dos pesos indica o maior diâmetro do conjunto S_ρ e este não deve exceder o diâmetro do paralelepípedo $\Pi_{i=1}^m[0, 2\pi\delta_i)$. Note ainda que, como ρ é sempre menor que dois, o intervalo de definição de f é não vazio.*

Lema 3.5.1 *A função $f(x) = 4x\left[arcsen^2\left(\frac{\rho}{2x^{1/2}}\right)\right]$ é decrescente em $[(\frac{k}{2})^2, 1]$.*

Demonstração : É equivalente demonstrar que a derivada de f é negativa, ou seja,

$$f'(x) = ArcSin\left[\frac{k}{2\sqrt{x}}\right]\left(\frac{-k}{\sqrt{4-\frac{k^2}{x}}\sqrt{x}} + ArcSin\left[\frac{k}{2\sqrt{x}}\right]\right) < 0.$$

Como $ArcSin\left[\frac{k}{2\sqrt{x}}\right]$ é positiva para $x \in [(\frac{k}{2})^2, 1]$, olhemos para a função

$$B(x) = \left(\frac{-k}{\sqrt{4-\frac{k^2}{x}}\sqrt{x}} + ArcSin\left[\frac{k}{2\sqrt{x}}\right]\right).$$

A derivada de B é $\frac{k^3}{2\left(4-\frac{k^2}{x}\right)^{3/2}x^{5/2}}$, portanto positiva. Portanto B é crescente e assume seu máximo em 1. Mas $g(k) = B(1) = \left(\frac{-k}{\sqrt{4-k^2}} + ArcSin\left[\frac{k}{2}\right]\right)$ é negativo para todo k em $[0, 2)$. De fato, $g(0) = 0$ e $\frac{dg}{dk} = -\frac{k^2}{(4-k^2)^{3/2}}$ é negativa. Sendo 0 o seu maior valor, o máximo de B é 0. Pelo fato de ser crescente, B é negativa em $[(\frac{k}{2})^2, 1]$. ■

Decorre direto da proposição anterior o seguinte corolário:

Corolário 3.5.1 *A área do conjunto S_ρ é no máximo $V_m(2\ \mu\ Arcsen(\frac{\rho}{2\mu}))^m$ e no mínimo $V_m(2\ Arcsen(\frac{\rho}{2}))^m$, onde V_m é o volume da esfera $S^{m-1} \subset \mathbb{R}^m$ de raio 1 e μ é o menor dos pesos δ_i.*

Tendo feito estas estimativas sobre a área de um chapéu esférico, voltemos ao problema de empacotamento de chapéus esféricos em T_δ.

Teorema 3.5.1 *Todo empacotamento de M chapéus esféricos $B^{T_\delta}(x_l, \rho)$ no toro T_δ satisfaz*

$$\bigcup_{l=1}^{M} B(\psi^{-1}(x_l), 2\arcsin(\rho/2)) \subset \bigcup_{l=1}^{M} \psi^{-1}(B_l^{T_\delta}(x_l, \rho)),$$

onde $B(\psi^{-1}(x_l), 2\arcsin(\rho/2)) = \{x \in R^m; |x - \psi^{-1}(x_l)| \leq 2\arcsin(\rho/2)\}$.

Demonstração : O chapéu esférico $B^{T_\delta}(\psi(0), \rho)$, segundo a proposição anterior, quando trazido pela isometria ψ^{-1} para o paralelepípedo $\Pi_{i=1}^m[0, 2\pi\delta_i)$ contém a bola centrada na origem de raio $2\arcsin(\rho/2)$. Por homogenenidade, $B(\psi^{-1}(x_l), 2\arcsin(\rho/2)) \subset \psi^{-1}(B_l^{T_\delta}(x_l, \rho))$, o que conclui a prova. ■

Todo código $\{x_l\}_{l=1}^M$ com distância mínima ρ em T_δ é um empacotamento de M chapéus $B^{T_\delta}(x_l, \rho/2)$, implicando na união disjunta de conjuntos $\cup_{l=1}^M \psi^{-1}(B^{T_\delta}(x_l, \rho/2))$ em $\Pi_{i=1}^m[0, 2\pi\delta_i)$, pois ψ é uma bijeção. Portanto a união $\cup_{l=1}^M B(\psi^{-1}(x_l), 2\arcsin(\rho/2))$ é disjunta. Consequentemente, reduzimos o problema de empacotamento em T^δ para um problema de empacotamento de M bolas no paralelepípedo $\Pi_{i=1}^m[0, 2\pi\delta_i]$. Como no paralelepípedo $\psi^{-1}(\{x_l\}_{l=1}^M)$ é um subconjunto de um subgrupo discreto de $\mathbb{R}^m$, ou seja, está contido em um reticulado de R^m, este empacotamento deve satisfazer Δ_m, a densidade máxima de empacotamento de um reticulado em R^m. Mais ainda, nos limitantes aparece o quociente $\Lambda_m = \frac{\Delta_m}{V_m}$, onde V_m é o volume da esfera de raio 1 em $\mathbb{R}^m$. Este quociente é conhecido como a máxima *densidade de centro* de um reticulado em $\mathbb{R}^m$. Os teoremas abaixo expressam este fato em termos da área deste novo empacotamento.

Teorema 3.5.2 *Limitante para códigos de grupo comutativo em dimensão par.*
Todo código de grupo comutativo em R^{2m} com M pontos, distância mínima ρ e vetor inicial $(u_1, u_2, \ldots, u_{2m})$ satisfaz

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

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

Como o toro de área máxima é aquele cujos pesos são iguais, temos

$$\sqrt{\Pi_{i=1}^{m}(u_{2i-1}^2 + u_{2i}^2)} \leq \frac{1}{m^{m/2}}.$$

Logo, obtemos um limitante que independe da escolha do toro.

Teorema 3.5.3 *Limitante para códigos de grupo comutativo em dimensão par. Todo código de grupo comutativo em R^{2m} com M pontos, distância mínima ρ e vetor inicial $(u_1, u_2, \ldots, u_{2m})$ satisfaz*

$$M \leq \frac{\pi^m \Lambda_m}{(\arcsin \frac{\rho}{4})^m m^{m/2}},$$

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

3.6 Limitantes para Códigos de Grupo Comutativo em Dimensão Ímpar

Do que foi feito no teorema 3.4.1 e na seção anterior, podemos enunciar o seguinte teorema sobre códigos de grupo cíclico em dimensão ímpar:

Teorema 3.6.1 *Limitante para códigos de grupo cíclico em dimensão ímpar.*

Em dimensão ímpar $2m+1$, todo código cíclico com M pontos, assinatura $(k_1, \ldots, k_m, -1)$, vetor inicial $X_0 = (x_1, x_2, \ldots, x_{2m+1})$ e distância mínima ρ satisfaz

$$M \leq \frac{2\Lambda_m \pi^m \sqrt{\Pi_{i=1}^{m}(x_{2i-1}^2 + x_{2i}^2)}}{(1 - x_{2m+1}^2)^{1/2}(ArcSen(\frac{\rho}{4(1-x_{2m+1}^2)^{1/2}}))^m},$$

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

Demonstração : O teorema 3.4.1 garante que todo código cíclico com M pontos, assinatura $(k_1, \ldots, k_m, -1)$ e vetor inicial $X_0 = (x_1, x_2, \ldots, x_{2m+1})$ é composto, a menos de uma homotetia H e uma translação T, por duas cópias do código cíclico em $\mathbb{R}^{2m}$ com $M/2$ pontos, assinatura

$(k_1, \ldots, k_m)$ e vetor inicial $\frac{1}{(\sum_{i=1}^{2m} x_i^2)^{1/2}}(x_1, \ldots, x_{2m})$. Se a distância mínima deste último código é $\widetilde{\rho}$, então vale a seguinte desigualdade

$$\frac{M}{2} \leq \frac{\pi^m \sqrt{\Pi_{i=1}^m (x_{2i-1}^2 + x_{2i}^2)} \Delta_m^c}{(\sum_{i=1}^{2m} x_i^2)^{1/2} (\arcsin \frac{\widetilde{\rho}}{4})^m}.$$

Mas as distâncias mínimas $d_{min}\mathcal{X}_1$ e $\widetilde{\rho}$ de $\mathcal{X}_1$ e $H \circ T(\mathcal{X}_1)$, respectivamente, satisfazem $\widetilde{\rho} = \frac{d_{min}\mathcal{X}_1}{(\sum_{i=1}^{2m} x_i^2)^{1/2}}$. Como $\rho \leq d_{min}\mathcal{X}_1$, segue que $\frac{\rho}{(\sum_{i=1}^{2m} x_i^2)^{1/2}} \leq \frac{d_{min}\mathcal{X}_1}{(\sum_{i=1}^{2m} x_i^2)^{1/2}} = \widetilde{\rho}$. Dado que a função $ArcSen(x)$ é crescente, vale o resultado enunciado. ■

Este limitante também é válido para códigos de grupo comutativo. De fato, o teorema 1.3.2 diz que se G é um grupo de matrizes ortogonais comutativas, toda matriz de G tem a forma de bloco $[R_1, \ldots, R_k, 1, \ldots, 1, -1, \ldots, -1]$, onde R_i é uma rotação 2-dimensional. É claro que os blocos 1 com "1" na entrada não podem ocorrer simultaneamente em todas as matrizes, pois o código estaria contido em um hiperplano. Da mesma maneira, os blocos "-1" não podem repetir-se, apesar de pelo menos um existir, dado que a dimensão é ímpar. Isto implica que a órbita de $X_0 = (x_1, x_2, \ldots, x_{2m+1})$ pelo grupo G mora em dois toros T_δ, cujos pesos satisfazem $\delta_i^2 = x_{2i}^2 + x_{2i-1}^2$. Temos, portanto, M pontos com distância mínima ρ nos dois toros T_δ. Apesar de não sabermos como estes pontos estão divididos entre os toros, a desigualdade do teorema anterior vale.

Para obter o limitante do toro independente do vetor inicial, basta ver que

$$\sqrt{\frac{\Pi_{i=1}^m (x_{2i-1}^2 + x_{2i}^2)}{\sum_{i=1}^{2m} x_i^2}} \leq \frac{1}{m^{m/2}} \;\; e \;\; (1 - \sum_{i=1}^{2m} x_i^2) < 1.$$

Assim, temos o seguinte teorema para códigos de grupo comutativo em dimensão ímpar:

Teorema 3.6.2 *Limitante para códigos de grupo comutativo em dimensão ímpar.*

Em dimensão ímpar $2m+1$, todo código de grupo comutativo com M pontos, vetor inicial $X_0 = (x_1, x_2, \ldots, x_{2m+1})$ e distância mínima ρ satisfaz

$$M \leq \frac{2\Lambda_m \pi^m \sqrt{\Pi_{i=1}^m (x_{2i-1}^2 + x_{2i}^2)}}{(1 - x_{2m+1}^2)^{1/2} (ArcSen(\frac{\rho}{4(1-x_{2m+1}^2)^{1/2}}))^m},$$

onde Λ_m é a densidade de centro máxima de empacotamentos de esferas em um reticulado contido em $\mathbb{R}^m$. Em particular,

$$M \leq \frac{2\Lambda_m \pi^m}{(ArcSen(\frac{\rho}{4}))^m m^{m/2}}.$$

3.7 Análise Comparativa do Limitante do Toro para Códigos de Grupo Comutativo

O quociente $\frac{\Delta_m}{V_m}$, denotado nos limitantes por Λ_m, é conhecido como densidade de centro de um empacotamento de esferas. Em nosso caso, os centros das esferas moram sobre reticulados, portanto Λ_m é a máxima densidade de centro de um reticulado de $\mathbb{R}^m$. Segundo [42], as melhores densidades de centro conhecidas para reticulados, para $m = 1, \ldots 10$, são as apresentadas na tabela 3.1.

m	Λ_m
1	0.5
2	0.28868
3	0.17678
4	0.125
5	0.08839
6	0.07217
7	0.06250
8	0.06250
9	0.04419
10	0.03608

Tabela 3.1: Densidade de centro para $m = 1, \ldots, 10$.

Após alguns cálculos, obtemos o gráfico comparativo 3.8 para os limitantes da união do toro em dimensão 4. O limitante do toro é melhor até distância mínima igual a $1,42324$.

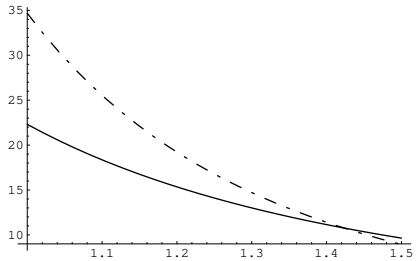


Figura 3.8: Limitante da união (hachurado) e o dos toros (cheio) encontrando em 1,42324 .

Os gráficos dos limitantes da união e do toro nas dimensões $6, 8$ e 10 estão esboçados na figura 3.9. Vê-se que os limitante do toro perde para distâncias maiores que 1.511, 1.5378 e 1.58548, respectivamente. Note que a densidade de centro decai com o aumento da dimensão. Isto provavelmente ajuda o limitante melhorar em relação ao limitante da união. Mas a densidade de centro não tem comportamento decrescente em função da dimensão, ela decresce até dimensão 14, assumindo o valor 0.03608, e , depois disso, tem comportamento assintótico variável. Além disso, para algumas dimensões não se sabe ainda se as densidades de centro conhecidas são ótimas.

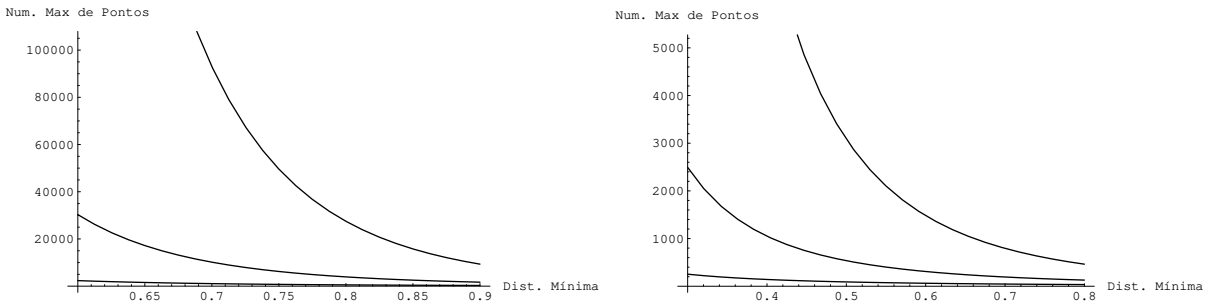


Figura 3.9: À esquerda, o limitante da união e , à direita, o limitante dos toros para códigos esféricos em dimensão $n = 6, 8$ e 10.

Em dimensão ímpar, comportamento similar acontece com os limitantes, conforme figura 3.10. Comparando-os (figura 3.11), vemos que o limitante do toro é melhor que o limitante da união até 1.2816, 1.37116 e 1.41708, nas dimensões 5, 7 e 9.

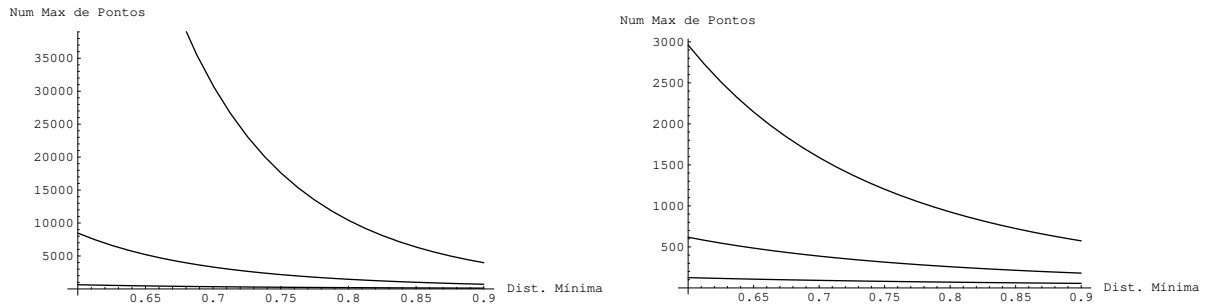


Figura 3.10: À esquerda, o limitante da união e , à direita, o limitante dos toros para códigos esféricos em dimensão $n = 5, 7$ e 9.

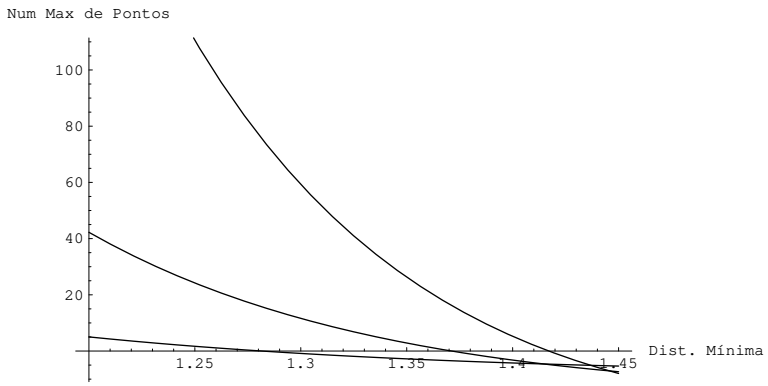


Figura 3.11: Gráfico da diferença entre os limitantes da união e do toro em dimensão 5, 7 and 9.

3.8 Limitantes para códigos sobre $\mathbb{Z}_M$

É comum associar a códigos sobre $\mathbb{Z}_M$ uma métrica inspirada na distância dos pontos do polígono regular de M lados. Se x_i e y_i pertencem a $\mathbb{Z}_M$, associamos a distância ao quadrado entre x_i e y_i como $4sen^2(\frac{(x_i-y_i)\pi}{M})$, que é o tamanho da corda definida pelo ângulo $(\frac{(x_i-y_i)\pi}{M})$. Se $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ são palavras de um código em $\mathbb{Z}_M^n$, então definimos a distância ao quadrado entre elas como

$$d_E^2(x,y) = \sum_{i=1}^{n} 4sen^2\left(\frac{(x_i - y_i)\pi}{M}\right).$$

Tal métrica nada mais é do que a distância euclidiana entre dois pontos de um código de grupo comutativo onde o grupo é $\mathbb{Z}_M^n$, a menos de uma escolha adequada de pesos. De fato, se $R_x = [R(\frac{2x_1\pi}{M}), \ldots, R(\frac{2x_n\pi}{M})]$ e $R_y = [R(\frac{2y_1\pi}{M}), \ldots, R(\frac{2y_n\pi}{M})]$ são as matrizes diagonais com as rotações de ângulo $\frac{2a\pi}{M}$ na diagonal e $X_0 = n^{1/2}(1,0,1,0,\ldots,1,0) \in R^{2n}$, então a distância ao quadrado euclidiana entre R_xX_0 e R_yX_0 é

$$\sum_{i=1}^{n} \frac{4}{n} sen^2\left(\frac{(x_i - y_i)\pi}{M}\right) = \frac{d_E^2(x,y)}{n}.$$

Isto quer dizer que códigos comutativos em $\mathbb{Z}_M^n$ com a métrica d_E podem ser vistos como códigos de grupo com o vetor inicial $X_0 = n^{1/2}(1,0,1,0,\ldots,1,0) \in R^{2n}$. Dividindo d_E por n, obtemos a distância euclidiana dos códigos de grupo. Utilizando tal relação, limitantes sobre a distância mínima de códigos de bloco sobre $\mathbb{Z}_M$ podem ser adaptados para limitantes de distância

mínima de códigos de grupo em dimensão par com vetor inicial $X_0 = n^{1/2}(1, 0, 1, 0, \ldots, 1, 0) \in R^{2n}$.

Capítulo 4

Desempenho dos Códigos de Grupo Cíclico

Este capítulo retoma a questão apresentada na introdução deste trabalho: Dada a dimensão e uma quantidade de pontos, qual é o melhor código de grupo cíclico com estes parâmetros? Qual é o seu vetor inicial ótimo? Em outras palavras, dado um grupo cíclico e sua representação, qual é o toro que contém o melhor código obtido através desta representação e, dentre todas as representações, qual é a melhor ?

Biglieri e Elia reduziram o problema do vetor inicial ótimo a um algoritmo de programação linear, cujo objetivo era minimizar uma forma linear restrita a um convexo. Utilizando alguns pacotes do Mathematica e o algoritmo de Biglieri e Elia, desenvolvemos um programa que obtem o melhor código de grupo cíclico em dimensão 4, para qualquer quantidade de pontos. Uma tabela com os melhores códigos de grupo cíclico em dimensão quatro, até 100 pontos, foi gerada, comparando com os melhores códigos esféricos conhecidos até agora.

Por fim, estudamos os códigos de grupo cíclico que moram em toros de maior área. Uma conjectura sobre uma classe de assinaturas cujos códigos de grupo cíclico ótimos associados moram em toros de área máxima é estabelecida.

4.1 O Problema do Vetor Inicial

Seja $\mathcal{X}$ o código de grupo cíclico com assinatura $(k_1, \ldots, k_\nu)$ e $x_0 = (x_1, x_2, \ldots, x_n)$ seu vetor inicial. Se $\mathcal{R}$ é a matriz que rotula $\mathcal{X}$, então a distância ao quadrado de x_0 as outras palavras $\mathcal{R}^l(x_0)$ é

$$d^2(x_0, \mathcal{R}^l(x_0)) = \begin{cases} 2 - 2\sum_{i=1}^{\nu} \mu_i cos(\frac{2\pi l k_i}{M}), & \text{para } n = 2\nu \\ 2 - 2(-1)^l \mu_{\nu+1} - 2\sum_{i=1}^{\nu} \mu_i cos(\frac{2\pi l k_i}{M}), & \text{para } n = 2\nu + 1 \end{cases}, \tag{4.1}$$

onde $\mu_i = x_{2i}^2 + x_{2i-1}^2$, para $i = 1, \ldots, \nu$ e , adicionalmente, $\mu_{\nu+1} = x_n^2$, quando n for ímpar.

Procuramos saber qual a melhor escolha dos pesos μ_i de tal maneira que o mínimo de $\{||x_0 - \mathcal{R}^l(x_0))||\}_{l=1}^{M}$ seja maior possível. Interpretaremos esta questão segundo [7].

Se d_{min}^2 é a distância mínima ao quadrado de $\mathcal{X}$, então $d^2(x_0, \mathcal{R}^l(x_0)) \geq d_{min}^2$, ou seja, em dimensão par,

$$4\sum_{i=1}^{\nu} \mu_i sen^2(\frac{\pi l k_i}{M}) \geq d_{min}^2, \text{ou seja,}$$

$$\sum_{i=1}^{\nu} \frac{4\mu_i}{d_{min}^2} sen^2(\frac{\pi l k_i}{M}) \geq 1.$$

Denote $y_i = \frac{4\mu_i}{d_{min}^2}$. Logo $\sum_{i=1}^{\nu} y_i = \frac{4}{d_{min}^2}$. Portanto, maximizar d_{min}^2 equivale a minimizar a forma linear

$$\sum_{i=1}^{\nu} y_i$$

sujeita às restrições $y_i \geq 0$ e $\sum_{i=1}^{\nu} y_i sen^2(\frac{\pi l k_i}{M}) \geq 1$, onde $l = 1, \ldots, \lfloor \frac{M}{2} \rfloor$. Dada a simetria da função $Sen^2(x)$, somente metade das restrições importam.

Em dimensão ímpar, $d^2(x_0, \mathcal{R}^l(x_0)) \geq d_{min}^2$ fica

$$\sum_{i=1}^{\nu} \frac{4\mu_i}{d_{min}^2} sen^2(\frac{\pi l k_i}{M}) + \frac{((-1)^{l-1} + 1)}{2} \frac{4\mu_{\nu+1}}{d_{min}^2} \geq 1.$$

Assim, da mesma maneira, denotando $y_i = \frac{4\mu_i}{d_{min}^2}$, queremos minimizar $\sum_{i=1}^{\nu+1} y_i$ restrito às condições $y_i \geq 0$ e $\sum_{i=1}^{\nu} y_i sen^2(\frac{\pi l k_i}{M}) + \frac{((-1)^{l-1} + 1)}{2} y_{\nu+1} \geq 1$, onde $l = 1, \ldots, \lfloor \frac{M}{2} \rfloor$.

Para saber qual é o melhor código cíclico $[M, n]$, deve-se então procurar entre todas as assinaturas qual a que dá a melhor distância mínima. Algumas restrições permitem que esta procura seja reduzida às assinaturas $(k_1, \ldots, k_m)$ que satisfazem as seguintes condições:

1. $MDC(k_1, \ldots, k_m, M) = 1$, segundo o teorema 2.2.1;

2. $k_i \leq \lfloor \frac{M}{2} \rfloor$, pois, do contrário, existiria k tal que $k_i + k = M$. Então, do item 2 da proposição 2.3.2, poderíamos trocar k_i por k, obtendo códigos equivalentes;

3. $MDC(k_1, \ldots, k_m) = 1$. De fato, se $MDC(k_1, \ldots, k_m) = a$, então duas possibilidades se abrem: a dividir M ou não. Se a dividir M, segue do item 1 que $a = 1$. Senão, o item 3 de 2.3.2 nos garante que há uma outra assinatura $(h_1, \ldots, h_m)$, com máximo divisor igual a 1 e que gera o mesmo código.

A releitura do problema do vetor inicial, feita no começo da seção, juntamente com as observações acima permitiram a construção de um programa numérico, desenvolvido no Mathematica, que calcula qual o melhor cíclico em dimensão quatro. A tabela 4.1 resume os resultados obtidos comparando com os melhores códigos esféricos conhecidos em dimensão quatro. Tanto os cálculos dos melhores cíclicos quanto a tabela dos melhores esféricos conhecidos em dimensão quatro podem ser encontrados no apêndice deste trabalho.

4.2 O Vetor Inicial Ótimo para os Códigos de Grupo Cíclico em Dimensão Três

O problema do vetor inicial ótimo pode ser resolvido em dimensão três. O resultado é um anti-prisma cuja base é um poliedro regular. O conjunto de vértices deste poliedro é composto por metade dos pontos da constelação.

Sejam (x_1, x_2, x_3) o vetor inicial e $(k, -1)$ a assinatura de um código cíclico com M pontos em $\mathbb{R}^3$. Podemos supor $x_2 = 0$, não alterando a configuração dos pontos da constelação. Deste modo, os pontos do código são

$$P(l) = \left(Cos\left(\frac{2\pi kl}{M}\right) x_1, Sen\left(\frac{2\pi kl}{M}\right) x_1, (-1)^l x_3 \right), \text{ para } l = 1, \ldots, M.$$

M	Cíclico	Geral	M	Cíclico	Geral	M	Cíclico	Geral
5	1.58114	1.58114	37	0.726279	0.859804	69	0.550862	0.703379
6	1.41421	1.41421	38	0.726504	0.847664	70	0.554069	0.701806
7	1.3569	1.41421	39	0.721177	0.840323	71	0.52921	0.698024
8	1.41421	1.41421	40	0.71449	0.836065	72	0.54199	0.695669
9	1.27549	1.29459	41	0.679374	0.830331	73	0.525076	0.693987
10	1.22474	1.29099	42	0.695895	0.826534	74	0.53858	0.693469
11	1.22652	1.24064	43	0.661994	0.82138	75	0.538464	0.692013
12	1.22474	1.22474	44	0.654098	0.813874	76	0.533996	0.691282
13	1.14516	1.17703	45	0.68404	0.803835	77	0.528206	0.68527
14	1.09456	1.1666	46	0.673878	0.797087	78	0.518023	0.680051
15	1.09132	1.1393	47	0.655368	0.79322	79	0.503411	0.673706
16	1.01959	1.10668	48	0.63924	0.787615	80	0.523802	0.669788
17	0.987552	1.0842	49	0.64574	0.783053	81	0.510436	0.666634
18	1.	1.07441	50	0.628092	0.782654	82	0.503273	0.663691
19	0.970361	1.06371	51	0.624104	0.772819	83	0.497614	0.661707
20	0.959849	1.06371	52	0.63805	0.769899	84	0.508177	0.659738
21	0.892013	1.02822	53	0.633893	0.764629	85	0.4948	0.657687
22	0.928783	1.00211	54	0.610561	0.761952	86	0.503664	0.655812
23	0.923038	1.	55	0.589275	0.754106	87	0.487678	0.654957
24	0.91018	1.	56	0.62184	0.749398	88	0.489188	0.654328
25	0.871154	0.96196	57	0.595236	0.745159	89	0.470343	0.650354
26	0.838353	0.958343	58	0.592924	0.741669	90	0.495054	0.64747
27	0.821316	0.940647	59	0.5899	0.739344	91	0.478631	0.645921
28	0.847216	0.930227	60	0.586215	0.736521	92	0.466671	0.644653
29	0.799272	0.92396	61	0.590391	0.732779	93	0.477262	0.643355
30	0.831254	0.911885	62	0.569237	0.729544	94	0.479411	0.642567
31	0.779902	0.904692	63	0.57549	0.722876	95	0.473237	0.637208
32	0.765367	0.899199	64	0.563177	0.721723	96	0.475506	0.635639
33	0.765671	0.893582	65	0.542568	0.717658	97	0.461932	0.633272
34	0.773165	0.883029	66	0.563465	0.712742	98	0.453171	0.631243
35	0.749627	0.87003	67	0.54398	0.708562	99	0.465511	0.629614
36	0.717261	0.862196	68	0.558859	0.705556	100	0.461448	0.627382

Tabela 4.1: Os melhores $[M, 4]$ códigos esféricos conhecidos, segundo Sloane [42], e os cíclicos, obtidos via o algoritmo de Elia e Biglieri.

Segue que $||P(l) - P(m)||^2 = ||P(l-m) - P(0)||^2 = x_1^2(2 - 2Cos(\frac{2\pi k(l-m)}{M})) + (-1 + (-1)^{l-m})^2 x_3^2$. Se $l - m$ é par,

$$||P(l) - P(m)||^2 = 2x_1^2(1 - Cos(\frac{2\pi k(l-m)}{M})), \text{ senão}$$

$$||P(l) - P(m)||^2 = -2x_1^2(1 + Cos(\frac{2\pi k(l-m)}{M})) + 4.$$

O mínimo destas duas expressões se dá quando $Cos(\frac{2\pi k(l-m)}{M})$ estiver mais perto de 1. Se $l - m$ for par, segue que $\overline{k(l-m)}$ é par em $\mathbb{Z}_M$, pois M é par. Da mesma maneira, se $l - m$ for ímpar, então $\overline{k(l-m)}$ é ímpar em $\mathbb{Z}_M$. Logo, o mínimo da distância para $l - m$ par é quando $\overline{k(l-m)} = 2$ e $\overline{k(l-m)} = 1$, quando $l - m$ for ímpar. Assim, o problema se resume a

$$Max_{0<x_1<1}\{2x_1^2(1 - Cos(\frac{4\pi}{M})), -2x_1^2(1 + Cos(\frac{2\pi}{M})) + 4\}.$$

Enquanto que uma expressão cresce, quando x_1 cresce, a outra decresce. Portanto, a melhor situação é quando as duas expressões são iguais, ou seja,

$$2x_1^2(1 - Cos(\frac{4\pi}{M})) = -2x_1^2(1 + Cos(\frac{2\pi}{M})) + 4.$$

Obtendo x_1 desta igualdade, segue que a melhor distância mínima é

$$\frac{4(1 - Cos(\frac{4\pi}{M}))}{(2 + Cos(\frac{2\pi}{M}) - Cos(\frac{4\pi}{M}))}.$$

Da mesma maneira que o caso 2-dimensional, o caso 3-dimensional independe da representação tomada. Mas, ao contrário do caso planar, ele depende do vetor inicial. De fato, o vetor inicial ótimo $(x_1, 0, x_3)$ tem as coordenadas satisfazendo

$$x_1^2 = \frac{2}{(2 + Cos(\frac{2\pi}{M}) - Cos(\frac{4\pi}{M}))} \text{ e } x_3^2 = 1 - x_1^2.$$

4.3 Códigos de Grupo Cíclico em Toros de Área Máxima

Em [11] e [12], Costa et alli propuseram uma nova classe de códigos esféricos com simetrias cíclicas que se relacionavam com grafos e códigos perfeitos sobre toros. Estes códigos eram códigos de grupo cíclico que moravam no toro de área máxima em $\mathbb{R}^4$ com assinatura (a, b) e $a^2 + b^2$ pontos, onde $mdc(a, b) = 1$. Algumas questões naturais aparecem: Vistos como órbitas de grupos de matrizes, os códigos de [11] e [12] são ótimos? Eles são os melhores, comparados

com os de mesma cardinalidade? Os melhores códigos de grupo cíclico moram nos toros de maior área?

Não é verdade que os melhores códigos de grupo cíclico moram em toros de maior área. Em dimensão quatro, até 100 pontos, os únicos que moram em toros de maior área e são os melhores possíveis são os de $M = 5, 6, 8, 10, 12, 13, 15, 17, 30$ e 41 pontos, vejam os resultados nos anexos. Destes, somente os de $5, 10, 13, 17$ e 41 pontos são da forma $a^2 + b^2$ pontos. Suas assinaturas são, respectivamente, $(1, 2)$, $(1, 3)$, $(2, 3)$, $(1, 4)$ e $(4, 5)$. A tabela 4.2 mostra todos os códigos ótimos em dimensão quatro que moram em toros de área máxima. Note que para uma mesma quantidade de pontos, duas ou mais representações distintas dão a mesma distância mínima. Por exemplo, para 15 pontos, as representações $(1, 4)$ e $(2, 7)$ dão a mesma distância mínima. A razão é simples: as assinaturas $(1, 4)$ e $(2, 8)$ dão o mesmo código cíclico, uma vez que diferem por 2, elemento invertível em $\mathbb{Z}_{15}$, e $(2, 8)$ é equivalente a $(2, 7)$, para 15 pontos, segundo a proposição 2.3.2. Operações similares mostram que na tabela 4.2, fixada a quantidade de pontos, todos os códigos são equivalentes.

4.3.1 Os cíclicos com assinatura (a, b) e $a^2 + b^2$ pontos, onde $mdc(a, b) = 1$

Um fenômero importante acontece na classe dos códigos de grupo cíclico com assinatura (a, b) e $a^2 + b^2$ pontos, onde $mdc(a, b) = 1$: Todos os casos analisados até 100 pontos possuem vetor inicial ótimo $\frac{\sqrt{2}}{2}(1, 0, 1, 0)$, ou seja, moram nos toros de maior área. A tabela 4.3 mostra suas respectivas distâncias mínimas, comparadas com os melhores cíclicos.

Afirmamos então:

Conjectura 01: Todos os códigos de grupo cíclico com assinatura (a, b) e $a^2 + b^2$ pontos, onde $mdc(a, b) = 1$, são ótimos quando moram nos toros de área máxima, ou seja, seu vetor inicial ótimo é $\frac{\sqrt{2}}{2}(1, 0, 1, 0)$.

Tal conjectura pode ser trocada por uma outra, aparentemente mais simples. Se $F(y_1, y_2) = y_1 + y_2$, então a conjectura 1 diz, de maneira mais explícita, que o mínimo do funcional F quando restrito ao conjunto convexo

$$A = \{(y_1, y_2) \in \mathbb{R}^2; y_1, y_2 > 0 \; e \; y_1 Sen^2\left(\frac{\pi a l}{a^2+b^2}\right) + y_2 Sen^2\left(\frac{\pi b l}{a^2+b^2}\right) \geq 1 \; para \; 1 \leq l \leq \left\lfloor \frac{a^2+b^2}{2} \right\rfloor\}$$

é assumido no ponto

$$\mathcal{P} = \left(\frac{1}{Sen^2\left(\frac{\pi a}{a^2+b^2}\right) + Sen^2\left(\frac{\pi b}{a^2+b^2}\right)}, \frac{1}{Sen^2\left(\frac{\pi a}{a^2+b^2}\right) + Sen^2\left(\frac{\pi b}{a^2+b^2}\right)} \right),$$

M	Representação	Distância Mínima	M	Representação	Distância Mínima
5	(1,2)	1.5811388	34	(3,5)	0.7396946
6	(1,2)	1.4142135	34	(7,11)	0.7396946
8	(1,3)	1.4142135	35	(1,6)	0.7363434
10	(1,3)	1.2247448	35	(3,17)	0.7363434
12	(2,3)	1.2247448	35	(4,11)	0.7363434
13	(1,5)	1.1451631	35	(8,13)	0.7363434
13	(2,3)	1.1451631	35	(9,16)	0.7363434
15	(1,4)	1.0913216	37	(1,6)	0.7000548
15	(2,7)	1.0913216	37	(4,13)	0.7000548
17	(1,4)	0.9875522	37	(5,7)	0.7000548
17	(3,5)	0.9875522	37	(8,11)	0.7000548
17	(6,7)	0.9875522	37	(9,17)	0.7000548
24	(1,5)	0.8804857	37	(15,16)	0.7000548
24	(7,11)	0.8804857	41	(1,9)	0.6793740
25	(1,7)	0.8574407	41	(3,14)	0.6793740
25	(2,11)	0.8574407	41	(4,5)	0.6793740
25	(3,4)	0.8574407	41	(7,19)	0.6793740
26	(1,5)	0.8212510	41	(11,17)	0.6793740
26	(3,11)	0.8212510	41	(11,17)	0.6793740
26	(7,9)	0.8212510	48	(1,7)	0.6322924
29	(1,12)	0.7899469	48	(5,13)	0.6322924
29	(2,5)	0.7899469	48	(11,19)	0.6322924
29	(3,7)	0.7899469	48	(17,23)	0.6322924
29	(8,9)	0.7899469	50	(1,7)	0.6086553
29	(11,13)	0.789946	50	(9,13)	0.6086553
30	(3,5)	0.8312538	50	(11,23)	0.6086553
			50	(17,19)	0.6086553

Tabela 4.2: Os códigos de grupo cíclico $[M, 4]$ ótimos, com $5 \leq M \leq 50$, que moram em toros de área máxima.

M	Representação	Distância Mínima	O Melhor Cíclico Possível
5	(1,2)	1.58114	1.58114
10	(1,3)	1.22474	1.22474
13	(2,3)	1.14516	1.14516
17	(1,4)	0.98755	0.98755
25	(3,4)	0.85744	0.87115
26	(1,5)	0.82125	0.83835
29	(2,5)	0.78994	0.79927
34	(3,5)	0.73969	0.77316
37	(1,6)	0.70005	0.72627
41	(4,5)	0.67937	0.67937
50	(1,7)	0.60865	0.62809
53	(2,7)	0.59413	0.63389
58	(3,7)	0.57127	0.59292
61	(5,6)	0.56096	0.59039
65	(1,8)	0.53765	0.54256
65	(4,7)	0.54235	0.54256
73	(3,8)	0.51087	0.52507
74	(5,7)	0.51015	0.53858
82	(1,9)	0.48108	0.50327
85	(2,9)	0.47345	0.4948
85	(6,7)	0.47714	0.4948
89	(5,8)	0.46577	0.47034
97	(4,9)	0.44559	0.46193

Tabela 4.3: Distância Mínima dos cíclicos $[M, 4]$, com $M = a^2 + b^2 \leq 100$ e a e b co-primos, cujo vetor inicial ótimo tem pesos $\mu_1 = \mu_2 = 0.5$.

o que implica que seu menor valor em A é $2/(Sen^2\left(\frac{\pi a}{a^2+b^2}\right) + Sen^2\left(\frac{\pi b}{a^2+b^2}\right))$.

A teoria da programação linear nos diz que o mínimo de F é um vértice de A. Portanto, antes de provar que $\mathcal{P}$ é ponto de mínimo de F em A é preciso mostrar que $\mathcal{P}$ é vértice de A. Note que $\mathcal{P}$ é encontro das retas

$$y_1 Sen^2\left(\frac{\pi a}{a^2+b^2}\right) + y_2 Sen^2\left(\frac{\pi b}{a^2+b^2}\right) = 1 \text{ e}$$

$$y_1 Sen^2\left(\frac{\pi b}{a^2+b^2}\right) + y_2 Sen^2\left(\frac{\pi a}{a^2+b^2}\right) = 1.$$

A primeira reta é obtida com $l = 1$. Provemos que a segunda existe como restrição em A. Como $mdc(a, b) = 1$, existem inteiros m e n tais que $am + bn = 1$, logo $b = b(am + bn) = bam + b^2n + a^2n - a^2n = n(a^2 + b^2) - a(an - bm)$, ou seja, se $l = an - bm$, $la = -b \; mod \; a^2 + b^2$. É fácil ver também que $lb = a - m(a^2 + b^2)$, ou seja, $lb = a \; mod \; a^2 + b^2$. Assim, para tal l, a segunda restrição é obtida.

Resta demonstrar que $\mathcal{P} = (p_1, p_2)$ está em A. É equivalente demonstrar que

$$p_1 Sen^2\left(\frac{\pi al}{a^2+b^2}\right) + p_2 Sen^2\left(\frac{\pi bl}{a^2+b^2}\right) \geq 1, \; para \; 1 \leq l \leq a^2 + b^2 - 1, \; ie,$$

$$\frac{Sen^2\left(\frac{\pi a}{a^2+b^2}\right) + Sen^2\left(\frac{\pi b}{a^2+b^2}\right)}{Sen^2\left(\frac{\pi al}{a^2+b^2}\right) + Sen^2\left(\frac{\pi bl}{a^2+b^2}\right)} \leq 1, \; para \; 1 \leq l \leq a^2 + b^2 - 1.$$

Agora podemos enunciar a segunda conjectura.

Conjectura 2: O máximo da função $f(x) = \dfrac{Sen^2\left(\frac{\pi a}{a^2+b^2}\right) + Sen^2\left(\frac{\pi b}{a^2+b^2}\right)}{Sen^2\left(\frac{\pi ax}{a^2+b^2}\right) + Sen^2\left(\frac{\pi bx}{a^2+b^2}\right)}$ no intervalo $[1, a^2 + b^2 - 1] \subset \mathbb{R}$ é 1, onde $mdc(a, b) = 1$.

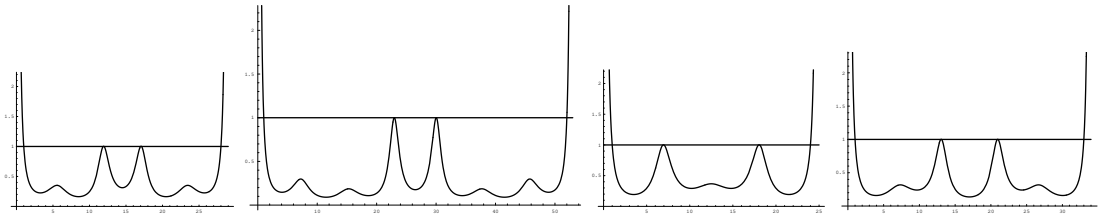


Figura 4.1: A função $f(x) = \dfrac{Sen^2\left(\frac{\pi a}{a^2+b^2}\right) + Sen^2\left(\frac{\pi b}{a^2+b^2}\right)}{Sen^2\left(\frac{\pi ax}{a^2+b^2}\right) + Sen^2\left(\frac{\pi bx}{a^2+b^2}\right)}$ para $(a, b) = (2, 5),\ (2, 7),\ (3, 4)$ e $(3, 5)$.

Uma vez demonstrada a conjectura 2, segue que $\mathcal{P}$ é ponto de mínimo de F. De fato, considere $(x_0, y_0) \in A$. Então

$$x_0 Sen^2\left(\frac{\pi a}{a^2+b^2}\right) + y_0 Sen^2\left(\frac{\pi b}{a^2+b^2}\right) \geq 1 \text{ e}$$

$$x_0 Sen^2\left(\frac{\pi b}{a^2+b^2}\right) + y_0 Sen^2\left(\frac{\pi b}{a^2+b^2}\right) \geq 1.$$

Somando estas duas desigualdades, obtemos que

$$(x_0 + y_0)(Sen^2\left(\frac{\pi a}{a^2+b^2}\right) + Sen^2\left(\frac{\pi b}{a^2+b^2}\right)) \geq 2.$$

Logo $F(x_0, y_0) \geq F(\mathcal{P})$.

Para todos pares (a, b), coprimos, testados até agora, f é limitada por 1 no intervalo $[1, a^2 + b^2 - 1]$. Mas não temos uma prova explícita para esse fato. A figura 4.1 mostra a função f para várias assinaturas.

Considerações Finais

"De tudo ficaram três coisas: a certeza de que ele estava sempre começando, a certeza de que era preciso continuar e a certeza de que seria interrompido antes de terminar. Fazer da interrupção um caminho novo. Fazer da queda um passo de dança, do medo uma escada, do sono uma ponte, da procura um encontro marcado." **Fernando Sabino**

Boa parte dos esforços deste trabalho direcionou-se para desenvolver uma teoria mais geométrica dos códigos de grupo cíclico e comutativo. Procurar, dentro destas classes, códigos ótimos foi também nosso objetivo.

O teorema 2.2.1 estabelece as condições necessárias para a existência de um código de grupo cíclico em termos de sua assinatura, que nada mais é que o gerador de um subgrupo cíclico de $(\mathbb{Z}_M)^n$. Ao que parece, estes subgrupos de $(\mathbb{Z}_M)^n$ desempenham papel importante na geração dos códigos esféricos associados, mas essa relação não está totalmente esclarecida. Quais condições deve satisfazer a assinatura e a deformação da malha que ela forma em $(\mathbb{Z}_M)^n$ para que o código esférico associado não esteja contido em um hiperplano do espaço ? São também suficientes as condições de 2.2.1 ?

Quanto a códigos ótimos e bons limitantes, o gráfico 4.2 ilustra bem a situação em que estamos: O limitante do toro é melhor que os limitantes clássicos para códigos sem simetrias até valores bastante grandes de distância mínima. Entretanto, ainda há espaço entre os códigos de grupo cíclico ótimos e o limitante do toro. Como o limitante é para códigos de grupo comutativo, é possível que haja códigos de grupo comutativo não cíclico que se aproximem mais do limitante. Isto demandaria um estudo, mais específico do que foi feito aqui, sobre códigos com simetrias comutativas não totalmente cíclicas.

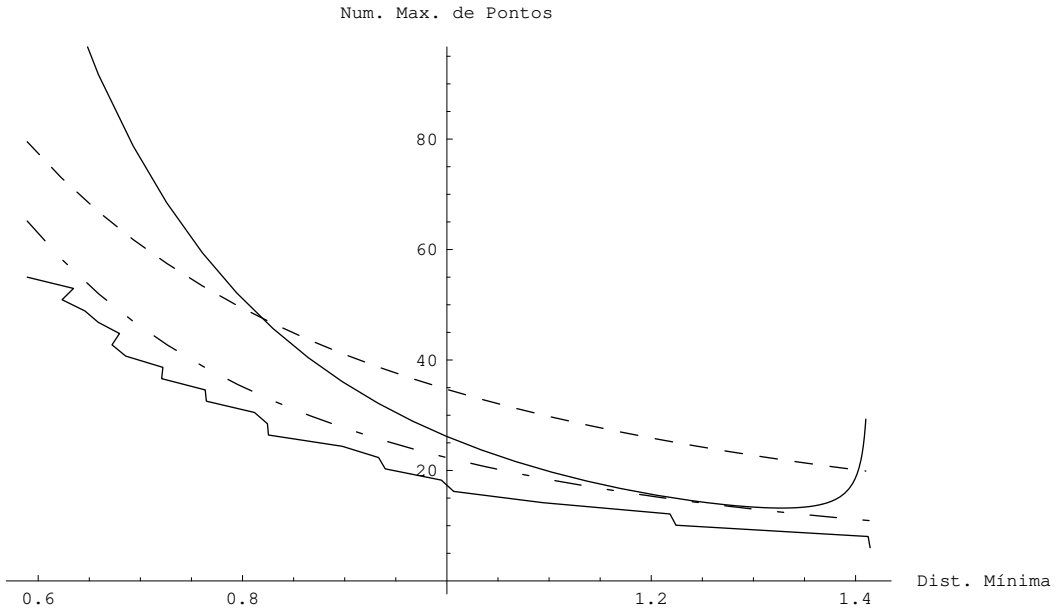


Figura 4.2: Os limitantes da união (hachurada) , de Rankin (linha cheia), do Toro (hachurada e pontos) e uma poligonal que contém os códigos ótimos obtidos em dimensão quatro.

Há ainda a relação, pouco explorada aqui, entre os códigos de grupo cíclico em dimensão ímpar e par. Sabemos que, em dimensão ímpar, os códigos de grupo cíclico são duas cópias de um código cíclico em dimensão par. Códigos ótimos em dimensão ímpar vêm de códigos ótimos em dimensão par? Que outras conexões entre códigos de grupo cíclico em dimensão ímpar e par podemos obter?

Por fim, parece indispensável o uso do computador na análise destas questões, tanto na procura de códigos melhores quanto para atestar a "qualidade" dos limitantes obtidos. É preciso ressaltar que a solução de problemas clássicos de mesma natureza, como a conjectura de Kepler, foram resolvidos com o intenso auxílio de programas computacionais.

Apêndice

Procedimento no programa Mathematica que calcula o melhor cíclico em dimensão quatro com M pontos

O programa abaixo, desenvolvido em Mathematica, calcula para uma determinada quantidade de pontos M, em dimensão quatro, a assinatura que dá a melhor distância mínima e os pontos (x_1, x_2) onde a forma linear, proposta por Biglieri e Elia, alcança essa distância mínima. Os pesos μ_i são obtidos calculando os quocientes $\mu_1 = \frac{x_1}{x_1+x_2}$ e $\mu_2 = \frac{x_2}{x_1+x_2}$. Os que moram em toros de área máxima estão indicados com asterisco.

```
clicotima := Function[M,
    A = Table[0, {i, Floor[M/2]}];(* vetor de restrições*)
    otima =
      Table[0, {i, Floor[M/2]*(Floor[M/2] - 1)/2}, {j,
          5}]; (*matriz que vai receber os resultados de todas as \
representações*)
    melhor = Table[0, {i, 5}];
l = 1 (*variável que indexa as linhas da matiz otima*); k1 = 1; k2 = 2;
(* (k1, k2) é o vetor gerador da representação matricial *)
Do[
      Do[ If[  GCD[k1, k2] == 1,
          Clear[R]

            Do[A[[i]] :=
                Sin[(k1*Pi*i)/M]^2*x1 + Sin[(k2*Pi*i)/M]^2*x2 >= 1 , {i, 1,
                Floor[M/2], 1}];
          R = 1 >= 1;
          Do[R = A[[i]] && R , {i, 1, Floor[M/2], 1}] ;
```

```
          Resul := NMinimize[{x1 + x2, R}, {x1, x2}];

          otima[[l]] = {k1, k2, Sqrt[4/Resul[[1]]], Resul[[2, 1]],
              Resul[[2, 2]]};
          l = l + 1],
        {k2, k1 + 1, Floor[M/2], 1}] ,
      {k1, 1, Floor[M/2] - 1, 1} ];

melhor := otima[[1]];
    For[k = 1, k < Floor[M/2]*(Floor[M/2] - 1)/2,
      If[otima[[k, 3]] > melhor[[3]], melhor = otima[[k]]],
      k++];
    (*Print["matriz de todas as representações"]; Print[otima];]*)
Print[M, "   (", melhor[[1]], "  ,  ", melhor[[2]], ")   ", melhor[[3]],
      "    ", melhor[[4]], "  ", melhor[[5]]];]

For[m=5, m<101, clicotima[m],m++]
```

```
 6  *  ( 1   ,   2 )    1.41421      x1->1.    x2->1.
 7     ( 1   ,   2 )    1.3569       x1->0.775369    x2->1.39717
 8  *  ( 1   ,   3 )    1.41421      x1->1.    x2->1.
 9     ( 1   ,   3 )    1.27549      x1->1.33333    x2->1.12537
 10 *  ( 1   ,   3 )    1.22474      x1->1.33333    x2->1.33333
 11    ( 1   ,   3 )    1.22652      x1->1.05467    x2->1.60426
 12 *  ( 2   ,   3 )    1.22474      x1->1.33333    x2->1.33333
 13 *  ( 1   ,   5 )    1.14516      x1->1.52509    x2->1.52509
 14    ( 1   ,   4 )    1.09456      x1->1.85285    x2->1.48587
 15 *  ( 1   ,   4 )    1.09132      x1->1.67929    x2->1.67929
 16    ( 1   ,   4 )    1.01959      x1->2.    x2->1.84776
 17 *  ( 1   ,   4 )    0.987552      x1->2.05074    x2->2.05074
 18    ( 1   ,   5 )    1.            x1->2.42028    x2->1.57972
 19    ( 1   ,   4 )    0.970361      x1->1.72096    x2->2.52713
 20    ( 1   ,   8 )    0.959849      x1->2.    x2->2.34164
 21    ( 1   ,   4 )    0.892013      x1->2.017    x2->3.01011
 22    ( 1   ,   6 )    0.928783      x1->2.96803    x2->1.6689
 23    ( 1   ,   5 )    0.923038      x1->2.29063    x2->2.40421
 24    ( 3   ,   4 )    0.91018       x1->2.    x2->2.82843
 25    ( 1   ,   10 )   0.871154     x1->2.89443    x2->2.37629
```

```
26    ( 1   ,   10 )   0.838353     x1->2.53951    x2->3.15172
27    ( 1   ,   6 )    0.821316      x1->3.62785    x2->2.30194
28    ( 1   ,   6 )    0.847216      x1->3.10034    x2->2.47244
29    ( 1   ,   5 )    0.799272      x1->2.61406    x2->3.64732
30 *  ( 3   ,   5 )    0.831254      x1->2.89443    x2->2.89443
31    ( 1   ,   12 )    0.779902      x1->3.76171    x2->2.81457
32    ( 1   ,   7 )    0.765367      x1->4.4499    x2->2.37852
33    ( 1   ,   6 )    0.765671      x1->3.51028    x2->3.31272
34    ( 1   ,   6 )    0.773165      x1->3.18068    x2->3.51069
35    ( 1   ,   10 )    0.749627      x1->2.89443    x2->4.22376
36    ( 1   ,   14 )    0.717261      x1->5.15688    x2->2.61822
37    ( 1   ,   8 )    0.726279      x1->4.88387    x2->2.69934
38    ( 1   ,   16 )    0.726504      x1->3.59381    x2->3.9847
39    ( 1   ,   7 )    0.721177      x1->4.28733    x2->3.40356
40    ( 4   ,   5 )    0.71449      x1->2.89443    x2->4.9411
41 *  ( 1   ,   9 )    0.679374      x1->4.33323    x2->4.33323
42    ( 1   ,   12 )    0.695895      x1->4.    x2->4.25985
43    ( 1   ,   12 )    0.661994      x1->3.69395    x2->5.43357
44    ( 1   ,   8 )    0.654098      x1->6.03302    x2->3.31619
45    ( 1   ,   19 )    0.68404      x1->4.15063    x2->4.398
46    ( 1   ,   7 )    0.673878      x1->4.17573    x2->4.63269
47    ( 1   ,   7 )    0.655368      x1->4.49542    x2->4.81758
48    ( 1   ,   18 )    0.63924      x1->4.    x2->5.78886
49    ( 1   ,   14 )    0.64574      x1->5.31194    x2->4.28086
50    ( 1   ,   14 )    0.628092      x1->5.07747    x2->5.06196
51    ( 1   ,   9 )    0.624104      x1->6.75337    x2->3.51605
52    ( 1   ,   22 )    0.63805      x1->5.5698    x2->4.25562
53    ( 1   ,   8 )    0.633893      x1->5.2471    x2->4.70761
54    ( 1   ,   12 )    0.610561      x1->4.    x2->6.73004
55    ( 1   ,   7 )    0.589275      x1->5.02807    x2->6.49116
56    ( 4   ,   7 )    0.62184      x1->5.31194    x2->5.03239
57    ( 1   ,   24 )    0.595236      x1->6.0615    x2->5.22817
58    ( 1   ,   22 )    0.592924      x1->5.26674    x2->6.11114
59    ( 1   ,   25 )    0.5899      x1->7.17249    x2->4.32237
60    ( 1   ,   9 )    0.586215      x1->6.8794    x2->4.76042
61    ( 1   ,   8 )    0.590391      x1->5.32794    x2->6.14779
```

```
62    ( 1   ,   8 )    0.569237      x1->6.01352    x2->6.33099
63    ( 1   ,   14 )    0.57549      x1->5.31194    x2->6.76576
64    ( 1   ,   19 )    0.563177      x1->4.69041    x2->7.92121
65    ( 1   ,   10 )    0.542568      x1->9.05544    x2->4.53245
66    ( 1   ,   10 )    0.563465      x1->7.92157    x2->4.67713
67    ( 1   ,   10 )    0.54398      x1->8.71435    x2->4.80307
68    ( 1   ,   9 )    0.558859      x1->6.76644    x2->6.04079
69    ( 1   ,   8 )    0.550862      x1->5.39007    x2->7.79173
70    ( 5   ,   7 )    0.554069      x1->5.31194    x2->7.71772
71    ( 1   ,   21 )    0.52921      x1->6.97719    x2->7.30528
72    ( 1   ,   16 )    0.54199      x1->6.82843    x2->6.78845
73    ( 1   ,   11 )    0.525076      x1->9.78426    x2->4.72401
74    ( 1   ,   22 )    0.53858      x1->5.59235    x2->8.1975
75    ( 1   ,   33 )    0.538464      x1->6.76617    x2->7.02962
76    ( 1   ,   10 )    0.533996      x1->7.91403    x2->6.11359
77    ( 1   ,   9 )    0.528206      x1->6.66387    x2->7.67296
78    ( 1   ,   9 )    0.518023      x1->7.04424    x2->7.8618
79    ( 1   ,   9 )    0.503411      x1->7.73475    x2->8.04916
80    ( 5   ,   8 )    0.523802      x1->6.82843    x2->7.75052
81    ( 1   ,   18 )    0.510436      x1->8.54863    x2->6.80379
82    ( 1   ,   30 )    0.503273      x1->5.61973    x2->10.1728
83    ( 1   ,   11 )    0.497614      x1->10.1287    x2->6.02515
84    ( 1   ,   25 )    0.508177      x1->7.14288    x2->8.34636
85    ( 1   ,   10 )    0.4948      x1->8.76668    x2->7.57137
86    ( 1   ,   10 )    0.503664      x1->8.01572    x2->7.75235
87    ( 1   ,   9 )    0.487678      x1->7.10117    x2->9.71761
88    ( 1   ,   16 )    0.489188      x1->6.82843    x2->9.88662
89    ( 1   ,   20 )    0.470343      x1->9.82749    x2->8.25381
90    ( 5   ,   9 )    0.495054      x1->8.54863    x2->7.7727
91    ( 1   ,   12 )    0.478631      x1->11.3724    x2->6.08815
92    ( 1   ,   12 )    0.466671      x1->12.156    x2->6.211
93    ( 1   ,   34 )    0.477262      x1->7.22791    x2->10.333
94    ( 1   ,   28 )    0.479411      x1->8.94285    x2->8.46094
95    ( 1   ,   11 )    0.473237      x1->10.0481    x2->7.81279
96    ( 1   ,   10 )    0.475506      x1->8.09631    x2->9.59447
97    ( 1   ,   10 )    0.461932      x1->8.9649    x2->9.78094
```

```
98    ( 1   ,   36 )    0.453171      x1->10.3693    x2->9.10828
99    ( 1   ,   18 )    0.465511      x1->8.54863    x2->9.90999
100    ( 1   ,   44 )    0.461448      x1->11.3462    x2->7.43892
101    ( 1   ,   30 )    0.461769      x1->9.84987    x2->8.90914
```

Tabela dos Melhores Códigos Esféricos Conhecidos em Dimensão Quatro

M	ângulo	distância	M	ângulo	distância	M	ângulo	distância
5	104.478	1.58114	37	50.9227	0.859804	69	41.1814	0.703379
6	90.	1.41421	38	50.1535	0.847664	70	41.0851	0.701806
7	90.	1.41421	39	49.6896	0.840323	71	40.8538	0.698024
8	90.	1.41421	40	49.4209	0.836065	72	40.7099	0.695669
9	80.6761	1.29459	41	49.0595	0.830331	73	40.6071	0.693987
10	80.4059	1.29099	42	48.8204	0.826534	74	40.5754	0.693469
11	76.679	1.24064	43	48.4964	0.82138	75	40.4865	0.692013
12	75.5225	1.22474	44	48.0251	0.813874	76	40.4419	0.691282
13	72.1037	1.17703	45	47.3962	0.803835	77	40.075	0.68527
14	71.3662	1.1666	46	46.9743	0.797087	78	39.7568	0.680051
15	69.452	1.1393	47	46.7329	0.79322	79	39.3705	0.673706
16	67.193	1.10668	48	46.3833	0.787615	80	39.1322	0.669788
17	65.6532	1.0842	49	46.0991	0.783053	81	38.9405	0.666634
18	64.9873	1.07441	50	46.0742	0.782654	82	38.7617	0.663691
19	64.2619	1.06371	51	45.4625	0.772819	83	38.6412	0.661707
20	64.2619	1.06371	52	45.2812	0.769899	84	38.5216	0.659738
21	61.876	1.02822	53	44.9542	0.764629	85	38.3972	0.657687
22	60.1399	1.00211	54	44.7883	0.761952	86	38.2835	0.655812
23	60.	1.	55	44.3025	0.754106	87	38.2316	0.654957
24	60.	1.	56	44.0114	0.749398	88	38.1934	0.654328
25	57.4989	0.96196	57	43.7496	0.745159	89	37.9526	0.650354
26	57.2626	0.958343	58	43.5342	0.741669	90	37.7779	0.64747
27	56.1106	0.940647	59	43.3908	0.739344	91	37.6841	0.645921
28	55.4351	0.930227	60	43.2167	0.736521	92	37.6074	0.644653
29	55.0299	0.92396	61	42.9862	0.732779	93	37.5288	0.643355
30	54.2512	0.911885	62	42.7871	0.729544	94	37.4811	0.642567
31	53.7886	0.904692	63	42.377	0.722876	95	37.1571	0.637208
32	53.436	0.899199	64	42.3062	0.721723	96	37.0622	0.635639
33	53.076	0.893582	65	42.0566	0.717658	97	36.9192	0.633272
34	52.4011	0.883029	66	41.755	0.712742	98	36.7967	0.631243
35	51.5725	0.87003	67	41.4988	0.708562	99	36.6983	0.629614
36	51.0745	0.862196	68	41.3146	0.705556	100	36.5636	0.627382

Tabela 4.4: Os melhores $[M, 4]$ códigos esféricos conhecidos, segundo ângulo mínimo e distância mínima (veja [42]).

Referências Bibliográficas

[1] S. Benedetto, E. Biglieri, *Principles of digital Transmition*, Kluwer Academic / Plenum Publishers, 2000.

[2] I. F. Blake, "Distance Properties of Group Codes", SIAM J. Appl. Math., vol 23, pp 312-324, 1972.

[3] I. F. Blake, "Configuration Matrices of Group Codes", IEEE Transaction of Information Theory, vol IT-20, pp 95-100, 1974.

[4] I. F. Blake and D.$\check{Z}$. Djoković, "An Optimization Problem for Unitary and Orthogonal Representations of finite Groups", Transaction of the American Mathematical Society, vol 164, pp 267-274, 1972.

[5] E. Biglieri and M. Elia, "On the Existence of Groups Codes for the Gaussian Channel", IEEE Transaction on Information Theory, vol IT-18, pp 399-402, 1972.

[6] E. Biglieri and M. Elia, "Optimum Permutation Modulation codes and Their Asymptotic Performance", IEEE Transaction on Information Theory, IT-22, pp 751-753,1976.

[7] E. Biglieri and M. Elia, "Cyclic-Group Codes for the Gaussian Channel", IEEE Transaction on Information Theory, IT-22, pp 624–629, 1976.

[8] E. Biglieri, J.K. Karlof and E. Viterbo, "Representing Group Codes as Permutation Codes", IEEE Transaction on Information Theory, vol 45, pp 2204-2207, 1999.

[9] K. Böröczky, "Packing of Spheres in Spaces of Constant Curvature", Acta Math. Acad. Scient. Hung., 32, 243-261, 1978.

[10] M. P. do Carmo, *Differential Geometry of Curves and Surfaces*, Prentice-Hall, 1976.

[11] S. I. R. Costa et alli, "Graphs, Tessellations, and Perfect Codes on Flat Tori", IEEE Transaction on Information Theory, vol 50, pp. 2363–2377, 2004.

[12] S. I. R. Costa, E. Agustini and R. Palazzo Jr, "On knotted M-PSK correct reception performance", Proc. VII Int. Workshop - ACCT 2000, Bansko, Bulgaria, June 19-24, pp 103-106, 2000.

[13] H. S. M. Coxeter, "Arragements of equal spheres in non-Euclidean spaces", acta Math. Acad. Sci. Hungar., 4, pp 263-274, 1954.

[14] H. S. M. Coxeter, *Regular Polytopes*, 3nd edition, Dover Publicatons, 1973.

[15] H. S. M. Coxeter, *Regular Complex Polytopes*, 2nd edition, Cambridge University Press, 1991.

[16] E. Lages Lima, *Álgebra Linear*,3a. edição, Coleção Matemática Universitária, IMPA, 1998.

[17] T Ericson, V. Zinoviev, *Codes on Euclidian Spheres*, Elsevier Science Pub Co, 2001.

[18] G. D. Forney,Jr, "Geometrically Uniform codes", IEEE Transactions on Information Theory, Vol 37, pp , 1991.

[19] F. R. Gantmacher, *The theory of matrices*, vol 1, Chelsea, 1959.

[20] A. Garcia e Y. Lequain, *Elementos de Álgebra*, Projeto Euclides, IMPA, 2002.

[21] T. C.Hales, "A Proof of the Kepler Conjecture."Ann. Math., 162, 1065-1185, 2005.

[22] I. Ingemarsson "Commutative Group codes for the Gaussian Channel", IEEE Transaction on Information Theory, vol IT-19, pp 215-219, 1973.

[23] I. Ingemarsson "Optimized Permutation Modulation", IEEE Transaction on information Theory, vol 36, pp 1098-1100,1990.

[24] J. Karlof "Permutation Codes for the Gaussian Channel", IEEE Transaction on Information Theory, vol 35, pp 726-732, 1989.

[25] J. Karlof and Y. O. Chang "Optimal Permutation Codes for the Gaussian Channel", IEEE Transaction on Information Theory, vol 43, pp 356-358, 1997.

[26] J. Karlof and C. P. Downey, "Optimal [M,3] Group Codes for the Gaussian Channel", IEEE Transaction on Information Theory, vol IT-24, pp 760-761, 1976.

[27] J. Karlof and C. P. Downey, "On the existence of [M,n] Group Codes for the Gaussian Channel With M and n Odd", IEEE Transaction on Information Theory, vol IT-23, pp 500-503, 1977.

[28] J. Karlof and C. P. Downey, "Odd Group codes for the gaussian channel", SIAM J. Appl. Math., vol 34, pp 715-716, 1978.

[29] J. Karlof and C. P. Downey, "Computation Methods for Optimal [M,3] group codes for the gaussian channel", Utilitas Mathematica, vol 18, 1980.

[30] H. Loeliger "Signals Sets Matched to Groups", IEEE Transaction on Information Theory, vol 37, pp 1675-1682, 1991.

[31] T. Mittelholzer "Group codes generated by finite reflection groups", IEEE Transaction on Information Theory, vol 42, pp 518-528, 1996.

[32] M. Nilsson and H. Lennerstad, "An upper bound on the minimum Euclidean distance for block-coded phase-shift keying". IEEE Transaction on Information Theory, 46, 656–662, 2000.

[33] R. A. Rankin, "The Closest Packing of Spherical Caps in n Dimensions", Proc. Glasgow Math. Assoc., vol. 2, pp 139-144, 1954.

[34] P. Ribenboin, *Linear Representation of Finite Groups*, Lecture Notes, Queen's Papers in Pure and Applied Mathematics, No. 5, Queen University, 1966.

[35] C. A. Rogers, "The Packing of Equal Spheres", Proc. London Math. Soc., 3, pp 609-620, 1958.

[36] K. Schütte und B.L. van der Waerden, "Auf welcher Kugel haben 5,6,7,8 oder 9 Punkte mit Mindestabstand l Platz?"Math Ann. 123, 96-124, 1951.

[37] R. Siqueira and S. I. R. Costa , " Minimum Distance Upper Bounds for Commutative Group Codes", Proceedings of IEEE Information Theory Workshop (ITW 2006), Uruguay, March 13-17, 2006.

[38] S. I. R. Costa, J. E. Strapasson, M. Muniz, T. B. Carlos and R. M. Siqueira, "Circulant Graphs Viewed as Graphs on Flat Tori", submetido para publicação,2006.

[39] R. Siqueira and S. I. R. Costa, "Sobre a Geometria dos códigos de Grupos Cíclicos", Anais do VII ERMAC/ 2005 - Vitória ES, 2005.

[40] D. Slepian,"Group codes for the Gaussian Channel", The Bell System Technical Journal, vol 47, pp. 575-602, 1968.

[41] N. J. A. Sloane, J. H. Conway *Sphere Packings, Lattices and Groups*, 3 edt, Springer-Verlag , 1991.

[42] N. J. A. Sloane, with the collaboration of R. H. Hardin, W. D. Smith and others, Tables of Spherical Codes, published electronically at www.research.att.com/ njas/packings/

[43] J. Stillwell, *Geometry of Surfaces*, Springer-Verlag, 1992.

[44] P. M. L. Tammes, "On the origin of number and arrangement of places of exit on the surface of pollen grains", Recueil des Travaux Botanique Neerlandais, 27, pp 1-84, 1930.

[45] L. F. Tóth, "Über die dichteste Kugellagerung", Math. Zeitschrift, 48, pp 676-684, 1943.

[46] L. F. Tóth, "Über eine Abschätzung des kr̈zesten Abstandes zweier Punkte eines auf einer Kugelfläche liegenden Punktsystems", Jahresbericht Deut. Math. Verein., vol 53, pp 66-68, 1943.

[47] L. F. Tóth, "On the Densest Packing of Spherical Caps", American Mathematical Monthly, 56 ,pp 330-331, 1949.

[48] L. F. Tóth, "Kreisausfüllungen der hyperbolischen Ebene", Acta Math. Acad. Sci. Hungar., 4, 103-110, 1953.

[49] L. F. Tóth, "Über die dichteste Horozyklenlagerung", Acta Math. Acad. Sci Hungar., 5, 41-44, 1954.

[50] V. Vaishampayan and S. I. R. Costa, "Curves on a Sphere, Shift-Map Dynamics, and Error Control for Continuos Alphabet Sources", IEEE Transaction on Information Theory, vol 49, pp 1658-1672, 2003.

[51] E. W. Weisstein. “Kepler Conjecture.”From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/KeplerConjecture.html

[52] J. M. Wozencraft and I. M. Jacobs, *Principles of Communication Engineering*, John Wiley and Sons, 1990.

Índice Remissivo