Universidade Estadual de Campinas

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Departamento de Matemática

Dissertação de Mestrado

De Códigos Binários a Reticulados e Códigos Esféricos

por

Anderson Tiago da Silva †

Mestrado em Matemática - Campinas - SP

Orientador: Prof(a). Dr(a). Sueli Irene Rodrigues Costa

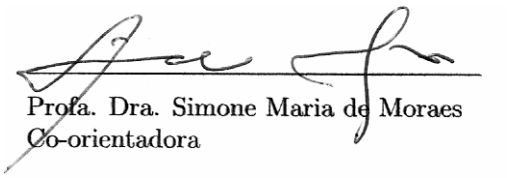
Co-orientador: Prof(a). Dr(a). Simone Maria de Moraes

†Este trabalho contou com apoio financeiro da CAPES.

De Códigos Binários a Reticulados e Códigos Esféricos

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Anderson Tiago da Silva e aprovada pela comissão julgadora.
Campinas, 12 de abril de 2007

Prof[a]. Dr[a]. **Sueli I. R. Costa**
Orientadora



Profa. Dra. Simone Maria de Moraes
Co-orientadora

Banca Examinadora

1. Prof. Dr. Francisco Cesar Polcino Milies
2. Prof. Dr. Marcelo Muniz Silva Alves
3. Profa. Dra. Sueli Irene Rodriques Costa

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

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

Silva, Anderson Tiago da
Si38c De códigos binários a reticulados e códigos esféricos / Anderson Tiago da Silva -- Campinas, [S.P. :s.n.], 2007.

Orientador : Sueli Irene Rodrigues Costa; Simone Maria de Moraes
Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos reticulados. 2. Códigos de controle de erros (Teoria da informação). 3. Empacotamento de esferas. I. Costa, Sueli Irene Rodrigues. II. Moraes, Simone Maria de. III. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título.

Título em inglês: From binary codes to lattices and spherical codes.

Palavras-chave em inglês (Keywords): 1. Lattice theory. 2. Error-correcting codes (Information theory). 3. Sphere packings.

Área de concentração: Geometria, topologia

Titulação: Mestre em Matemática

Banca examinadora: Prof. Dr. Francisco Cesar Polcino Milies (USP-SP)
Prof. Dr. Marcelo Muniz Silva Alves (UFPR)
Profa. Dra. Sueli Irene Rodrigues Costa (IMECC-UNICAMP)

Data da defesa: 12/04/2007

Programa de Pós-Graduação: Mestrado em Matemática

Dissertação de Mestrado defendida em 12 de abril de 2007 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

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

Prof. (a). Dr (a). FRANCISCO CESAR POLCINO MILIES

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

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me iluminado neste caminho cheio de espinhos e obstáculos.

Aos meus pais Rosino e Marinalva por estarem sempre presentes, me apoiando nas horas mais difíceis, apesar da distância.

Aos meus irmãos Alexsandro, Andréia e Andreza por me darem força, sabendo o quanto é difícil a carreira acadêmica.

A Daniela por ter me proporcionado momentos felizes e por ter me apoiado sempre e apesar de toda dificuldade estar sempre do meu lado.

Aos meus amigos da república, Rogério(Casa), Rogério(Rogerinho), Bruno(Pluck), Maurício (Baiano), José Antonio(Jota), pelas boas gargalhadas na sala e pela ótima convivência, em especial ao meu amigo José António que sempre me ajudou quando precisei.

Aos meus amigos de GV, Rodrigo(Mister), Bruninho(Mister), Leo(mister), Cristiano(Mister), que sempre me fizeram esquecer de todos os problemas durante minhas supostas férias e pela nossa amizade desde a nossa infância.

Aos meus amigos de curso que sempre me fizeram dar boas risadas desde o predinho até o bandejão.

Aos meus amigos do grupo, Cristiano e João, que ajudaram bastante no fim da dissertação.

A todos os meus professores de Viçosa e Unicamp que contribuiram com o meu amadurecimento, em especial a Simone e a Sueli, que me orientaram nesta dissertação com perfeição, paciência, disposição e compreensão.

A Capes pelo apoio financeiro e a todos que contribuiram diretamente ou indiretamente com este trabalho.

Muito obrigado.

Resumo

Este trabalho está dividido essencialmente em quatro tópicos. O primeiro capítulo é dedicado a uma introdução à teoria dos códigos corretores de erros com algumas propriedades e exemplos. No segundo capítulo abordamos reticulados e suas propriedades com foco na análise do quociente de reticulados gerando grafos em toros planares, grafos circulantes obtidos através de quociente de reticulados e ladrilhamentos associados. O terceiro capítulo é dedicado a códigos esféricos, com ênfase na obtenção de códigos ótimos. Foram introduzidos alguns limitantes importantes como o de Rankim, e a demonstração de que alguns códigos esféricos como o simplex e biortogonal são ótimos. No capítulo quatro apresentamos uma construção de reticulados através de códigos binários e também a construção de códigos esféricos a partir de reticulados que possuem sub-reticulados com base ortogonal. Analisamos o caso especial do reticulado BCC que é o de melhor densidade no espaço e pode ser gerado por código binário. Mostramos que o quociente deste por um sub reticulado especial produz o melhor código esférico associado ao grupo comutativo $\mathbb{Z}_2^2 \times \mathbb{Z}_4$. Também identificamos o reticulado que é associado ao melhor código de grupo comutativo de 16 elementos em $\mathbb{R}^6$.

Abstract

In this work it is presented through examples a connection between binary codes, lattices and spherical codes. A brief introduction to coding theory, properties and examples is included in the first chapter. In Chapter 2 lattices are approached with focus on the quotient of lattices, graphs on flat tori and connections with circulant graphs. An introduction to spherical codes and some of their bounds, as the Ranking bound, are described in Chapter 3. Finally in Chapter 4 the three topics above are connected. The construction of lattices from linear binary codes and the construction of spherical codes from the lattices which have orthogonal sub-lattices are presented. We analyze specifically the case of the three dimensional BCC lattice, which has the best packing density for this dimension, and show that a quotient of this lattice give rise to the best spherical code associate to the commutative group $Z_2^2 \times Z_4$. We also identify the lattice which is associate to the best commutative group code with 16 elements in em R^6.

Sumário

Introdução

O objetivo deste trabalho é apresentar através de exemplos uma conexão entre códigos binários, reticulados e códigos esféricos gerados por grupos de matrizes ortogonais. Nos três primeiros capítulos são apresentados de forma resumida, mas com exemplos, numa seleção de tópicos, conceitos e propriedades destes três temas com referências para os resultados e extensões. O propósito foi a redação de um texto razoavelmente auto-contido com o estabelecimento de resultados importantes neste contexto e a fixação de notação.

O primeiro capítulo é dedicado a uma breve introdução à teoria dos códigos corretores de erros com algumas propriedades e exemplos.Foram destacados aspectos como distância de Hamming e correção de erros, códigos perfeitos, códigos binários lineares e em particular o código de Hamming. As principais referências aqui foram [1, 3, 16].

No segundo capítulo abordamos reticulados e suas propriedades com foco na densidade de empacotamento, na análise do quociente de reticulados gerando grafos em toros planares, grafos circulantes obtidos através de quociente de reticulados e ladrilhamentos associados. Principais referências aqui são [2, 3, 5]. Destaque foi dado a detalhamentos de [2] sobre reticulados que admitem sub-reticulados com base ortogonal, caso em que ao mergulharmos o grafo contido num toro e gerado pelo quociente de reticulados, obteremos um código esférico gerado por um grupo comutativo de matrizes ortogonais.

O terceiro capítulo é dedicado a uma introdução aos códigos esféricos e alguns limitantes importantes como o de Rankim para o número de pontos fixado um patamar inferior para distância entre dois pontos , e à apresentação de dois códigos esféricos ótimos (com máxima distância mínima) para a respectiva dimensão e número de pontos: os códigos simplex e bi-ortogonal. Foram também introduzidos os conceitos de códigos de grupo e em particular os gerados por grupos comutativos. Principais referências utilizadas para neste capítulo

são:[3, 10, 11].

No capítulo quatro apresentamos a construção A de reticulados através de códigos binários exemplificando com os códigos D_n e em particular o D_3 que é equivalente ao BCC (body-centered cubic lattice) e ao FCC (face- centered cubic lattice-ou pilha de laranja) , que é o reticulado com maior densidade de empacotamento no espaço tri-dimensional. Ilustramos a construção de códigos esféricos em dimensão $2n$ a partir de reticulados n- dimensionais que possuem sub-reticulados com base ortogonal tomando diversos sub-reticulados do BCC. Analisamos a distância mínima dos códigos esféricos obtidos e determinamos a deformação a um parâmetro do reticulado que produz o melhor código esférico em dimensão 6 de 16 palavras associado ao grupo comutativo $Z_2^2 \times Z_4$. No sentido inverso, identificamos o reticulado que é associado ao melhor código de grupo comutativo de 16 elementos em R^6. As distâncias mínimas obtidas foram comparadas ao limitante especifico para códigos esféricos de grupos comutativos apresentado em [14].

Capítulo 1

Códigos Corretores de Erros

Apresentaremos neste capítulo, os conceitos básicos da **Teoria de Códigos**, introduzindo algumas ferramentas úteis para sua construção e alguns tipos de códigos como exemplo.

As principais referências para este capítulo são [1], [3] , [16] e [17].

1.1 Introdução

A teoria de códigos corretores de erros é parte da teoria da informação que tem como marco fundamental o trabalho de **C.E.Shannon** de 1948, "A mathematical theory of communications". Esta teoria teve um desenvolvimento considerável nas décadas de 50 e 60. A partir da década de 70, com o avanço das pesquisas espaciais e da grande popularização dos computadores, este desenvolvimento passa a ser mais acentuado. Os códigos corretores de erros são utilizados principalmente quando se deseja transmitir ou armazenar uma informação de forma segura.

A **teoria de códigos corretores de erros** trata da correção de dados obtidos na transmissão e armazenamento através de canais ruidosos de modo confiável, visto que ao se transmitir uma informação pode ocorrer alguma forma de interferência no trajeto ocasionando alguma alteração, e este tipo de problema é comum nos meios de comunicação e de transmissão de informações. Para solucionar, incorpora-se alguma forma de redundância

aos dados originais. Através destas redundâncias é possível recuperar a informação original quando erros forem introduzidos (até algum nível de tolerância), ou detectar a presença de erros. Trata-se portanto de analisar um método eficiente de se introduzir estas redundâncias.

1.2 Códigos Corretores de Erros

Partimos de um **alfabeto** A, que consiste de um conjunto finito. O número de elementos de A será denotado por $\mid A \mid$ e será simbolizado por q.

Definição 1.2.1. *Seja A um alfabeto. Um* **código corretor de erros** *C é um subconjunto próprio de A^n, onde n é um número natural. Os elementos do código são chamados de* **palavras-código***, ou simplesmente de* **palavras***.*

Apresentaremos agora alguns exemplos para uma melhor familiarização dos conceitos definidos acima.

Exemplo 1.2.2. *O exemplo mais familiar de um Código Corretor de Erros é um idioma. Por exemplo: Seja A o alfabeto formado pelas 23 letras do alfabeto da língua portuguesa, mais o espaço em branco, bem como o c cedilha e as vogais acentuadas, sendo estes também considerados como palavras do alfabeto.*

Uma palavra da língua portuguesa pode ser considerada como um elemento de A^{27}, onde o 27 é o comprimento da palavra mais longa da língua portuguesa.

Como o conjunto das palavras da língua portuguesa é um subconjunto próprio de A^{27}, temos que ele é capaz de detectar e corrigir erros, mas não de forma eficiente, pois se a palavra cama fosse erroneamente escrita como cana ou casa, nós não detectaríamos o erro. Este não é um bom código, porque algumas palavras deste código são muito próximas umas das outras.

A forma de solucioná-lo é incorporar redundâncias aos dados originais.

Exemplo 1.2.3. *Em 1972, a nave espacial Mariner 4 transmitiu 22 fotos em preto e branco de Marte usando o seguinte sistema: Cada foto foi decomposta em 200×200 elementos de imagem, a cada elemento de imagem, foi atribuído um dos 64 tons de cinza pré-escolhidos e codificados como elementos de $\{0,1\}^6$, correspondente ao código da fonte.*

Exemplo 1.2.4. *Suponhamos que temos um robô que se move sobre um tabuleiro quadriculado, de modo que ao darmos um comando (Leste, Oeste, Norte, Sul), o robô se desloca do centro de uma casa para o centro da casa indicada pelo comando.*

Os quatro comandos acima podem ser codificados como elementos de $\{0,1\}\times\{0,1\}$ *como se segue:*

$$\begin{array}{cccccc} Leste & \mapsto & 00 & Norte & \mapsto & 10 \\ Oeste & \mapsto & 01 & Sul & \mapsto & 11 \end{array}$$

O código do lado direito da tabela acima é chamado de **código fonte**. *Suponhamos agora que um destes pares ordenados, ou melhor dizendo uma palavra, seja enviada por algum meio de transmissão(rádio por exemplo), como o* 00 *e por causa de alguma interferência que ocorreu durante o caminho, seja recebida como* 01. *O que faria com que o robô, em vez de ir para o Leste que era a ordem inicial fosse para o Oeste que é o caminho ordenado pela palavra recebida? O que fazemos então é introduzir alguns dígitos, ou redundâncias, que permitam detectar e corrigir erros como este apresentado por exemplo.*

Podemos então modificar o nosso código como se segue:

$$\begin{array}{ccc} 00 & \mapsto & 00000 \\ 01 & \mapsto & 01011 \\ 10 & \mapsto & 10110 \\ 11 & \mapsto & 11101 \end{array}$$

Nessa codificação, as duas primeiras posições reproduzem o código da fonte, enquanto que as outras três restantes são redundâncias introduzidas. O novo código introduzido na codificação é chamado de **código de canal**.

1.3 Métrica de Hamming

A fim de que se possa tornar possível uma noção intuitiva de proximidade de palavras dentro de um código, apresentaremos a seguir um modo de medir a distância entre palavras em A^n.

Definição 1.3.1. *Dados dois elementos* $u=(u_1,...,u_n)$, $v=(v_1,...,v_n)\in A^n$, *a* **distância**

de Hamming *entre u e v é definida como*

$$\mathbf{d(u,v)} =\mid \{\mathbf{i} : \mathbf{u_i} \neq \mathbf{v_i}, \mathbf{1} \leq \mathbf{i} \leq \mathbf{n}\} \mid,$$

onde $\mid x \mid$ indica o número de elementos de x.

Proposição 1.3.2. *[1] (A^n, d) é um espaço métrico, onde d é a métrica de Hamming*

Prova:

(i) Como $d(u,v) =\mid \{i : u_i \neq v_i, 1 \leq i \leq n\} \mid$, e $\mid \{i : u_i \neq v_i, 1 \leq i \leq n\} \mid \geq 0$, pois é um número natural, temos que $d(u,v) \geq 0$, $\forall u, v \in A^n$.

Agora $d(u,v) = 0$ significa que $u_i = v_i$, para todo i com $1 \leq i \leq n$, portanto $u = v$.

(ii) É imediato a verificação que $d(u,v) = d(v,u)$.

(iii) Para mostrarmos que $d(u,v) \leq d(u,w) + d(w,v)$ observemos inicialmente que $d(u,v) = |\{i; u_1 \neq v_i\}| = n - |A|$, onde $A = \{i; u_i = v_i\}$. Daí se $B = \{i|u_i = w_i\}$ e $C = \{i|w_i = v_i\}$, temos que: Se $i \in B$ e C, então $i \in A$. Daí $B \cap C \subset A$. Logo $A^c \subset (B \cap C)^c = B^c \cup C^c$. Portanto, $d(u,v) = |A^c| \leq |B^c \cup C^c| \leq |B^c| + |C^c| = d(u,v) + d(w,v)$.

■

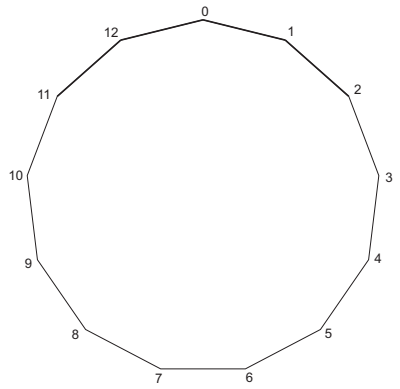
Definição 1.3.3. *Sejam a, $b \in Z_q^n$, onde $a = (a_1, ..., a_n)$ e $b = (b_1, ..., b_n)$. A distância de Lee é definida sobre $\mathbb{Z}_q^n$ da seguinte forma:*

$$d_L(a,b) = \sum_{i=1}^{n} \min\{\mid a_i - b_i \mid, \mid q - (a_i - b_i) \mid\}$$

Com a distância definida desta forma, pode-se provar que d_L é uma métrica e esta métrica é chamada de **métrica de Lee**. $\mathbb{Z}_q^n$ com esta métrica é chamado espaço de Lee.

Exemplo 1.3.4. *Considere em $\mathbb{Z}_{15}$ as classes $\overline{1}$, $\overline{4}$ e $\overline{12}$, temos que*

$$d_L(\overline{1}, \overline{4}) = 3 \text{ e } d_L(\overline{1}, \overline{12}) = 4.$$



Se colocarmos as classes de $\mathbb{Z}_q$ como vértices de um polígono regular de q lados, a distância de Lee entre duas classes será o menor número de arestas que conectam estes vértices. A figura abaixo ilustra o exemplo em $\mathbb{Z}_{13}$.

Observe que $d_L(\bar{1}, \bar{11}) = 3$ e $d_L(\bar{1}, \bar{4}) = 3$.

Definição 1.3.5. *Sejam $a \in A^n$ e $t \in \mathbb{R}$, $t > 0$. Definimos o* **disco** *e a* **esfera** *de centro a e raio t em A^n, como os seguintes subconjuntos respectivamente:*

$$D(a,t) = \{u \in A^n : d(u,a) \leq t\}$$

$$S(a,t) = \{u \in A^n : d(u,a) = t\}.$$

Definição 1.3.6. *Seja C um código. A* **distância mínima** *de C é o número*

$$d = min\{d(u,v) : u, v \in C \quad e \quad u \neq v\}.$$

A distância mínima de um Código é um parâmetro muito importante, pois como veremos mais adiante, ela determina a capacidade de correção de erros deste Código.

Dado um código C com distância mínima d, denotaremos por k o número

$$k = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

onde $\lfloor t \rfloor$ representa a parte inteira de um número real positivo t.

Ao longo deste capítulo, a menos de menção ao contrário, ao falarmos em distância "d"estaremos assumindo a distância de hamming.

Lema 1.3.7. *Seja C um código com distância mínima d. Se c e c' são palavras distintas de C, então*

$$D(c,k) \cap D(c',k) = \emptyset.$$

Prova: Se $x \in D(c,k) \cap D(c',k)$, então $D(x,c) \leq k$ e $D(x,c') \leq k$, e assim, pela simetria e pela desigualdade triangular, temos que

$$d \leq d(c,c') \leq d(c,x) + d(x,c') \leq 2k \leq d-1$$

■

O teorema a seguir irá nos fornecer uma idéia para efetuarmos uma correção de erros ocorridos na transmissão de alguma palavra de um código C.

Teorema 1.3.8. *[17] Um código C com distância mínima d corrige t erros se, e somente se, $d \geq 2t+1$*

Prova: Dada uma palavra c do código, podemos introduzir até $d-1$ erros sem encontrar outra palavra do código, e assim, a detecção do erro será possível.

Por outro lado, se d é ímpar, $t = \left\lfloor \frac{d-1}{2} \right\rfloor = \frac{d-1}{2}$.. Se tomamos $t+1 = \frac{d+1}{2}$, já encontramos $u \in \mathbb{Z}_2^n$ e $v \in C$ tais que $u \in B(o, t+1) \cap B(v, t+1)$. Sem perda de generalidade, tome $v = 11...100...0$. Daí tome u como abaixo

$$\begin{array}{l} u = 00...011...110... \\ v = 11...111...100... \end{array}.$$

Para d par é análogo. No caso do alfabeto ser diferente de $\mathbb{Z}_2^n$, tome

$$v = \alpha_1\alpha_2...\alpha_{\frac{d+1}{2}}\beta_1\beta_2...\beta_{\frac{d-1}{2}}0...0,$$

com $\alpha_i,\ \beta_i \neq 0$ e

$$u = \underbrace{00...0}_{\frac{d+1}{2}}\beta_1\beta_2...\beta_{\frac{d-1}{2}}10...0.$$

■

Observação 1.3.9. *Outro fato importante que decorre do teorema acima é que um código terá maior capacidade de correção de erros quanto maior for a sua distância mínima. Portanto, é fundamental, para a teoria de códigos, ser possível calcular d ou pelo menos determinar uma cota inferior para ele.*

Será apresentado agora uma estratégia simples para efetuar uma correção de uma palavra recebida quando isso for possível.

Seja C um código com distância mínima d e $k = \lfloor \frac{d-1}{2} \rfloor$.

Suponhamos que o receptor receba uma palavra r. O algoritmo abaixo irá efetuar a correção do erro quando for possível.

(i) Estabeleça os discos de raio k em torno das palavras do código e assim, se r pertencer à algum destes discos, basta trocar a palavra r pela palavra do centro do disco.

(ii) Se r não pertencer a nenhum disco de raio k em torno de uma palavra $c \in C$ então não será possível decodificar r com boa margem de segurança.

1.4 Códigos Perfeitos

Definição 1.4.1. *Seja $C \subset A^n$ um código com distância mínima d e seja $k = \left\lfloor \frac{d-1}{2} \right\rfloor$. Diremos que o código C é* **perfeito** *se*

$$\bigcup_{c \in C} D(c,k) = A^n.$$

Note que quando um código for perfeito, o item (ii) da estratégia dada na seção anterior para corrigir erros não vai acontecer, pois a palavra recebida r sempre estará am algum disco $D(c,k)$, para alguma palavra c do código C, sendo este disco único pelo lema 1.3.7.

Denotemos por $A_q(n,d)$ o número máximo de palavras sobre F_q de comprimento n e distância mínima d, e $B_q(n,d)$ o número máximo de palavras de um código linear de comprimento n e peso mínimo menor que d.

Claramente $B_q(n,d) \leq A_q(n,d)$.

Teorema 1.4.2. *[21] Seja C um código sobre F_q de comprimento n e distância mínima d e $k = \lfloor \frac{d-1}{2} \rfloor$. Então*

$$A_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{k} \binom{n}{i} (q-1)^i}.$$

Prova: Suponhamos que C tenha M palavras. Por 1.3.7, temos que as esferas centradas nas palavras de C de raio k são disjuntas. Assim, $\alpha = \sum_{i=0}^{k} \binom{n}{i} (q-1)^i$são todos os vetores destas esferas, e como as esferas são disjuntas, temos que $M\alpha$ não pode ultrapassar o número q^n de vetores em F^n. ■

1.5 Equivalência de Códigos

Quando estabelecemos uma equivalência, do ponto de vista matemático, estamos estabelecendo classes de objetos que possuem algum tipo de informação semelhante, referente a equivalência dada. A noção de equivalência de códigos será dada a partir das isometrias, que definiremos logo abaixo.

Definição 1.5.1. *Seja (M, d) um espaço métrico. Dizemos que $F : M \to M$ é uma isometria se, e somente se, para quaisquer $x, y \in M$,*

$$d(F(x), F(y)) = d(x, y); \forall x, y \in M.$$

Como isometrias são necessariamente bijeções e a inversa e composta de isometrias são isometrias, podemos aplicar estas propriedades em (A^n, d) onde d é a métrica de hamming. A equivalência de códigos é definida a partir de isometrias.

Definição 1.5.2. *Dados dois códigos C e C' em A^n, diremos que C' é* **equivalente** *a C se existir uma isometria F de A^n tal que $F(C) = C'$.*

Das propriedades de isometrias, segue-se que esta é realmente uma relação de equivalência:

(i) É reflexiva: Todo código é equivalente a si proprio. Para verificar isto basta usar a aplicação identidade.

(ii) É simétrica: Se C' é equivalente a C, então C é equivalente a C'. Para verificar isto basta usar a aplicação inversa.

(iii) É transitiva: Se C'' é equivalente a C' e C' é equivalente a C, então C'' é equivalente a C. Para verificar isto basta usar a aplicação composição.

A proposição abaixo fornece-nos um mecanismo para reproduzir uma família de isometrias.

Proposição 1.5.3. *[20] Se $f : A \to A$ é uma bijeção e i é um número inteiro tal que $1 \leq i \leq n$, a aplicação*

$$\begin{array}{rccc} T_f^i: & A^n & \to & A^n \\ & (a_1, ...a_n) & \mapsto & (a_1, ..., f(a_i), ..., a_n) \end{array}$$

é uma isometria.

Prova: Sejam $x = (x_1, ..., x_n)$ e $y = (y_1, ..., y_n) \in A^n$. Como f é bijeção, se $x_i \neq y_i$, então $f(x_i) \neq f(y_i)$. Logo se $x \neq y$, então $T_f^i(x) \neq T_f^i(y)$. Assim,

$$d(T_f^i(x), T_f^i(y)) = d((x_1, ..., f(x_i), ..., x_n), (y_1, ..., f(y_i), ..., y_n)).$$

Suponhamos que $d((x_1, ..., x_n), (y_1, ..., y_n)) = k$, onde $k \leq n$. Assim,

$$d((x_1, ..., f(x_i), ..., x_n), (y_1, ..., f(y_i), ..., y_n)) = k,$$

por que f é bijeção.

■

Assim dado um código C podemos construir uma família de códigos equivalentes a C através de T_f^i.

1.6 Códigos Lineares

Nesta seção estudaremos um tipo de código muito importante, que são os códigos lineares. Na prática esta é de modo geral a classe mais utilizada de códigos.

Definição 1.6.1. *Um código $C \subset K^n$ será chamado de* **código linear** *se for um subespaço vetorial de K^n.*

Observação 1.6.2. *Uma definição equivalente e importante é que Códigos Lineares são obtidos como imagem de uma transformação linear injetiva:*

$$\begin{array}{rccc} \phi: & A^K & \to & A^n \\ & (a_1,...,a_k) & \mapsto & G_{n\times k}\cdot(a_1,...,a_k)^T \end{array}$$

onde $G_{n\times k}$ é uma matriz de posto k formada por elementos do corpo A.

Como todo espaço vetorial de dimensão finita possui uma base, então, dada uma base B de C, onde $B = \{v_1, ..., v_n\}$, temos que todo elemento de C se escreve de maneira única na forma

$$\lambda_1 v_1 + ... + \lambda_k v_k,$$

onde $\lambda_i, \in K, \forall i = 1, ..., k$. Segue daí que $M =\mid C \mid= q^k$, e conseqüentemente $dim_K C = k = \log_q q^k = \log_q M$, onde q é o número de elementos do corpo associado ao espaço vetorial.

Definição 1.6.3. *Dado $x \in K^n$, o* **peso** *de x é o número inteiro dado por*

$$\omega(x) :=\mid \{i : x_i \neq 0\} \mid .$$

Em outras palavras temos que

$$\omega(x) = d(x, 0),$$

onde d representa a métrica de Hamming.

Definição 1.6.4. *O* **peso** *de um código linear C é o inteiro*

$$\omega(C) := \min\{\omega(x) : x \in C - \{0\}\}.$$

Proposição 1.6.5. *[16] Seja $C \subset K^n$ um código linear com distância mínima d. Temos que*

i) $\forall\ x,\ y \in K^n, \quad d(x, y) = \omega(x - y).$

ii) $d = \omega(C).$

Prova: A prova é imediata. ■

Observe que a proposição acima nos mostra que, em códigos lineares com M elementos, podemos calcular a distância mínima d a partir de $M-1$ cálculos de distâncias, em vez dos $\begin{pmatrix} M \\ 2 \end{pmatrix}$ cálculos anteriormente requeridos.

Como conseqüência da proposição acima, a distância mínima de um código linear C será também chamada de **peso do código C**.

Dada uma base $B = \{v_1, ..., v_k\}$ de C, para saber se um elemento v de K^n pertence a C, é necessário resolver o sistema de n equações e k incógnitas $x_1, ..., x_k$ abaixo

$$x_1v_1 + x_2v_2 + ... + x_kv_k = v.$$

Essa resolução na maioria das vezes representa um custo computacional bem elevado. Utilizando conhecimentos de álgebra linear podemos utilizar ferramentas que deixam computacionalmente muito mais simples de determinar se um dado elemento v de K^n pertence ou não a C. Para isto usaremos uma outra técnica para construirmos um código linear. Como já vimos anteriormente, um código linear é um subespaço vetorial de K^n. Isso nos incentiva a pensar no código de duas maneiras, sendo uma já descrita acima, como a imagem de uma transformação linear, e a outra como sendo o núcleo de uma transformação linear. Para isto, dado C um código linear, consideremos um subespaço C' de K^n de forma que

$$C \oplus C' = K^n,$$

e a aplicação linear

$$H: \begin{array}{ccc} C \oplus C' & \rightarrow & K^{n-k} \\ u \oplus v & \mapsto & v \end{array},$$

cujo núcleo é precisamente C.

Observe que agora para verificar se um dado elemento v pertence ou não a C, basta verificar se $H(v)$ é ou não o vetor nulo de K^{n-k}, o que tem um custo computacional bem pequeno.

Exemplo 1.6.6. *Considere o corpo finito com três elementos* $\mathbb{F}_3 = \{0, 1, 2\}$ *e seja* $C \subset \mathbb{F}_3^4$ *o código gerado pelos vetores* $v_1 = 1011$ *e* $v_2 = 0112$. *Esse código possui* $9 = q^k = 3^2$ *elementos,*

pois tem dimensão 2 *sobre um corpo de* 3 *elementos. Uma representação paramétrica de* C *é dada por*

$$x_1v_1 + x_2v_2,$$

ao variar x_1 *e* x_2 *em* $\mathbb{F}_3$*. O código* C *pode ser representado como núcleo da transformação linear*

$$\begin{array}{rccc} H: & \mathbb{F}_3^4 & \to & \mathbb{F}_3^2 \\ & (x_1,...,x_4) & \mapsto & (2x_1+2x_2+x_3, 2x_1+x_2+x_4) \end{array}.$$

Definição 1.6.7. *Seja* K *um corpo finito. Dois códigos lineares* C *e* C' *são linearmente equivalentes se existir uma isometria linear* $T : K^n \to K^n$ *tal que* $T(C) = C'$*.*

Os códigos lineares fazem parte de uma familia mais geral de códigos chamados de códigos geometricamente uniformes.

Definição 1.6.8. *Um código* $C \subset A^n$ *é chamado* **código geometricamente uniforme** *se e somente se, dadas duas palavras quaisquer* x *e* y *do código existe uma isometria* $\phi : A^n \to A^n$ *tal que:*

(i) $\phi(C) = C$*;*

(ii) $\phi(x) = y$*.*

Proposição 1.6.9. *[3] Seja* C *um código geometricamente uniforme contido em* A^n*. Escolhida uma palavra* a *do código, a distância mínima* d *de* C *é dada por*

$$d = \min\{d(a, v); v \in C, v \neq a\}.$$

Prova: Como C tem um número finito de pontos, temos que existem $x, y \in C$ tal que $d = d(x, y)$.

Seja a o ponto escolhido. Como C é geometricamente uniforme, existe uma isometria ϕ em A^n que leva x em a. Logo,

$$d = d(x, y) = d(\phi(x), \phi(y)) = d(a, \phi(y)).$$

Assim, $d = \min\{d(a, \phi(z)), z \in C\}$, onde $\phi(z) \neq a$, pois $d > 0$. Como $\phi(C) = C$, podemos reescrever a distância mínima da seguinte forma $d = \min\{d(a, v), v \in C, v \neq a\}$

■

1.6.1 Matriz Geradora de um Código

Sejam K o corpo finito com q elementos e $C \subset K^n$ um código linear. Chamaremos de **parâmetros do código linear C** à terna de inteiros (n, k, d), onde k é a dimensão de C sobre K, e d representa a distância mínima de C, que é também igual ao peso $\omega(C)$ do código C.

Definição 1.6.10. *Seja $\beta = \{v_1, ..., v_k\}$ uma base ordenada de C e considere a matriz G, cujas linhas são os vetores $v_i = (v_{i1}, ..., v_{in})$, $i = 1, ..., k$, isto é:*

$$G = \begin{pmatrix} v_1 \\ . \\ . \\ . \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & . & . & . & v_{1n} \\ . & . & & & & . \\ . & . & & & & . \\ . & . & & & & . \\ v_{k1} & v_{k2} & . & . & . & v_{kn} \end{pmatrix}.$$

A matriz G é chamada de **matriz geradora** *de C associada à base β.*

Considere a transformação linear definida por

$$\begin{array}{rccc} T: & K^k & \to & K^n \\ & x & \mapsto & xG \end{array},$$

onde G é uma matriz geradora de C. Se $x = (x_1, ..., x_k)$, temos que

$$T(x) = xG = x_1v_1 + ... + x_kv_k,$$

logo $T(K^k) = C$. Podemos então considerar K^k como sendo o código fonte, C o código de canal e a transformação T uma codificação.

Observe que a matriz G não é univocamente determinada por C, pois ela depende da base ordenada β. De fato, dada uma base ordenada β, podemos encontrar outras bases efetivando uma das seguintes operações:

(L_1) Permutação de dois elementos da base;

(L_2) Multiplicação de um elemento da base por um escalar não nulo

(L_3) Substituição de um vetor da base per ele mesmo somando com um múltiplo escalar de outro vetor da base.

Como toda matriz $T : C \to C$ invertível é produto(composta) de operações do tipo L_1, L_2, L_3, podemos concluir que duas matrizes geradoras de um mesmo código C podem ser obtidas uma da outra por uma seqüencia de operações L_1, L_2 e L_3.

Pelo que já vimos até agora, podemos então a partir de uma matriz G cujas linhas são linearmente independentes construir códigos, como sendo a imagem da transformação linear T definida acima.

1.6.2 Matriz Geradora na Forma Padrão

A fim de facilitar o processo de codificação e decodificação, iremos estudar agora a matriz geradora na forma padrão.

Definição 1.6.11. *Diremos que uma matriz G está na* **forma padrão** *se tivermos*

$$G = (I_k \mid A),$$

onde I_k é a matriz identidade $k \times k$ e A é uma matriz $k \times (n-k)$.

Dado um código C, existe um código equivalente C' com matriz geradora na forma padrão. Este é um resultado é obtido escalonando-se a matriz G.

1.6.3 Códigos Duais e Matriz Teste de Paridade

Observemos que, para verificarmos se um determinado vetor $v \in K^n$ pertence ou não a um código C com matriz geradora G, é preciso verificar se o sistema de n equações com k incógnitas $x = (x_1, ..., x_k)$, dado por

$$xG = v,$$

admite solução. Em geral, essa questão requer um custo computacional elevado para ser respondida. No entanto, trabalhando com uma matriz teste de paridade que definiremos no fim desta seção, a solução pode ser encontrada rapidamente.

Sejam $u = (u_1, ..., u_n)$ e $v = (v_1, ..., v_n)$ elementos de K^n. Consideremos o **produto interno usual** de u e v como sendo

$$\langle u, v\rangle = u_1v_1 + ... + u_nv_n.$$

Definição 1.6.12. *Seja $C \subset K^n$ um código linear, O* **subespaço ortogonal** *de C é dado por*

$$C^{\perp} = \{v \in K^n : \langle v, u\rangle = 0,\ \forall u \in C\}.$$

Lema 1.6.13. *[1][17] Se $C \subset K^n$ é um código linear, com matriz geradora G, então*

i) $C^{\perp}$ *é um código linear de* K^n *de dimensão* $n - k$*;*

ii) $x \in C^{\perp} \Leftrightarrow Gx^t = 0$.

Prova:

ii) $x \in C^{\perp}$ se, e somente se, x é ortogonal a todos os elementos de C se, e somente se, x é ortogonal a todos os elementos de uma base de C, o que é equivalente a dizer que $Gx^t = 0$, pois as linhas de G são uma base de C.

i) Por *ii*, temos que $x \in C^{\perp} \Leftrightarrow Gx^t = 0$. Assim, $dim(Im(G)) = posto(G) = k$ e $n = dim(Im(G)) + dim(C^{\perp})$.

■

Definição 1.6.14. *Seja C um código em K^n. O subespaço ortogonal a C, denotado por $C^{\perp}$, é também um código linear e é chamado de* **código dual** *de C.*

Lema 1.6.15. *[1] Suponha que C seja um código de dimensão k em K^n com matriz geradora G. Uma matriz H de ordem $(n - k) \times n$, com coeficientes em k e com linhas linearmente independentes, é uma matriz geradora de $C^{\perp}$ se, e somente se,*

$$G \cdot H^t = 0.$$

Prova: O subespaço gerado pelas linhas de H geram um subespaço de dimensão $n-k$, portanto, igual à dimensão de $C^{\perp}$. Por outro lado, representado por $h_1, ..., h_{n-k}$ e por $g_1, ..., g_{n-k}$ respectivamente, as linhas de H e G, temos que

$$(G \cdot H^t)_{i,j} = \langle g_i, h_i \rangle.$$

Portanto, $G \cdot H^t = 0$ equivale a dizer que todos os vetores do subespaço gerado pelas linhas de H estão em $C^{\perp}$. Por outro lado esse subespaço tem a mesma dimensão de $C^{\perp}$, logo,

$$G \cdot H^t = 0 \Leftrightarrow C^{\perp}$$

é gerado pelas linhas de H. ■

Proposição 1.6.16. *[1] Seja $C \subset K^n$ um código de dimensão k com matriz geradora $G = (I_k \mid A)$, na forma padrão. Então $H = (-A^t \mid I_{n-k})$ é uma matriz geradora de $C^{\perp}$ e $(C^{\perp})^{\perp} = C$.*

Prova: Observemos que as linhas de H são linearmente independentes (por causa do bloco I_{n-k}), portanto, geram um subespaço de dimensão $n-k$. Como as linhas de H são ortogonais as linhas de G, temos que o espaço gerado pelas linhas de H está contido em $C^{\perp}$; e como esses dois subespaços têm mesma dimensão, eles coincidem, provando assim que $H = (-A^t \mid I_{n-k})$ é uma matriz geradora de $C^{\perp}$.

Agora provemos que $(C^{\perp})^{\perp} = C$. Sejam G (matriz geradora qualquer) e H as matrizes geradoras de C e $C^{\perp}$. Logo, $G \cdot H^t = 0$. Tomando transpostas nessa última igualdade, temos que $H \cdot G^t = 0$, logo, G é matriz geradora de $(C^{\perp})^{\perp}$, como queríamos demonstrar. ■

Observe que esta proposição ensina a achar a matriz teste de paridade quando a matriz geradora está na forma padrão. De modo geral, se a matriz $G = (B \mid A)$, onde B é uma matriz inversível de ordem k, e A é uma matriz de ordem $k \times n-k$, então teremos que

$$H^t = \begin{pmatrix} -B^{-1}A \\ I \end{pmatrix}.$$

Observe que se $B = I$, cai no caso da proposição acima e como $I^{-1} = I$, temos que $H^t = \begin{pmatrix} -A \\ I \end{pmatrix}$ e assim, $H = (-A^t \mid I)$, como já tínhamos provado.

Proposição 1.6.17. *[1] Seja C um código linear e suponhamos que H seja uma matriz geradora de $C^{\perp}$. Temos então que*

$$v \in C \Leftrightarrow Hv^t = 0.$$

Prova: Temos que $v \in C \Leftrightarrow v \in (C^{\perp})^{\perp} \Leftrightarrow Hv^t = 0$. ■

A proposição acima nos permite caracterizar os elementos de um código C por uma condição de anulamento.

Definição 1.6.18. *A matriz geradora H de $C^{\perp}$ é chamada* **matriz teste de paridade** *de C.*

Definição 1.6.19. *Dado um código C com matriz teste de paridade H e um vetor $v \in K^n$, o vetor Hv^t é chamado de* **síndrome de** *v.*

Exemplo 1.6.20. *Dado o código C sobre $\mathbb{F}_2$ com matriz geradora na forma padrão*

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Pela proposição 1.5.19*, temos que:*

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Por exemplo, dados $v = (100111)$ e $v' = (010101)$. Como $Hv^t = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ e $H(v')^t = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \neq 0$, temos que v pertence a C e v' não pertence a C.

Proposição 1.6.21. ??*[1] Seja H a matriz teste de paridade de um código C. Temos que $\omega(C) \geq s$ se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

Prova: Suponhamos que $\omega(C) \geq s$. Suponhamos também, por absurdo, que H tenha $s-1$ colunas linearmente dependentes, digamos $h^{i_1},\ h^{i_2}, ..., h^{i_{s-1}}$. Logo, existiriam $c_{i_1}, ..., c_{i_{s-1}}$ no corpo, nem todos nulos, tais que

$$c_{i_1}h^{i_1} + ... + c_{i_{s-1}}h^{i_{s-1}} = 0.$$

Portanto, $c = (0, ..., c_{i_1}, 0, ..., c_{i_{s-1}}, 0, ..., 0) \in C$ e conseqüentemente, $\omega(c) \leq s-1 < s$, o que seria um absurdo.

Reciprocamente, suponhamos que cada conjunto de $s-1$ colunas de H é linearmente independente. Sejam $c = (c_1, ..., c_n)$ uma palavra não nula de C e $h^1, ..., h^n$ as colunas de H. Como $Hc^t = 0$, temos que

$$0 = H \cdot c^t = \sum c_i h^i. \qquad (*)$$

Sew $\omega(c) = t$, temos uma dependência linear envolvendo t colunas, logo $t \geq s$ e $\omega(c) \geq s$.

■

Teorema 1.6.22. *[1] Seja H a matriz teste de paridade de um código C. Temos que o peso de C é igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Prova: Suponhamos que $\omega(C) = s$. Agora, sabemos que existe $x \in C$ tal que $\omega(x) = s$, como já foi feito no teorema anterior, temos que $Hx^t = 0$, daí temos uma combinação linear não trivial de colunas de H dando o vetor nulo. Portanto, H possui s colunas linearmente dependentes.

Agora suponhamos que quaisquer $s-1$ colunas de H são L.I e existem s colunas L.D. Pelo teorema anterior sabemos que $\omega(C) \geq s$. Agora vamos supor que $\omega(C) \geq s+1$. Então novamente pelo teorema anterior, teríamos que qualquer conjunto de s colunas de H seria L.I, o que nos dá uma contradição. Logo, $\omega(C) = s$, como queríamos demonstrar. ■

Teorema 1.6.23. *(Cota de Singleton) Seja C um código com parâmetros (n, k, d). Então*

$$d \leq n - k + 1.$$

Prova: Seja H uma matriz teste de paridade de C.

Como H é matriz geradora de $C^{\perp}$ podemos supor que H está na forma padrão, ou seja $H = (I_{n-k}|A^t)$. Como os $(n-k)$ vetores coluna do bloco (I_{n-k}) formam uma base de K^{n-k}, temos que H possui $n-k+1$ colunas linearmente independentes. Assim, por **??** temos que d é no máximo $n-k+1$, ou seja $d \leq n-k+1$. ■

Exemplo 1.6.24. *Seja* $C = \{(x_1, x_2, x_3) \in \mathbb{Z}_2^3; x_1 + x_2 + x_3 = 0\}$. *Melhor dizendo, temos que* $C = \{(1,1,0), (1,0,1), (0,1,1), (0,0,0)\}$. *Assim, temos que* $d = 2$ *e que* $n = 3$, $k = 2$ *e portanto,* $n - k + 1 = 3 - 2 + 1 = 2 = d$. *portanto a distância mínima assume o valor máximo possível para um código de comprimento* $n = 3$ *e* $k = 2$.

1.7 Códigos de Hamming

Alguns exemplos de códigos lineares conhecidos e com muitas aplicações são os códigos de hamming, de Golay, de Reed-Muller([1]).

Ilustramos com os códigos de Hamming que são perfeitos e corrigem 1 erro.

O código de Hamming é um exemplo de código linear que tem a capacidade de corrigir 1 erro, e sua construção se dá a partir da matriz teste de paridade. Estes códigos foram introduzidos por R.W. Hamming em 1950.

Definição 1.7.1. *Um código de Hamming,* $H_m \subset \mathbb{Z}_2^{2^m-m-1}$ *é um* $(2^m - 1, 2^m - m - 1)$*-código linear binário, que tem matriz teste de paridade,* H_m*, tendo por colunas todos os elementos não nulos de* $\mathbb{Z}_2^m$.

Exemplo 1.7.2. *Como exemplo, daremos a matriz de paridade na forma sistemática para um* H_3*:*

$$H_3 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Sua matriz geradora correspondente será então:

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Portanto a codificação de uma seqüência abcd por este código fica sendo abcdxyz, onde $x = b + c + d$, $y = a + c + d$ *e* $z = a + b + d$.

Agora enunciaremos e provaremos um resultado muito importante sobre os códigos de Hamming.

Proposição 1.7.3. *[1] Todo código de Hamming é perfeito, corrigindo um erro(*$d = 3$*).*

Prova: Em H_m verificamos facilmente que $d = 3$, pois é fácil achar três colunas linearmente dependentes, e duas delas nunca o são. A partir daí, temos que $k = \left[\frac{d-1}{2}\right] = 1$.

Seja $c \in \mathbb{F}_2^n$. Temos que

$$| D(c, 1) | = 1 + n.$$

Portanto,

$$| \bigcup_{c \in C} D(c, 1) | = [1 + n]2^k = [1 + 2^m - 1]2^{n-m} = 2^n,$$

onde $k = n - m$ e $n = 2^m - 1$. Assim,

$$\bigcup_{c \in C} D(c, 1) = \mathbb{F}_2^n.$$

■

Exemplo 1.7.4. *Seja* C *um* $(n, t, 3)$ *código, onde* $n = \frac{(q^r-1)}{(q-1)}$ *e* $t = n - r$. *Assim,* $k = 1$ *e*

$$\frac{q^n}{\sum_{i=0}^{k} \binom{n}{i} (q-1)^i} = \frac{q^n}{1 + n(q-1)} = \frac{q^n}{q^r} = q^k.$$

Observe que C *satisfaz 1.4.2, tendo igualdade.*

Códigos de hamming permitem um processo sistemático simples de decodificação.([1])

Capítulo 2

Reticulados

Este capítulo será dedicado a Teoria de Reticulados. Abordaremos alguns conceitos básicos, propriedades e exemplos desta teoria, dando ênfase a Teoria de Códigos. As principais referências para este capítulo são: [3] e [2].

2.1 Relação entre Reticulados e Empacotamento de Esferas

O problema do empacotamento de esferas consiste em distribuir esferas de raio r em $\mathbb{R}^n$, de modo que:

1. Duas esferas quaisquer deste arranjo apenas se toquem em um ponto da “casca", ou não possuam intersecção nenhuma;

2. este arranjo de esferas ocupe o “maior espaço possível".

Quando os centros das esferas formam um reticulado, os empacotamentos são chamados de empacotamentos reticulados. Daí o problema se transforma em encontrar reticulados com a maior densidade possível.

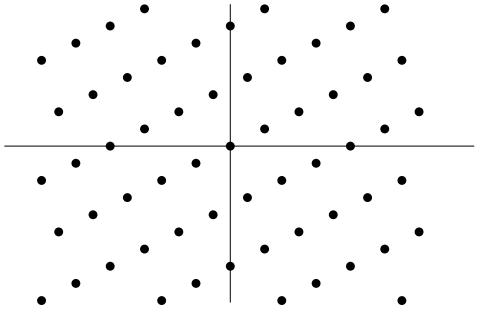
2.2 Introdução

Definição 2.2.1. *Seja $\beta = \{u_1, u_2, ..., u_n\}$ uma base de $\mathbb{R}^n$. Chamaremos de* **reticulado** *ao seguinte conjunto*

$$\Lambda = \{x = a_1u_1 + a_2u_2 + ... + a_nu_n; a_i \in \mathbb{Z}, 1 \leq i \leq n\},$$

β é chamada de base do reticulado.

Exemplo 2.2.2. *Considere a base dada por $\beta = \{(2,1), (-1,3)\}$ A figura abaixo ilustra o reticulado gerado por esta base.*



A base de um reticulado não é única

Proposição 2.2.3. *Dado um reticulado Λ gerado por uma base β, uma base α será base deste reticulado se, e somente se, α está contida em Λ e a respectiva matriz mudança de base possui entradas inteiras e determinante ± 1 ([5]).*

Prova: Seja $[T]_\alpha^\beta$ a matriz mudança de base de β para α e $[T]_\beta^\alpha$ a matriz mudança de base de α para β. Como cada elemento da base β pode ser escrito como combinação inteira dos elementos de α e vice versa, temos que a matriz $[T]_\alpha^\beta$ e $[T]_\beta^\alpha$ possuem apenas entradas inteiras e $[T]_\beta^\alpha = ([T]_\alpha^\beta)^{-1}$. Assim, $[T]_\alpha^\beta \cdot [T]_\beta^\alpha = I$. Daí, temos que $\det[T]_\beta^\alpha \cdot \det[T]_\alpha^\beta = 1$. Como $[T]_\alpha^\beta$ e $[T]_\beta^\alpha$ so possuem entradas inteiras, temos que o determinante também é inteiro, assim, $\det[T]_\beta^\alpha = \det[T]_\alpha^\beta = \pm 1$. A volta segue do fato de que como a matriz mudança de base possui apenas entradas inteiras e determinante ± 1, então todo elemento da base β pode ser escrita como combinação inteira dos elementos da base α e portando todo elemento do reticulado gerado por β pertence ao reticulado gerado por α e vice versa. ■

Proposição 2.2.4. *Sejam Λ um reticulado em $\mathbb{R}^n$ e T a translação em $\mathbb{R}^n$ dada por $T(x) = x + u$, onde $u \in \Lambda$. Então T é uma isometria que leva Λ em Λ.*

Prova: É claro que toda translação é uma isometria. Devemos provar que T leva Λ em Λ, ou seja, dado $x \in \Lambda$, então $T(x) \in \Lambda$.

De fato, seja $\beta = \{u_1, ..., u_n\}$ uma base de Λ, e $x \in \Lambda$. Como $x, u \in \Lambda$, temos que existem $a_1, ..., a_n$ e $b_1, ..., b_n$ tais que $x = a_1u_1 + ... + a_nu_n$ e $u = b_1u_1 + ... + b_nu_n$.

Assim, $T(x) = x + u = (a_1 + b_1)u_1 + ... + (a_n + b_n)u_n$. Como $a_i,\ b_i \in \mathbb{Z}$, temos que $(a_i + b_i) \in \mathbb{Z}$.

Portanto $T(x) \in \Lambda$. ■

2.3 Reticulados no Plano

Observemos que $\mathbb{Z}^2$ é o reticulado gerado pela base canônica de $\mathbb{R}^2$. Além disso, se tomarmos discos de raio $r = \frac{1}{2}$ centrados em cada ponto do reticulado $\mathbb{Z}^2$, teremos um empacotamento de esferas de $\mathbb{R}^2$, e se tomarmos discos de raio maior que $\frac{1}{2}$ haverá sobreposição, então $\frac{1}{2}$ é o maior raio possível para um empacotamento de discos do reticulado $\mathbb{Z}^2$.

Definição 2.3.1. *O maior raio de um dado empacotamento é chamado de* **raio do empacotamento** *ρ, sendo que $r = \rho$ é o maior raio tal que $B_r(u) \cap B_r(v) = \emptyset$ se $u, v \in \Lambda$, com $u \neq v$.*

Definição 2.3.2. *Dado $v \in \mathbb{R}^2$, a* **Região de Voronoi** *associada a v, denotada por $R(v)$, é o seguinte subconjunto: de $\mathbb{R}^2$,*

$$R(v) = \{x \in \mathbb{R}^2; \parallel v - x \parallel \leq \parallel v - u \parallel, \forall u \in \Lambda\}.$$

Para um reticulado mais geral do plano, uma região de Voronoi é determinada do seguinte modo:

Dados u e v, o conjunto dos pontos que estão mais próximos de v do que u corresponde ao semiplano determinado pelo bissetor perpendicular(mediatriz) do segmento $[u, v]$, que contém o ponto v. Tomando-se a intersecção de todos estes semiplanos, obteremos a região $R(v)$.

A Figura 2.3 ilustra as regiões de Voronoi de $\mathbb{Z}^2$ e do reticulado Λ gerado pela base $\beta = \{(2,1),(-1,3)$.

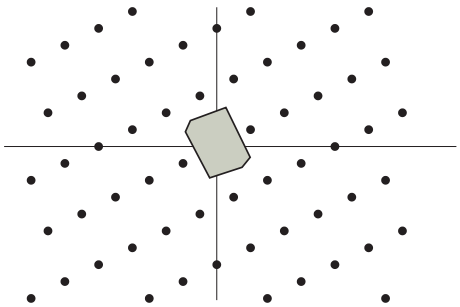


Figura 2.1: região de voronoi do reticulado Λ gerado por β

Tendo construído uma região de Voronoi, todas as outras regiões podem ser obtidas a partir desta região inicialmente construída, através de translações. Então basta construir $R(0)$ por exemplo e teremos que:

$$R(v) = R(0) + v = \{v + x \in \mathbb{R}^2; x \in R(0)\}.$$

Como cada translação é uma isometria, todas as regiões possuem as mesmas propriedades geométricas. Assim, basta estudarmos a região $R(0)$.

Observe que do modo que foi definido uma região de Voronoi, temos que estas regiões constituem um ladrilhamento perfeito do plano, pois elas cobrem o plano inteiro e se sobrepõem apenas ao longo de pontos de fronteira (vértices ou arestas).

Definição 2.3.3. *Definimos a densidade do reticulado (ou a densidade do empacotamento de discos determinado pelo reticulado) como a razão $\triangle$ entre a área do disco de empacotamento D e a área da região de Voronoi, ou seja,*

$$\triangle = \frac{\textit{área}(D)}{\textit{área}(R(0))},$$

onde D é o disco de raio ρ, com ρ o raio de empacotamento, e $R(0)$ a região de Voronoi de 0.

A densidade do reticulado fornece então uma medida de quanto do plano foi preenchido pelos discos de raio ρ.

2.4 Regiões Fundamentais e Densidade

A definição de região de Voronoi que segue abaixo é a mesma definida anteriormente para dimensão 2 só que agora para $\mathbb{R}^n$.

Definição 2.4.1. *Se v é um ponto de Λ, a região de Voronoi de v é o conjunto*

$$R(v) = \{x \in \mathbb{R}^n; \parallel v - x \parallel \leq \parallel v - u \parallel, \forall u \in \Lambda\}.$$

Proposição 2.4.2. *[3] Para todo $v \in \Lambda$, temos que*

$$R(v) = v + R(0) = \{v + x \in \mathbb{R}^n; x \in R(0)\}.$$

Desta forma, podemos ladrilhar todo o $\mathbb{R}^n$ com estas regiões, ou seja, cada ponto de $\mathbb{R}^n$ está em um dos translados de $R(0)$ e dois destes translados ou são os mesmos ou se interceptam apenas nos bordos ou não tem intersecção.

A definição de densidade do reticulado em $\mathbb{R}^n$ é também é análoga ao caso planar.

Definição 2.4.3. *Seja $r = \rho$, o raio do empacotamento de Λ, isto é, o maior número positivo tal que $B_r(0) \subset R(0)$. Definimos a* **densidade** *de Λ por*

$$\triangle = \frac{vol(B_\rho(0))}{vol(R(0))}.$$

Observação 2.4.4. *Observe que determinar a região de Voronoi de um reticulado não é um problema trivial e, na forma em que foi definida a densidade, esta é de difícil aplicabilidade.*

Agora mostraremos que dado o raio do empacotamento ρ e uma base de Λ, podemos calcular a densidade do reticulado sem maiores problemas.

Definição 2.4.5. *Seja Λ um reticulado em $\mathbb{R}^n$. Dizemos que F é uma* **região fundamental** *de Λ se F é fechado em $\mathbb{R}^n$, com interior não vazio e $\mathbb{R}^n$ pode ser ladrilhado por cópias de F, onde $\bigcup_{v\in\Lambda} v + F = \mathbb{R}^n$ e $int(v + F) \cap int(u + F) = \emptyset$ se $u \neq v$..*

Exemplo 2.4.6. *A região de Voronoi $R(0)$ é um exemplo de região fundamental de Λ.*

Definição 2.4.7. *Dada uma base $\beta = \{u_1, u_2, ..., u_n\}$, definimos o* **politopo fundamental** *gerado por esta base como sendo o sólido*

$$P = \{\sum_{i=1}^{n} a_i u_i; 0 \leq a_i \leq 1\}.$$

Proposição 2.4.8. *[3] Um politopo fundamental P é uma região fundamental de Λ.*

Prova: De fato P é fechado, devemos provar apenas que tomando os translados $P+v$ onde $v \in \Lambda$ conseguimos cobrir todo o $\mathbb{R}^n$ de modo que dois ladrilhos ou não tem intersecção ou se interceptam apenas nos bordos.

Se

$$v + P = \{x + v; x \in P\},$$

então temos que:

(i) Cada vetor de $\mathbb{R}^n$ pertence a um destes sólidos. De fato, se $\lfloor a \rfloor$ é a parte inteira do número real a, então $\lfloor a \rfloor \in \mathbb{Z}$ e $0 \leq a - \lfloor a \rfloor \leq 1$ e para cada vetor $v = \sum_{i=1}^{n} a_i u_i$ de $\mathbb{R}^n$, temos que

$$v = \sum_{i=1}^{n} a_i u_i = \underbrace{\sum_{i=1}^{n} \lfloor a_i \rfloor u_i}_{\in \Lambda} + \underbrace{\sum_{i=1}^{n} (a_i - \lfloor a_i \rfloor) u_i}_{\in P}.$$

Portanto, $\mathbb{R}^n = \bigcup_{v \in \Lambda} v + P$.

(ii) O interior de $v + P$ é dado por:

$$int(v + P) = \{v + \sum_{i=1}^{n} a_i u_i; 0 < a_i < 1\}.$$

Suponhamos que $x \in \overline{v}_1 + P$ e $x \in \overline{v}_2 + P$. Assim, existem $a_1, ..., a_n$ e $b_1, ..., b_n \in \mathbb{Z}$ e $\alpha_1, ..., \alpha_n$ e $\beta_1, ..., \beta_n \in \mathbb{R}$, onde $0 < \alpha_i, \beta_i < 1, 1 \leq i \leq n$, tal que

$$x = a_1 v_1 + ... + a_n v_n + \alpha_1 v_1 + ... + \alpha_n v_n \quad e$$

$$x = b_1 v_1 + ... + b_n v_n + \beta_1 v_1 + ... + \beta_n v_n.$$

Como $\{v_1, ..., v_n\}$ é base de $\mathbb{R}^n$ temos que

$$a_1 - b_1 + \alpha_1 - \beta_1 = ... = a_n - b_n + \alpha_n - \beta_n = 0.$$

Agora, como $a_i - \beta_i \in \mathbb{Z}$ e $\alpha_i - \beta_i = 0$ ou não pertence a $\mathbb{Z}$, temos que $a_i = b_i$ e $\alpha_i = \beta_i$. E dai se conclui que nenhum ponto de $v + P$ pode estar em nenhum outro translado $u + P$.

■

Proposição 2.4.9. *[3] O volume de qualquer região fundamental de um reticulado em $\mathbb{R}^n$ é o mesmo.*

Não faremos a demonstração deste resultado, ela pode ser encontrada em [6].

Esta proposição nos mostra que a noção de politopos fundamentais é crucial no estudo de reticulados, pois trata-se de uma região fundamental em que o volume é fácil de ser calculado. A partir daí, torna-se mais fácil calcular a densidade do reticulado.

2.5 Matriz de Gram e o Determinante de um Reticulado

Definição 2.5.1. *Dada a base $\beta = \{v_1, ..., v_n\}$ do reticulado Λ a* **matriz geradora** *de Λ é dada por*

$$A = \begin{pmatrix} v_{11} & . & . & . & v_{n1} \\ . & & & & . \\ . & & & & . \\ . & & & & . \\ v_{1n} & . & . & . & v_{nn} \end{pmatrix},$$

onde $v_1 = (v_{11}, ..., v_{1n}), ..., v_n = (v_{n1}, ..., v_{nn})$.

Observação 2.5.2. *Observe que dado um elemento $x = \kappa_1 v_1 + ... + \kappa_n v_n \in \Lambda$, podemos escrever os vetores na forma coluna, com as coordenadas na base canônica da seguinte forma:*

$$x = \kappa_1 \begin{pmatrix} v_{11} \\ . \\ . \\ . \\ v_{1n} \end{pmatrix} + ... + \kappa_n \begin{pmatrix} v_{n1} \\ . \\ . \\ . \\ v_{nn} \end{pmatrix} = \begin{pmatrix} v_{11} & . & . & . & v_{n1} \\ . & & & & . \\ . & & & & . \\ . & & & & . \\ v_{1n} & . & . & . & v_{nn} \end{pmatrix} \begin{pmatrix} \kappa_1 \\ . \\ . \\ . \\ \kappa_n \end{pmatrix},$$

isto nos diz que Λ é a imagem de $\mathbb{Z}^n$ pela matriz A.

Exemplo 2.5.3. *Para cada n, temos o reticulado*

$$\mathbb{Z}^n = \{(a_1, ..., a_n); a_i \in \mathbb{Z}\}.$$

Sua base é a base canônica e a matriz geradora é a matriz identidade.

Definição 2.5.4. *Se A é a matriz geradora de um reticulado Λ, definimos a* **matriz de Gram** *G associada a A como sendo,*

$$G = A^T A.$$

Pela forma que foi definida, a matriz de Gram G é uma matriz simétrica e suas entradas são os produtos escalares $< v_i, v_j >$.

Assim, G possui informações métricas importantes com respeito a base escolhida.

Como um reticulado pode ter mais de uma base, temos o problema que a matriz de Gram pode mudar com a mudança da base inicial.

Exemplo 2.5.5. *Considere o reticulado gerado pela base $\beta = \{(n, n+1), (-n-1, n)\}$, onde n um número inteiro não nulo. A base $\beta' = \{(n, n+1), (-1, 2n+1)\}$ também é base do reticulado gerado por β, mas as matrizes de Gram são dadas por*

$$G = \begin{pmatrix} 2n^2+2n+1 & 0 \\ 0 & 2n^2+2n+1 \end{pmatrix}$$

e

$$G' = \begin{pmatrix} 2n^2+2n+1 & 2n^2 \\ 2n^2 & 2n^2+2n+1 \end{pmatrix}.$$

Assim, um reticulado pode possuir varias matrizes de Gram diferentes, mas o determinante é o mesmo e só depende do reticulado.

Proposição 2.5.6. *[3] Sejam $\beta = \{u_1, ..., u_n\}$ e $\beta' = \{v_1, ..., v_n\}$ duas base de um reticulado Λ e sejam G e G' as matrizes de Gram correspondentes. Então,* $\det G = \det G'$.

Prova: Como β é base de Λ, podemos escrever

$$v_j = a_{1j}u_1 + a_{2j}u_2 + ... + a_{nj}u_n; 1 \leq j \leq n,$$

onde cada a_{ij} está em $\mathbb{Z}$. A transformação linear $T : \mathbb{R}^n \to \mathbb{R}^n$, que leva u_j em v_j faz a mudança de base e tem matriz M com determinante ± 1. Daí $B = MA$ e assim

$$\det(B^T B) = \det(A^T M^T M A) = \det(A^T)\det(M^T)\det(M)\det(A) = \det(A^T A).$$

■

Definição 2.5.7. *Definimos o* **determinante de** Λ *, denotado por* $\det(\Lambda)$*, como o determinante de uma matriz de Gram de* Λ*.*

Como $\det(\Lambda) = \det(G) = \det(A^TA) = \det^2(A)$, temos que o volume de P é $(\det(\Lambda))^{\frac{1}{2}}$.

A partir disto já podemos formalizar a definição de densidade de Λ em função do determinante de Λ.

Definição 2.5.8. *Definimos a densidade de um reticulado* Λ *como sendo*

$$\triangle = \frac{vol(B_\rho(0))}{(\det(\Lambda))^{\frac{1}{2}}}.$$

Agora já podemos calcular a densidade de um reticulado se tivermos uma base do reticulado e sua distância mínima.

Exemplo 2.5.9. *Considere o reticulado* Λ *gerado por* $u = (a, b)$ *e* $v = (-b, a)$*.*

Temos que a distância mínima é a norma mínima dos vetores do reticulado. Resolvendo a norma mínima de um elemento genérico $xu + yv$ *de* Λ*, teremos que os vetores de norma mínima são* $\pm u$ *e* $\pm v$*. Assim,* $r = \rho = \frac{1}{2} \parallel u \parallel$*, visto que* $\parallel u \parallel = \parallel v \parallel$*. Portanto,* $\rho = \frac{1}{2}(a^2 + b^2)^{\frac{1}{2}}$*.*

Como $(\det(\Lambda))^{\frac{1}{2}} = vol(P) = \det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 + b^2$*, temos que* $\triangle = \frac{\pi \frac{a^2+b^2}{4}}{a^2+b^2} = \frac{\pi}{4}$*.*

Uma densidade muito melhor é atingida pelo reticulado A_2 gerado pela base $\beta = \{(1, 0)(\frac{1}{2}, \frac{\sqrt{3}}{2})\}$. As regiões deste reticulado são hexágonos e sua densidade é $\triangle = \frac{\pi}{\sqrt{12}}$. Este é o reticulado no plano que possui a melhor densidade.

2.6 Reticulados Congruentes e Reticulados Equivalentes

Definição 2.6.1. *Diremos que dois* **reticulados** Λ_1 *e* Λ_2 *são* **equivalentes** *se existirem uma aplicação ortogonal* $U : \mathbb{R}^n \to \mathbb{R}^n$ *e um número positivo* λ *tais que* $(\lambda U)(\Lambda_1) = \Lambda_2$*.*

Observação 2.6.2. *Note que* $< \lambda Uu, \lambda Uv >= \lambda^2 < u, v >$ *e que* $\parallel \lambda Uv \parallel = \lambda \parallel v \parallel$ *. Diremos que* λ *é a* **razão de semelhança** *de* Λ_1 *para* λ_2*.*

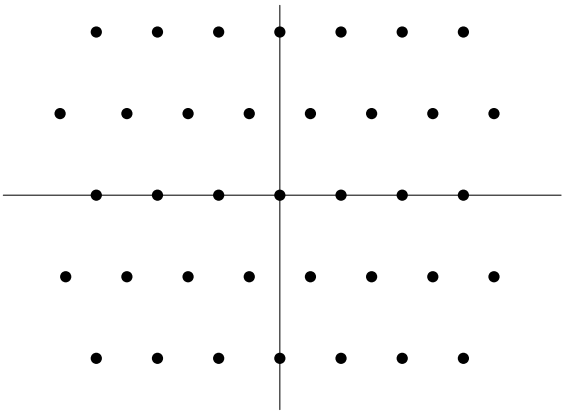


Figura 2.2: Reticulado A_2

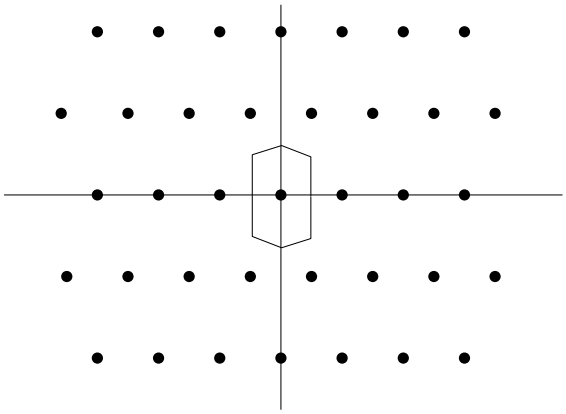


Figura 2.3: Região fundamental do reticulado A_2

Proposição 2.6.3. *[3] Se Λ_1 e Λ_2 são reticulados equivalentes, então a densidade de Λ_1 é igual a de λ_2.*

Prova: Seja ρ_i e $\triangle_i$ o raio de empacotamento e a densidade de Λ_i, para $i = 1, 2$, respectivamente. Temos que

$$\begin{aligned} \min\{\| x \|; x \in \Lambda_2\} &= \min\{\lambda \| y \|; y \in \Lambda_1\} \\ &= \lambda \min\{\| y \|; y \in \Lambda_1\} \end{aligned}$$

e segue que o raio de empacotamento de Λ_2 é $\rho_2 = \lambda\rho_1$.

Se A é a matriz geradora de Λ_1, então λUA é a matriz geradora de Λ_2 e

$$\det(\lambda UA) = \det(\lambda I)\det(U)\det(A) = \lambda^n \det(A),$$

e daí, $\det(\Lambda_2) = \lambda^{2n}\det(\Lambda_1)$. Portanto,

$$\triangle_2 = \frac{vol(B_{\rho_2}(0)}{(\det(\Lambda_2))^{\frac{1}{2}}} = \frac{\lambda^n vol(B_{\rho_1}(0)}{\lambda^n(\det(\Lambda_1))^{\frac{1}{2}}} = \triangle_1.$$

■

Definição 2.6.4. *Diremos que Λ_1 e Λ_2 são* **congruentes** *se existir uma aplicação ortogonal $U : \mathbb{R}^n \to \mathbb{R}^n$ tal que $U(\Lambda_1) = \Lambda_2$.*

Observação 2.6.5. *Observe que o caso de congruência é um caso particular do caso de equivalência entre dois reticulados, ou seja, quando o valor de λ é igual a 1.*

Exemplo 2.6.6. *Um exemplo importante é o dos reticulados D_n, $n \geq 3$. Os reticulados D_3, D_4 e D_5 são definidos pelas seguintes matrizes de Gram*

$$\begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix} \quad e \quad \begin{pmatrix} 2 & 0 & -1 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 \\ -1 & -1 & 2 & -1 & 0 \\ 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & -1 & 2 \end{pmatrix}.$$

A matriz de Gram do reticulado D_n, para $n \geq 6$ tem as mesmas 4 primeiras linhas de D_5 (completadas com zeros a direita) e as linhas 5, 6, 7,..., n são obtidas da quarta linha, que é o vetor $(0, 0, -1, 2, -1, 0, ..., 0)$, por deslocamento à direita:

$$\begin{pmatrix} 2 & 0 & -1 & 0 & & & \dots & & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 & & & & & 0 \\ -1 & -1 & 2 & -1 & 0 & 0 & \dots & & & \\ 0 & 0 & -1 & 2 & -1 & 0 & & & & \\ 0 & 0 & 0 & -1 & 2 & -1 & & & \vdots & \\ \vdots & & & & \ddots & & & & & \\ & & & & & 0 & -1 & 2 & -1 & 0 \\ 0 & & & & \dots & & 0 & -1 & 2 & -1 \\ 0 & 0 & & & & & & 0 & -1 & 2 \end{pmatrix}.$$

A matriz de Gram pode ser especificada em termos dos produtos internos dos elementos da base correspondente, da seguinte forma:

(i) $< e_1, e_3 >= -1$

(ii) $< e_1, e_2 >= 0$

(iii) $< e_i, e_{i+1} >= -1$ para $i = 3, ..., n-1$

(iv) $< e_i, e_j >= 0$ para $i,\ j = 3, ..., n$ e $\mid i - j \mid \geq 2$.

(v) $< e_i, e_j = 2$ para $i = 1, 2, ..., n$.

2.7 Reticulados e Grafos

Um grafo consiste num conjunto V de cardinalidade finita ou enumerável (vértices) e de um subconjunto de $V \times V$ que define quais vértices são conectados (arestas). Representa-se o grafo geometricamente por um conjunto discreto de pontos (os vértices) ligados por curvas (as arestas).

Uma superfície orientada M tem gênero g se, e somente se, M é homeomorfo a um g-toro, ou seja, M é homeomorfo à soma conexa de uma esfera com g toros (esfera com g alças).

Dizemos que um grafo mergulha sobre uma superfície se puder ser representada sobre ela sem intersecção das arestas.

Teorema 2.7.1. *[8][18] Todo grafo pode ser mergulhado sem auto intersecção em uma superfície de gênero g.*

O gênero de um grafo é o menor gênero de superfície onde ele mergulha.

Estaremos interessados aqui em grafos de gênero 1 que estão mergulhados em toros planares.

Como exemplo consideremos grafos cujos vértices são pontos de $\mathbb{Z}_M$ ($\mathbb{Z}$ Módulo M). Estes formam uma classe especial de grafos chamados **grafos circulantes**. Eles tem despertado interesse nos anos recentes inclusive por terem aplicação no desenho de redes de computadores, onde os vértices correspondem às máquinas e as arestas representam conexões entre estas máquinas.

Definição 2.7.2. *Um* **grafo circulante** $C_M(a_1, ..., a_n)$ *é o grafo cujos vértices são elementos de $\mathbb{Z}_M$, onde a e b são conectados se, e somente se, $b = a \pm a_i$ (operação em $\mathbb{Z}_M$), para algum i.*

Exemplo 2.7.3. *A figura abaixo mostra o grafo circulante $C_{13}(1, 5)$.*

Observe que a bijeção $\tau(a) = a + 1$ em $\mathbb{Z}_M$ preserva todas as arestas, ou seja, se a e b estão conectados, então $\tau(a)$ e $\tau(b)$ também estão. O mesmo vale para $\tau_\kappa(a) = a + \kappa$. Assim para construir o grafo, basta ligar os $\pm a_i's$ ao 0 e rodar a figura obtida pelos vértices.

Grafos circulantes também podem ser vistos como quociente de reticulados sobre toros planares (2.9).

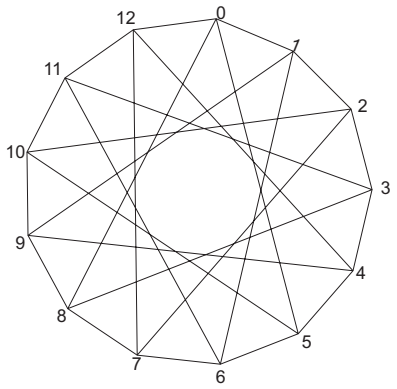


Figura 2.4: grafo circulante $C_{13}(1,5)$

Reticulados podem ser considerados grafos se a partir de uma base $\{w_1, ..., w_n\}$ fixada tomarmos as arestas definidas por: u e v são conectadas se, e somente se, $v - u = \pm w_i$.

Teorema 2.7.4. *Seja $\beta = \{w_1, ..., w_n\}$ uma base de um reticulado Λ. Temos que o grafo definido pela relação de que dados $u, v \in \Lambda$, u e v são conectados se, $v - u = \pm w_i$, é conexo.*

Prova: Como $w_i - 0 = w_i$, temos que todo elemento da base β está conectado ao 0. Como $2w_i - w_i = 3w_i - 2w_i = 4w_i - 3w_i = ... = w_i$, temops que todos elementos αw_i estão cenectados a w_i, para $\alpha \in \mathbb{Z}$, portanto estão conectados ao 0. Da mesma forma, temos que $\alpha w_i + \beta w_j$ está conectado tanto a w_i quanto a w_j e portanto está conectado ao 0. Assim, para todo elemento x do reticulado visto como um vértice do grafo está conectado ao 0. Portanto o grafo é conexo. ■

O quociente de reticulados de mesma dimensão por sua vez determina grafos finitos sobre toros planares, como descrevemos a seguir.

Dado um reticulado Λ com base $\alpha = \{v_1, ..., v_n\}$ e um sub-reticulado Λ' de Λ. O quociente $\Gamma = \dfrac{\Lambda}{\Lambda'}$ estabelecido pela relação $x \sim y \Leftrightarrow x - y \in \Lambda'$ define um grafo cujos vértices são dados por um conjunto completo de representantes, $V = \{a_1, ..., a_M\}$ das classes de $\dfrac{\Lambda}{\Lambda'}$. A relação de adjacência de Γ são as induzidas de Λ.

Por exemplo para $\Lambda = \mathbb{Z}^2$ com a base usual e $\Lambda' = \langle (3,2), (-2,3) \rangle$, teremos um grafo de 13 vértices, malha quadrada, que estará contido no toro planar dado pelo quociente de $\mathbb{R}^2$ por translações dos vetores de Λ'. Este grafo é equivalente ao grafo circulante $C_{13}(1,5)$ ([13]). O isomorfismo de grafos neste caso é dado por $\Phi : \mathbb{Z}_{13} \to \dfrac{\Lambda}{\Lambda'}$, onde $\Phi(x) = (0, x)$.

Com a notação acima seja $w_j = \sum_{i=1}^{n} h_{ij} v_i$, $1 \leq i, j \leq n$ e $H = \{h_{ij}\}$, onde $\{v_i\}$ é uma base de Λ', então temos a seguinte proposição:

Proposição 2.7.5. *[13]* $\frac{\Lambda}{\Lambda'}$ *define um grafo sobre o toro planar* $\frac{\mathbb{R}^n}{\Lambda'}$ *com conjunto de vértices* $V = \{a_1, ...a_M\}$ *formado por uma classe completa de representantes de* $\frac{\Lambda}{\Lambda'}$ *e relação de adjacência induzida por* Λ *onde* $M = \mid \det H \mid$ *e* a_i *pertence a Região Fundamental de* Λ.

O toro planar e sua relação com reticulados, grafos e ladrilhamentos associados serão descritos na próxima seção.

2.8 Toros Planares

Nesta seção iremos fazer uma relação entre reticulados, grafos circulantes que estão mergulhados em toros planos.

Definição 2.8.1. *Dada uma base* $\alpha = \{u_1, ..., u_n\}$ *de* $\mathbb{R}^n$, *seja* Λ_α *o reticulado gerado por* α. *O* **toro planar** T_α *é definido como o espaço quociente* $T_\alpha = \frac{\mathbb{R}^n}{\Lambda_\alpha}$. *Isto é,* $x \sim y \Leftrightarrow x - y \in \Lambda_\alpha$.

O toro planar T_α pode também ser definido como quociente pela aplicação

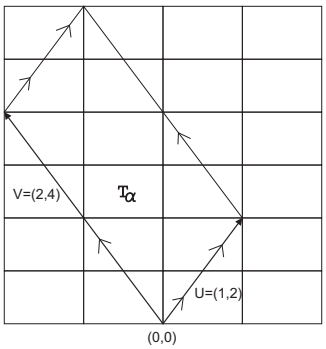
$$\begin{array}{rccl} \mu_\alpha : & \mathbb{R}^n & \rightarrow & \mathbb{R}^n \\ & x & \mapsto & \mu_\alpha(x) = x \; mod \Lambda_\alpha = x - \sum_{i=1}^{n} \lfloor x_i \rfloor u_i \end{array},$$

onde $x = \sum_{i=1}^{n} x_i u_i$ e $\lfloor x_i \rfloor$ denota a parte inteira de x_i, isto é, o maior inteiro que é menor ou igual a x_i.

Para $n = 2$ e $\alpha = \{u, v\}$, o toro planar T_α pode ser visto como um paralelogramo gerado por u e v com seus lados opostos identificados.

Exemplo 2.8.2. *Considere o reticulado* Λ *gerado por* $\alpha = \{u, v\}$, *onde* $u = (1, 2)$ *e* $v = (-2, 4)$. *Quando fazemos o quociente* $\frac{\mathbb{R}^n}{\Lambda_\alpha}$, *teremos o toro plano* T_α, *que pode ser visto como o paralelogramo gerado por* u *e* v *com seus lados opostos identificados.*

A distância euclidiana d induz de forma natural uma distância em T_α.



Definição 2.8.3. *A* **distância** d_α *entre duas classes* $\overline{a}$ *e* $\overline{b}$ *com* $a, b \in \mathbb{R}^n$ *no toro planar* T_α *é dada por:*

$$d_\alpha(\overline{a}, \overline{b}) = \min\{d(z, y) = \| z - y \|; z \in \overline{a}, y \in \overline{b}\},$$

onde $\| \, . \, \|$ *é a norma euclidiana em* $\mathbb{R}^n$*.*

2.9 Ladrilhamentos e Grafos em Toros Planares

Ladrilhamentos de $\mathbb{R}^n$ por polígonos regulares e grafos associados podem sob certas condições induzir grafos e ladrilhamentos em toros planares. Um exemplo disto pode ser visto em 2.5.

Vamos considerar um toro planar T_α gerado por uma base α, associado a uma aplicação quociente $\overline{\mu}_\alpha$ induzida por μ_α dada por:

$$\begin{array}{rccc} \overline{\mu}_\alpha : & \mathbb{R}^n & \to & T_\alpha \\ & x & \mapsto & \overline{\mu}_\alpha(x) \end{array},$$

definido em termos do politopo P_α em $\mathbb{R}^n$ com suporte em α.

É importante observar que $\overline{\mu}_\alpha$ é injetiva e que é uma isometria local quando restrito à região dentro do politopo. Isto implica que toda medida, área ou volume, induzida pela distância $\overline{d}$ no toro plano pode ser medida em $\mathbb{R}^n$ dentro de P_α.

Começaremos agora, introduzindo algumas definições e resultados gerais de ladrilhamentos.

Definição 2.9.1. *Seja* G *um grupo discreto de isometrias de um espaço* M*. Um subconjunto* Π *de* M *é chamado uma* **região fundamental associada a** G *se e somente se* Π *é fechada*

e,

(i) $\bigcup_{g\in G} g\Pi = M;$

(ii) $\mathring{\Pi} \cap g\mathring{\Pi} = \emptyset;$

(iii) $\mathring{\Pi} \neq \emptyset.$

Uma cobertura de M dada pelas cópias de Π sob a ação de G é chamado de **ladrilhamento** *de M associado a G, ou G-ladrilhamento.*

Observemos que alguns grafos circulantes podem ser mergulhados em toros planares com a estrutura geométrica adquirida pelo reticulado. Como o toro plano tem gênero 1, estes grafos não sendo planares também o terão. Para visualizar melhor isto, observe o exemplo abaixo.

Exemplo 2.9.2. *Considere o reticulado Λ_α gerado por $\alpha = \{(4,3),(-5,2)\}$. Realizando o quociente acima, teremos o toro plano que será ladrilhado por 23 quadrados.*

Observemos que o grafo circulante $C_{23}(1,5)$ (figura 2.4) é isomorfo ao grafo mergulhado no toro plano gerado por α, mais especificamente, o que ladrilha T_α.

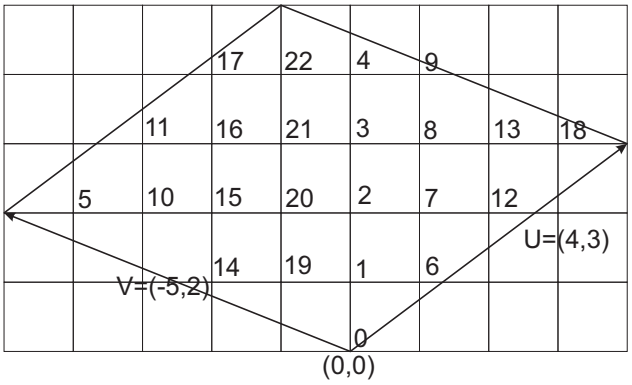


Figura 2.5: grafo circulante $C_{23}(1,5)$ mergulhado no toro plano

Todos os ladrilhamentos que vamos considerar aqui são induzidos por reticulados em $\mathbb{R}^n$.

A proposição 2.7.5 tem uma versão ampliada:

Lema 2.9.3. *[2]*

Sejam $\alpha = \{u_1, u_2, ..., u_n\}$ e $\beta = \{v_1, v_2, ..., v_n\}$ bases de $\mathbb{R}^n$, e $\mathcal{T}_\beta$ o Λ_β ladrilhamento de $\mathbb{R}^n$ que tem região fundamental o politopo Π com suporte em β. Se Λ_α é um sub-reticulado de Λ_β e $\overline{\mu}_\alpha$ é a aplicação quociente no toro planar, temos o seguinte:

(i) $\mathcal{T}_\beta$ induz um G-ladrilhamento em T_α com região fundamental $\overline{\mu}_\alpha(\Pi)$ e $G = \dfrac{\Lambda_\beta}{\Lambda_\alpha}$;

(ii) Λ_β induz um grafo homogêneo em T_α sobre $\mathcal{T}_\alpha^\beta$, Γ_α^β. Os vértices e os lados de Γ_α^β são induzidos por $\overline{\mu}_\alpha$.

Será enunciado agora uma proposição em $\mathbb{R}^2$, que se estende para o $\mathbb{R}^n$ e sua demonstração é análoga a que será exposta logo abaixo.

Proposição 2.9.4. *[2] Seja $\alpha = \{u, v\}$, onde $u = (a, b)$ e $v = (c, d)$ vetores de $\mathbb{R}^2$, linearmente independentes, T_α o toro planar associado. Temos então que:*

(a) O reticulado canônico $\mathbb{Z}^2 \subset \mathbb{R}^2$ induz por μ_α um grafo Γ_α e um ladrilhamento por quadrados unitários no toro planar T_α se, e somente se, u e v possuem coordenadas inteiras.

Neste caso temos que:

(b) $\mu_\alpha(\mathbb{Z}^2)$ são os vértices de Γ_α;

(c) $\mu_\alpha(\{m\} \times [n, n+1])$ e $\mu_\alpha([n, n+1] \times \{m\})$ são as arestas;

(d) $\mu_\alpha([i, i+1] \times [j, j+1])$, $i, j \in \mathbb{Z}$ são as faces quadradas;

(e) o número de vértices V e o número de faces F de Γ_α são iguais a $\mid \det[u, v] \mid = \mid ad - bc \mid$.

Prova: Os ítens (a), (b), (c) e (d) seguem diretamente do lema 2.9.3 aplicado ao reticulado canônico $\mathbb{Z}^2$ associado ao grupo de isometrias $G_\beta < T_{e_1}, T_{e_2} >$, onde $e_1 = (1, 0)$ e $e_2 = (0, 1)$, a região fundamental Π em $\mathbb{R}^2$ e $G_\alpha =< T_u, T_v >$ subgrupo de G_α.

O ítem (e) segue da relação de Euler para grafos em superfícies $V - A + F = 2 - 2g$, onde V é o número de vértices, A o número de arestas, F o número de faces e g é o gênero da superfície. No caso do toro, como $g = 1$, temos que $V + F = A$. Como cada face tem 4

arestas, e cada aresta pertence a duas faces, temos que $A = \frac{4F}{2} = 2F$. Como $V + F = A$, segue que $V = 2F - F = F$. Desde que a área do paralelogramo gerado por u e v é dado por $|\det[u, v]| = |ad - bc|$, e cada face é unitária, temos que $F = V = |ad - bc|$, concluindo a demonstração.

■

Procedendo a raciocínio da demonstração do teorema 2.9.4 para $\mathbb{R}^3$, temos que o número $|\det[u_1, u_2, u_3]|$ é o número de cubos unitários do ladrilhamento, e o volume do toro plano é o volume do prisma gerado por $\alpha = \{u_1, u_2, u_3\}$.

O número de vertices de cada cubo neste ladrilhamento é $2^3 = 8$, mas cada vértice pertence a 8 cubos, daí, $V = \frac{8F}{F} = F = |\det[u_1, u_2, u_3]|$.

A prova para R^n com n qualquer segue analogamente. O toro plano é homogeneamente ladrilhado por hipercubos e $\overline{\mu}_\alpha$ é uma isometria local que é injetiva quando restrita ao interior de P_α, logo o volume n-dimensional de P_α é igual ao volume n-dimensional de T_α, que é igual ao número F de hipercubos do ladrilhamento.

2.10 Ladrilhamentos por Quadrados

Daremos ênfase nesta seção ao ladrilhamento do toro planar por quadrados. Trataremos daqui em diante apenas do caso particular $\mathbb{R}^2$, mas os resultados podem ser estendidos para $\mathbb{R}^n$.([2])

Vamos considerar $\Lambda_\beta = \mathbb{Z}^2$, translações planas associadas a $\mathbb{Z}^2$, o ladrilho $\Pi = [0, 1]\times[0, 1]$, $\alpha = \{u, v\}$, $u = (a, b)$ e $v = (c, d)$, onde a, b, c e d são inteiros.

2.10.1 Ladrilhamentos induzidos por Translações

Translações verticais e horizontais no planar induzem de forma natural um ladrilhamento no toro planar.

Para começar vejamos um exemplo.

Exemplo 2.10.1. *Seja $u = (4, 3)$ e $v = (-5, 2)$, nos temos um toro planar gerado por $M = \det[u, v] = |ad - bc| = 23$ quadrados, ilustrados pela figura 2.5.*

Observe que neste exemplo, os segmentos verticais do grafo são conectados onde identificamos os lados opostos do paralelogramo e eles formam uma curva fechada no toro plano.

As translações verticais no plano pela unidade induzem uma ação no toro plano. Mais especificamente, se começarmos de qualquer vértice do grafo inscrito no toro e andarmos sempre ao norte pela translação vertical de uma unidade, passaremos por todos os vértices do grafo.

Proposição 2.10.2. *[7] Sejam $\alpha = \{u, v\}$, onde $u = (a, b)$ e $v = (c, d)$ e $M =\mid ad - bc \mid$. Se $mdc(a, c) = 1$, então o grupo $\dfrac{\mathbb{Z}^2}{\Lambda_\alpha}$ é isomorfo ao grupo cíclico $\mathbb{Z}_M$ e a translação vertical pela unidade é um de seus geradores e pode ser usado para ladrilhar isometricamente Γ_α^β. Da mesma forma, o resultado vale se $mdc(b, d) = 1$ e a translação horizontal.*

A extensão deste resultado para $\mathbb{R}^n$ é dada a seguir:

Proposição 2.10.3. *[2] Seja $A = (a_{ij})$ uma matriz geradora de Λ_α sobre $\mathbb{Z}_n$ e c_{ij} o valor absoluto do cofator de A associado com o elemento a_{ij}. Então temos o seguinte:*

(a) *Se para cada i, existem j_1 e j_2 tal que $mdc(c_{ij_1}, c_{ij_2}) = 1$ então a translação gerada por e_i gera um ladrilhamento cíclico de Γ_α^β por $\mathbb{Z}^n/\Lambda_\alpha \cong \mathbb{Z}_{|A|}$.*

(b) *Se $mdc(c_{ij}, \mid a \mid) = 1$ para algum i, j, temos que a translação gerada por e_i gera um ladrilhamento cíclico de Γ_α^β por $\mathbb{Z}_{|A|}$.*

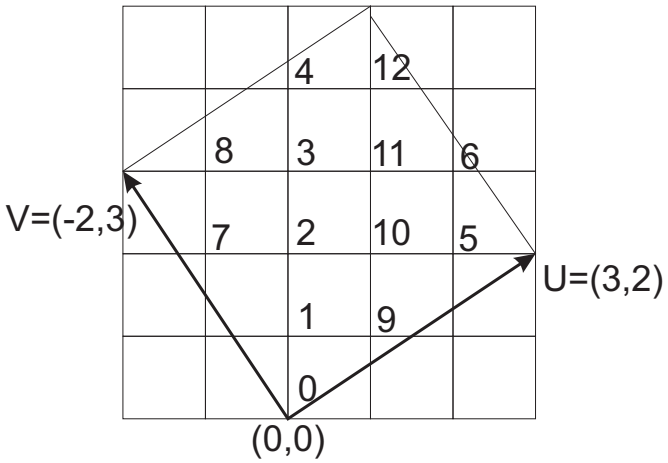
Naturalmente o quociente de dois reticulados nem sempre gera um ladrilhamento (ou rotulamento) dado por um grupo cíclico. Como pode ser visto na proposição mais geral a seguir:

Proposição 2.10.4. *[2] Sejam α e β bases do $\mathbb{R}^n$ e Λ_α e Λ_β os reticulados gerados por α e β respectivamente, com $\Lambda_\alpha \subset \Lambda_\beta$. Sejam A a matriz geradora de Λ_α sobre Λ_β, v um vetor de Λ_β e A_i a matriz obtida de A substituindo v^t pela i-ésima coluna de A. Então a ordem de $\overline{v} = v + \Lambda_\alpha$ em $\dfrac{\Lambda_\beta}{\Lambda_\alpha}$ é dado por $\dfrac{\mid A \mid}{\gcd\{\mid A \mid, \mid A_1 \mid, ..., \mid A_n \mid\}}$, onde $\mid A \mid =\mid \det A \mid$.*

2.10.2 Toros Gerados por Quadrados

Agora vamos considerar toros gerados por quadrados, isto é, gerado por $u = (a, b)$ e $v = (-b, a)$, a e b inteiros. O conjunto Γ_α^β é um conjunto sinal de $a^2 + b^2$ pontos.

A figura a ilustra o caso em que $a = 3$ e $b = 2$



Um conjunto de sinais de um toro planar gerado por quadrados pode ter mesma ordem mas diferentes tipos de performance. Considere os números a, b e $c \in \mathbb{N}$ tal que $a^2 + b^2 = c^2$, com $mdc(a, b) = 1$, os vetores $u = (c, 0)$, $v = (0, c)$, $\widetilde{u} = (a, b)$ e $\widetilde{v} = (-b, a)$ e a base associada $\alpha = \{u, v\}$ e $\overline{\alpha} = \{\widetilde{u}, \widetilde{v}\}$. Γ_α^β e $\Gamma_{\overline{\alpha}}^\beta$, onde β é a base canônica, tem a mesma ordem, mas o último possui um ladrilhamento dado por um grupo cíclico, enquanto o anterior, que é o espaço de Lee $\mathbb{Z}_{a^2+b^2}^2$ pode não possuir como no caso em que $a = 4$ e $b = 3$.

Capítulo 3

Códigos Esféricos

Este capítulo será dedicado a um tipo especial de código, os códigos esféricos.

As principais referências para este capítulo são [3], [10], [11] e [14].

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. Achar este código é um problema difícil. Na esfera euclidiana $S^2 \subset \mathbb{R}^3$, este problema é conhecido como o problema de Tammes.

Os dois principais meios de atacar este problema são:

- Construção de limitantes para o número de pontos de um código esférico que envolva a dimensão n e a distância mínima d.
- Construção de códigos que tenham distâncias mínimas melhores que as conhecidas até o momento, sendo estes códigos, os melhores conhecidos.

3.1 Introdução

Identificamos a **esfera unitária** S^n como sendo o conjunto de todos os vetores unitários, ou seja,

$$S^n = \{x = (x_1, x_2, ..., x_n) \in \mathbb{R}^n; \parallel x \parallel = 1\},$$

onde $\parallel x \parallel = \sqrt{x_1^2 + x_2^2 + ... + x_n^2}$.

Definição 3.1.1. *Um* **código esférico** $\mathcal{X}$ *é um subconjunto finito de* S^n.

Dada uma dimensão n *e um número de pontos* M*, o código esférico* $[m, n]$ *com a maior distância mínima é chamado* **código ótimo**. *A distância a ser considerada é a distância usual de* $\mathbb{R}^n$.

Definição 3.1.2. *Um* **código planar** $\mathcal{X} = \{x_1, x_2, ..., x_M\} \subset S^n$ *é um código esférico com a propriedade que para um vetor unitário* $a \notin \mathcal{X}$, $\langle x_i, a\rangle = \theta$, *para todo* i, *com* $\theta \neq 0$.

Proposição 3.1.3. *[11] Nenhum código planar é ótimo.*

Prova: Vamos supor que $\theta \neq \pm 1$, pois trataremos apenas de códigos que possuam mais de duas palavras.

Seja $\widetilde{\mathcal{X}} = \{y_1, y_2, ..., y_M\}$, onde $y_i = \dfrac{1}{\sqrt{1-\theta^2}}(x_i - \theta a)$.

Notemos que $\langle y_i, a\rangle = 0$ e portanto $\widetilde{\mathcal{X}}$ está contido num equador de S^n.

Como $\| y_i - y_j \|^2 = \dfrac{< x_i - \theta a - (x_j - \theta a), x_i - \theta a - (x_j - \theta a) >}{\sqrt{1-\theta^2}} = \dfrac{\| x_i - x_j \|^2}{1-\theta^2}$, temos que o conjunto $\widetilde{\mathcal{X}}$ é um código esférico e a distância mínima ao quadrada $\rho_{\widetilde{\mathcal{X}}}$ é dada por

$$\rho_{\widetilde{\mathcal{X}}} = \frac{\rho_{\mathcal{X}}}{1-\theta^2}.$$

Logo, $\rho_{\widetilde{\mathcal{X}}} > \rho_{\mathcal{X}}$. ■

3.2 Exemplos de Códigos esféricos

Exemplo 3.2.1. *Seja* A *um código binário com parâmetros* (n, d, M). *Considere a aplicação* $\phi : \{0, 1\} \to \mathbb{R}$ *definida por* $\phi(\theta) = (-1)^\theta$.

Agora considere a aplicação $\Phi : A \to \mathbb{R}^n$ *tal que* $\Phi((x_1, ..., x_n)) = (\phi(x_1), ..., \phi(x_n))$. *Como* $\phi(x_i) = \pm 1$, *temos que* $E = \| (x_1, ..., x_n) \|^2 = n$, *onde a quantidade* E *é chamada de* **energia**.

O código $A \subset F_2^n$ *é aplicado em um código* $\mathcal{X} \subset \mathbb{R}^n$ *com distância mínima ao quadrado* $d_E^2 = 4d$.

As palavras de $\mathcal{X}$ *não estão na esfera unitária* $S^n \subset \mathbb{R}^n$, *mas normalizando cada palavra, obtemos um código esférico com parâmetros* $(n, \rho, M) = (n, \frac{4d}{n}, M)$

Exemplo 3.2.2. *Seja $\mathcal{C}$ um código binário com parâmetros (n, w, d, M), onde n é o comprimento, w é o peso e é único, d é a distância mínima e M é a ordem de $\mathcal{C}$. Seja $\phi : \{0, 1\} \to \mathbb{R}$ dada por $\phi(\theta) = w - \theta n$. Aplicando ϕ em cada coordenada da palavra $u = (u_i, ..., u_n)$ do código $\mathcal{C}$, obtemos novos vetores $x = (x_1, ..., x_n)$ em $\mathbb{R}^n$ satisfazendo as seguintes equações:*

$$\begin{aligned} x_1 + x_2 + ...x_n &= 0 \\ x_1^2 + x_2^2 + ... + x_n^2 &= nw(n - w). \end{aligned}$$

A primeira igualdade significa que o novo código está localizado em um subespaço de $\mathbb{R}^n$ de dimensão $(n - 1)$, enquanto que a segunda igualdade significa que todas as palavras do código possuem a mesma norma. Note também que este código é planar. A distância mínima ao quadrado $d_E^2 = n^2 d$. Normalizando cada palavra do código obtemos um código esférico com parâmetros $(N, \rho, M) = (n - 1, \dfrac{nd}{nw - w^2}, M)$.

Exemplo 3.2.3. *O M-PSK*

PSK são as inicias para a expressão em ingles, Phase-Shift Keying. Se pudermos associar uma informação a um representante binário por exemplo 0 ou 1 e depois associar cada tipo de informação a uma fase de um sinal contínuo, conforme a figura 3.1, um código sobre a círculo S' será criado a partir dos representantes de cada fase.

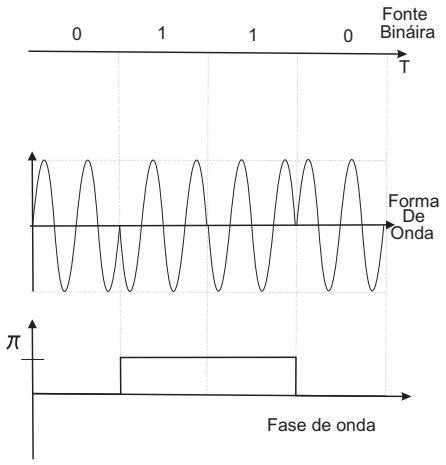


Figura 3.1: Modulação de um 2-PSK

Ao 0 associamos a fase zero e ao 1 associamos a fase π. Tais fases, por seguinte, estão

associados 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* $x_2(t) = -\cos[\pi t]$. x_1 *e* x_2 *escritas como combinação linear da funções*

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

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

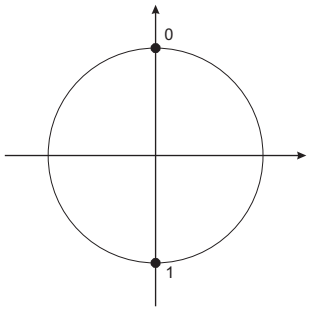


Figura 3.2: Representação Geométrica de um 2-PSK

Assim, representamos "0" *por* $(0,1)$ *e* "1" *por* $(0,-1)$*, conforme a figura 3.2.*
Esta construção pode ser feita para um conjunto de M *sinais*

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

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

$$x_i(t) = \cos(\pi t) \cdot \cos(2(i-1)\pi/M) - \sin(\pi t) \cdot \sin(2(i-1)\pi/M)$$

e, portanto ao sinal i *associamos o vetor* $(\cos(2(i-1)\pi/M), \sin(2(i-1)\pi/M))$.

3.3 Limitantes para Códigos Esféricos

Nesta seção apresentaremos alguns limitantes que envolvem a dimensão e o número de pontos de um código esférico e através de alguns deles é possível provar que códigos como o simplex que será apresentado na proxima seção, são ótimos. Antes porém iremos introduzir alguns conceitos.

Dados x e $y \in S^n$, o ângulo entre estes pontos é $\cos^{-1}(\langle x, y\rangle)$. Se d é a distância mínima de um código esférico, então o ângulo mínimo entre os pontos é

$$\theta = 2\sin^{-1}\left(\frac{d}{2}\right).$$

O conjunto de 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, ou seja,

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

Se o ponto central do chapéu for irrelevante, denotaremos simplesmente por $C(n,\phi)$.

É possível demonstrar ([11]) que a área do chapéu esférico é dada por:

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

onde

$$\kappa_n = \begin{cases} \frac{(2\pi)^{n/2}}{(n-2)!!} & \text{se } n = 2,4,... \\ 2\cdot\frac{(2\pi)^{(n-1)/2}}{(n-2)!!} & \text{se } n = 3,5,... \end{cases}$$

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

Em geral, a área total da esfera é

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

Teorema 3.3.1. *[10][11]Limitante da União*

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

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

Teorema 3.3.2. *[10][11]Limitante de Tóth*

Em $\mathbb{R}^3$, *todo código esférico com M pontos tem ângulo mínimo* θ *satisfazendo*

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

Em 1954, Rankin propôs alguns limitantes para códigos esféricos euclidianos que, além de serem de fácil manipulação, possibilitaram a demonstração de que as classes de códigos Simplex e biortogonal são ótimas.

Teorema 3.3.3. *[10][11] Limitante de Rankin I*

Todo código com M pontos e ângulo mínimo 2ϕ *contido na esfera* S^{n-1} *satisfaz as seguintes desigualdades:*

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

Alguns cálculos simples podem ser feitos para reescrever o teorema acima em função da distância mínima. Por exemplo, a segunda desigualdade é equivalente à:

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

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

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

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

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

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

Como o ângulo mínimo é 2ϕ, temos que a distância mínima do código é $d = 2\sin\phi$. Conseqüentemente, se a distância mínima ao quadrado de um código esférico com M pontos satisfazer a seguinte desigualdade

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

então $M \leq n+1$.

Da mesma forma, com a primeira e terceira desigualdade obtemos o seguinte:

1. $M \leq \left[\frac{d^2}{d^2-2}\right]$, 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 serão demonstrados três limitantes equivalentes as desigualdades acima.

Teorema 3.3.4. *[3][10]Rankin A*

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

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

Prova: 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 que

$$\langle x_i, x_j\rangle \leq \frac{2-\rho}{2} \text{ e}$$

$$\sum_{i,j}\langle x_i, x_j\rangle = \sum_i \underbrace{\| x_i \|}+\sum_{i\neq j} < x_i, x_j > \leq M + M(M-1)(\frac{2-\rho}{2}).$$

Como $x_i = (x_{i1}, ..., x_{in})$, temos por outro lado que

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

Portanto,

$$M + M(M-1)(\frac{2-\rho}{2}) \geq 0,$$

daí temos que $(\frac{2-\rho}{2}) \geq -(\frac{1}{M-1})$ e assim

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

como queríamos demonstrar. ■

Teorema 3.3.5. *[3][10]Rankin B*

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

$$M \leq n + 1.$$

Prova: Como $\langle x_i, x_j\rangle = \cos\theta \leq 1$, temos que $2 < 2 - 2\langle x_i, x_j\rangle \leq 4$, para todos x_i, x_j distintos em $\mathcal{X}$.

Segue que $-1 \leq \langle x_i, x_j\rangle < 0$, ou seja, $\langle x_i, x_j\rangle < 0$ e $-1 \leq \langle x_i, x_j\rangle$, para $i = 1, ..., M-1$..

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

Agora seja $y_i = 1 - \langle x_i, x_M\rangle^2 > 0$ e $w_i = \frac{1}{\sqrt{y_i}}(x_i - \langle x_i, x_M\rangle x_M)$, para $i = 1, 2, ..., M-1$.

Observe que

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

Portanto, $\langle w_i, w_j\rangle < 0$ pois $\langle x_i, x_j\rangle < 0$ para $i \neq j$ distintos.

Assim, temos um novo código $\mathcal{X}_{n-1} = \{w_1, ..., w_{M-1}\}$ com $M-1$ pontos e distância mínima ao quadrado maior que dois contido num hiperplano normal a x_M, e por conseqüência disto, de dimensão $n-1$.

Recursivamente, construímos um código $\mathcal{X}_\kappa$ com distância mínima ao quadrado maior que dois e $M - n + \kappa$ pontos que está contido em $\mathbb{R}^\kappa$.

Para finalizar a demonstração, basta observar que o código $\mathcal{X}_1$, contido em espaço de dimensão 1, tem $M-n+1$ pontos, e por ter dimensão 1, $M-n+1 \leq 2$, ou seja, $M \leq n+1$, como queríamos demonstrar. ■

Teorema 3.3.6. *[3][10]Rankin C*

Qualquer código esférico em $\mathbb{R}^n$ com distância mínima ao quadrado $\rho \geq 2$ e M pontos satisfaz $M \leq 2n$.

Prova: Para demonstrar este teorema, basta repetir a construção da família de códigos $\mathcal{X}_\kappa$ do teorema anterior, observando que a distância mínima ao quadrado pode ser 2. Assim, a cardinalidade diminui de um ou dois pontos. Portanto o número de pontos de $\mathcal{X}_\kappa$ é maior ou igual a $M - 2(n - \kappa)$.

Portanto, para $\kappa = 1$, temos que $2 \geq M - 2(n - 1)$ e assim, $M \leq 2n$. ■

Uma conseqüência do teorema de Rankin B e C é que se $n+2$ pontos podem ser colocados na esfera S^{n-1}, então $2n$ pontos também podem ser colocados com a mesma distância mínima, em outras palavras, isto significa que apesar da densidade do código esférico aumentar, a distância mínima permanece constante.

Códigos esféricos podem ser gerados a partir de grupos, assim, definiremos códigos gerados por grupos.

Definição 3.3.7. *Seja $x_0 \in \mathbb{R}^n$ e G um grupo de matrizes $n \times n$. Chamamos de* **órbita** *de x_0 por G ao conjunto*

$$Gx_0 = \{gx_0; g \in G\}.$$

Definição 3.3.8. *Definimos um código de grupo C como sendo a órbita de um vetor v na esfera unitária S^{n-1} por um subgrupo $G = \{O_i\}_{i=1}^M$ do grupo das matrizes ortogonais $O(n)$.*

Quando o subgrupo de $O(n)$ for comutativo, teremos um código de grupo comutativo.

Teorema 3.3.9. *[19] Um grupo comutativo de matrizes ortogonais reais $O = \{O_i\}_{i=1}^M$ de ordem M pode ser levado por uma transformação ortogonal Q em matrizes de bloco diagonais da forma*

$$\tilde{O}_i = [R\Big(\frac{2\pi b_{i1}}{M}\Big), ..., \Big(\frac{2\pi b_{iq}}{M}\Big), \mu(i)_{2q+1}, ..., \mu(i)_n]_{n\times n} = Q^T O_i Q,$$

onde os blocos $R\left(\frac{2\pi b_{ij}}{M}\right)$ *são rotações em dimensão* 2 *e* $b_{ij} \in \mathbb{Z}$,

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

e $\mu(i)_l = \pm 1$, $l = 2q+1, ..., n$.

A partir deste resultado temos uma importante caracterização para códigos de grupos comutativos.

Teorema 3.3.10. *[14] Todo código de grupo comutativo é equivalente a um código de grupo comutativo* X *com vetor inicial* $u = (u_1, ..., u_n)$, *tendo seus pontos da forma,* $O(u) = \{(R_1(i)(u_1, u_2), ..., R_q(i)(u_{2q-1}, u_{2q}), \mu(i)_{2q+1}u_{2q+1}, ..., \mu(i)_n u_n)\}_{i=1}^{M}$.

Denotaremos por $\triangle_m$ a densidade máxima de empacotamento de um reticulado em $\mathbb{R}^m$. Chamaremos de densidade de centro de um empacotamento, o quociente da densidade deste reticulado pelo volume da esfera unitária em R^m, e denotaremos por $\Lambda_m = \frac{\triangle_m}{V_m}$. A seguir, enunciaremos um limitante de código de grupo comutativo envolvendo algumas propriedades de reticulados. Neste teorema, λ_m é a densidade de centro máxima de um reticulado em $\mathbb{R}^m$.

Proposição 3.3.11. *[14] Todo código de grupo comutativo em* $\mathbb{R}^{2m}$ *de ordem* M *com distância mínima* ρ *e vetor inicial* $u = (u_1, u_2, ..., u_{2m})$ *satisfaz*

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

3.4 Os Códigos Simplex e Biortogonal

Esta seção será dedicada a duas classes de códigos esféricos que são ótimos, os códigos simplex e o biortogonal. Estas classes de códigos, definidas em qualquer dimensão, são generalizações do triângulo isósceles e do quadrado em dimensão 2, e do tetraedro e do octaedro em dimensão 3.

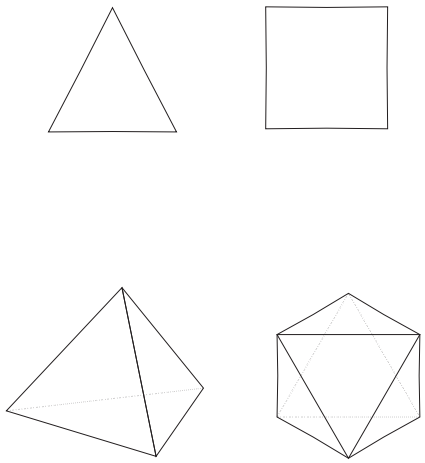


Figura 3.3: Os códigos simplex e biortogonal em dimensão dois e três

3.4.1 O Código Simplex

Considere a órbita de $x_0 = (1, ..., 1, -n)$ 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 $n \times n$.

Definição 3.4.1. *O* **código simplex** S_n *é a órbita de* x_0 *por* S*, ou seja,* S_n *é o conjunto formado pelo ponto* $x_0 = (1, ..., 1, -n)$ *em* $\mathbb{R}^{n+1}$ *e seus deslocamentos cíclicos.*

Segue da definição que se $x = (x_1, ..., x_{n+1}) \in \{S^l(1, ..., 1, -n)\}_{l=1}^{n+1}$, onde $S^l = \underbrace{S \cdot S \cdots S}_{\text{l vezes}}$, então

$$x_1 + ... + x_{n+1} = 0 \text{ e } x_1^2 + ... + x_{n+1}^2 = n + n^2.$$

Portanto, S_n é um código que quando normalizado (normalizando cada palavra) se torna um código esférico que mora em um hiperplano de $\mathbb{R}^{n+1}$, portanto em $\mathbb{R}^n$.

Como $S^{n+1} = S$, temos que o espaço S_n têm dimensão n, o código simplex é um código com $M = n + 1$ pontos em $\mathbb{R}^n$, com distância mínima ao quadrado $\dfrac{2(1+n)^2}{n^2+n} = \dfrac{2(1+n)}{n}$.

Exemplo 3.4.2. *Vejamos um exemplo para $n = 2$, ou seja, S_2 formado pelo ponto $(1, 1, -2)$ em $\mathbb{R}^3$ e sua órbita através da matriz*

$$S = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Segue que, $S_2 = \{S(1,1,-2), S^2(1,1,-2), Id(1,1,-2)\}$, onde $S^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ e $S^3 = Id = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Assim, $S_2 = \{(-2, 1, 1), (1, -2, 1), (1, 1, -2)\}$.

3.4.2 O Código Biortogonal

Definição 3.4.3. *Seja B_n o conjunto formado pela órbita de $(1, 0, ..., 0) \in \mathbb{R}^n$ pelo grupo gerado pela matriz $B = \begin{pmatrix} 0 & \dots & 0 & -1 \\ & & & 0 \\ & Id_{n-1} & & \vdots \\ & & & 0 \end{pmatrix}$, onde Id_{n-1} é a matriz identidade $(n-1) \times (n-1)$. B_n é chamado de* **código Biortogonal** *e possui $2n$ pontos, ou palavras.*

B_n também pode ser visto como o conjunto formado por $(0, ..., 0, \pm 1)$ e seus deslocamentos cíclicos em $\mathbb{R}^n$.

Observe que B_n é um código esférico e todas suas palavras possuem norma 1. Existem duas distâncias ao quadrado possíveis entre os pontos de B_n: $2 = |\ (1, 0, ..., 0) - (0, ..., 0, 1)\ |^2$ e $4 = |\ (1, 0, ..., 0) - (-1, 0, ..., 0)\ |^2$. Assim, B_n possui distância mínima ao quadrado igual a 2 e possui $2n$ pontos e pelo limitante de rankin C, B_n é um código ótimo.

Exemplo 3.4.4. *Como no caso simplex, vejamos um exemplo em $\mathbb{R}^3$, só que neste caso,*

$n = 3$, ou seja, B_3 formado pela órbita de $x = (1, 0, 0)$ pelo grupo gerado pela matriz

$$B = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Assim, $B_n = \{Bx, B^2x, B^3x, B^4x, B^5x, B^6x\}$, onde $B^2 = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}$,

$B^3 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, $B^4 = \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$, $B^5 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}$ *e*

$B^6 = Id = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Portanto, $B_3 = \{(0, 1, 0), (0, 0, 1), (-1, 0, 0), (0, -1, 0), (0, 0, -1), (1, 0, 0)\}$.

Capítulo 4

De Código Binário a Reticulados e Códigos Esféricos

Neste capítulo, será feita uma ligação entre os três capítulos anteriores. Iremos construir reticulados a partir de códigos binários e também códigos esféricos a partir de reticulados que possuam sub-reticulados gerados por vetores ortogonais. Para finalizar, será exposto através de exemplos reticulados associados a códigos esféricos gerados por grupos comutativos de matrizes ortogonais.

As principais referências para este capítulo são [2], [3] e [12].

4.1 Reticulados Obtidos a partir de Códigos Binários

Esta seção é essencialmente um resumo de [3] deste tópico.

Uma das formas de se associar reticulados a códigos é nela chamada **construção A**. Para realiza-la consideremos a aplicação $\Phi : \mathbb{Z}^n \to \mathbb{Z}_2^n$, dada por:

$$\Phi(a_1, a_2, ..., a_n) = (\bar{a_1}, \bar{a_2}, ..., \bar{a_n}).$$

Esta aplicação é sobrejetora e satisfaz a condição que $\Phi(u + v) = \Phi(u) + \Phi(v)$, ou seja, Φ é um homomorfismo de grupos.

Dado um código binário $C \subset \mathbb{Z}_2^n$ linear, obtemos então um reticulado $\Lambda(C)$, calculando $\Phi^{-1}(C)$.

Alguns reticulados podem ser obtidos fazendo-se uma pertubação na pré-imagem da aplicação Φ, ou seja, $\Lambda(C) = a\Phi^{-1}(C)$, onde $a > 0$.

Em [5], a construção A é feita multiplicando um fator $\frac{1}{\sqrt{2}}$. A construção A por ele é feita da seguinte forma: Seja C um (n, M, d) código linear binário. Os pontos de um reticulado $\Lambda(C) \in \mathbb{R}^n$ são todos os pontos $x = (x_1, ..., x_n)$ de $\mathbb{R}^n$ tal que $\sqrt{2}x(mod2) \in C$.

Dada a forma que o reticulado $\Lambda(C) = a\Phi^{-1}(C)$ foi criado, é possível determinar alguns parâmetros do reticulado com base nos parâmetros do código C.

Lema 4.1.1. *[3] O reticulado $2a\mathbb{Z}^n$ está contido em $\Lambda(C) = a\Phi^{-1}(C)$ e a norma mínima de $\Lambda(C)$ é, no máximo $2a$.*

Prova: Seja $x \in 2a\mathbb{Z}^n$. Devemos provar que $x \in a\Phi^{-1}(C)$. Temos que existem $x_1, ..., x_n \in \mathbb{Z}$ tal que $x = 2a(x_1, ..., x_n) = a(2x_1, ..., 2x_n)$.

Devemos provar que $x \in a\Phi^{-1}(C)$, ou seja, $x = ay$, onde $y \in \Phi^{-1}(C)$, e por conseguinte, $c = \Phi(y)$, para algum $c \in C$. De fato, $\Phi(2x_1, ..., 2x_n) = (0, ..., 0)$, logo, $x \in \Lambda(C) = a\Phi^{-1}(C)$.

A distância mínima do reticulado $\mathbb{Z}^n$ é 1, da mesma forma, o reticulado $2a\mathbb{Z}^n$ possui distância mínima $2a \cdot 1$, que é a norma de $a(2 \cdot 1, 0, ..., 0)$. Além disso, se $u \in C$, dentre todos os vetores v tais que $\Phi(v) = u$, o de menor norma é exatamente u, e neste caso, $\| u \|^2 = w(u)$ e qualquer outra pré-imagem de u tem norma maior do que 2. Daí, se au tem norma menor do que $2a$, então

$$\| au \| = a\sqrt{w(u)} \leq 2a,$$

o que implica em $w(u) \leq 4$. Logo, existirão outros vetores de norma mínima em $\Lambda(C)$ distintos dos elementos de $2a\mathbb{Z}^n$ se, e somente se, $d \leq 4$, onde d é a distância de Hamming mínima de C. ■

A partir deste lema podemos concluir o seguinte:

Proposição 4.1.2. *[3] Sejam C um código linear binário com parâmetros $[n, \kappa, d]$, onde d é a distância de Hamming e $\Lambda(C) = a\Phi^{-1}(C)$. Então,*

1. *Se $d < 4$, a norma mínima é $a\sqrt{d}$ e os vetores de norma mínima de $\Lambda(C)$ são os vetores av, com $v \in C$ de peso menor ou igual a 4, bem como os vetores av', obtidos deste trocando-se alguns dos 1's por -1's.*

2. *Se $d = 4$, a norma mínima é $2a$ e todos os vetores listados no item anterior são de norma mínima e possuem a única entrada não-nula igual a $\pm 2a$.*

3. *Se $d > 4$, a norma mínima é $2a$ e os vetores de norma mínima são os vetores cuja única entrada não-nula é $\pm 2a$.*

Este resultado nos fornece o raio do empacotamento e o número de vetores de norma mínima.

Outro resultado importante para o cálculo de densidade de empacotamento é o que segue([12]).

Proposição 4.1.3. *[12] Sejam C um código linear binário com parâmetros $[n, \kappa, d]$ e $\Lambda(C) = \Phi^{-1}(C)$. Então, o volume do reticulado é dado por: $|\det \Lambda(C)|^{\frac{1}{2}} = 2^{n-k}$.*

Prova: Sejam $\Phi : \mathbb{Z}^n \to \mathbb{Z}_2^n$ onde $\Phi(a_1, ..., a_n) = (\bar{a_1}, ..., \bar{a_n})$, e $B = (I_{k\times k} \; A_{k\times n-k})$ uma matriz geradora de C na forma padrão. Temos que $\tilde{B} = \begin{pmatrix} I_k & A_{k\times n-k} \\ 0 & 2I_{n-k} \end{pmatrix}$ é uma matriz geradora de $\Phi^{-1}(C) = \Lambda(C)$. De fato, Como $B = (I_k \;\; A_{k\times n-k})$ é uma matriz geradora de C, temos que $\Lambda(C) = \{(w + 2h \quad wA + 2m)\} \subset \mathbb{Z}^n$, onde $w \in \mathbb{Z}_2^k$, $h \in \mathbb{Z}^k$ e $m \in \mathbb{Z}^{n-k}$. Seja $\Theta(C) = \{[\tilde{w_1} \;\; \tilde{w_1}A + 2\tilde{w_2}], (\tilde{w_1}, \tilde{w_2}) \subset \mathbb{Z}^n\}$ o reticulado que da forma que foi definido, possui matriz geradora $\begin{pmatrix} I_k & A_{k\times n-k} \\ 0 & 2I_{n-k} \end{pmatrix}$. Provemos que $\Lambda(C) = \Theta(C)$. Tomando $h = 0$ e $m = \tilde{w_2}$, temos que $\Lambda(C) \subset \Theta(C)$. Tomando agora $w = \tilde{w_1}(mod 2)$, ou seja $\tilde{w_1} = w+2h$ e $\tilde{w_2} = m-hA$, temos que $\tilde{w_1}A + 2\tilde{w_2} = (w + 2h)A + 2(m - hA) = wA + 2hA + 2m - 2hA = wA + 2m$. Assim provamos que $\Theta(C) \subset \Lambda(C)$.

Portanto, $|\det \Lambda(C)|^{\frac{1}{2}} = det \begin{pmatrix} I & A \\ 0 & 2I \end{pmatrix} = 2^{n-k}$.

■

4.1.1 Reticulados Obtidos pela Construção A

Um exemplo importante e simples é o do reticulado D_n. Considere o código

$$C_n = \{(x_1, x_2, ..., x_n) \in \mathbb{Z}_2^n; \sum_{i=1}^{n} x_i = 0\},$$

de parâmetros $[n, n-1, 2]$.

O reticulado D_n é obtido calculando $\Lambda(C_n) = \Phi^{-1}(C_n)$. Neste caso tomaremos a constante $a = 1$.

Mostremos como exemplo, o caso $n = 3$, ou seja, o reticulado D_3, gerado pelo código binário C_3.

Exemplo 4.1.4. *Consideremos o código linear binário*

$$C_3 = \{(x_1, x_2, x_3) \in \mathbb{Z}_2^3; \sum_{i=1}^{3} x_i = 0\} = \{(1,1,0), (1,0,1), (0,1,1), (0,0,0)\}.$$

A partir de C_3, iremos construir o reticulado D_3 através da aplicação $\Phi^{-1}(C_3)$.

Devemos conseguir uma base de $\Lambda(C_3) = \Phi^{-1}(C_3)$ cuja matriz de Gram coincida com a de D_3 vista anteriormente no capítulo 2. Pela forma da matriz de D_3, precisamos encontrar uma base $\beta = \{v_1, v_2, v_3\}$ de $\Lambda(C_3)$ que satisfaça as equações

$$\langle v_1, v_3 \rangle = -1, \quad \langle v_2, v_3 \rangle = -1, \quad \langle v_1, v_2 \rangle = 0.$$

Então, consideremos $u = (x, y, z)$ em $\Lambda(C_3)$. Como $x + y + z \equiv 0 \ mod 2$, ou seja, $y \equiv -x - z \ mod 2$, temos que

$$u = (x, -x - z, z) + (0, 2m, 0),$$

para algum m inteiro. Daí segue que $u = x(1,-1,0) + z(0,-1,1) + m(0,2,0)$ e a terna $\{(1,-1,0), (0,-1,1), (0,2,0)\}$ é uma base de $\Lambda(C_3)$.

Podemos melhorar esta base, substituindo o vetor $(0,2,0)$ por algum outro que tenha norma quadrada em $\Lambda(C_3)$ igual a 2. Observe que $(0,2,0) = (1,1,0) + (-1,1,0)$. Assim, podemos trocar $(0,2,0)$ por $(1,1,0)$ e obter a base $\{(1,-1,0), (0,-1,1,), (1,1,0)\}$. A partir desta base, temos que basta multiplicar por -1 os vetores $(0,-1,1)$ e $(1,1,0)$ e trocar a ordem dos vetores e obter a nova base $\beta = \{(1,-1,0), (-1,-1,0), (0,1,-1)\}$ cuja matriz de Gram coincide com a de D_3.

Exemplo 4.1.5. *A construção de D_4 segue de forma análoga, assim, podemos aproveitar a base β de D_3 acrescentando apenas a ultima coordenada nula em cada vetor. Desta forma, já obtemos três vetores da nossa base $\beta = \{(1,-1,0,0), (-1,-1,0,0), (0,1,-1,0), v_4\}$.*

O vetor v_4 deve estar no subespaço ortogonal a $v_1 = (1, -1, 0, 0)$ e $v_2 = ((-1, -1, 0, 0)$ e deve satisfazer $\langle v_3, v_4 \rangle = -1$, onde $v_3 = (0, 1, -1, 0)$. Isso nos dá um sistema linear de três equações que tem por solução o subespaço afim $S = \{(0, 0, 1, z); z \in \mathbb{R}\}$. Como v_4 deve ter norma quadrada 2, tomamos então $z = \pm 1$. Para manter uma simetria na escolha da base, tomaremos $v_4 = (0, 0, 1, -1)$ e obteremos a base

$$\beta = \{(1, -1, 0, 0), (-1, -1, 0, 0), (0, 1, -1, 0), (0, 0, 1, -1)\},$$

cuja matriz de Gram coincide com a de D_4.

Vários outros reticulados importantes podem ser construídos desta forma, como o reticulado E_8 que possui matriz de Gram

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 & -1 & 2 \end{pmatrix},$$

que é o reticulado de maior densidade em $\mathbb{R}^8$.

4.2 Códigos Esféricos Obtidos a Partir de Reticulados

Inicialmente iremos considerar reticulados em $\mathbb{R}^2$ e mergulhar este em uma esfera em $\mathbb{R}^4$. Daqui em diante, iremos sempre chamar de código esférico, qualquer código que esteja em um esfera de raio qualquer, visto que basta normalizar cada palavra deste código para este estar em uma esfera unitária.

Para podermos obter Códigos esféricos a partir de reticulados, precisaremos que o reticulado possua um sub- reticulado com base ortogonal. Com base nisto iremos iniciar com reticulados gerados por bases cujo politopos associados são retângulos.

Seja Λ_α o reticulado gerado pela base $\alpha = \{u, v\}$, onde $u = (r_1, 0)$ e $v = (0, r_2)$, onde $r_1, r_2 \in \mathbb{N}$.

Realizando o quociente $\dfrac{\mathbb{Z}^2}{\Lambda_\alpha}$, obtemos um toro plano que pode ser visto como a região retangular $[r_1, 0] \times [0, r_2]$, com os bordos identificados.

Agora considere a aplicação $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ dada por:

$$\varphi(x, y) = \Big(\frac{r_1}{2\pi}\Big(\cos\frac{2\pi x}{r_1}, \sin\frac{2\pi x}{r_1}\Big), \frac{r_2}{2\pi}\Big(\cos\frac{2\pi y}{r_2}, \sin\frac{2\pi y}{r_2}\Big)\Big).$$

Observe que $\varphi(x, y) = \varphi(\tilde{x}, \tilde{y})$ se, e somente se, $\mu_\alpha(x, y) = \mu_\alpha(\tilde{x}, \tilde{y})$, isto é,

$$(x, y) - (\tilde{x}, \tilde{y}) = mu + nv;$$

e como todo ponto de $\mathbb{R}^2$ possui um representante no toro plano T_α, temos que $\varphi(\mathbb{R}^2) = \varphi([r_1, 0] \times [0, r_2])$ e φ identifica os lados opostos do retângulo. Formalmente, φ induz uma correspondência $\tilde{\varphi}$ um a um entre T_α e $\varphi(\mathbb{R}^2)$ em $\mathbb{R}^4$.

Observe que esta correspondência é uma isometria. De fato:

$$\| \frac{\partial\varphi}{\partial x}(x, y) \| = \sqrt{(\frac{r_1}{2\pi} \cdot \frac{2\pi}{r_1}\cos^2\frac{2\pi x}{r_1} + \frac{r_1}{2\pi} \cdot \frac{2\pi}{r_1}\sin^2\frac{2\pi x}{r_1})} = 1,$$

$$\| \frac{\partial\varphi}{\partial y}(x, y) \| = \sqrt{(\frac{r_2}{2\pi} \cdot \frac{2\pi}{r_2}\cos^2\frac{2\pi y}{r_2} + \frac{r_2}{2\pi} \cdot \frac{2\pi}{r_2}\sin^2\frac{2\pi y}{r_2})} = 1 \text{ e}$$

$$\langle \frac{\partial\varphi}{\partial x}(x, y), \frac{\partial\varphi}{\partial y}(x, y) \rangle = 0.$$

Através desta isometria, temos que os pontos do toro plano (que podem ser vistos como os vértices do grafo mergulhado), obtidos através do quociente $\dfrac{\mathbb{Z}^2}{\Lambda_\alpha}$, são mergulhados e transformados em pontos em uma esfera de raio $\rho = \dfrac{\sqrt{(r_1^2 + r_2^2)}}{2\pi}$. Normalizando estes pontos, temos um novo código esférico, que possui o número de palavras igual ao número de vértices do grafo mergulhado em T_α.

Uma outra situação da base do reticulado é quando $\lambda = \{u, v\}$, onde $u = (a, b)$ e $v = t(-b, a), t \in \mathbb{R}$. Assim o mergulho em $\mathbb{R}^4$ pode ser feito através da isometria Φ que é a composição de φ com uma rotação de $\theta = \angle(u, e_1)$, onde $e_1 = (1, 0)$, isto é,

$$\Phi(x, y) = \varphi(R_\theta(x, y)),$$

onde $R_\theta(x,y) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$.

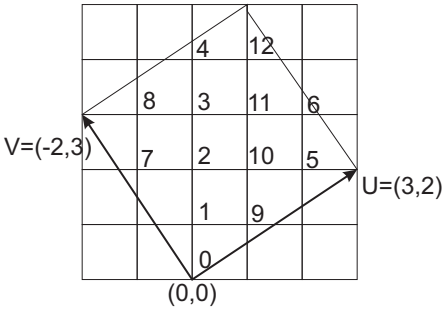
Portanto, $\Phi(\mathbb{R}^2) \subset \mathbb{R}^4$ está contido em uma esfera 3-dimensional de raio $\rho = \frac{\sqrt{\|u\|^2+\|v\|^2}}{2\pi}$.

Quando $t = 1$, o toro T_α é gerado por um quadrado e temos:

$$\Phi(x,y) = \frac{\sqrt{a^2+b^2}}{2\pi}\Big(\cos\frac{2\pi(bx-ay)}{a^2+b^2}, \sin\frac{2\pi(bx-ay)}{a^2+b^2}, \cos\frac{2\pi(ax+by)}{a^2+b^2}, \sin\frac{2\pi(ax+by)}{a^2+b^2}\Big).$$

Um exemplo é o caso do reticulado gerado pela base $\lambda = \{(2,3),(-3,2)\}$.

Exemplo 4.2.1. *Seja Λ_α o reticulado gerado pela base $\alpha = \{(2,3),(-3,2)\}$. Fazendo o quociente de $\frac{\mathbb{Z}^2}{\Lambda_\alpha}$ temos o grafo no toro plano T_α.*



A aplicação Φ que identifica pontos de $\mathbb{R}^2$, por translações associadas a Λ_α é dada por

$$\Phi(x,y) = \frac{\sqrt{13}}{2\pi}\Big(\cos\frac{2\pi(3x-2y)}{13}, \sin\frac{2\pi(3x-2y)}{13}, \cos\frac{2\pi(2x+3y)}{13}, \sin\frac{2\pi(2x+3y)}{13}\Big).$$

Agora para sabermos os pontos do código esférico, basta calcular a imagem dos pontos do grafo no toro plano. Como o grafo no toro plano T_α tem 13 pontos (2.9.4), a saber

$$\begin{array}{llll} 0=(0,0) & 4=(0,4) & 8=(-1,3) & 12=(1,4) \\ 1=(0,1) & 5=(2,2) & 9=(1,1) & \\ 2=(0,2) & 6=(2,3) & 10=(1,2) & \\ 3=(0,3) & 7=(-1,2) & 11=(1,3) & \end{array}$$

temos que o código esférico terá também 13 pontos.

Como este código é gerado por um grupo cíclico, poia à translação vertical no plano por $(0,1)$ corresponde a rotação em $\mathbb{R}^4$ dada pela matriz $\begin{pmatrix} ROT(\frac{2}{13}2\pi) & 0 \\ 0 & ROT(\frac{3}{13}2\pi) \end{pmatrix}$,

basta calcular a imagem por exemplo do 0 *e dos pontos ligados a ele pelas arestas do grafo mergulhado em* T_α*. Neste caso, pela simetria das inclinações das retas geradas por* $(2,3)$ *e* $(-3,2)$*e pelo tamanho de* u *e* v*, podemos afirmar que à menor distância entre pontos do reticulado corresponde a menor distância no código esférico.*

Neste caso, os pontos que são vizinhos do ponto $0=(0,0)$ *são os pontos* $1=(0,1)$*,* $5=(2,2)$ *e* $8=(-1,3)$*, e a imagem por* Φ *destes pontos são:*

$$\begin{aligned}
\Phi(0,0) &= \frac{\sqrt{13}}{2\pi}(1,0,1,0);\\
\Phi(0,1) &= \frac{\sqrt{13}}{2\pi}(\cos\frac{4\pi}{13},\sin\frac{4\pi}{13},\cos\frac{6\pi}{13},\sin\frac{6\pi}{13})\\
\Phi(2,2) &= \frac{\sqrt{13}}{2\pi}(\cos\frac{4\pi}{13},\sin\frac{4\pi}{13},\cos\frac{20\pi}{13},\sin\frac{20\pi}{13})\\
\Phi(-1,3) &= \frac{\sqrt{13}}{2\pi}(\cos\frac{18\pi}{13},\sin\frac{18\pi}{13},\cos\frac{14\pi}{13},\sin\frac{14\pi}{13}).
\end{aligned}$$

Calculando a distância mínima entre eles, temos que $d=0.929339$*. Se normalizarmos os vetores, teremos que a distância mínima na esfera unitária será* $d=1.1451631$*.*

Este é um código ótimo em $\mathbb{R}^4$ *para o número de pontos* $M=13$ *com rotulamento por grupos abelianos ([10] e [13]).*

Este procedimento pode ser generalizado para dimensões maiores. O toro planar T_α, onde $\alpha=\{u_1,u_2,...,u_n\}$ pode ser identificado com o politopo fundamental com suporte em α e com os bordos paralelos identificados. Se α é uma base ortogonal, o toro plano T_α pode ser mergulhado em uma esfera de $\mathbb{R}^{2n}$, que irá depender da base α. Para $x=\sum_{i=1}^{n}x_iu_i$, temos que

$$\Phi(x)=\Big(\frac{\mid u_1\mid}{2\pi}\cos\frac{2\pi x_1}{\mid u_1\mid},\frac{\mid u_1\mid}{2\pi}\sin\frac{2\pi x_1}{\mid u_1\mid},\ldots,\frac{\mid u_n\mid}{2\pi}\cos\frac{2\pi x_n}{\mid u_n\mid},\frac{\mid u_n\mid}{2\pi}\sin\frac{2\pi x_n}{\mid u_n\mid}\Big). \tag{4.1}$$

Um outro exemplo que consideremos a seguir é o do código esférico associado ao reticulado D_3, já que este foi um reticulado obtido de um código binário.

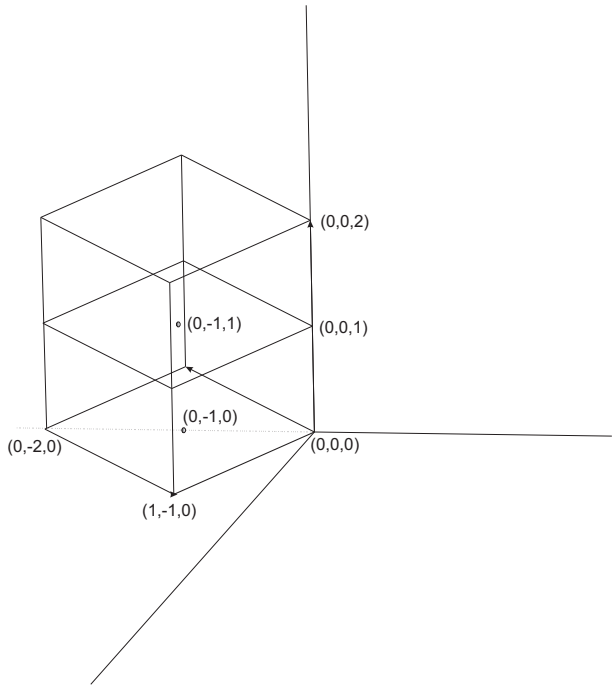
Exemplo 4.2.2. *Este exemplo é interessante, porque neste caso, uma base natural de* D_3 *é dada por* $\beta=\{(1,-1,0),(-1,-1,0),(0,1,-1)\}$*, e ela não é ortogonal, mas o procedimento a seguir é tentar achar um sub reticulado de* D_3 *que possua uma base ortogonal. Como os*

dois primeiros vetores da base são ortogonais, devemos procurar inicialmente um vetor $\widetilde{w}$ *no reticulado, tal que* u, v *e* $\widetilde{w}$ *sejam ortogonais. Como* u *e* v *possuem a última coordenada nula, temos que o vetor* $\widetilde{w} = (0, 0, k)$ *é ortogonal a* u *e* v, *mas resta saber se este novo reticulado é um sub reticulado de* Λ_β. *De fato ele é um sub reticulado de* Λ_β *pois,*

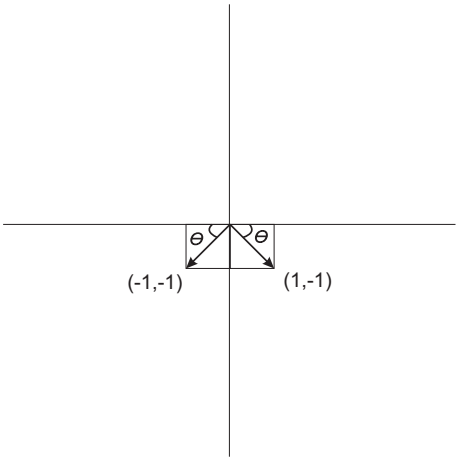
$$(0, 0, k) = \frac{-k}{2}(1, -1, 0) + \frac{-k}{2}(-1, -1, 0) - k(0, 1, -1). \tag{4.2}$$

Pela fórmula acima, k *deve ser um múltiplo de* 2, *para que os múltiplos dos vetores da base sejam inteiros, ou seja* $k = 2m$, $m \in \mathbb{Z}$.

Para acharmos um código esférico associado, tomemos $k = 2$. *Assim, obtemos um sub-reticulado* $\Lambda_{\widetilde{\beta}}$ *onde* $\widetilde{\beta} = \{(1, -1, 0), (-1, -1, 0), (0, 0, 2)\}$. *Quando fazemos o quociente* $\dfrac{\mathbb{Z}^3}{\Lambda_{\widetilde{\beta}}}$, *teremos um grafo plano mergulhado no toro planar* $T_{\widetilde{\beta}}$ *com* $M = |\det A|$ *pontos(vértices), onde* $A = \begin{pmatrix} 1 & -1 & 0 \\ -1 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$, *ou seja, 4 pontos, a saber,* $v_1 = (0, -1, 0)$, $v_2 = (0, 0, 0)$, $v_3 = (0, 0, 1)$ *e* $v_4 = (0, -1, 1)$.



Vale lembrar que a aplicação $\Phi = \varphi \circ R_\theta$. *Como neste caso o eixo* z *não precisa ser rotacionado, podemos como no caso* $\mathbb{R}^2$ *rotacionar apenas os eixos* x *e* y *da seguinte forma.*



$$R_\theta = \begin{pmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

Assim a aplicação Φ, *de acordo com a base* $\widetilde{\beta}$ *e 4.1 é dada por*

$$\Phi(x,y,z) = \left(\tfrac{\sqrt{2}}{2\pi}\cos\pi(x-y), \tfrac{\sqrt{2}}{2\pi}\sin\pi(x-y), \tfrac{\sqrt{2}}{2\pi}\cos\pi(-x-y), \tfrac{\sqrt{2}}{2\pi}\sin\pi(-x-y), \tfrac{1}{\pi}\cos\pi z, \tfrac{1}{\pi}\sin\pi z\right).$$

Os pontos do código esférico associado são:

$$\begin{aligned}
\Phi(0,-1,0) &= (-\tfrac{1}{\sqrt{2}\pi}, 0, -\tfrac{1}{\sqrt{2}\pi}, 0, \tfrac{1}{\pi}, 0) \\
\Phi(0,0,0) &= (\tfrac{1}{\sqrt{2}\pi}, 0, \tfrac{1}{\sqrt{2}\pi}, 0, \tfrac{1}{\pi}, 0) \\
\Phi(0,0,1) &= (\tfrac{1}{\sqrt{2}\pi}, 0, \tfrac{1}{\sqrt{2}\pi}, 0, -\tfrac{1}{\pi}, 0) \\
\Phi(0,-1,1) &= (-\tfrac{1}{\sqrt{2}\pi}, 0, -\tfrac{1}{\sqrt{2}\pi}, 0, -\tfrac{1}{\pi}, 0)
\end{aligned}$$

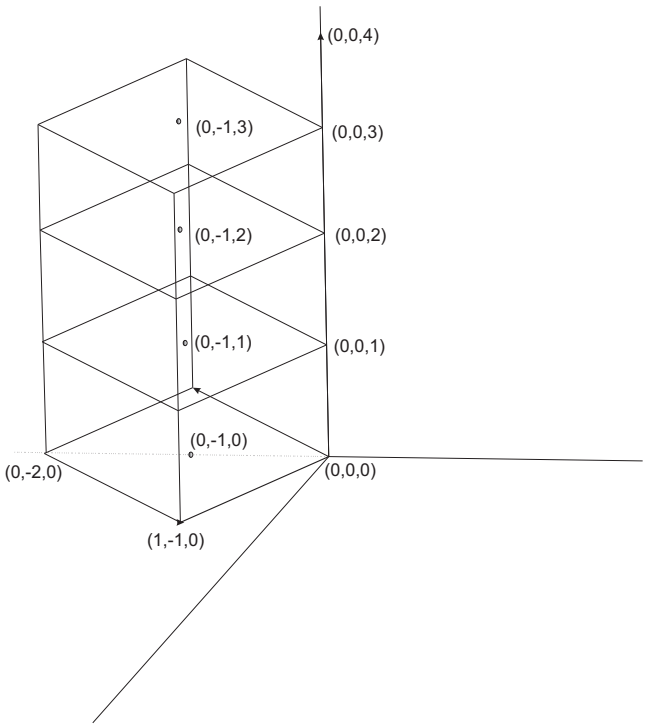
e a distância de v_1 *a* $v(i)$, $2 \leq i \leq 4$ *são:* $\dfrac{2}{\pi}$, $\dfrac{2\sqrt{2}}{\pi}$ *e* $\dfrac{2}{\pi}$. *Assim, a distância mínima é aproximadamente* $d = 0.63662$. *Normalizando os vetores para o código ficar na esfera de raio* 1, *temos que a distância mínima é dada por* $d = 1.41421$.

Observação 4.2.3. *Este código não é "substancial", pois, para* $x = (x_1, x_2, ..., x_6) \in C$, *temos que* $x_1 = x_3$, $x_2 = x_4 = x_6 = 0$, *logo* x *está contido num plano e portanto num círculo. Como a dimensão do espaço em que se encontra mergulhado o código esférico é* 2, *temos que a melhor distribuição possível no círculo unitário são os vértices de polígonos*

regulares, ou seja, os códigos ótimos em dimensão 2 *são os códigos M-PSK. Neste caso o código possui* 4 *pontos e o código ótimo é dado pelos vértices de um quadrado inscrito no circulo unitário. Assim, a distância mínima deste código ótimo é* $d = \sqrt{2} \approx 1.41421$. *Logo o código acima é o código ótimo para* 4 *pontos em dimensão* 2. *O melhor código contido na esfera unitária em* $\mathbb{R}^6$ *é o códigos cujos pontos são os vértices de um tetraedro, com distância mínima* $d = 1.6330$.

Se tomarmos $k = 4$, *na base do sub-reticulado de* D_3*(4.2), teremos uma nova base* $\widetilde{\beta} = \{(1, -1, 0), (-1, -1, 0), (0, 0, 4)\}$ *para o sub reticulado. O grafo mergulhado no toro plano* $T_{\widetilde{\beta}}$ *terá* $M = 8$ *pontos(vértices). A saber*

$$((0, 0, 0), (0, 0, 1), (0, 0, 2), (0, 0, 3), (0, -1, 0), (0, -1, 1), (0, -1, 2), (0, -1, 3).$$



A nova aplicação Φ *é dada por*

$\Phi(x,y,z) = \left(\frac{\sqrt{2}}{2\pi}\cos\pi(x-y), \frac{\sqrt{2}}{2\pi}\sin\pi(x-y), \frac{\sqrt{2}}{2\pi}\cos\pi(-x-y), \frac{\sqrt{2}}{2\pi}\sin\frac{\pi(-x-y)}{\sqrt{2}}, \frac{2}{\pi}\cos\frac{\pi z}{2}, \frac{2}{\pi}\sin\frac{\pi z}{2}\right)$.

Calculando os pontos na esfera, teremos que a distância mínima deste código é $d = 0.63662$*, aproximadamente. Normalizando os vetores do código, teremos que a distância mínima na esfera unitária é* $d = 0.894427$*. Este novo código também não é substancial em* $\mathbb{R}^6$*, pois para* $x = (x_1, ..., x_6) \in C$*, temos que* $x_1 = x_3$*,* $x_2 = x_4 = 0$*. Logo, este código está contido num espaço de dimensão* 3*, e o melhor código de* 8 *pontos em dimensão* 3 *é o antiprisma quadrado, cuja distância mínima é de* $d \approx 1.21556$*.*

Uma coisa importante a ser observada é o que acontece quando modificamos a base de forma a deixar o paralelepípedo que define o toro mais próximo de um cubo. Como o último vetor da base é $u_3 = (0, 0, 2k)$*, temos de encontrar* α_1*,* α_2 *e* α_3 *tal que* $\alpha_1 u_1$*,* $\alpha_2 u_2$*,* $\alpha_3 u_3$ *tenham aproximadamente a mesma norma. Tomemos como exemplo,* $\alpha_1 = 2$*,* $\alpha_2 = 2$ *e* $\alpha_3 = 1$*, com* $k = 1$*. Teremos então um novo sub reticulado gerado pela base*

$$\widetilde{\beta} = \{(2, -2, 0), (-2, -2, 0), (0, 0, 2)\}. \tag{4.3}$$

Desta vez, o grafo mergulhado no toro plano $T_{\widetilde{\beta}}$ *terá* $M = |\det A| = 16$ *pontos, onde* $A = \begin{pmatrix} 2 & -2 & 0 \\ -2 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$*. Os pontos são :*

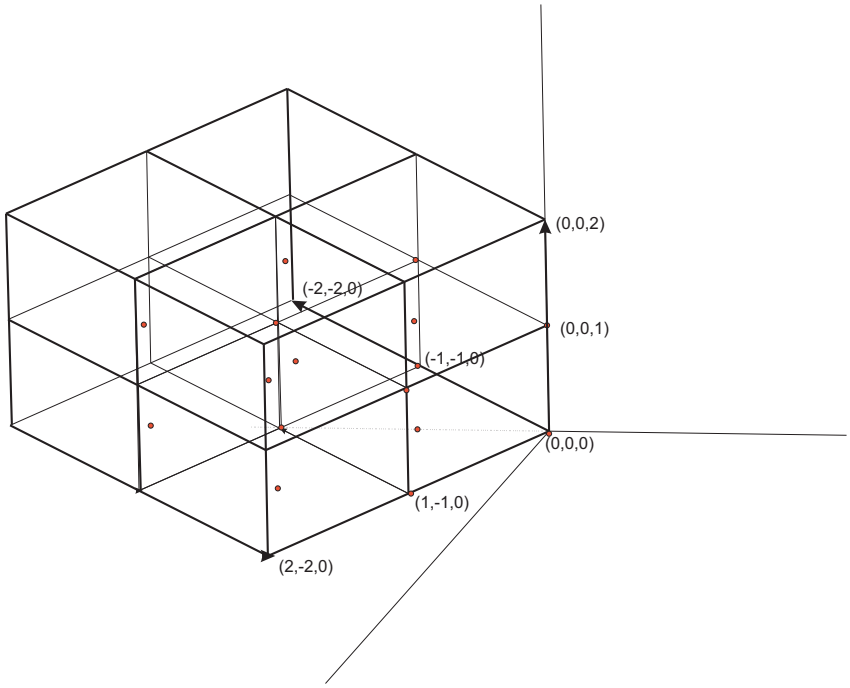
$$\begin{array}{cccc} (0,-1,0) & (0,0,0) & (0,-1,1) & (0,0,1) \\ (1,-2,0) & (1,-1,0) & (1,-2,1) & (1,-1,1) \\ (0,-3,0) & (0,-2,0) & (0,-3,1) & (0,-2,1) \\ (-1,-2,0) & (-1,-1,0) & (-1,-2,1) & (-1,-1,1) \end{array} \tag{4.4}$$

A aplicação Φ*, dada de acordo com a nova base* $\widetilde{\beta}$ *é dada por:*

$\Phi(x,y,z) = \left(\frac{\sqrt{2}}{\pi}\cos\pi(x-y), \frac{\sqrt{2}}{\pi}\sin\pi(x-y), \frac{\sqrt{2}}{\pi}\cos\pi(-x-y), \frac{\sqrt{2}}{\pi}\sin\pi(-x-y), \frac{1}{\pi}\cos\pi z, \frac{1}{\pi}\sin\pi z\right)$.

A imagem dos pontos em 4.4 por Φ *irá gerar um código esférico com distância mínima aproximada* $d = 0.63662$*, e este código está sobre a esfera de raio* $\rho = \frac{\sqrt{5}}{\pi}$*.*

Normalizando os vetores do código teremos que a distância mínima na esfera unitária é $d = 0.894427$*.*



Uma pergunta relevante seria: É possível encontrar k_1, k_2 e k_3 de forma a melhorar a distância mínima(ou encontrar uma distância mínima na esfera unitária a maior possível) do código esférico associado ao reticulado gerado pela base $\beta = \{k_1(2,-2,0), k_2(-2,-2,0), k_3(0,0,2)\}$?

A resposta para esta pergunta é sim.

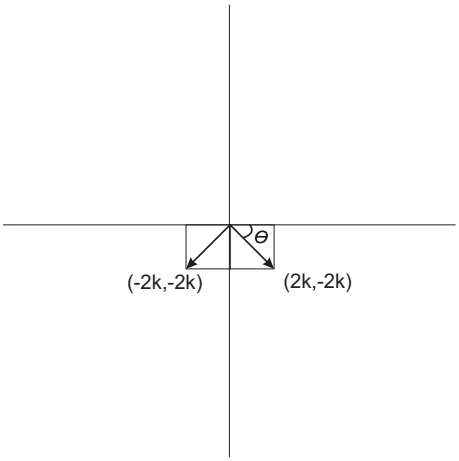
Pelo fato dos dois primeiros vetores da base terem o mesmo comprimento, iremos tomar $k_1 = k_2$, e pelo fato deste novo código esférico estar sob a mesma esfera do código esférico da base $\widetilde{\beta}$ de raio $\rho = \frac{\sqrt{5}}{\pi}$ temos que k_1 e k_3 devem satisfazer a seguinte igualdade

$$\frac{\sqrt{16k_1^2 + 4k_3^2}}{2\pi} = \frac{\sqrt{20}}{2\pi}.$$

Daí temos que $k_3 = \sqrt{5 - 4k_1^2}$.

O valor de $k_1 = \lambda$ deverá variar no intervalo $[\sqrt{\frac{5}{6}}, 1]$, onde $\lambda = \sqrt{\frac{5}{6}}$ deixa todos os vetores da base com mesma norma e na mesma esfera de raio $\rho = \frac{\sqrt{5}}{\pi}$, e o valor $\lambda = 1$ é o valor que ira deixar a base β igual a base $\widetilde{\beta}$ original.

Para acharmos a aplicação Φ e então a norma mínima a ser maximizada, temos que encontrar a matriz de rotação do eixo x em torno de $e_1 = (1,0)$ e compor com a aplicação φ definida em 4.1.



A matriz R_θ será $R_\theta = \begin{pmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$.

Portanto, teremos que

$$\Phi(x,y,z) = (\frac{\sqrt{2}\lambda}{\pi}\cos(\frac{\pi(x-y)}{2\lambda}), \frac{\sqrt{2}\lambda}{\pi}\sin(\frac{\pi(x-y)}{2\lambda}), \frac{\sqrt{2}\lambda}{\pi}\cos(\frac{\pi(x+y)}{2\lambda}), \frac{\sqrt{2}\lambda}{\pi}\sin(\frac{\pi(x+y)}{2\lambda}),$$

$$\frac{\sqrt{5-4\lambda^2}}{\pi}\cos(\frac{\pi z}{5-4\lambda^2}), \frac{\sqrt{5-4\lambda^2}}{\pi}\sin(\frac{\pi z}{5-4\lambda^2}))$$

Os pontos do grafo imerso no toro plano gerado pela base β são:

$v_1 = (0,0,0)$ $\quad v_5 = (\lambda,-2\lambda,0)$ $\quad v_9 = (0,-3\lambda,0)$

$v_2 = (0,-\lambda,0)$ $\quad v_6 = (\lambda,-\lambda,0)$ $\quad v_{10} = (0,-2\lambda,0)$

$v_3 = (0,0,\sqrt{5-4\lambda^2})$ $\quad v_7 = (\lambda,-2\lambda,\sqrt{5-4\lambda^2})$ $\quad v_{11} = (-\lambda,-\lambda,\sqrt{5-4\lambda^2})$

$v_4 = (0,-\lambda,\sqrt{5-4\lambda^2})$ $\quad v_8 = (\lambda,-\lambda,\sqrt{5-4\lambda^2})$ $\quad v_{12} = (0,-3\lambda,\sqrt{5-4\lambda^2})$

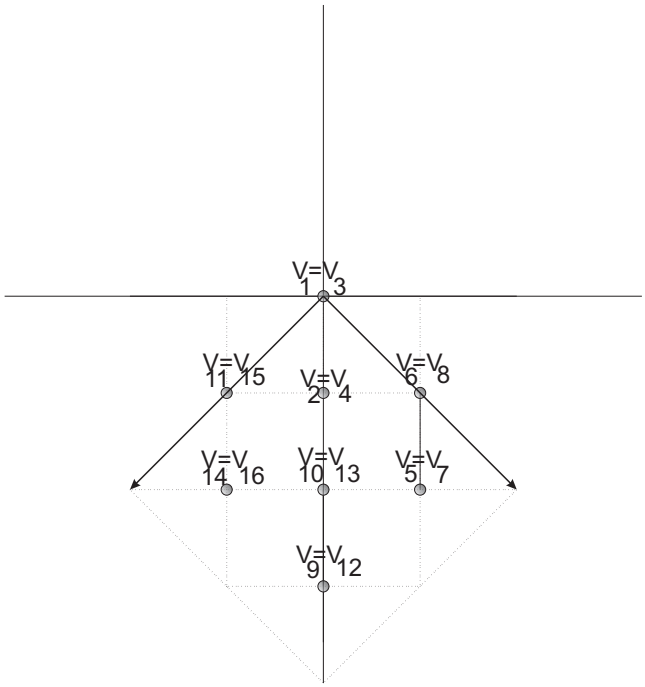
$v_{13} = (0,-2\lambda,\sqrt{5-4\lambda^2})$

$v_{14} = (-\lambda,-2\lambda,0)$

$v_{15} = (-\lambda,-\lambda,0)$

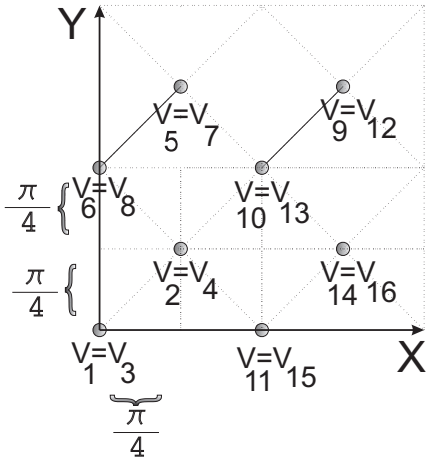
$v_{16} = (-\lambda,-2\lambda,\sqrt{5-4\lambda^2})$

Para maximizar a distância mínima, devemos saber qual a menor distância entre as imagens dos vetores $v_i's$ que terá o maior valor para $\lambda \in [\sqrt{\frac{5}{6}}, 1]$. Para facilitar, vamos olhar a imagem de Φ como $S \times S \times S$. Para analisar a distância entre $v[i]$ e $v[j]$ vamos projetar os pontos do toro plano $T_{\widetilde{\beta}}$ no plano xy e analisar o ângulo de rotação que cada ponto vai fazer na esfera, e a partir disto calcular a distância mínima.



A figura acima representa as projeções dos pontos de $T_{\widetilde{\beta}}$ no eixo xy.

Fazendo uma rotação de $\frac{\pi}{4}$ teremos agora o toro plano abaixo.



Representando cada ponto pela rotação sofrida em cada esfera S^2, poderemos analisar facilmente a menor distância entre as imagens dos vetores $v_i's$ pela aplicação Φ.

Na figura 4.1, $R_1 = \frac{\sqrt{2}\lambda}{\pi}$ e $R_3 = \frac{\sqrt{5-4\lambda^2}}{\pi}$. Assim, para $\lambda \in [\sqrt{\frac{5}{6}}, 1]$, temos que $2R_3 \leq 2R_1$ e $2R_3 \leq 2D$. Portanto, para todo $\lambda \in [\sqrt{\frac{5}{6}}, 1]$, a distância de V_1 até V_3 é menor que qualquer outra distância. A distância de V_1 até V_3 é dada por $d = 2R_3 = 2\frac{\sqrt{5-4\lambda^2}}{\pi}$. Assim, temos que

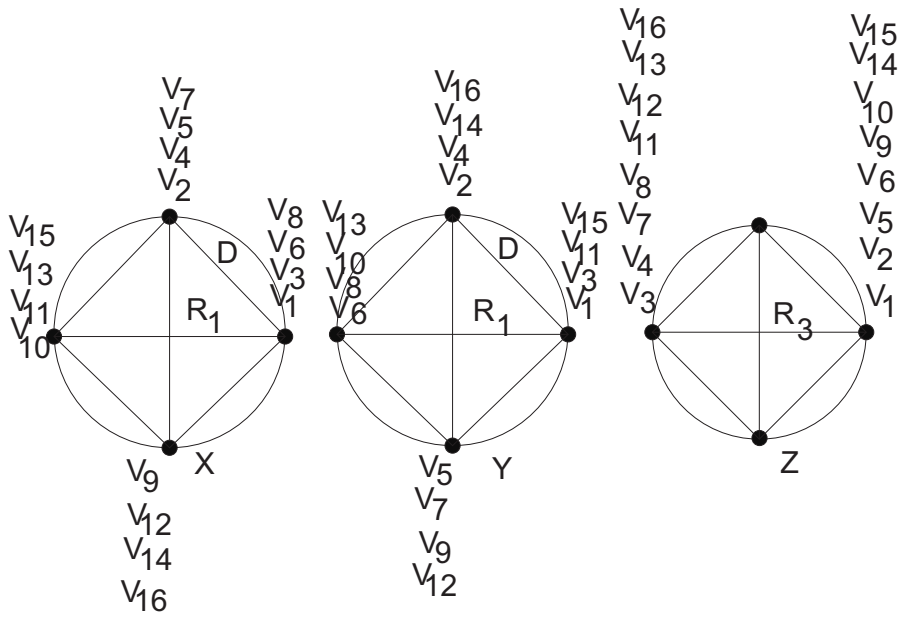


Figura 4.1: Representação da rotação sofrida por cada ponto

minimizar $d(\lambda) = 2R_3 = 2\frac{\sqrt{5-4\lambda^2}}{\pi}$ no intervalo $[\sqrt{\frac{5}{6}}, 1]$. Como $d' < 0$ neste intervalo, temos que o valor máximo da distância vai ser atingido para $\lambda = \sqrt{\frac{5}{6}}$. Assim, o reticulado gerado pela base

$$\beta = \{(\sqrt{\frac{5}{6}}, -\sqrt{\frac{5}{6}}, 0), (-\sqrt{\frac{5}{6}}, -\sqrt{\frac{5}{6}}, 0), (0, 0, \sqrt{\frac{5}{3}}) \tag{4.5}$$

terá um código esférico associado com distância mínima $d = 0.821873$ e também com 16 pontos. Normalizando os pontos do código, temos que a distância mínima na esfera unitária é $d = 1.1547$, bem melhor que o anterior para 16 pontos(0.8944).

Podemos representar cada ponto do código esférico através da matriz de rotação associada a este. Para construir a matriz de rotação do grupo, basta observar na figura 4.1 o ângulo de rotação em cada esfera e montar a matriz geral da seguinte forma: Dado um ponto V_i onde os ângulos nas esferas feitas em 4.1 são a, b e c respectivamente, então, a matriz de

rotação de V_i é dada por

$$\begin{pmatrix} ROT(a) & 0 & 0 \\ 0 & ROT(b) & 0 \\ 0 & 0 & ROT(c) \end{pmatrix} = \begin{pmatrix} \cos a & -\sin a & 0 & 0 & 0 & 0 \\ \sin a & \cos a & 0 & 0 & 0 & 0 \\ 0 & 0 & \cos b & -\sin b & 0 & 0 \\ 0 & 0 & \sin b & \cos b & 0 & 0 \\ 0 & 0 & 0 & 0 & \cos c & -\sin c \\ 0 & 0 & 0 & 0 & \sin c & \cos c \end{pmatrix}.$$

Desta forma, a matriz que representa os pontos do código esférico são:

$$V_1 = \begin{pmatrix} ROT(0) & 0 & 0 \\ 0 & ROT(0) & 0 \\ 0 & 0 & ROT(0) \end{pmatrix}, V_2 = \begin{pmatrix} ROT(\frac{\pi}{2}) & 0 & 0 \\ 0 & ROT(\frac{\pi}{2}) & 0 \\ 0 & 0 & ROT(0) \end{pmatrix},$$

$$V_3 = \begin{pmatrix} ROT(0) & 0 & 0 \\ 0 & ROT(0) & 0 \\ 0 & 0 & ROT(\pi) \end{pmatrix}, V_4 = \begin{pmatrix} ROT(\frac{\pi}{2}) & 0 & 0 \\ 0 & ROT(\frac{\pi}{2}) & 0 \\ 0 & 0 & ROT(\pi) \end{pmatrix},$$

$$V_5 = \begin{pmatrix} ROT(\frac{\pi}{2}) & 0 & 0 \\ 0 & ROT(\frac{3\pi}{2}) & 0 \\ 0 & 0 & ROT(0) \end{pmatrix}, V_6 = \begin{pmatrix} ROT(0) & 0 & 0 \\ 0 & ROT(\pi) & 0 \\ 0 & 0 & ROT(0) \end{pmatrix},$$

$$V_7 = \begin{pmatrix} ROT(\frac{\pi}{2}) & 0 & 0 \\ 0 & ROT(\frac{3\pi}{2}) & 0 \\ 0 & 0 & ROT(\pi) \end{pmatrix}, V_8 = \begin{pmatrix} ROT(0) & 0 & 0 \\ 0 & ROT(\pi) & 0 \\ 0 & 0 & ROT(\pi) \end{pmatrix},$$

$$V_9 = \begin{pmatrix} ROT(\frac{3\pi}{2}) & 0 & 0 \\ 0 & ROT(\frac{3\pi}{2}) & 0 \\ 0 & 0 & ROT(0) \end{pmatrix}, V_{10} = \begin{pmatrix} ROT(\pi) & 0 & 0 \\ 0 & ROT(\pi) & 0 \\ 0 & 0 & ROT(0) \end{pmatrix},$$

$$V_{11} = \begin{pmatrix} ROT(\pi) & 0 & 0 \\ 0 & ROT(0) & 0 \\ 0 & 0 & ROT(\pi) \end{pmatrix}, V_{12} = \begin{pmatrix} ROT(\frac{3\pi}{2}) & 0 & 0 \\ 0 & ROT(\frac{3\pi}{2}) & 0 \\ 0 & 0 & ROT(\pi) \end{pmatrix},$$

$$V_{13} = \begin{pmatrix} ROT(\pi) & 0 & 0 \\ 0 & ROT(\pi) & 0 \\ 0 & 0 & ROT(\pi) \end{pmatrix}, V_{14} = \begin{pmatrix} ROT(\frac{3\pi}{2}) & 0 & 0 \\ 0 & ROT(\frac{\pi}{2}) & 0 \\ 0 & 0 & ROT(0) \end{pmatrix},$$

$V_{15} = \begin{pmatrix} ROT(\pi) & 0 & 0 \\ 0 & ROT(0) & 0 \\ 0 & 0 & ROT(0) \end{pmatrix}$ e $V_{16} = \begin{pmatrix} ROT(\frac{3\pi}{2}) & 0 & 0 \\ 0 & ROT(\frac{\pi}{2}) & 0 \\ 0 & 0 & ROT(\pi) \end{pmatrix}$. Para simplificar a notação de matrizes, iremos representar por $(a\ b\ c)$ a matriz dada por

$$\begin{pmatrix} ROT(\frac{2\pi a}{M}) & 0 & 0 \\ 0 & ROT(\frac{2\pi b}{M}) & 0 \\ 0 & 0 & ROT(\frac{2\pi c}{M}) \end{pmatrix},$$

onde M é o número de pontos do código. No caso acima, as matrizes V_3, V_4 e V_6 são as matrizes geradoras do grupo comutativo de matrizes e estas possuem ordem 2, 4 e 2. Portanto o grupo comutativo de matrizes associado é isomorfo a $\mathbb{Z}_2^2 \times \mathbb{Z}_4$. Este código esférico é o melhor código de grupo comutativo possível para esta decomposição.

Notemos que neste exemplo, multiplicamos o fator $k = 2$ para definir o sub reticulado de D_3, de forma que geramos um código com 16 pontos, mas se tivéssemos multiplicado por outro número par, iríamos obter outro código esférico e fazendo o mesmo processo de tornar a caixa do reticulado quadrada geraríamos outro com distância mínima boa, para um número maior de pontos.

Mais comentários serão feitos nas observações finais.

De Códigos de Grupo a Quociente de Reticulados

O melhor código de grupo comutativo para 16 pontos pode ser obtido pelo algoritmo desenvolvido em [15] com distância mínima $d = 1.2649$ e é associado ao grupo $\mathbb{Z}_4 \times \mathbb{Z}_4$.

No exemplo retratado anteriormente fazendo o processo inverso do que foi feito, chegaremos ao reticulado associado ao código esférico.

Este código de grupo comutativo ótimo em $\mathbb{R}^6$ com 16 pontos ocorre com um grupo de rotações isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_4$, tendo como geradores as matrizes de rotação $\{(4\ 8\ 0), (4\ 0\ 4)\}$, e $V = (\frac{2}{3}, 0, \frac{1}{3}, 0, \frac{2}{3}, 0)$ como vetor inicial. Isto é, o código esférico ótimo é obtido pelo produto do grupo gerado por $(4, 8, 0)$ e $(4, 0, 4)$.

$$A = [(4\ 8\ 0)] = \{(4\ 8\ 0), (8\ 0\ 0), (12\ 8\ 0), (0\ 0\ 0)\}$$

$$B = [(4\ 0\ 4)] = \{(4\ 0\ 4), (8\ 0\ 8), (12\ 0\ 12), (0\ 0\ 0)\}$$

$$A{\times}B = \left\{ \begin{array}{cccccccc} 8\ 0\ 0), & (0\ 0\ 8), & (4\ 0\ 12), & (12\ 8\ 8), & (0\ 8\ 12), & (4\ 8\ 0), & (8\ 0\ 4), & (4\ 8\ 8), \\ (8\ 8\ 12), & (12\ 8\ 0), & (0\ 8\ 4), & (12\ 0\ 4), & (8\ 0\ 8), & (12\ 0\ 12), & (4\ 0\ 4), & (0\ 0\ 0) \end{array} \right\}$$

Agora, basta multiplicar a matriz associada a cada elemento do conjunto acima pelo vetor inicial e teremos os pontos do código esférico associado. Por exemplo, a palavra do código esférico associada ao elemento (8 0 0) é dada por

$$\begin{pmatrix} ROT(2\pi 8/16) & 0 & 0 \\ 0 & ROT(2\pi 0/16) & 0 \\ 0 & 0 & ROT(2\pi 0/16) \end{pmatrix} \cdot \begin{pmatrix} \frac{2}{3} \\ 0 \\ \frac{1}{3} \\ 0 \\ \frac{2}{3} \\ 0 \end{pmatrix} = (-\tfrac{2}{3}, 0, \tfrac{1}{3}, 0, \tfrac{2}{3}, 0).$$ Para encontrarmos o reticulado associado a este código esférico, observemos que quando realizamos a imersão do reticulado na esfera, foi feita uma colagem de modo que o comprimento de cada aresta do politopo associado ao reticulado era o raio da esfera corespondente à aquela aresta dividido por 2π. Assim, para determinar a caixa(região fundamental) do sub-reticulado Λ' subdividivos o paralelepípedo gerado pela base $v_1 = 2\pi(\frac{2}{3}, 0, 0)$, $v_2 = 2\pi(0, \frac{1}{3}, 0)$ e $v_3 = (2\pi(0, 0, \frac{2}{3})$ na malha $16 \times 16 \times 16$ e selecionamos nesta malha os vértice do reticulado Λ associado as rotações de $A \times B$, por exemplo, a matriz (**8** 0 0) corresponde ao vértice $2\pi(\frac{2}{3}\frac{\mathbf{8}}{16}, 0, 0)$.

Portanto o reticulado associado ao código esférico de grupo comutativo ótimo tem como elementos dentro do paralelepípedo fundamental que define o toro planar de 16 pontos em $\mathbb{R}^6$ o seguinte conjunto:

$$\left\{ \begin{array}{cccc} (\frac{32\pi}{3}, 0, 0), & (0, 0, \frac{32\pi}{3}), & (\frac{16\pi}{3}, 0, 16\pi), & (16\pi, \frac{16\pi}{3}, \frac{32\pi}{3}), \\ (0, \frac{16\pi}{3}, 16\pi), & (\frac{16\pi}{3}, \frac{16\pi}{3}, 0), & (\frac{32\pi}{3}, 0, \frac{16\pi}{3}), & (\frac{16\pi}{3}, \frac{16\pi}{3}, \frac{32\pi}{3}), \\ (\frac{32\pi}{3}, \frac{16\pi}{3}, 16\pi), & (12, \frac{16\pi}{3}, 0), & (0, \frac{16\pi}{3}, \frac{16\pi}{3}), & (16\pi, 0, \frac{16\pi}{3}), \\ (\frac{32\pi}{3}, 0, \frac{32\pi}{3}), & (16\pi, 0, 16\pi), & (\frac{16\pi}{3}, 0, \frac{16\pi}{3}) & (0, 0, 0) \end{array} \right\}$$

Portanto, pelo exemplo acima, podemos generalizar de forma que dado um código esférico gerado por um grupo de matrizes ortogonais de rotação, sempre existe um reticulado associado a ele, onde o processo de se encontrar o reticulado é análogo ao que foi feito acima.

4.3 Observações Finais

Do desenvolvimento feito em [10] podemos enunciar o teorema 3.3.11 como limitação para a distância mínima.

Teorema 4.3.1. *Todo código de grupo comutativo dado pelo quociente de reticulados* $\frac{\Lambda'}{\Lambda}$ *em* $\mathbb{R}^{2n}$ *de ordem* M *com distância mínima* ρ *e vetor inicial* $u = (u_1, u_2, ..., u_{2n})$ *satisfaz*

$$\rho \leq 4\sin\Big(\pi\Big(\frac{\sqrt{\prod_{i=1}^{n}(u_{2i-1}^2 + u_{2i}^2)}\Lambda_n}{M}\Big)^{\frac{1}{n}}\Big) \leq 4\sin\Big(\pi\Big(\frac{n^{-\frac{1}{2}} \cdot \Lambda_n^{\frac{1}{n}}}{M^{\frac{1}{n}}}\Big)\Big),$$

onde Λ_n *é a densidade máxima de centro de um reticulado associado ao código.*

No teorema acima, a segunda desigualdade segue do fato $\prod_{i=1}^{n}\sqrt{u_{2i-1}^2 + u_{2i}^2} \leq \left(\frac{1}{\sqrt{n}}\right)^n$, pois $\sum_{i=1}^{n} u_i^2 = 1$.

No caso $n = 3$ e $M = 16$, obtemos do teorema que $d \leq 1,57232$ aproximadamente, e obtivemos respectivamente distâncias mínimas $d = 0.8944$ e $d = 1.1547$. Para o código de grupo ótimo, $d = 1.2649$.

Um fato que explica em parte esta diferença é que não é possível no $\mathbb{R}^3$ obtermos para o reticulado de maior densidade um sub reticulado cúbico. Se fosse este o caso atingiríamos o maior valor para Λ_m e para o produto $\prod_{i=1}^{n}\sqrt{u_{2i-1}^2 + u_{2i}^2}$ que é equivalente a

$$\Big(\frac{1}{2\pi}\Big) \cdot \text{volume da região fundamental do reticulado}$$

(caixa que define o toro).

Bibliografia

[1] HEFEZ, A. e VILLELA, M.L.T.; *Códigos Corretores de Erros*; IMPA, 2002.

[2] COSTA, S.I.R., MUNIZ, M., AGUSTINI, E. e PALAZZO, R.; Graphs, Tesselations and Perfect Codes on Flat Tori;*IEEE-Transactions on Informations Theory*; vol 50, pp 2363-2377, Oct 2004.

[3] COSTA, S.I.R., SIQUEIRA, R.M., LAVOR, C.C., ALVES, M.M.S, *Uma Introdução à Teoria de Códigos*, SBMAC-Notas em Matemática Aplicada,vol 21, 2006;

[4] MIRANDA, D.S., Códigos:*Uma Abordagem Geométrica*, Relatório de Iniciação Científica, CNPQ, 2006.

[5] CONWAY,J.H., SLOANE, N.J.A., Sphere, Packings, Lattices and Groups, *Grundlehren der mathematischen Wissenchaften, Springer*, 3rd edition, 1998.

[6] BEARDON,A.F., *The geometry of discrete groups*, Springer, 1995.

[7] MINAMI, L.T. *"Códigos sobre Grafos que são Quocientes de Reticulados*;Tese de mestrado, unicamp, 2004.

[8] MAUNDER,C.R.F;*Algebraic Topology*; Van nostrand Reinhold Company; London, 1970.

[9] COSTA.S.I.R., MUNIZ, M., AUGUSTINE, E.,and PALAZZO, R.Jr. The symmetry group of $\mathbb{Z}_q^n$ in the Lee space and the $\mathbb{Z}_q^n$-Linearity, *in Lecture Notes in Computer Science*. New York; Springer-Verlag,1997, vol.1255,pp.66-77.

[10] SIQUEIRA, R.M., *Códigos Esféricos com Simetrias Cíclicas*; tese de doutorado, Tese de doutorado-Imecc, Unicamp,2006.

[11] ERICSON, T., ZINOVIEV, V., *Codes on Euclidean Spheres*, Elsevier, North-Holland Mathematical library, vol63, 2001.

[12] EBELING,W., *Lattices and Codes*, 2nd edition, Advanced Lectures in Mathematics, Vieweg, 2002.

[13] COSTA, S.I.R., STRAPASSON, J.E., SIQUEIRA, R.M. and MUNIZ, M., Circulant Graphs, Lattices and Spherical Codes, a ser publicado *International Journal of Applied Mathematics*.

[14] SIQUEIRA, R.M., COSTA. S.I.R., Lattices and Bound for Commutative Group Codes, *Procedings of the WWC-2007, Workshop on Codings and Criptography*.

[15] SIQUEIRA, R.M., COSTA. S.I.R., TOREZZAN, C., *Searching for Optimal Commutative Group Codes*, Pre Print, 2007.

[16] PRETZEL, O., *Error-Correcting Codes and Finite Fields*, Clarendon Press-Oxford, Oxford Applied Mathematics and Computing Science Series, 1992.

[17] GARETH, A.J. and JONES, J.M., *Information and Coding Theory*, Springer-Verlag London Heidelberg.

[18] DIESTEL, R., *Graph Theory*, second edition, Springer, 2000.

[19] GANTMACHER, F.R., *The Theory of Matrices*, vol1, Chelsea, 1959.

[20] HEISE, w., On Codes Isomorphy, *Jornal of Geometry*,565,pp 63-69,1996.

[21] CARY, W.H. and PLESS, V., *Fundamentals of Error-Correction Codes*, Cambridge University Press, 2003.