Notas em Matemática Aplicada e-ISSN 2236-5915

Volume 21, 2012

Editado por

Eliana X.L. de Andrade
Universidade Estadual Paulista - UNESP
São José do Rio Preto, SP, Brasil

Rubens Sampaio
Pontifícia Universidade Católica do Rio de Janeiro -
Rio de Janeiro, RJ, Brasil

Geraldo N. Silva
Universidade Estadual Paulista - UNESP
São José do Rio Preto, SP, Brasil

Sociedade Brasileira de Matemática Aplicada e Computacional

2012

A Sociedade Brasileira de Matemática Aplicada e Computacional - SBMAC publica, desde as primeiras edições do evento, monografias dos cursos que são ministrados nos CNMAC.

Para a comemoração dos 25 anos da SBMAC, que ocorreu durante o XXVI CNMAC em 2003, foi criada a série **Notas em Matemática Aplicada** para publicar as monografias dos minicursos ministrados nos CNMAC, o que permaneceu até o XXXIII CNMAC em 2010.

A partir de 2011, a série passa a publicar, também, livros nas áreas de interesse da SBMAC. Os autores que submeterem textos à série Notas em Matemática Aplicada devem estar cientes de que poderão ser convidados a ministrarem minicursos nos eventos patrocinados pela SBMAC, em especial nos CNMAC, sobre assunto a que se refere o texto.

O livro deve ser preparado em **Latex (compatível com o Miktex versão 2.7), as figuras em eps** e deve ter entre **80 e 150 páginas**. O texto deve ser redigido de forma clara, acompanhado de uma excelente revisão bibliográfica e de **exercícios de verificação de aprendizagem** ao final de cada capítulo.

Veja todos os títulos publicados nesta série na página
http://www.sbmac.org.br/notas.php

SBMAC **Sociedade Brasileira de Matemática Aplicada e Computacional**

2012

UMA INTRODUÇÃO À TEORIA DE CÓDIGOS

Carlile Campos Lavor - UNICAMP
clavor@ime.unicamp.br

Marcelo Muniz Silva Alves - UFPR
marcelo@mat.ufpr.br

Rogério Monteiro de Siqueira - UNICAMP
rogerms@ime.unicamp.br

Sueli Irene Rodrigues Costa - UNICAMP
sueli@ime.unicamp.br

Sociedade Brasileira de Matemática Aplicada e Computacional

São Carlos - SP, Brasil
2012

Coordenação Editorial: Sandra Augusta Santos

Coordenação Editorial da Série: Eliana Xavier Linhares de Andrade

Editora: SBMAC

Capa: Matheus Botossi Trindade

Patrocínio: SBMAC

Catalogação elaborada pela Biblioteca do IBILCE/UNESP
Bibliotecária: Maria Luiza Fernandes Jardim Froner

Lavor, Carlile Campos.
Uma Introdução à Teoria de Códigos.
- São Carlos, SP: SBMAC, 2012, 90 p.,20.5 cm
- (Notas em Matemática Aplicada; v. 21)

e-ISBN 978-85-86883-86-6

1. Códigos Corretores de Erros 2. Reticulados.
3. Códigos Esféricos 4. Códigos Quânticos.
I. Lavor, Carlile Campos. II. Alves, Marcelo Muniz Silva.
III. Siqueira, Rogério Monteiro. IV. Costa, Sueli Irene Rodrigues.
V. Título. VI Série.

CDD - 51

Esta é uma republicação em formato de e-book do livro original do mesmo título publicado em 2006 nesta mesma série pela SBMAC.

Conteúdo

Prefácio

A onipresença do computador na nossa sociedade, com o uso de sistemas de comunicação digital nas mais diversas áreas, tem levado ao estudo e desenvolvimento de novas estruturas e métodos matemáticos que dêem suporte a essas novas tecnologias digitais. Estes vêem a integrar a teoria da informação, uma área de pesquisa e aplicações em pleno desenvolvimento, cujo marco inicial é o trabalho de C. E. Shannon, "A Mathematical Theory of Communication", publicado em 1948.

A teoria de códigos corretores de erro é uma subárea da teoria da informação que lida com o problema geral da transmissão de mensagens de forma confiável. Ela é utilizada de modo essencial nas comunicações via computador, rádio, televisão e satélites.

A proposta deste texto é a de ser uma introdução a esta teoria, enfatizando o instrumental matemático associado e explorando as propriedades das estruturas envolvidas numa abordagem, sempre que possível, geométrica. Procuramos manter os pré-requisitos a um mínimo: o conteúdo usual de um primeiro curso de álgebra linear e das disciplinas de cálculo da graduação.

O texto está organizado em quatro capítulos. No primeiro, cuja leitura deve anteceder a dos demais, é apresentada uma breve introdução à teoria de códigos. Os capítulos 2, 3 e 4 são razoavelmente independentes e introduzem o leitor a três subáreas da teoria de códigos: reticulados, códigos esféricos e códigos quânticos.

Este trabalho reflete, em parte, a experiência de pesquisa dos autores que integram o projeto temático interdisciplinar "Códigos Geometricamente Uniformes", que tem o suporte da FAPESP e conta com pesquisadores e alunos de pós-graduação de engenharia elétrica e de matemática.

Os autores agradecem o apoio de suas instituições de origem, da Sociedade Brasileira de Matemática Aplicada e Computacional (SBMAC) e dos órgãos de fomento à pesquisa: CNPq (processos 304573/2002-7 e 305282/2003-4) e FAPESP (processos 02/07473-7 e 02/14072-9).

Também agradecemos o suporte técnico de João Strapasson na elaboração da versão final deste trabalho.

Ressaltamos que o texto foi um trabalho de equipe de todos os autores, aqui listados em ordem alfabética.

Campinas, 27 de abril de 2006.

Os Autores

Capítulo 1

Códigos Corretores de Erros: Uma Breve Introdução

1.1 Introdução

Sistemas de comunicação são onipresentes em nossa sociedade hoje. Em particular, o advento dos computadores e seu uso nos mais diversos setores levaram à busca de bons sistemas onde a informação é transmitida e processada na forma digital. Por exemplo, fotos são transmitidas de um satélite através da decomposição do retângulo em $m \times n$ elementos de imagem e a cada um destes elementos é atribuído um número correspondente à cor. Assim, se o instrumento a bordo distingue 64 tons de cinza para uma foto em preto e branco, esta transmissão pode ser feita através de "mensagens binárias", isto é, seqüências de zeros e uns que representem o número da tonalidade. Por exemplo, a seqüência específica 101011 representará a tonalidade 43. É fácil deduzir alguns dos problemas que ocorrem em sistemas de comunicação digital. Erros podem ocorrer na codificação original, no canal de transmissão, onde surgem "ruídos" que distorcem os bits, e também na hora da leitura (decodificação) dos sinais enviados. Decorre daí a necessidade de se estudar códigos que sejam "bons corretores de erros" e que possibilitem, com a utilização de redundâncias, resgatar o sinal original, mesmo depois destas distorções. Tais códigos têm largo uso nas comunicações internas de um computador, no armazenamento de dados em meios magnéticos (HD, CD, etc), nas transmissões via satélite, etc.

A teoria dos códigos corretores de erros é parte integrante da área conhecida como teoria da informação, uma área de pesquisa que tem como marco inicial o trabalho "A Mathematical Theory of Communications" de Claude E. Shannon [30], do Laboratório Bell, E.U.A., em 1948. Desde então, diferentes subáreas da matemática têm sido utilizadas na resolução de problemas de informação. Importantes trabalhos em teoria de códigos que contemplam uma abordagem geométrica, que é o foco deste texto, são os de D. Slepian [35], na década de 60, e o de G. D. Forney [16], na

década de 90, que introduz o conceito de códigos geometricamente uniformes.

Exemplos muito conhecidos de códigos são os dígitos de controle. Por exemplo, o registro ISBN (International Standard Book Number) de um livro é uma seqüência de nove dígitos seguidos de um dígito de controle, $n_1n_2n_3...n_9 - n_{10}$, onde n_i é inteiro entre 0 e 9, para $i = 1, ..., 9$, e o dígito de controle n_{10} é assim obtido: $n_{10} = 11 - (\sum_{i=1}^{9}(11-i)n_i) \bmod 11$. Aqui, $r \bmod 11$ significa o resto da divisão de r por 11.

Assim, o controle n_{10} poderá ser $0, 1, 2, ..., 9$ ou 10, sendo que neste último caso representa-se por X. Exemplo: o livro [18], que é uma referência sugerida para leitura, tem ISBN 85 -244-0169. Seu dígito de controle é $11 - 233 \bmod 11 = 11 - 2 = 9$. Verifique este cálculo em outros livros. A pergunta natural é: por que definir uma expressão como esta para o controle? Note, por exemplo, que se definíssemos o dígito de controle para o registro de livros por uma expressão mais simples, como fazer a soma dos dígitos módulo 10, o controle não detectaria a troca de ordem na digitação, que é um erro muito comum. O código ISBN é um exemplo de código que detecta (embora não corrija) um erro (veja o Exemplo 1.1). Um outro exemplo de código detector de erro pode ser encontrado nos dígitos do seu CPF (veja o Exercício 1.15.2).

Um esquema simplificado para representar a transmissão de sinais é descrito na figura 1.1.

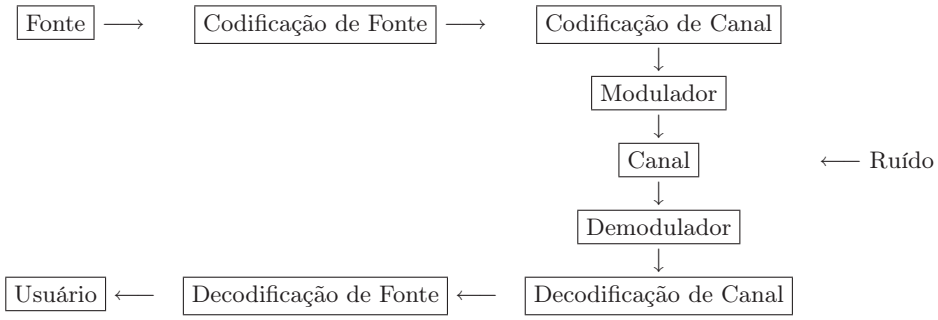


Figura 1.1: Um esquema para a transmissão de sinais.

Neste texto, estaremos abordando apenas *sistemas de transmissão simétricos,* onde todos os símbolos têm a mesma probabilidade de serem recebidos errados e a probabilidade de que um símbolo recebido errado seja qualquer um dos outros é a mesma.

A ênfase será nos chamados *códigos geometricamente uniformes.* Tais códigos são caracterizados pela existência de isometrias (simetrias) internas. Estas simetrias dão instrumentos para uma análise muito mais aprofundada da performance de um código.

Neste capítulo, os "geometricamente uniformes" serão representados pelos códigos lineares, no Capítulo 2, por reticulados no espaço euclidiano n-dimensional e, no Capítulo 3, por códigos esféricos. No Capítulo 4, serão introduzidos os códigos quânticos, que são códigos em espaços vetoriais complexos.

1.1.1 Exemplos de codigos binários

Vamos exemplificar formas do processo de codificação com três códigos bínários.

Exemplo 1.1. O código de tripla repetição. *Como proposto em [18], consideramos um robô que pode se mover em quatro direções: leste (L), norte (N), oeste (O) e sul (S). Um código-fonte pode ser estabelecido associando a L, N, O e S respectivamente as sequências 00, 01, 10 e 11. Para o código-canal vamos escolher o código de tripla repetição. Teremos então as associações*

$$\begin{array}{ccccc} L & \rightarrow & 00 & \rightarrow & 000000 \\ N & \rightarrow & 01 & \rightarrow & 010101 \\ O & \rightarrow & 10 & \rightarrow & 101010 \\ S & \rightarrow & 11 & \rightarrow & 111111 \end{array}$$

Verifique experimentalmente que este código corrige um erro e pode detectar até dois - a detecção de erros é útil quando temos a possibilidade de retransmissão.

Note que esta não é uma forma econômica de codificar (triplicamos o número de dígitos). Será que com menor redundância conseguimos um código-canal que também permita corrigir um erro? (Veja exercício 1.1)

Exemplo 1.2. O código de verificação de paridade $(8, 7)$. *Muitos computadores usam a seqüência de 8 bits (um byte) como unidade de informação. O código ASCII, que é praticamente de uso geral em microcomputadores representa letras do alfabeto maiúscula e minúsculas, dígitos de 0 a 9, etc, por uma destas seqüências. Para escrever em português ou ingles não precisamos mais que 80 símbolos, o que é um número bem menor que o número de bytes, 256, e assim podemos utilizar apenas sete dos bits para os símbolos (código- fonte) e oitavo bit para controle. Este será colocado como* 0 *se o número de* "1*s*" *for par e* 1 *no caso contrário. Por exemplo, a letra A e o número* 1 *são codificados em ASCII por* 1000001 *e* 1000110 *respectivamente e com o último digito ficam* 10000010 *e* 10001101.

Este é um código muito econômico que detecta mas não corrige um erro.

Exemplo 1.3. Código de tripla verificação de paridade. *Suponhamos agora que o nosso robô do exemplo 1.1) possa se mover num tabuleiro também para as posições diagonais, NL,NO,SO e SL. Nosso código- fonte será feito então com 3 dígitos abc onde cada letra é* 0 *ou* 1. *Para o código-canal acrescentaremos outros 3 digamos xyz, com checagem de paridade da seguinte forma : i) O número de* "1*s*" *em abx é par ii) O número de* "1*s*" *em acy é par e iii) O número de* "1*s*" *em bcz é par.*

Exercício 1.1. *Monte uma tabela com os códigos fonte e canal para a movimentação do robô no exemplo 1.3 e discuta cuidadosamente porque este código não só detecta mas também é capaz de corrigir um erro e pode também detectar até 2 erros. Note que este é um código bem mais econômico que o proposto no exemplo 1.1.*

1.2 Códigos de Bloco, Distâncias e Equivalência de Códigos

Seja A um conjunto finito com q elementos ($|A| = q$), um *código corretor de erros*, $\mathcal{C}$, de comprimento n é um subconjunto de A^n. Cada elemento de $\mathcal{C}$ é chamado palavra-código (no alfabeto A).

Seja $m = |\mathcal{C}|$, o número de palavras do código. A taxa de informação de $\mathcal{C}$ é definida como:

$$R(\mathcal{C}) = \frac{\log_q m}{n}$$

Se o conjunto A for um corpo finito e $\mathcal{C}$ for um subespaço vetorial de dimensão k de A^n, teremos que $|\mathcal{C}| = q^k$ e portanto $R(\mathcal{C}) = \frac{k}{n}$.

A taxa de informação permite, de certa forma, comparar a eficiência de códigos de diferentes tamanhos.

Nos exemplos 1.1, 1.2 e 1.3 da primeira seção os códigos são binários: o alfabeto pode ser considerado como $A = \mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, corpo dos inteiros módulo 2, com a operações soma e multiplicação dadas pelas tabelas.

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

(identificamos $\overline{0}$ com 0 e $\overline{1}$ com 1).

O código (de canal) no exemplo 1.1 é

$$\mathcal{C} = \{(0,0,0,0,0,0), (0,0,0,1,1,1), (1,1,1,0,0,0), (1,1,1,1,1,1)\},$$

que é um subespaço de dimensão dois em $\mathbb{Z}_2^6$. A taxa deste código é $\frac{\log_2 4}{6} = \frac{1}{3}$. Nos exemplos 1.2 e 1.3 as taxas dos códigos são respectivamente $\frac{\log_2 2^7}{8} = 0,875$ e $\frac{\log_2 8}{6} = \frac{1}{2}$. Como era de se esperar o código 3) tem melhor taxa que o 1) refletindo o fato de que embora os códigos 1.1 e 1.3 permitam ambos corrigir um erro e detectar 2, no código 3 a redundância é menor, pois o número de palavras é maior para o mesmo comprimento.

Qual a taxa de informação do código do CPF (exercício 1.15.2)?

Assumindo que todas as palavras do código são equiprováveis, escolhemos para decodificar o princípio da máxima *verossimilhança*. Isto é, se no receptor chega uma

palavra com distorção, vamos interpretá-la como a palavra do código que está mais "próxima" desta. A noção de proximidade é geralmente expressa por uma função distância definida no conjunto A^n.

Uma função $d : A^n \times A^n$ é chamada *função distância* se, e somente se, satisfaz as três seguintes propriedades:
i) $d(\mathbf{x}, \mathbf{y}) \geq 0$ e $d(\mathbf{x}, \mathbf{y}) = 0 \Leftrightarrow \mathbf{x} = \mathbf{y}$
ii) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$
iii) $d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \geq d(\mathbf{x}, \mathbf{z})$ (desigualdade triangular).

Uma função distância muito utilizada é a *distância de Hamming*, que conta o número de símbolos diferentes entre duas palavras-código: dados dois pontos $\mathbf{x} = (x_1, x_2, ..., x_n)$ e $\mathbf{y} = (y_1, y_2, ..., y_n)$ de A^n definimos a distância de Hamming entre $\mathbf{x}$ e $\mathbf{y}$ como

$$d_h(\mathbf{x}, \mathbf{y}) = |\{i; x_i \neq y_i\}|$$

Por exemplo em $\mathbb{Z}_2^5$, $d_h((1,0,1,1,1),(0,1,0,1,0)) = 4$ e em $\mathbb{Z}_{10}^3$, $d_h((2,3,4),(1,7,4)) = 2$.

Neste capítulo, salvo menção em contrário, estaremos denotando por $d = d_h$ a distância de Hamming.

Geometricamente, para $A = \mathbb{Z}_2$, temos que $\mathbb{Z}_2^n$ são os vértices de um hipercubo em $\mathbb{R}^n$ e códigos binários são subconjuntos destes conjuntos de vértices. A distância de Hamming em $\mathbb{Z}_2^n$ entre dois deste vertices é dada pelo caminho com menor número de arestas conectado estes vertices. A figura 1.2 representa $\mathbb{Z}_2^3$ e $\mathbb{Z}_2^4$. Observe geometricamente no cubo e no hipercubo quais são os vértices que estão a distância um, dois, três e quatro de um vértice fixado.

Exercício 1.2. *Considere os códigos*

$$C_1 = \{(1,1,1),(0,0,0)\} \subset \mathbb{Z}_2^3 \ \ e$$

$$C_2 = \{(1,1,1,0),(0,0,0,0),(1,0,0,1),(1,1,1,1)\} \subset \mathbb{Z}_2^4.$$

Localize-os na figura 1.2. Quais as distâncias mínima e máxima entre as palavras destes códigos ?

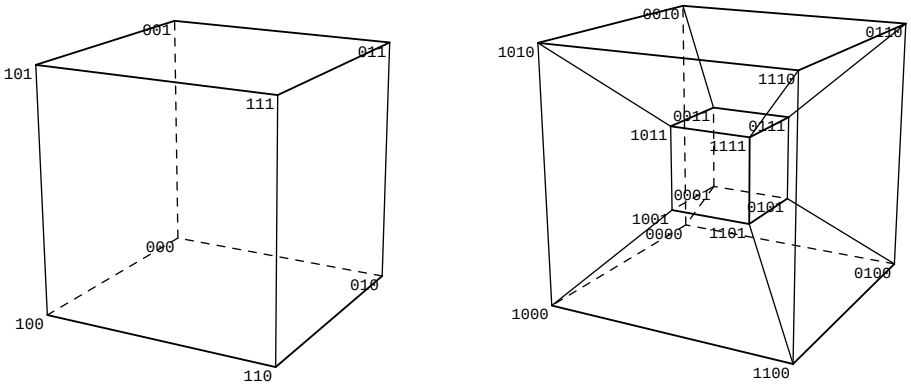


Figura 1.2:

Exercício 1.3. *Quantos pontos existem em $\mathbb{Z}_2^5$ que distam exatamente dois de um determinado elemento?*

Exercício 1.4. *Verifique que a distância de Hamming satisfaz as três propriedades que caracterizam uma função distância.*

Definimos a esfera, $S(\mathbf{a}, r)$, e a bola, $B(\mathbf{a}, \mathbf{r})$, de centro em $\mathbf{a}$ e raio r em A^n da forma usual :

$$S(\mathbf{a}, r) = \{\mathbf{x} \in A^n; d_h(\mathbf{x}, \mathbf{a}) = r\} \text{ e } B(\mathbf{a}, r) = \{\mathbf{x} \in A^n; d_h(\mathbf{x}, \mathbf{a}) \leq r\}$$

Exercício 1.5. *Quantos elementos tem a esfera em $\mathbb{Z}_2^5$ de centro em $(0,0,0,0,0)$ e raio 4 ? E a bola em $\mathbb{Z}_{10}^3$ de centro em $(1,2,3)$ e raio 2? Explore outros exemplos e veja o exercício 1.14*

Para um código $\mathcal{C} \subset A^n$, definimos a *distância mínima* de $\mathcal{C}$ como sendo

$$d(\mathcal{C}) = \min\{d_h(\mathbf{x}, \mathbf{y}); \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\}$$

Verifique que a distância mínima dos códigos dos exemplos 1.1 e 1.3 da seção anterior é 3. Qual é a distância mínima do código do exemplo 1.2? E dos códigos do exercício 1.3?

Veremos depois que para códigos especiais, como os códigos lineares, não precisamos verificar a distância de todos os pares de palavras do código para determinar a distância mínima.

A distância mínima é que determina a capacidade de correção de um código, como veremos na proposição a seguir. As bolas centradas em palavras do código com raio menor que a metade desta distância conterão apenas uma palavra do código dentro delas(o centro da bola). Esta é a idéia utilizada na proposição a seguir onde a notação $\lfloor t \rfloor$ designa o maior inteiro que é menor ou igual a t. Por exemplo, $\lfloor 12,3 \rfloor = 12, \lfloor \pi \rfloor = 3$.

Proposição 1.1. *Um código pode corrigir até* $\left\lfloor \frac{d-1}{2} \right\rfloor$ *erros e detectar até* $(d-1)$ *erros se e somente se sua distância de Hamming mínima for* d.

Demonstração: ($\Leftarrow$) Se a distância mínima for d temos que, como

$$d \geq 2\left\lfloor \frac{d-1}{2} \right\rfloor + 1 \text{ (a igualdade só vale se } d \text{ for ímpar)},$$

as bolas de centro em uma palavra do código e raio $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, não conterão nenhuma outra palavra do código. Ou seja, se o sinal recebido é $\mathbf{r}$, e menos de t símbolos estão errados, existe uma única palavra $\mathbf{a}$ do código que dista de r menos que t (corrigir o erro por verossimilhança será tomar esta palavra). De fato, para qualquer outra palavra do código $\mathbf{b}$ a distância seria estritamente maior que t,pois, da desigualdade triangular

$$d(\mathbf{a},\mathbf{r}) + d(\mathbf{r},\mathbf{b}) \geq d(\mathbf{a},\mathbf{b}) \Longrightarrow d(\mathbf{r},\mathbf{b}) \geq d(\mathbf{a},\mathbf{b}) - d(\mathbf{a},\mathbf{r}) \geq 2t+1-t = t+1 > t$$

Também pode-se detectar $(d-1)$ erros se a distância mínima for d. De fato: se o sinal recebido $\mathbf{r}$ difere no mínimo em uma e máximo em $(d-1)$ posições de alguma palavra $\mathbf{a}$ do código (de um até $(d-1)$ erros) então ele não terá distância nula de nenhuma palavra do código e saberemos que houve erro na transmissão:

$$d(\mathbf{b},\mathbf{r}) \geq d(\mathbf{a},\mathbf{b}) - d(\mathbf{a},\mathbf{r}) \geq 2t+1-2t = 1$$

($\Longrightarrow$) Deixamos como exercício a demonstração da recíproca. ■

Dado um conjunto A e uma função distância $d : A^n \times A^n \to \mathbb{R}$, uma *isometria* $\varphi : A^n \to A^n$, segundo d, é uma aplicação que satisfaz:

$$d(\varphi(\mathbf{a}),\varphi(\mathbf{b})) = d(\mathbf{a},\mathbf{b}) \text{ para todo } \mathbf{a},\mathbf{b} \text{ em } A^n$$

Isometrias são necessariamente bijeções (Verifique!).

Pode-se mostrar ([18]) que isometrias, segundo a distância de Hamming d, são sempre obtidas compondo-se bijeções de A para cada coordenada com uma permutação de coordenadas.

Dois *códigos* $\mathcal{C}$ e $\mathcal{C}'$ em A^n são ditos *Hamming-equivalentes* se existir uma isometria segundo a distância de Hamming $\alpha : A^n \to A^n$, tal que $\mathcal{C}' = \alpha(\mathcal{C})$. Do que comentamos acima, dois códigos Hamming-equivalentes são essencialmente permutações um do outro.

Alguns códigos possuem propriedades especiais em relação a uma função distância. Um código $\mathcal{C} \subset A^n$ com distância mínima d é dito *t-perfeito,* $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, se, e somente se a reunião das bolas disjuntas centradas em palavras do código com raio t cobre todo A^n.

$$\bigcup_{\mathbf{a}\in\mathcal{C}} B(\mathbf{a},t) = A^n$$

Um código é t-perfeito se, e somente se, para cada elemento w de A^n (recebido) existe uma única palavra a do código que dista deste elemento no máximo t. Desta maneira, w será decodificado como a por verossimilhança e até t erros serão corrigidos.

Exercício 1.6. *1. Verifique que o código C_1 do exercício 1.2 é 1-perfeito. existem outros códigos perfeitos em $\mathbb{Z}_2^3$?*

2. Procure identificar códigos perfeitos em $\mathbb{Z}_2^4$ usando a figura 1.2 como apoio.

Como sempre acontece, perfeição é em geral coisa rara e isto vale também em códigos.

Um código $\mathcal{C} \subset A^n$ é chamado *geometricamente uniforme* se, e somente se, dadas duas palavras quaisquer $\mathbf{x}$ e $\mathbf{y}$ do código existe uma isometria $\varphi : A^n \to A^n$ tal que:
(i) $\varphi(\mathcal{C}) = \mathcal{C}$ (a isometria leva o código no código)
(ii) $\varphi(\mathbf{x}) = \mathbf{y}$.

A próxima seção introduz os códigos lineares, que são geometricamente uniformes e, dentre eles, os códigos de Hamming, que são perfeitos.

1.3 Códigos Lineares e Códigos de Hamming

Se o alfabeto A for um corpo finito com q elementos e se $\mathcal{C}$ for um subespaço vetorial de dimensão k de A^n, diremos que o código q-ário $\mathcal{C}$ é linear (ou de grupo) e teremos que $|\mathcal{C}| = q^k$ (veja o apêndice).

Uma definição equivalente é: *Códigos lineares* são os obtidos como imagem de uma transformação linear injetiva:

$$\Phi : A^k \to A^n,$$
$$(a_1, a_2, ..., a_k) \mapsto G_{n\times k} \cdot (a_1, a_2, ..., a_k)^T$$

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

A matriz G é denominada *matriz geradora* do código e $\mathcal{C}$ será dito um (n, k)-*código de bloco linear* .

Observação: Nos textos sobre códigos, muitas vezes o que é chamado de matriz geradora é a transposta desta. Neste caso a transformação linear será dada por $\mathbf{a} \mapsto \mathbf{a} \cdot G_{n\times k}^T$.

Estas definições são de fato equivalentes: Se Φ é injetiva as colunas de G, que são imagem da base canônica de A^k, são linearmente independentes e portanto geram um subespaço $\mathcal{C}$, de dimensão k em A^n. Reciprocamente dado um subespaço $\mathcal{C}$ de dimensão k em A^n, se tomarmos por vetores coluna de uma matriz uma base de $\mathcal{C}$, a transformação definida por esta matriz (em relação às bases canônicas de A^k e A^n) terá por imagem o subespaço $\mathcal{C}$.

A matriz geradora de um código linear $\mathcal{C}$ não é portanto única (pois é uma escolha de uma base de $\mathcal{C}$), mas sempre existe uma matriz geradora na forma padrão ou sistemática, isto é, de modo que as primeiras k linhas de G formem uma matriz identidade de ordem k,

$$G = \begin{bmatrix} I_{k\times k} \\ B_{(n-k)\times k} \end{bmatrix}.$$

Se tivermos um código definido por uma matriz geradora na forma não padrão, podemos efetuar operações elementares por colunas nestas até obter uma matriz na forma padrão (veja apêndice). (Por quê ? Observe que toda matriz geradora tem posto k). O subespaço gerado pelas colunas da matriz padrão obtida é o mesmo e, portanto, temos o mesmo código (Justifique!).

Note que, se a matriz geradora está na forma padrão, a codificação é dada na forma

$$\Phi(a_1, a_2, ..., a_k) = (a_1, a_2, ..., a_k, h_1, h_2, ..., h_{n-k}),$$

onde os $h_i s$ são combinações lineares das primeiras coordenadas.

Note ainda que a codificação da palavra $e_j = (0, 0, ..., 1, 0, ...0)$ (1 na j-ésima posição) é a j-ésima coluna de G.

Nos exemplos 1.1 e 1.3 da primeira seção as matrizes geradoras são:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ e } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Exercício 1.7. *Qual a matriz geradora do exemplo 1.2?*

Exercício 1.8. *Escolha matrizes geradoras na forma padrão e construa outros códigos binários lineares com estas matrizes geradoras. Pesquise a distância mínima de seus códigos.*

Uma *matriz de verificação ou matriz de paridade* $H_{(n-k)\times n}$ de um código linear $\mathcal{C}$ com matriz geradora G, é uma matriz com a propriedade de detectar se um vetor $\mathbf{w}$ de A^n é uma palavra do código:

$$H\mathbf{w}^T = \mathbf{0} \in A^{n-k} \Leftrightarrow \mathbf{w} \in \mathcal{C} \subset A^n$$

Exercício 1.9. *Mostre que as linhas de H são vetores do subespaço $\mathcal{C}^\perp$, ortogonal ao código, e que o posto de H é $n-k$ (use o teorema do núcleo e da imagem). Conclua que as linhas de H geram $\mathcal{C}^\perp$.*

Verifique que, se G é uma matriz geradora na forma padrão para $\mathcal{C}$, $G = \begin{bmatrix} I_{k\times k} \\ B_{(n-k)\times k} \end{bmatrix}$, então uma matriz de paridade para $\mathcal{C}$ é

$$H_{(n-k)\times n} = \begin{bmatrix} -B & I_{(n-k)\times(n-k)} \end{bmatrix}.$$

Note que se o código for binário, $A = \mathbb{Z}_2$ e teremos $B = -B$ que podemos substituir na expressão acima. Quais as matrizes de paridade para os códigos de

tripla repetição e de verificação de paridade dos exemplos 1.1 e 1.3 da seção 1? E do exemplo 1.2? E dos códigos que construiu?

Dado $\mathbf{w} \in A^n$, a imagem deste elemento pela matriz de paridade, $H\,\mathbf{w}^T \in A^{n-k}$, é chamada *síndrome* de $\mathbf{w}$. Os elementos do código linear $\mathcal{C}$ são então os que tem por síndrome o vetor nulo.

Um fato importante sobre os códigos lineares é que existem formas não diretas de se calcular a distância mínima para estes códigos. Estas decorrem do fato de que códigos lineares são geometricamente uniformes.

Se um código C contido em A^n, com $|A| = q$, é geometricamente uniforme, para encontrarmos a distância mínima, não precisamos calcular todas as $\binom{q^n}{2} = \frac{q^n(q^n-1)}{2}$ distâncias entre dois pontos. Podemos fixar uma palavra qualquer e calcular as $q^n - 1$ distâncias entre esta palavra e uma outra:

Lema 1.1. *Seja C um código geometricamente uniforme contido em A^n. Escolhida uma palavra $\mathbf{a}$ do código, a distância mínima d de C é dada por*

$$d = \min_{\mathbf{v} \neq \mathbf{a}} d(\mathbf{a}, \mathbf{v})$$

Demonstração: Como C tem um número finito de pontos, sua distância mínima ocorre para um par de palavras $\mathbf{x}$ e $\mathbf{y}$, isto é,

$$d = d(\mathbf{x}, \mathbf{y}).$$

Seja $\mathbf{a}$ o ponto escolhido. Como C é geometricamente uniforme, existe uma isometria φ em A^n que preserva C e leva $\mathbf{x}$ em $\mathbf{a}$. Logo,

$$d = d(\mathbf{x}, \mathbf{y}) = d(\varphi\mathbf{x}, \varphi\mathbf{y}) = d(\mathbf{a}, \varphi\mathbf{y}).$$

Para códigos lineares o ponto escolhido costuma ser o $\mathbf{0}$ de A^n e definimos a distância de Hamming de uma palavra $\mathbf{x}$ do código a $\mathbf{0}$ como o *peso* de $\mathbf{x}$:

$$w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0}).$$

Temos então:

Proposição 1.2. *A distância (de Hamming) mínima de um código linear binário C é o menor peso de um elemento não nulo deste código.*

Demonstração: Códigos lineares são geometricamente uniformes. De fato: as translações em A^n, $\varphi(\mathbf{x}) = \mathbf{x} + \mathbf{b}$ são isometrias para a distância de Hamming, isto é,

$$d(\mathbf{u}, \mathbf{v}) = d(\mathbf{u} + \mathbf{b}, \mathbf{v} + \mathbf{b}) \text{ para quaisquer } \mathbf{u} \text{ e } \mathbf{v} \text{ em } A^n,$$

pois o número de coordenadas distintas é preservado pela soma. Além disso, para $\mathbf{b} \in C$, φ preserva C e dadas duas palavras x e y no código, tomando $\mathbf{b} = \mathbf{y} - \mathbf{x}$, a

translação leva $\mathbf{x}$ em $\mathbf{y}$. Portanto, pelo Lema anterior, escolhendo o ponto $\mathbf{u} = \mathbf{0}$, concluímos que a distância mínima é sempre igual ao menor peso para uma palavra-código. ■

Um (n, k) código linear com distância de Hamming mínima d é dito ter *parâmetros* (n, k, d).

Proposição 1.3. *Um código linear $\mathcal{C}$ tem distância de Hamming mínima d se e somente se o número mínimo de vetores-coluna da matriz de paridade linearmente dependentes é d.*

Demonstração: Seja H matriz de paridade para $\mathcal{C}$. Então, para $\mathbf{w} = (w_1, w_2, ..., w_n)$, $\mathbf{w} \in \mathcal{C} \iff H\,\mathbf{w}^T = \mathbf{0}$ mas isto significa que se $\mathbf{w} \neq \mathbf{0}$, as coordenadas de $\mathbf{w}$ compõem uma combinação linear nula de vetores coluna de H: $\sum_{i=1}^{m} w_i H^i = 0$. Reciprocamente, a toda combinação linear não nula das colunas da matriz de paridade corresponde uma palavra do código cujo peso é o numero de elementos não nulos desta combinação linear. Portanto, o peso mínimo de uma palavra do código é exatamente o número mínimo de vetores que podem ser combinados para dar o vetor nulo. Usando a proposição anterior, concluímos a demonstração. ■

Exercício 1.10. *Considere o código linear binário dado pela matriz geradora abaixo:*

$$G = \begin{bmatrix} I_{8\times 8} \\ B_{4\times 8} \end{bmatrix}; \text{onde } B_{4\times 8} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Verifique que este código tem 256 palavras e distância mínima 3.

Observe que, como a matriz de paridade tem posto $n - k$, o menor número de vetores-coluna linearmente dependentes é pelo menos $n - k + 1$ e portanto temos uma limitação para a distância mínima, dada pela última proposição:

Corolário 1.1. *Cota de Singleton Seja $\mathcal{C}$ um (n, k)-código de bloco linear binário com distância de Hamming mínima d. Então temos a limitação:*

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

Códigos lineares satisfazendo a igualdade são chamados de separação máxima, MDS (Maximum distance separable).

Outra consequência da última proposicão para códigos binários é:

Corolário 1.2. *Códigos binários corrigem pelo menos um erro se, e só se, todos os vetores da matriz de paridade são distintos. (Verifique!)*

1.3.1 Códigos de Hamming

Os códigos de Hamming tem a propriedade requerida no último corolário além de outras. Tais códigos foram introduzidos em 1950 por R.W. Hamming ([17]) e tem sido muito utilizados desde então.

Um *código de Hamming* $\mathcal{H}_m \subset \mathbb{Z}_2^{2^m-1}$ é um $(2^m-1, 2^m-m-1)$-código linear binário que tem matriz de paridade H_m, cujas colunas são todos os elementos não nulos de $\mathbb{Z}_2^m$.

Por exemplo, uma matriz de paridade na forma sistemática para um $\mathcal{H}_3$ é

$$H_3 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Sua matriz geradora correspondente será então:

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

Portanto a codificação de uma sequência *abcd* por este código fica sendo

$$abcdxyz$$

onde, utilizando as operações de $\mathbb{Z}_2$,

$$x = b + c + d; y = a + c + d \text{ e } z = a + b + d.$$

Exercício 1.11. *Se você escolher uma outra matriz de paridade para gerar um $\mathcal{H}_3$ este código será equivalente ao dado aqui?*

Exercício 1.12. *Encontre uma matriz de paridade e matriz geradora correpondente para o $(15, 11)$-código de Hamming $\mathcal{H}_4$.*

Utilizando os resultados anteriores você poderá deduzir que:

i) A distância de Hamming mínima de um código $\mathcal{H}_m$ é 3 e portanto ele detecta até dois erros e corrige até um.

ii)Este é um código perfeito, isto é, todo elemento de $\mathbb{Z}_2^{2^m-1}$ está a uma distância de no máximo um de uma palavra do código:

$$\bigcup_{a \in \mathcal{H}_{\mathbb{t}}} B(\mathbf{a}, 1) = \mathbb{Z}_2^{2^m-1}.$$

Note que a condição dada em ii) retrata uma distribuição muito uniforme do código no espaço de dimensão maior. No exemplo do $\mathcal{H}_3$ teremos as $2^4 = 16$ palavras do código muito bem distribuidas nos $2^7 = 128$ elementos de $\mathbb{Z}_2^7$ de forma que nenhum destes dista mais que um de alguma destas palavras.

1.3.2 Decodificação de um código de Hamming

Exercício 1.13. *A) Discuta e justifique cuidadosamente o seguinte algoritmo para decodificar um elemento do código de Hamming $\mathcal{H}_3$ dado acima pelo critério da verossimilhança (supondo que a palavra correta do código que corresponde a sequência recebida é a mais próxima a este):*

- Tome a sequência recebida na forma de um $\mathbf{r}$ *vetor- coluna* 7×1

- Encontre o vetor-coluna $H_3\mathbf{r}$*. (Note que* $H_3\mathbf{r}$ *será o vetor nulo ou uma coluna de* H_3*. Por quê?)*

- Se a síndrome $H_3\mathbf{r}$ *for o vetor nulo de ordem* 3×1*, então* $\mathbf{r} \in \mathcal{H}_3$*; caso contrário tome* $\mathbf{w}$ *como a palavra código que troca o* j*-ésimo bit de* $\mathbf{r}$*, se* $H_3\mathbf{r}$ *for a* j*-ésima coluna de* H_3*.*

- Finalmente dada a palavra $\mathbf{r}$ *ou a palavra* $\mathbf{w}$*, conforme* $H_3\mathbf{r} = 0$ *ou não, considere apenas os quatro primeiros dígitos.*

B) Ilustre este procedimento escolhendo 3 seqüências de 7 bits para decodificar.

C) O procedimento acima é válido para códigos de Hamming de qualquer ordem?

D) Ao tentar adaptar este procedimento para códigos que corrijam um erro mas não sejam perfeitos, pode ser que na terceira etapa $H_3\mathbf{r}$ *não seja nem o vetor nulo nem um vetor-coluna de* H_3*. O que estará ocorrendo então?*

Há muitos outros códigos lineares conhecidos e de grande utilização, como os códigos de Golay, Reed-Solomon e de Reed- Muller. (Consulte por exemplo [18]).

O código de Golay G_{24} pode ser construído a partir de "combinações "de códigos de Hamming ([28]). Este código e seu associado o G_{23} tem excelentes propriedades ([24] e [36]) e são essencialmente os únicos que tem os parâmetros $(n, k, d) = (24, 12, 8)$ e $(n, k, d) = (23, 12, 7)$ respectivamente. Uma matriz geradora para o código G_{24} é:

$$G = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1
\end{bmatrix}$$

Todas as palavras do código G_{24} têm peso par (Por quê?), o que significa que G_{24}, que é um subespaço de dimensão 12 em $\mathbb{Z}_2^{24}$, na verdade está contido num subespaço de dimensão 23 e podemos eliminar um bit gerando o G_{23}. O Golay G_{24} tem distância mínima 8. Como você verificaria isto usando o computador? O G_{23} tem distância mínima 7 e é um código perfeito que corrige 3 erros.

1.4 Códigos q-ários: A Distância de Lee

Chamamos códigos q-arios os que têm por alfabeto o anel $\mathbb{Z}_q$ dos inteiros módulo q. Como comentamos, em função da tecnologia computacional disponível atualmente os códigos em uso são essencialmente os binários. Mas outros códigos são também usados em etapas intermediárias e posteriormente convertidos em binários. Este é o caso dos códigos de bloco q-ários que introduzimos a seguir com alguns exemplos e a noção de distância de Lee, adaptada a estes códigos.

O anel $\mathbb{Z}_q = \{\overline{0}, \overline{1}, \ldots, \overline{q-1}\}$, onde a classe $\overline{a}$ é formada pelos inteiros cuja divisão por q tem resto a. Uma boa referência para o estudo deste conceito e suas propriedades é [18].

As operações de soma e mutiplicação nestas classes são as induzidas das operações nos inteiros, sempre ficando com o "resto "da divisão por q: $\overline{a} + \overline{b} =$

$\overline{(a+b)\ mod\ q}$ e $\overline{a}.\overline{b} = \overline{(a.b)\ mod\ q}$ (ver apêndice).

Já vimos as operações para $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$; qúando trabalhamos com os códigos binários. Para $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}, Z_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ e $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, as tabelas de adição e multiplicação são colocadas a seguir:

$$\left[\begin{array}{c|ccc} + & \overline{0} & \overline{1} & \overline{2} \\ \hline \overline{0} & \overline{0} & \overline{1} & \overline{2} \\ \overline{1} & \overline{1} & \overline{2} & \overline{0} \\ \overline{2} & \overline{2} & \overline{0} & \overline{1} \end{array}\right] \left[\begin{array}{c|ccc} \cdot & \overline{0} & \overline{1} & \overline{2} \\ \hline \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} & \overline{2} \\ \overline{2} & \overline{0} & \overline{2} & \overline{1} \end{array}\right]$$

$$\left[\begin{array}{c|cccc} + & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \hline \overline{0} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{0} \\ \overline{2} & \overline{2} & \overline{3} & \overline{0} & \overline{1} \\ \overline{3} & \overline{3} & \overline{0} & \overline{1} & \overline{2} \end{array}\right] \left[\begin{array}{c|cccc} \cdot & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \hline \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{2} & \overline{0} & \overline{2} & \overline{1} & \overline{0} \\ \overline{3} & \overline{0} & \overline{3} & \overline{2} & \overline{1} \end{array}\right]$$

$$\left[\begin{array}{c|ccccc} + & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \hline \overline{0} & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{0} \\ \overline{2} & \overline{2} & \overline{3} & \overline{4} & \overline{0} & \overline{1} \\ \overline{3} & \overline{3} & \overline{4} & \overline{0} & \overline{1} & \overline{2} \\ \overline{4} & \overline{4} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \end{array}\right] \left[\begin{array}{c|ccccc} \cdot & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \hline \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{2} & \overline{0} & \overline{2} & \overline{4} & \overline{1} & \overline{3} \\ \overline{3} & \overline{0} & \overline{3} & \overline{1} & \overline{4} & \overline{2} \\ \overline{4} & \overline{0} & \overline{4} & \overline{3} & \overline{2} & \overline{1} \end{array}\right]$$

$\mathbb{Z}_q$ com estas operações será um corpo se, e somente se, q for um número primo (Apêndice e [18]). Neste caso, teremos a definição de códigos lineares, com as propriedades já estudadas anteriormente.

Uma outra noção de distância pode ser definida em $\mathbb{Z}_q$ e $\mathbb{Z}_q^n$, que é conhecida como *distância ou métrica de Lee* ([10] e [25]).

Dados $\overline{a}$ e $\overline{b}$ em Z_q definimos:

$$d_{Lee}(\overline{a}, \overline{b}) = \min\{|a-b|, q-|a-b|\}$$

Assim, por exemplo, em $\mathbb{Z}_{13}$, $d_{Lee}(\overline{1}, \overline{4}) = 3$ e $d_{Lee}(\overline{1}, \overline{12}) = 2$. Se colocarmos as classes de $\mathbb{Z}_q$ como os 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 1.3 ilustra $\mathbb{Z}_{13}$.

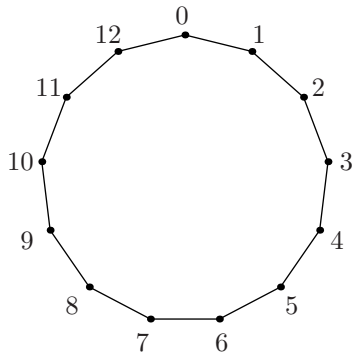


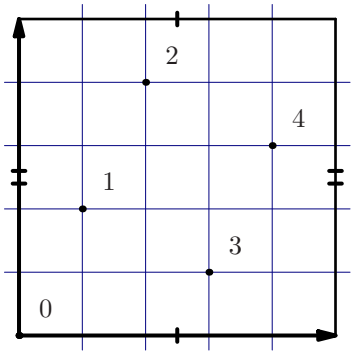
Figura 1.3: Uma representação geométrica de $\mathbb{Z}_{13}$ com a distância de Lee.

A distância de Lee em $\mathbb{Z}_q^n$ é definida como a soma das distâncias nas coordenadas:

$$d_{Lee}((\overline{a_1}, \overline{a_2}, ..., \overline{a_n}), (\overline{b_1}, \overline{b_2}, ..., \overline{b_n})) = \sum_{i=1}^{n} d_{Lee}(\overline{a}_i, \overline{b}_i)$$

Podemos definir os conceitos de esfera e bola como fizemos com a distância de Hamming. Para $n = 2$, os pontos de $\mathbb{Z}_q^2$ são correspondentes aos vértices de uma malha quadriculada desenhada num quadrado de lado q. Os bordos deste quadrado devem ser identificados e portanto esta malha irá estar sobre um toro. A distância de Lee entre dois vértives é a distância do grafo, ou seja, o número mínimo de arestas nesta malha para ir de um vértice a outro.

A figura 1.4 representa $\mathbb{Z}_5^2$. Observe na figura que $d_{Lee}((\overline{2}, overline3), (\overline{4}, \overline{4})) = 3$. Verifique que dado o elemento $(2, 3)$ (e na verdade qualquer outro), existem na distância de Lee: 1 ponto a distância 0, 4 a distância 1,8 a distância 2, 8 a distância 3 e 4 a distância 4.



Se neste mesmo conjunto $\mathbb{Z}_5^2$ você considerar a distância de Hamming, quais são as possibilidades para as distâncias?

Considere agora o código linear $\mathcal{C}$ dado por:

$$\mathcal{C} = \{j(2,1), j = 0,1,2,3,4\}$$

Verifique que a distância de Lee mínima é 3 e ele é um código 1-perfeito com esta distância.

Este é um exemplo de um resultado mais geral ([10]):

$$\mathcal{C} = \{j(m+1,m), j = 0,1,2,...,m-1\}$$

é um código com distância de Lee mínima $2m+1$ e é m-perfeito em $\mathbb{Z}^2_{(m+1)^2+m^2}$ segundo esta distância. Verifique este fato no exemplo $m = 3$.

1.5 Probabilidade de Erro em Canais Binários Simétricos

Uma questão natural a respeito de códigos é o que ganhamos em troca da perda de informação que ocorre (a taxa de informação é sempre menor que um)?

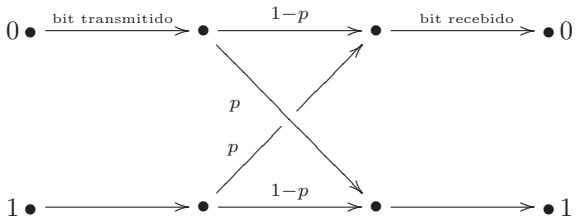


Figura 1.4:

Vamos assumir que a transmissão seja através de um canal binário simétrico BSC (de binary symmetric channel). Um modelo simples de um canal assim é esquematizado na figura 1.4. A probabilidade de se inverter um bit, seja este 0 ou 1, é assumida como sendo p, $0 < p < \frac{1}{2}$, e é independente do que ocorre com qualquer outro bit. Notamos que este tipo de modelo nem sempre é realista, mas representa bem, por exemplo, uma rápida transferêcia de dados num computador.

No exemplo do $(7,4)-$código de Hamming, $\mathcal{H}_3$, temos uma taxa de informação de $\frac{4}{7} \approxeq 0,57$. O que ganhamos com esta perda de 43% ? Qual a probabilidade não termos erro ?

Se simplesmente transmitirmos 4 bits sem redundância a probabilidade de acerto será de $(1-p)^4$. Usando o código de Hamming $\mathcal{H}_3$ com a decodificação de máxima verossimilhança, a probabilidade de não termos erros será:

$$
\begin{aligned}
p_H = &\text{ probabilidade de termos 7 bits corretos e 0 incorretos +} \\
&\text{probabilidade de termos 6 bits corretos e um incorreto} \\
&= (1-p)^7 + \begin{pmatrix} 7 \\ 6 \end{pmatrix}(1-p)p \\
&= (1-p)^4(6p^3 - 11p^2 + 4p + 1)
\end{aligned}
$$

Então o polinômio $f(p) = 6p^3 - 11p^2 + 4p + 1$ é quem dá uma medida do ganho na probabilidade de não haver erro. Note que $f(0) = f(\frac{1}{2}) = 1$ e, neste caso,o valor máximo de f no intervalo será em $p = \frac{2}{9}$ (Verifique!), onde $f(p) \approx 1.41$. e portanto teríamos um ganho máximo de 41% caso p tivesse este valor. Naturalmente para valores pequenos de p o ganho seria bem menor (Ex. para $p = 0,01$, ganho de 4%).

Exercício 1.14. *Considere um código de tripla repetição para codificar mensagens iniciais de 4 bits. Compare este código com o $\mathcal{H}_3$ analisando: distância mínima, detecção e correção de erros, taxa de informação e probabilidade de transmissão correta.*

1.6 Leituras de Aprofundamento e Extensão

Uma ótima referência em português é [18]. Este é um texto que introduz a teoria de códigos aprofundando nos conceitos algébricos, numa abordagem que complementa o texto aqui apresentado. Outras excelentes referências para consulta e aprofundamento dos temas aqui abordados são [24], [28], [23] e [33] que, como [18], serviram de base para a edição deste capítulo. Para suporte e revisão de Álgebra Linear, consulte [8] e [14].

1.7 Exercícios Complementares

Exercício 1.15. *1. Discuta a afirmação de que o código ISBN detecta um erro.*

2. Os dígitos de controle, $n_{10}n_{11}$, ao final do seu CPF são assim estabelecidos:
CPF: $n_1n_2n_3...n_9/\ n_{10}n_{11}$

$$n_{10} = ((\sum_{i=1}^{9} i.n_i) \bmod 11) \bmod 10$$

$$n_{11=}((\sum_{i=2}^{10} (i-1).n_i) \bmod 11) \bmod 10$$

a) Teste a expressão acima no seu CPF e de algum amigo

b) Este código corrige erro?

c) Detecta algum erro?

3. *Suponha que o robo do exemplo 3 possa mover-se nas oito direções cardeais e também levantar o braço esquerdo e direito separadamente. Proponha códigos fonte e canal e discuta. Acrescente movimento de cabeça.*

4. *Estenda o problema anterior para um "tabuleiro 3D ".*

5. *Estenda a definição de do código de verificação de paridade* $(8, 7)$ *para* $(n+1, n)$

6. *Pense em aperfeiçoar o código de tripla checagem de paridade de forma que a cada quatro dígitos ele acrescente 3 de verificação e continue corrigindo um erro.*

7. *Mostre que não é possível a um código binário que a 5 dígitos acrescente mais três corrigir um erro.*

8. *Mostre que, se* $|A| = q$, *dado* $\mathbf{a} \in A^n$ *e* $r \in \mathbb{N}; 0 < r \leq n$, *os números de elementos da esfera e da bola segundo a distância de Hamming são respectivamente:*

$$|S(\mathbf{a}, r)| = \binom{n}{r}(q-1)^r \text{ e } |D(\mathbf{a}, r)| = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$$

9. *Encontre uma matriz geradora para o código que é ortogonal ao do 1.15.3.*

10. *Um código de n repetições é uma extensão do que foi abordado no 1.15.1. a) Defina-o formalmente, mostre que ele é um código linear exibindo uma matriz geradora. b) Encontre uma matriz de paridade, a distância mínima, o número de erros que pode corrigir e taxa de informação deste código. c) Estes códigos são perfeitos ?*

11. *Para cada n construa um código linear binário de posto máximo com distância mínima* 2.

Capítulo 2

Reticulados

2.1 Introdução

O problema de encontrar o melhor código possível em $\mathbb{Z}_2^n$ corresponde, em $\mathbb{R}^n$, ao *problema do empacotamento esférico*. Ou seja, queremos distribuir esferas de raio r em $\mathbb{R}^n$, de modo que
(i) duas esferas quaisquer deste arranjo apenas se toquem em um ponto da "casca", ou não possuam intersecção nenhuma;
(ii) este arranjo de esferas ocupe o "maior espaço possível" .

No ambiente de $\mathbb{Z}_2^n$, vimos no Capítulo 1 que o problema fica um pouco menos complicado quando se tem alguma estrutura algébrica no código (códigos lineares), ou seja, nos centros das esferas. O mesmo vale para o empacotamento de esferas em $\mathbb{R}^n$ e, neste caso, a estrutura algébrica é a de *reticulado*.

Um subconjunto Λ de $\mathbb{R}^n$ é um reticulado se existe uma base $\beta = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ de $\mathbb{R}^n$ tal que

$$\mathbf{x} \in \Lambda \text{ se, e somente se, } \mathbf{x} = a_1\mathbf{u}_1 + \ldots + a_n\mathbf{u}_n \text{ com } a_i \in \mathbb{Z} \text{ para todo } i.$$

β é chamada de base do reticulado Λ. A figura 2.1 ilustra dois reticulados em $\mathbb{R}^2$: o reticulado $\mathbb{Z}^2$, dos pontos de coordenadas inteiras no plano, que tem por base $\beta = \{(1,0),(0,1)\}$, e o reticulado gerado pela base $\beta = \{(2,1),(-1,3)\}$.

A base de um reticulado não é única: por exemplo, $\beta' = \{(1,3),(0,1)\}$ também é base de $\mathbb{Z}^2$, pois o reticulado gerado por β' está contido em $\mathbb{Z}^2$ e, por outro lado,

$$(m,n) = m(1,3) + (n-3m)(0,1).$$

Pode-se mostrar que dado um reticulado Λ gerado por uma base β, uma base α de $\mathbb{R}^2$ também é base deste reticulado se, e somente se, α está contida em Λ e a matriz de mudança de base M tem entradas inteiras e determinante ± 1 [36].

Vimos também, no capítulo anterior, que um código geometricamente uniforme possui várias propriedades interessantes e que, neste caso, há mais ferramentas para o estudo da geometria do código. Isso dá mais uma boa razão para estudar o

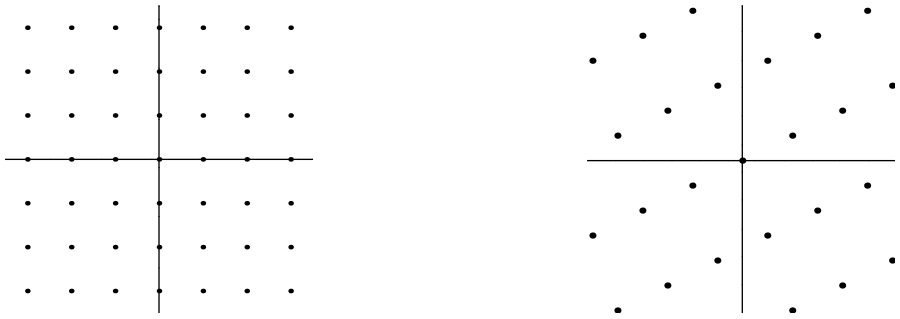


Figura 2.1: Dois reticulados no plano.

problema de empacotamento via reticulados, pois todo reticulado é geometricamente uniforme.

Exercício 2.1. *Mostre que as translações são isometrias de $\mathbb{R}^n$ com a distância usual; mostre também que se Λ é um reticulado e $\mathbf{u} \in \Lambda$, então a translação $\mathbf{x} \mapsto \mathbf{x} + \mathbf{u}$ é uma isometria que leva Λ em Λ. Finalmente, mostre que Λ é geometricamente uniforme.*

No que se segue, estudaremos ferramentas e conceitos básicos da teoria de reticulados em $\mathbb{R}^n$, tendo a densidade como conceito central. Mostraremos também uma técnica de construção de reticulados, a partir de códigos binários, e uma aplicação da teoria de reticulados ao estudo de grafos.

2.2 Reticulados no Plano

Como primeiro exemplo de empacotamento determinado por um reticulado, consideremos o reticulado $\mathbb{Z}^2$. Um empacotamento esférico (por discos, neste caso) é feito colocando-se um disco D, de raio $1/2$, centrado em cada ponto $\mathbf{v}$ do reticulado.

Observe que, se tomarmos discos de raio maior do que $1/2$, haverá sobreposição; portanto, $1/2$ é o maior raio possível para um empacotamento de discos com centros nos pontos de $\mathbb{Z}^2$. Este maior raio possível é chamado de *raio de empacotamento* ρ do reticulado. Pode-se mostrar que ρ é a metade da distância mínima entre pontos do reticulado.

Para medir a proporção da área do plano que foi ocupada pelo empacotamento, recorremos a um arranjo "complementar", dado pelas *regiões de Voronoi* dos pontos do reticulado. A região de Voronoi de um ponto $\mathbf{v}$ de $\mathbb{Z}^2$ é o conjunto $R(\mathbf{v})$ dos pontos de $\mathbb{R}^2$ que estão mais próximos de $\mathbf{v}$ do que de qualquer outro ponto de $\mathbb{Z}^2$ que, neste caso, é um quadrado unitário centrado no ponto $\mathbf{v}$.

Para um reticulado mais geral do plano, uma região de Voronoi é determinada do seguinte modo: dados dois pontos $\mathbf{u}$ e $\mathbf{v}$, o conjunto dos pontos que estão mais próximos de $\mathbf{v}$ do que de $\mathbf{u}$ corresponde ao semiplano determinado pelo bissetor perpendicular (mediatriz) do segmento $[\mathbf{u}, \mathbf{v}]$, que contém o ponto $\mathbf{v}$. Tomando-se a

intersecção de todos estes semiplanos (na verdade, apenas dos semiplanos relativos a pontos próximos de $\mathbf{v}$), obtemos a região $R(\mathbf{v})$. A figura 2.2 ilustra as regiões de Voronoi de $\mathbb{Z}^2$ e do reticulado Λ gerado por $(2,1)$ e $(-1,3)$.

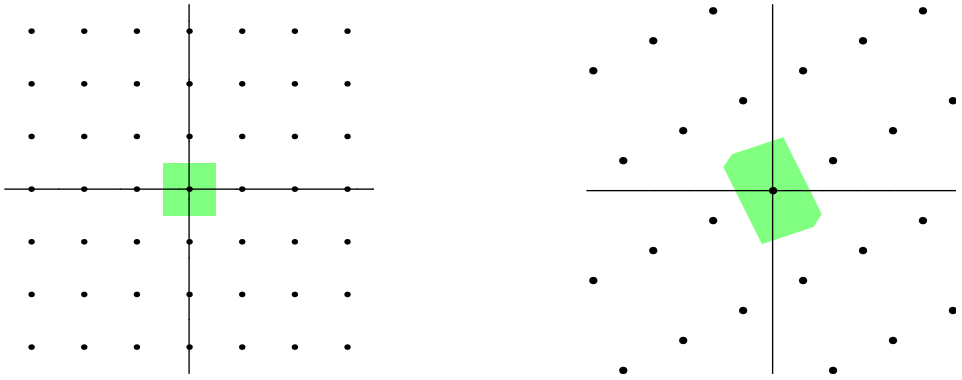


Figura 2.2: Regiões de Voronoi de $\mathbb{Z}^2$ e do reticulado Λ gerado por $(2,1)$ e $(-1,3)$

Tendo construído uma destas regiões, todas as outras são obtidas por translações: se começarmos de $R(\mathbf{0})$, por exemplo, teremos

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

Como cada translação é uma isometria, todas estas regiões possuem as mesmas propriedades geométricas. Logo, basta estudar a região $R(\mathbf{0})$.

O importante é que estas regiões constituem um ladrilhamento perfeito no plano: as regiões $R(\mathbf{v})$ cobrem o plano inteiro e se sobrepõem apenas ao longo de pontos da fronteira (vértices ou arestas). Assim, a densidade do reticulado ou, mais claramente, a densidade do empacotamento de discos determinado pelo reticulado, é definida como a razão Δ entre a área do disco de empacotamento D e a área da região de Voronoi, e fornece uma medida de quanto do plano foi preenchido pelos discos. Temos, então,

$$\Delta = \frac{\text{área}(D)}{\text{área}(R(\mathbf{0}))},$$

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

Exercício 2.2. *Mostre que, para* $\mathbb{Z}^2$*, temos* $\Delta = \pi/4 \cong 0,7804$.

Voltemos ao reticulado Λ gerado pela base $\beta = \{\mathbf{v}_1, \mathbf{v}_2\}$, onde $\mathbf{v}_1 = (2,1)$ e $\mathbf{v}_2 = (-1,3)$. Qual é o raio de empacotamento?

Se $\mathbf{u} = x(2,1) + y(-1,3)$, então $||\mathbf{u}||^2 = 5x^2 + 2xy + 10y^2$. Daí, se $xy = 0$, o menor valor que $||\mathbf{u}||^2$ assume é 5, e isto ocorre nos vetores $\pm(2,1)$. Se $xy < 0$, então

$$5x^2 + 2xy + 10y^2 \geq 5x^2 + 2xy + 5y^2 \geq 4x^2 + 4y^2 + (x+y)^2 \geq 8,$$

pois $x, y \in \mathbb{Z}$ e $xy \neq 0$; e é lógico que se $xy > 0$, então $||\mathbf{u}||^2 > 5$. Portanto, os vetores de menor norma são os dois vetores $(2,1)$ e $(-2,-1)$; logo, o raio de empacotamento é $\rho = \sqrt{5}/2$. Para calcular a densidade de empacotamento, temos que determinar a área de uma região de Voronoi deste reticulado que, neste caso, é um polígono de seis lados. Lógico que podemos calculá-la diretamente (e deixaremos isso como exercício para o leitor), mas existe uma maneira mais simples de fazê-lo.

Observamos inicialmente que não apenas a região de Voronoi ladrilha o plano pelas translações por vetores de Λ, mas que também podemos tomar como ladrilhos, relativos a estas mesmas translações, o paralelogramo P apoiado na base do reticulado, isto é,

$$P = \{a\mathbf{v}_1 + b\mathbf{v}_2 | 0 \leq a \leq 1, 0 \leq b \leq 1\}.$$

Na Figura 2.3 vemos o paralelogramo P gerado pela base $\{(2,1),(-1,3)\}$.

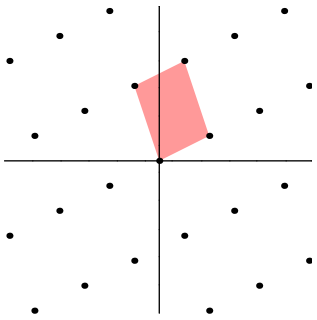


Figura 2.3: Paralelogramo gerado pela base $\{(2,1),(-1,3)\}$

Como veremos na próxima seção, ladrilhos que tesselam pelas mesmas translações possuem a mesma área, e calcular a área de um paralelogramo com suporte em $\mathbf{v}_1 = (v_{11}, v_{21})$ e $\mathbf{v}_2 = (v_{12}, v_{22})$ é muito simples:

$$\text{área}(P) = \det \left| \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix} \right|.$$

Finalmente, podemos calcular a densidade de Λ: a área do paralelogramo é 7 e a densidade é

$$\Delta = \frac{5\pi}{28} \cong 0,561.$$

Exercício 2.3. *Construa a região de Voronoi da origem do reticulado Λ gerado por $\beta = \{(2,1),(-1,3)\}$ e verifique que sua área é igual à área do paralelogramo apoiado em β.*

2.3 Regiões Fundamentais e Densidade

A definição de região de Voronoi para dimensão n é a mesma de dimensão 2: se $\mathbf{v}$ é um ponto de Λ, a região de Voronoi de $\mathbf{v}$ é o conjunto

$$R(\mathbf{v}) = \{\mathbf{x} \in \mathbb{R}^n; ||\mathbf{v} - \mathbf{x}|| \leq ||\mathbf{v} - \mathbf{u}||, \text{ para todo } \mathbf{u} \in \Lambda\}.$$

Uma primeira propriedade destas regiões é

Proposição 2.1. *Para todo* $\mathbf{v} \in \Lambda$*,*

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

Exercício 2.4. *Prove o resultado acima.*

Uma segunda propriedade importante é que podemos ladrilhar $\mathbb{R}^n$ com estas regiões. Informalmente, isto significa que cada ponto de $\mathbb{R}^n$ está em um dos transladados de $R(\mathbf{0})$ e que dois destes transladados só se tocam nos bordos (ou não têm intersecção).

Como no caso planar, vamos avaliar o quão denso é um reticulado, comparando o volume de uma região de Voronoi $R(\mathbf{v})$ com o volume da maior bola $B_r(\mathbf{v})$ que ela contém. Para isso, seja $r = \rho$, o *raio de empacotamento* de Λ, isto é, o maior número positivo tal que $B_r(\mathbf{0}) \subset R(\mathbf{0})$ (pode-se verificar, como antes, que ρ é metade da norma mínima de Λ, isto é, $\rho = \frac{1}{2}\min\{||\mathbf{x}||; x \in \Lambda\}$). Definimos a densidade de Λ por

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

Verifique, por exemplo, que a densidade do reticulado $\mathbb{Z}^3$ dos pontos de coordenadas inteiras no espaço é $\Delta = \frac{\pi}{6} \cong 0,5236$.

É claro que determinar a região de Voronoi de um reticulado não é um problema nada trivial e, na forma em que está, a definição de densidade é de difícil aplicabilidade. Vamos mostrar agora que, tendo o raio de empacotamento ρ e uma base de Λ, podemos calcular a densidade do reticulado sem problemas (na prática, o cálculo de ρ também pode trazer dificuldades, mas isso já é outra história).

Seja Λ um reticulado em $\mathbb{R}^n$. Uma *região fundamental* F de Λ é um subconjunto fechado de $\mathbb{R}^n$ que ladrilha $\mathbb{R}^n$, isto é, tomando os transladados $F + \mathbf{v}$, com $\mathbf{v} \in \Lambda$, conseguimos cobrir todo o $\mathbb{R}^n$ de modo que dois ladrilhos ou não têm intersecção ou se intersectam apenas nos bordos.

A região de Voronoi $R(\mathbf{0})$ é um exemplo de região fundamental de Λ. Uma segunda região fundamental bastante útil para nós é o *politopo fundamental* gerado por uma base de Λ.

Dada uma base $\beta = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$, o politopo fundamental gerado por esta base é o sólido

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

Para $n = 2$, este é o paralelogramo gerado por β. Da mesma forma que nos reticulados planos, o volume deste sólido n-dimensional é dado por $vol(P) = |\det(A)|$, onde A é a matriz cujas colunas são os vetores da base β.

Proposição 2.2. *P é uma região fundamental de Λ.*

Demonstração: De fato, P é fechado, e se

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

então

(i) cada vetor de $\mathbb{R}^n$ está em um destes sólidos. De fato, se $\lfloor a \rfloor$ é a parte inteira do número real a (ou seja, $\lfloor a \rfloor \in \mathbb{Z}$ e $0 \leq a - \lfloor a \rfloor < 1$), então para cada vetor $\mathbf{v} = \sum_{i=1}^{n} a_i \mathbf{u}_i$ de $\mathbb{R}^n$, temos

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

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

(ii) o interior de $\mathbf{v} + P$, isto é, o conjunto dos pontos de $\mathbf{v} + P$ que não estão na fronteira, é o conjunto

$$\text{int}(\mathbf{v} + P) = \{\mathbf{v} + \sum_{i=1}^{n} a_i \mathbf{u}_i; 0 < a_i < 1\},$$

e disso se conclui que nenhum ponto de $\mathbf{v} + P$ pode estar em outro transladado $\mathbf{u} + P$ (use o fato de que os pontos de Λ são combinações *inteiras* dos $\mathbf{u}_i$'s). ■

O fato de P ser uma região fundamental de Λ é crucial no estudo dos reticulados, pois

Proposição 2.3. *O volume de qualquer região fundamental de Λ é o mesmo.*

A demonstração desta proposição envolve pré-requisitos de geometria que estão além do escopo deste texto [5].

2.4 Matriz de Gram e o Determinante de um Reticulado

Seja $\beta = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$, uma base do reticulado Λ, e seja $x = k_1\mathbf{u}_1 + \ldots k_n\mathbf{u}_n$ um elemento de Λ. Escrevendo os vetores na forma de colunas, com as coordenadas na base canônica, temos

$$\mathbf{x} = k_1 \begin{bmatrix} u_{11} \\ \vdots \\ u_{1n} \end{bmatrix} + \ldots + k_n \begin{bmatrix} u_{n1} \\ \vdots \\ u_{nn} \end{bmatrix} = \begin{bmatrix} u_{11} & \cdots & u_{1n} \\ \vdots & & \vdots \\ u_{n1} & \cdots & u_{nn} \end{bmatrix} \begin{bmatrix} k_1 \\ \vdots \\ k_n \end{bmatrix}.$$

Isso nos mostra que Λ é a imagem de $\mathbb{Z}^n$ pela matriz $M = (u_{ij})$, ou seja, todo $\mathbf{x}$ de Λ é da forma $A\mathbf{v}^T$, para algum $\mathbf{v} = (k_1, \ldots, k_n)$ em $\mathbb{Z}^n$. A matriz A é chamada de *matriz geradora* [1] de Λ. Por exemplo, para cada n, temos o reticulado

$$\mathbb{Z}^n = \{(a_1, a_2, \ldots, a_n); a_i \in \mathbb{Z}\}.$$

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

Se A é uma matriz geradora de Λ, a *matriz de Gram* associada é $G = A^T A$.

Exercício 2.5. *Verifique que G é uma matriz simétrica e que suas entradas são os produtos escalares $\langle \mathbf{u}_i, \mathbf{u}_j \rangle$.*

Assim, G guarda informações métricas importantes sobre a base escolhida.

Claro que um reticulado tem várias bases diferentes e, infelizmente, as matrizes de Gram podem mudar com a base. Considere, por exemplo, o reticulado Λ gerado por $\beta = \{\mathbf{u}, \mathbf{v}\}$, com $\mathbf{u} = (n, n+1)$ e $\mathbf{v} = (-n-1, n)$, sendo n um número inteiro não-nulo. Os vetores $\mathbf{u}' = (n, n+1)$ e $\mathbf{v}' = (-1, 2n+1)$ também formam uma base β' de Λ.

Exercício 2.6. *Verifique que β' também é base do reticulado Λ. Verifique que as matrizes de Gram correspondentes a β e β' são*

$$G = \begin{bmatrix} 2n^2+2n+1 & 0 \\ 0 & 2n^2+2n+1 \end{bmatrix} \quad e \quad G' = \begin{bmatrix} 2n^2+2n+1 & 2n^2 \\ 2n^2 & 4n^2+4n+2 \end{bmatrix}.$$

Assim, um reticulado possui várias matrizes de Gram diferentes. No entanto, o determinante de cada uma delas é o mesmo e só depende do reticulado.

Para verificar isso, considere as bases $\beta = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ e $\beta' = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ de Λ e sejam A e B as matrizes geradoras associadas. Como β é base de Λ, podemos escrever

$$\mathbf{v}_j = a_{1j}\mathbf{u}_1 + a_{2j}\mathbf{u}_2 + \cdots + a_{nj}\mathbf{u}_n, \text{ para } j = 1, 2, \ldots, n,$$

onde cada a_{ij} está em $\mathbb{Z}$. A transformação linear $T : \mathbb{R}^n \to \mathbb{R}^n$, que leva $\mathbf{u}_j$ em $\mathbf{v}_j$, faz a mudança de base e tem matriz M com determinante ± 1. Daí

$$B = MA$$

e $\det(B^T B)$ é igual a

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

Como ilustração, é fácil verificar no exemplo anterior que ambas as matrizes de Gram têm determinante igual a $(2n^2+2n+1)$. Por isso, definimos o *determinante* de Λ, $\det(\Lambda)$, como o determinante de uma matriz de Gram (qualquer) de Λ. Este número tem uma interpretação geométrica que parece surpreendente: é o quadrado do volume de uma região fundamental de Λ.

[1] Em boa parte dos textos sobre reticulados, escreve-se vA e não $A\mathbf{v}^T$. Nesta outra convenção, são as linhas de A que geram o reticulado.

Exercício 2.7. *Mostre que o volume de P é* $\det(\Lambda)^{1/2}$.

Pela proposição 2.3, o volume da região de Voronoi $R(\mathbf{0})$ é igual ao volume de P; assim, o volume de $R(\mathbf{0})$ é igual à raiz quadrada do determinante de Λ. Portanto, expressamos a densidade de Λ como

$$\Delta = \frac{vol(B_\rho(\mathbf{0}))}{\det(\Lambda)^{1/2}}$$

e o problema de calcular Δ fica resolvido se tivermos uma base do reticulado Λ e sua distância mínima (a expressão para o volume da bola n-dimensional pode ser encontrada em [36]).

Por exemplo, para o reticulado Λ gerado por (a, b) e $(-b, a)$, temos $\Delta = \frac{\pi}{4} \cong 0,7854$ (veja o exercício 2).

Uma densidade muito melhor é atingida pelo reticulado A_2 (figura 2.4), que é o reticulado mais denso em $\mathbb{R}^2$ e é gerado pela base $\beta = \{(1, 0), (1/2, \sqrt{3}/2)\}$. As regiões de Voronoi deste reticulado são hexágonos e sua densidade é $\Delta = \frac{\pi}{\sqrt{12}} \cong 0,9069$ (veja exercício 3). este é o reticulado no plano com a melhor densidade possível [36].

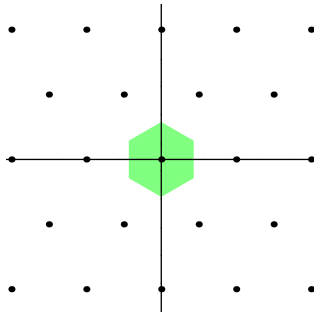


Figura 2.4: Região fundamental do reticulado A_2.

2.5 Reticulados Congruentes e Reticulados Equivalentes

Quando trabalhamos com códigos binários, utilizamos o conceito de *códigos equivalentes*: dois códigos lineares C_1 e C_2 são equivalentes se existir uma isometria φ tal que $\varphi(C_1) = C_2$. Códigos equivalentes têm os mesmos parâmetros n, k, d.

No caso dos reticulados, temos a definição análoga de reticulados congruentes. Veremos que se dois reticulados são congruentes, então possuem mesmo raio de empacotamento, mesma densidade e uma mesma matriz de Gram. Um conceito mais flexível, específico para reticulados, é o da equivalência; se Λ_1 e Λ_2 são equivalentes,

sua densidade é a mesma e, embora não sejam os mesmos, os raios de empacotamento e as matrizes de Gram são relacionados por um simples fator escalar. Como a congruência é um caso particular da equivalência, começaremos nosso estudo por esta última.

Diremos que Λ_1 e Λ_2 são *equivalentes* se existirem uma aplicação ortogonal $U : \mathbb{R}^n \to \mathbb{R}^n$ e um número real positivo λ tais que $(\lambda U)(\Lambda_1) = \Lambda_2$. Note que $\langle \lambda U\mathbf{u}, \lambda U\mathbf{v}\rangle = \lambda^2 \langle \mathbf{u}, \mathbf{v}\rangle$ e que, por tabela, $||\lambda U\mathbf{v}|| = \lambda||\mathbf{v}||$. Diremos que λ é a *razão de semelhança* de Λ_1 para Λ_2.

Se ρ_i e Δ_i são o raio de empacotamento e a densidade de Λ_i, para $i = 1, 2$, respectivamente, temos

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

e segue que o raio de empacotamento de Λ_2 é $\rho_2 = \lambda\rho_1$. E também: se A é matriz geradora de Λ_1, então λUA é matriz geradora de Λ_2 e

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

o que mostra que $\det(\Lambda_2) = \lambda^{2n}\det(\Lambda_1)$. Portanto,

$$\begin{aligned} \Delta_2 &= \frac{vol(B_{\rho_2(0)})}{\det(\Lambda_2)^{1/2}} \\ &= \frac{\lambda^n vol(B_{\rho_1(0)})}{\lambda^n \det(\Lambda_1)^{1/2}} \\ &= \Delta_1 \end{aligned} .$$

Assim, reticulados equivalentes possuem a mesma densidade. Resumindo as contas,

Proposição 2.4. *Se Λ_1 é semelhante a Λ_2 com razão de semelhança λ, então existem matrizes de Gram G_1 e G_2 para Λ_1 e Λ_2 tais que*

1. $G_2 = \lambda^2 G_1$,
2. $\rho_2 = \lambda\rho_1$,
3. $\Delta_2 = \Delta_1$.

Note que, como tanto o raio de empacotamento quanto o volume podem ser calculados a partir de uma matriz de Gram do reticulado, a propriedade (1) implica nas condições (2) e (3) (verifique!). Outro fato importante é que, se vale a condição (1), então os reticulados são semelhantes. Para isso, suponha que $\beta_1 = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ e $\beta_2 = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ são bases de Λ_1 e Λ_2, com matrizes de Gram G_1 e G_2 tais que $G_2 = \lambda^2 G_1$. Então, a aplicação linear $T : \mathbb{R}^n \to \mathbb{R}^n$, definida por $T(\mathbf{u}_i) = \mathbf{v}_i$, é uma semelhança de razão λ. Para verificar isso, tome $\mathbf{u} = \sum_{i=1}^n a_i\mathbf{u}_i$ e $\mathbf{v} = \sum_{i=1}^n b_i\mathbf{u}_i$ em $\mathbb{R}^n$. Temos, então,

$$\begin{aligned}
\langle T\mathbf{u}, T\mathbf{v}\rangle &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_i b_j \ \langle T\mathbf{u}_i, T\mathbf{u}_j\rangle \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} a_i b_j \ \langle \mathbf{v}_i, \mathbf{v}_j\rangle \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} a_i b_j \lambda^2 \ \langle \mathbf{u}_i, \mathbf{u}_j\rangle \ \text{(por (1))} \\
&= \lambda^2 \ \langle \mathbf{u}, \mathbf{v}\rangle .
\end{aligned}$$

Quando $\lambda = 1$, dizemos que os reticulados são *congruentes* . Neste caso, as matrizes de Gram e os raios de empacotamentos são iguais.

Como no caso dos códigos, não se costuma fazer distinção entre reticulados congruentes e vários reticulados são identificados na literatura pela matriz de Gram. Um primeiro exemplo importante é o dos reticulados D_n, $n \geq 3$. Os reticulados D_3, D_4 e D_5 são definidos pelas matrizes de Gram

$$\begin{bmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}, \qquad \begin{bmatrix} 2 & 0 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{bmatrix} \qquad \text{e} \qquad \begin{bmatrix} 2 & 0 & -1 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 \\ -1 & -1 & 2 & -1 & 0 \\ 0 & 0 & -1 & 2 & 1 \\ 0 & 0 & 0 & -1 & 2 \end{bmatrix}.$$

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

$$\begin{bmatrix}
2 & 0 & -1 & 0 & & & \cdots & & 0 & 0 \\
0 & 2 & -1 & 0 & 0 & & & & & 0 \\
-1 & -1 & 2 & -1 & 0 & 0 & \cdots & & & \\
0 & 0 & -1 & 2 & -1 & 0 & & & & \\
0 & 0 & 0 & -1 & 2 & -1 & & & \vdots & \\
\vdots & & & & \ddots & & & & & \\
 & & & & & 0 & -1 & 2 & -1 & 0 \\
0 & & & & \cdots & & 0 & -1 & 2 & -1 \\
0 & 0 & & & & & & 0 & -1 & 2
\end{bmatrix}.$$

A matriz de Gram também pode ser especificada em termos dos produtos internos dos elementos da base correspondente. Ou seja,

$$\begin{aligned}
&\text{(i)} && \langle \mathbf{e}_1, \mathbf{e}_3\rangle &&= \langle \mathbf{e}_2, \mathbf{e}_3\rangle = -1 \\
&\text{(ii)} && \langle \mathbf{e}_1, \mathbf{e}_2\rangle &&= 0 \\
&\text{(iii)} && \langle \mathbf{e}_i, \mathbf{e}_{i+1}\rangle &&= -1 \text{ para } i = 3, \ldots, n-1 \\
&\text{(iv)} && \langle \mathbf{e}_i, \mathbf{e}_j\rangle &&= 0 \text{ para } i, j = 3, \ldots, n \text{ e } |i-j| \geq 2.
\end{aligned}$$

Na seção seguinte, mostraremos como obter uma base deste reticulado. Um segundo exemplo importante é o reticulado E_8, que é o reticulado de maior densidade em $\mathbb{R}^8$.

O reticulado E_8 é determinado pela matriz de Gram

$$\begin{bmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 & -1 & 2 \end{bmatrix}.$$

Das várias realizações deste reticulado, uma das mais simples, encontrada em [36], é dada pela base formada pelos vetores

$$\begin{aligned} \mathbf{e}_1 &= (-1,1,0,0,0,0,0,0), \\ \mathbf{e}_2 &= (0,-1,1,0,0,0,0,0), \\ &\vdots \\ \mathbf{e}_7 &= (0,0,0,0,0,0,-1,1) \text{ e} \\ \mathbf{e}_8 &= \tfrac{1}{2}(1,1,1,1,1,-1,-1,-1). \end{aligned}$$

Pode-se verificar que estes vetores satisfazem

$$\begin{aligned} (i) \quad \langle \mathbf{e}_i, \mathbf{e}_i \rangle &= 2, \\ (ii) \quad \langle \mathbf{e}_i, \mathbf{e}_{i+1} \rangle &= -1 \text{ para } i = 1,2,\ldots,7, \\ (iii) \quad \langle \mathbf{e}_i, \mathbf{e}_j \rangle &= 0 \text{ se } |i-j| \geq 2 \text{ e } i,j \neq 5,8, \\ (iv) \quad \langle \mathbf{e}_5, \mathbf{e}_8 \rangle &= -1, \end{aligned}$$

que são as relações expressas na matriz de Gram de E_8.

O reticulado E_8 possui $\det = 1$, norma mínima igual a 2, $\rho = \dfrac{\sqrt{2}}{2}$ e densidade igual a $\dfrac{\pi}{384} \cong 0,254$. Ele é o único reticulado (a menos de isometrias) com esta norma mínima e esta densidade, e ainda determina o melhor empacotamento por esferas conhecido em dimensão 8. A seguir, mostraremos como obter este reticulado e o anterior a partir de códigos binários.

2.6 Reticulados e Códigos

2.6.1 Construção A

Existem várias relações entre reticulados e códigos. Nesta seção, apresentaremos apenas uma delas, chamada "*construção A*", dada em [36]. Mencionamos apenas que, neste mesmo livro, são descritos outros métodos "clássicos" de construção de reticulados a partir de códigos e que vários trabalhos recentes têm por base uma

generalização do método que descreveremos a seguir. A principal aplicação deste método, neste texto, será a construção de E_8 a partir de um código binário, sendo que a identificação do reticulado obtido com o reticulado E_8 será feita pela matriz de Gram.

A aplicação

$$\begin{array}{rcl} \Phi : \mathbb{Z}^n & \longrightarrow & \mathbb{Z}_2^n \\ (a_1, a_2, \ldots, a_n) & \mapsto & (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}) \end{array}$$

é sobrejetora e satisfaz a condição [2]

$$\Phi(\mathbf{u} + \mathbf{v}) = \Phi(\mathbf{u}) + \Phi(\mathbf{v}).$$

Isso faz com que a cada código binário linear C seja associado um reticulado, o reticulado $\Lambda(C) = \Phi^{-1}(C)$.

Para obter o reticulado E_8, teremos que fazer uma pequena perturbação na pré-imagem: tomaremos $\Lambda(C) = a\Phi^{-1}(C)$, para uma constante $a > 0$, que será escolhida de modo conveniente. Vamos primeiro ver como determinar alguns parâmetros de $\Lambda(C)$ com base nos parâmetros de C.

Exercício 2.8. *Mostre que o reticulado $2a\mathbb{Z}^n$ sempre está contido em $\Lambda(C)$; conclua que a norma mínima em $\Lambda(C)$ é, no máximo, $2a$ (que é a norma de $a(2, 0, \ldots, 0)$).*

Além disso, se $\mathbf{u} \in C$, dentre todos os vetores $\mathbf{v}$ tais que $\Phi(\mathbf{v}) = \mathbf{u}$, o de menor norma é exatamente $\mathbf{u}$ (considerado como vetor de $\mathbb{R}^n$), e neste caso, $||\mathbf{u}||^2 = \omega(\mathbf{u})$; qualquer outra pré-imagem de $\mathbf{u}$ tem norma maior do que 2. Daí, se $a\mathbf{u}$ tem norma menor do que $2a$, então

$$||a\mathbf{u}|| = a||\mathbf{u}|| = a\sqrt{\omega(\mathbf{u})} \leq 2a,$$

o que implica em $\omega(\mathbf{u}) \leq 4$. Logo, existirão outros vetores de norma mínima em $\Lambda(C)$ distintos dos elementos de $2a\mathbb{Z}^n$ se, e somente se, $d \leq 4$. Concluímos o seguinte:

Proposição 2.5. *Sejam C um código linear binário com parâmetros $[n, k, d]$ 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 $a\mathbf{v}$, com $\mathbf{v} \in C$ de peso menor ou igual a 4, bem como os vetores $a\mathbf{v}'$, 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 de empacotamento e o número de vetores de norma mínima. Outro resultado importante é

[2] Isto é, é um homomorfismo de grupos.

Proposição 2.6. *Sejam C um código linear binário com parâmetros $[n,k,d]$ e $\Lambda(C) = \frac{1}{\sqrt{2}}\Phi^{-1}(C)$. Então,* $\det(\Lambda(C)) = 2^{n-k}$.

A demonstração desta proposição utiliza alguns conceitos a mais da teoria de grupos e pode ser encontrada em [13]. Prosseguimos agora com a aplicação desta construção aos reticulados D_n e E_8.

2.6.2 Reticulados obtidos pela construção A

Um primeiro exemplo importante, e razoavelmente simples, é o do reticulado D_n . Se C_n é o código

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

de parâmetros $[n, n-1, 2]$, então o reticulado D_n é igual a $\Lambda(C_n) = \Phi^{-1}(C_n)$ (aqui, tomaremos o escalar $a = 1$). Mostraremos os casos $n = 3$ e $n = 4$ e deixaremos o caso geral como exercício.

Consultando a matriz de Gram de D_3, vemos que precisamos encontrar uma base $\beta = \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ de $\Lambda(C_3) = \Phi^{-1}(C_3)$ que satisfaça as equações

$$\langle \mathbf{e}_1, \mathbf{e}_3 \rangle = -1, \quad \langle \mathbf{e}_2, \mathbf{e}_3 \rangle = -1, \quad \langle \mathbf{e}_1, \mathbf{e}_2 \rangle = 0.$$

Tendo isso em mente, considere $\mathbf{u} = (x, y, z)$ em $\Lambda(C_3)$; como $x+y+z \equiv 0 \mod 2$, temos também $y \equiv -x - z \mod 2$, ou seja,

$$\mathbf{u} = (x, -x - z, z) + (0, 2m, 0),$$

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

Uma primeira melhoria a ser feita é tentar substituir $(0,2,0)$ por um vetor de norma quadrada 2; como

$$(0,2,0) = (1,-1,0) + (-1,-1,0)$$

e $(-1,-1,0)$ é um vetor de norma mínima de $\Lambda(C_3)$, podemos trocar $(0,2,0)$ por $(-1,-1,0)$ e obter a base $\{(1,-1,0),(0,-1,1),(-1,-1,0)\}$.

Tomando produtos internos dois a dois, vemos que basta multiplicar $(0,-1,1)$ por -1 e trocar a ordem dos elementos da última base para chegar a uma nova base, a saber,

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

cuja matriz de Gram coincide com a de D_3.

Façamos agora o caso $n = 4$. Antes de mais nada, sugerimos ao leitor que volte à matriz de Gram de D_4. Nota-se que as relações entre $\mathbf{e}_1, \mathbf{e}_2$ e $\mathbf{e}_3$ são as mesmas para qualquer n; assim, vamos aproveitar o trabalho feito para D_3 e tomar $\mathbf{e}_1 = (1,-1,0,0)$, $\mathbf{e}_2 = (-1,-1,0,0)$, $\mathbf{e}_3 = (0,1,-1,0)$.

O vetor $\mathbf{e}_4$ tem que estar no subespaço ortogonal a $\mathbf{e}_1$ e $\mathbf{e}_2$, e deve satisfazer $\langle \mathbf{e}_3, \mathbf{e}_4 \rangle = -1$. Isso nos dá um sistema linear de três equações que tem por solução o subespaço $S = \{(0,0,1,z); z \in \mathbb{R}\}$. Como $\mathbf{e}_4$ é um vetor de norma quadrada 2 que está nesta reta e z é um número inteiro, obtemos $z = \pm 1$. Apenas para manter uma simetria na escolha dos vetores, tomamos $\mathbf{e}_4 = (0,0,1,-1)$ e obtemos a base

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

Isso mostra que $D_4 \subseteq \Lambda(C_4)$; deixamos ao leitor a tarefa de verificar que $D_4 = \Lambda(C_4)$. Continuando deste modo, pode-se provar que $\Lambda(C_n) = D_n$.

Vamos agora ao reticulado E_8 . Considere a seguinte versão do código de Hamming $\mathcal{H}_3$ com parâmetros $[7,4,3]$: o código é o núcleo da matriz

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Exercício 2.9. *Encontre o núcleo dessa matriz.*

Resolvendo este exercício, o leitor encontrará 7 vetores de peso 3, 7 de peso 4 e 1 de norma 7 (além do vetor nulo, lógico). Esta informação será importante no que se segue.

Agora, vamos estender $\mathcal{H}_3$ a um código de comprimento 8. Este é um processo geral: dado um código C de comprimento n, o código estendido $\widetilde{C}$ consiste das palavras da forma $(x_1, x_2, \ldots, x_n, (x_1 + \ldots + x_n))$, onde $(x_1, x_2, \ldots, x_n)$ está em C. Ou seja, acrescentamos a cada palavra de C uma nova coordenada que é a soma das coordenadas originais.

Exercício 2.10. *Mostre que $\widetilde{C}$ possui parâmetros $[n+1, k, d']$, sendo que $d' = d+1$, se d for ímpar, e $d' = d$, se d for par.*

Aplicando isto a $\mathcal{H}_3$, obtemos um código $\widetilde{\mathcal{H}_3}$ de parâmetros $[8,4,4]$ que chamamos de *código de Hamming estendido*. O leitor poderá (deverá!) verificar que o código $\widetilde{\mathcal{H}_3}$ possui 14 palavras de peso 4, sendo 7 com $x_8 = 0$ e 7 com $x_8 = 1$. Precisamos selecionar a base de E_8 dentre estas palavras de peso 4. Para isso, o seguinte resultado é muito útil (a prova fica como exercício): considerando vetores de $\mathbb{Z}_2^n$ como vetores de $\mathbb{R}^n$ de coordenadas 0 e 1,

Lema 2.1. *Dados $\mathbf{u}$ e $\mathbf{v}$ em $\mathbb{Z}_2^n$, sendo $\omega(\mathbf{u})$ o peso de $\mathbf{u}$ e $\langle \mathbf{u}, \mathbf{v} \rangle$ o produto interno de $\mathbf{u}$ e $\mathbf{v}$ em $\mathbb{R}^n$, temos*

$$\omega(\mathbf{u} + \mathbf{v}) = \omega(\mathbf{u}) + \omega(\mathbf{v}) - 2 \langle \mathbf{u}, \mathbf{v} \rangle .$$

Daí, tiramos o seguinte: como os pesos não-nulos que $\widetilde{\mathcal{H}_3}$ atinge são 4 e 8, se $\mathbf{u}$ e $\mathbf{v}$ têm peso 4 e $\mathbf{u} \neq \mathbf{v}$, então $\omega(\mathbf{u}+\mathbf{v}) = 8 - 2\langle \mathbf{u}, \mathbf{v} \rangle$. Temos, então, $\omega(\mathbf{u}+\mathbf{v}) = 8$, e portanto $\langle \mathbf{u}, \mathbf{v} \rangle = 0$, ou $\omega(\mathbf{u}+\mathbf{v}) = 4$, e $\langle \mathbf{u}, \mathbf{v} \rangle = 2$. Restringindo-nos ao conjunto dos vetores com última coordenada não-nula, obtemos sempre $\langle \mathbf{u}, \mathbf{v} \rangle = 2$.

Vamos considerar primeiro os 7 vetores $\mathbf{u}_1, \mathbf{u}_2 \ldots, \mathbf{u}_7$, cuja última coordenada é 1, e vamos construir uma base de E_8, a partir destes vetores. Nesta construção, faremos $a = 1/\sqrt{2}$. Tome $\mathbf{f}_i = \dfrac{1}{\sqrt{2}}\mathbf{u}_i$; pelo exposto acima,

$$\begin{array}{c} \langle \mathbf{f}_i, \mathbf{f}_j \rangle = 1, \text{ se } i \neq j, \text{ e} \\ \langle \mathbf{f}_i, \mathbf{f}_i \rangle = 2, \text{ para cada } i. \end{array}$$

Está bem perto, mas ainda não é o que precisamos. Agora, tomamos os seguintes vetores:

$$\begin{array}{rcl} \mathbf{e}_1 & = & \mathbf{f}_1, \\ \mathbf{e}_2 & = & \mathbf{f}_2 - \mathbf{f}_1, \\ & \vdots & \\ \mathbf{e}_7 & = & \mathbf{f}_7 - \mathbf{f}_6. \end{array}$$

Das relações anteriores entre os $\mathbf{f}_i's$, tiramos que

$$\begin{array}{lcll} \langle \mathbf{e}_i, \mathbf{e}_{i+1} \rangle & = & -1, & \text{para } i = 1, \ldots, 6, \\ \langle \mathbf{e}_i, \mathbf{e}_{i-1} \rangle & = & -1, & \text{para } i = 2, \ldots, 7, \\ \langle \mathbf{e}_i, \mathbf{e}_j \rangle & = & 0, & \text{se } |i-j| \geq 2, \end{array}$$

e todos os produtos internos de pares de vetores em $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_7\}$ "batem"com o especificado para E_8. Conferindo a matriz de Gram de E_8, vemos que falta apenas mais um vetor $\mathbf{e}_8$ tal que $\langle \mathbf{e}_8, \mathbf{e}_8 \rangle = 2$, $\langle \mathbf{e}_8, \mathbf{e}_5 \rangle = -1$ e $\langle \mathbf{e}_8, \mathbf{e}_i \rangle = 0$, para $i \neq 5, 8$. Resolvendo este sistema de equações, obtemos o vetor

$$\mathbf{e}_8 = \frac{1}{\sqrt{2}}(-1, -1, 0, 0, 1, 0, -1, 0).$$

Como este vetor está em $\Lambda(\widetilde{\mathcal{H}_3})$ (verifique), concluimos que $E_8 = \Lambda(\widetilde{\mathcal{H}_3})$.

Vários outros reticulados importantes podem ser construídos desta forma, como pode ser visto em [36]. Recentemente, vários exemplos foram feitos usando-se generalizações deste método para códigos sobre outros alfabetos.

2.7 Reticulados e Grafos

Um *grafo* Γ consiste de um conjunto de vértices V e um conjunto de arestas A conectando (alguns destes) vértices. Representa-se o grafo geometricamente por pontos (os vértices) ligados por curvas (as arestas) - veja a figura 2.5.

Nesta seção, estamos interessados em uma classe especial de grafos, os *grafos circulantes* . Estes grafos são aplicados no desenho de redes de computadores - os vértices correspondem às máquinas e as arestas representam conexões entre estas máquinas. Também são estudados do ponto de vista teórico, pois, embora sejam exemplos relativamente simples, possuem várias propriedades interessantes. Para apresentá-los, precisamos antes do conjunto dos "inteiros módulo M".

O conjunto $\mathbb{Z}_M$ dos inteiros módulo M, introduzido no capítulo 1, pode ser identificado com o conjunto dos números (na verdade classes) $\{0, 1, 2, \ldots, m-1\}$, com as seguintes operações:

$$a +_M b = \text{resto de } a + b \text{ na divisão por } M,$$

$$a \times_M b = \text{resto de } a \times b \text{ na divisão por } M.$$

Exercício 2.11. *Mostre que*

1. $a +_M b = b +_M a$,
2. $(a +_M b) +_M c = a +_M (b +_M c)$,
3. $(M - a) +_M a = 0$,
4. $0 +_M a = a$.

Estas propriedades mostram que $\mathbb{Z}_M$, com a soma módulo M, é um grupo abeliano finito (ver o Apêndice). Como todos os elementos de $\mathbb{Z}_m$ são múltiplos de um deles (o elemento 1), $\mathbb{Z}_m$ é um *grupo cíclico* .

Para simplificar a notação, daqui em diante usaremos o mesmo sinal de adição para a soma módulo m e a soma em $\mathbb{R}^2$. O produto será usado apenas para abreviar somas, como em $4 \cdot a = a + a + a + a$.

Exercício 2.12. *Prove que toda sequência da forma $\{a, 2a, 3a, \ldots\}$, com $a \in \mathbb{Z}_M$, é cíclica, isto é, mostre que existe um q que satisfaz (i) $qa = 0$ em $\mathbb{Z}_M$, (ii) se $0 < q' < q$, então $q'a \neq 0$ em $\mathbb{Z}_M$). O inteiro q é chamado ordem de a e $\mathbb{Z}_M$.*

Exercício 2.13. *Verifique que 3 também é gerador de $\mathbb{Z}_8$, e que 2 não é (veja Apêndice).*

Agora, podemos apresentar os grafos circulantes definidos sobre $\mathbb{Z}_M$. O grafo circulante $C_M(a_1, a_2, \ldots, a_k)$ é o grafo cujos vértices são os elementos de $\mathbb{Z}_M$, onde a e b são conectados se, e somente se, $b = a \pm a_i$, para algum i. A figura 2.5 mostra o grafo circulante $C_{13}(1, 5)$.

Neste exemplo, vê-se claramente que a bijeção $\tau(a) = a + 1$ preserva todas as arestas, ou seja, se a e b estão conectados, então $\tau(a)$ e $\tau(b)$ também estão (ver também exercício 7). O mesmo vale para $\tau_k(a) = a + k$. Assim, para construir o grafo, basta ligar os $\pm a_i$'s ao 0 e rodar a figura obtida pelos vértices.

Vamos mostrar agora como obter este grafo a partir de um grafo sobre $\mathbb{Z}^2$. Este método tem várias aplicações no estudo de grafos circulantes e códigos em grafos [10, 11, 19].

Dados um reticulado Λ em $\mathbb{R}^2$ e uma base $\beta = \{\mathbf{e}_1, \mathbf{e}_2\}$ deste reticulado, definimos um grafo Γ sobre Λ pela seguinte regra:

$$\mathbf{u} \text{ e } \mathbf{v} \text{ estão conectados se, e somente se, } \mathbf{v} - \mathbf{u} = \pm\mathbf{e}_1 \text{ ou } \pm\mathbf{e}_2.$$

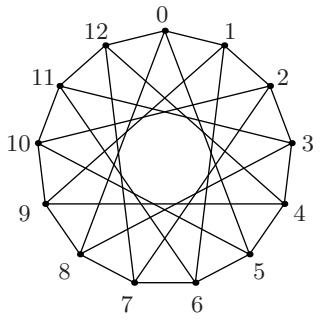


Figura 2.5: O grafo circulante $C_{13}(1, 5)$.

Aplicando isso ao reticulado $\mathbb{Z}^2$ e à base canônica, obtemos uma malha quadrada (infinita); note que as arestas do grafo são as arestas das translações do politopo fundamental. Para tirar um grafo finito daí, basta tomar um conjunto finito de pontos de $\mathbb{Z}^2$ e as arestas correspondentes, mas podemos fazer algo ainda melhor.

Considere um subreticulado Λ' de $\mathbb{Z}^2$ e a relação de equivalência que este define no plano:

$$\mathbf{u} \equiv \mathbf{v} \text{ se, e somente se, } \mathbf{u} - \mathbf{v} \text{ pertence a } \Lambda'.$$

Dito de outro modo, se pudermos obter $\mathbf{v}$ somando a $\mathbf{u}$ um elemento $\mathbf{w}$ de Λ', então $\mathbf{u}$ e $\mathbf{v}$ são equivalentes e diremos que são equivalentes módulo Λ'. Fixando uma base β' para Λ', temos o seguinte: todo ponto de $\mathbb{R}^2$ é equivalente a um ponto que está no politopo gerado por β'. Agora, construímos um grafo *finito* $\Gamma_{\beta'}$ do modo definido abaixo.

Os *vértices* de $\Gamma_{\beta'}$ são definidos por um conjunto $V = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_M\}$ completo de representantes módulo Λ', isto é,
(i) não há nenhum par de pontos equivalentes em V;
(ii) todo ponto de $\mathbb{Z}^2$ é equivalente a um elemento de V.

Um modo simples de encontrar um conjunto destes é tomar os pontos de $\mathbb{Z}^2$ que estão em um politopo fundamental P de Λ' e depois descartar, se necessário, alguns pontos "repetidos" módulo Λ', porque pode haver pontos equivalentes sobre as arestas de P.

As *arestas* de $\Gamma_{\beta'}$ são determinadas pela seguinte regra: dois pontos $\mathbf{u}$ e $\mathbf{v}$ de V são conectados se, e somente se, existirem $\mathbf{u}'$ e $\mathbf{v}'$ de V tais que $\mathbf{u} \equiv \mathbf{u}'$, $\mathbf{v} \equiv \mathbf{v}'$ e $\mathbf{u}'$ e $\mathbf{v}'$ estão conectados no grafo de $\mathbb{Z}^2$.

No conjunto V podemos definir a seguinte operação de soma módulo Λ: dados $\mathbf{u}_i, \mathbf{u}_j \in V$,

$$\mathbf{u}_i + \mathbf{u}_j = \mathbf{u}_k,$$

onde $\mathbf{u}_k$ é o único elemento de V que é equivalente a $\mathbf{u}_i + \mathbf{u}_j$. Pode-se mostrar que esta operação satisfaz as mesmas propriedades que a soma módulo M e que isso faz com que V seja um grupo abeliano também. Nosso interesse é descobrir se também

V é cíclico. Para isso, deve existir um elemento $\mathbf{u}_{i_0}$ tal que, tomando a sequência $\{\mathbf{u}_{i_0}, 2\mathbf{u}_{i_0}, 3\mathbf{u}_{i_0}, \ldots\}$, conseguimos todos os elementos de V (claro que aqui estamos identificando $n\mathbf{u}_i$ com seu correspondente em V). Neste caso, pode-se mostrar que, trocando o vértice $\mathbf{u}_j$ de $\Gamma_{\beta'}$ por k, quando $\mathbf{u}_j \equiv k\mathbf{u}_{i_0}$, obtemos um grafo circulante.

Um resultado que garante que V seja cíclico é o que segue.

Proposição 2.7. *Seja Λ' o reticulado gerado por $\beta' = \{\mathbf{e}_1, \mathbf{e}_2\}$, com $\mathbf{e}_1 = (a, b)$ e $\mathbf{e}_2 = (c, d)$ de $\mathbb{Z}^2$, e seja $\mathbf{u} = (m, n)$ um ponto do paralelogramo gerado por β'. Sejam A a matriz geradora de Λ' com colunas $\mathbf{e}_1$ e $\mathbf{e}_2$ e sejam M_i os determinantes das matrizes obtida de A, substituindo $\mathbf{e}_i$ por $\mathbf{u}$. Então,*

1. *O grafo $\Gamma_{\beta'}$ possui $M = |\det(A)|$ vértices;*
2. *$V = \{k\mathbf{v}\}_{i=0}^{M-1}$ é um conjunto completo de representantes módulo Λ' se, e somente se,* $\mathrm{mdc}(A_1, A_2) = 1$.

Para obter o grafo $C_{13}(1, 5)$ deste modo, tomemos o reticulado Λ' gerado por $\beta' = \{(2, 3), (-3, 2)\}$. O conjunto V consiste da origem e dos pontos no interior do politopo gerado por β' (Figura 2.6).

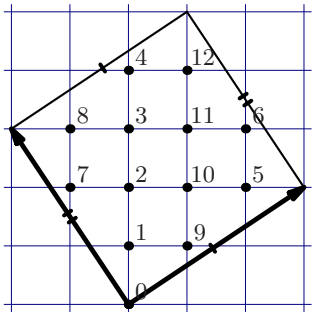


Figura 2.6: Paralelogramo gerado por $\beta' = \{(2, 3), (-3, 2)\}$ e um conjunto completo de representantes módulo Λ'.

Agora, faça o seguinte: tome $\mathbf{u} = (0, 1)$ e a seqüência $\{k\mathbf{u}\}_{k=0}^{12}$; você verá que ela percorre todos os pontos de V. Conectando a e b de $\mathbb{Z}_{13}$, sempre que $a\mathbf{u}$ e $b\mathbf{u}$ estiverem conectados, você irá reconstruir o grafo circulante $C_{13}(1, 5)$.

Este processo pode ser estendido para grafos circulantes com mais arestas de modo natural: para construir $C_n(a_1, a_2, \ldots, a_k)$, definimos um grafo em $\mathbb{Z}^k$ da mesma maneira que fizemos no plano e procuramos um reticulado Λ' conveniente. Pode-se mostrar que este reticulado sempre existe [19] e que esta técnica tem várias aplicações no estudo de grafos circulantes [10, 11, 19].

2.8 Leituras de Aprofundamento e Extensão

Para aprender mais sobre propriedades básicas e exemplos importantes recomendamos os capítulos 1 e 4 de [36] e o capítulo 1 de [13].

Um estudo mais aprofundado depende dos gostos e interesses do leitor; Em geral, quase tudo que foi feito nesta área encontra-se em [36], [4] ou [13]. Uma vertente mais próxima da teoria algébrica de números pode ser estudada nos artigos [1] e [3]; as conexões entre reticulados e grafos podem ser estudadas em [10], [11] e [19].

2.9 Exercícios Complementares

1. Seja Λ o reticulado gerado por $(2,1)$ e $(-1,3)$. Determine a matriz de Gram, o raio de empacotamento ρ e a densidade Δ.

2. Seja Λ gerado por $\mathbf{u} = (a,b)$ e $\mathbf{v} = (-b,a)$, onde tanto a quanto b são não-nulos. Mostre que

   (a) Os vetores de norma mínima são $\pm\mathbf{u}, \pm\mathbf{v}$. Sugestão: determine a norma de um elemento genérico $x\mathbf{u} + y\mathbf{v}$ de Λ.

   (b) A densidade de Λ é $\dfrac{\pi}{4}$.

3. O reticulado A_2 é gerado por $\mathbf{u} = (1,0)$ e $\mathbf{v} = \left(\frac{-1}{2}, \frac{\sqrt{3}}{2}\right)$, e é o mais denso no plano.

   (a) Determine a matriz de Gram associada a esta base.

   (b) Mostre que a norma mínima é igual a 1 e que existem seis vetores de norma mínima. Sugestão: verifique que $||x\mathbf{u} + y\mathbf{v}||^2 = x^2 - xy + y^2$ e procure os x, y inteiros que minimizam esta função.

   (c) Mostre que $\det(A_2) = \frac{3}{4}$.

   (d) Mostre que $\Delta = \frac{\pi}{\sqrt{12}}$.

   (e) Mostre que a região de Voronoi de A_2 é um hexágono.

4. Prove a Proposição 2.1

5. Prove o Lema 2.1.

6. Considerando o reticulado D_n, definido na seção 2.6.2, mostre que $D_n = \Lambda(C_n)$. Para isso, estude os casos 3 e 4 para "chutar" uma base para o caso geral (caso não consiga, dê uma olhadinha em [36]).

7. Seja Γ um grafo circulante. Mostre que

   (a) se a e b estão conectados, então $a+k$ e $b+k$ estão conectados para todo k;

   (b) a e b estão conectados se, e somente se, $a-b$ ou $b-a$ estão conectados ao 0.

Capítulo 3

Códigos Esféricos

3.1 Introdução

Um *código esférico* é um subconjunto finito da esfera unitária euclidiana S^n, contida em $\mathbb{R}^{n+1}$. A razão para que um código esférico seja também chamado de constelação de sinais é que todo conjunto de sinais contínuos pode ser representado por um conjunto de pontos na esfera euclidiana. Esta maneira geométrica de ver os sinais possibilita um manuseio mais fácil desses conjuntos. Um dos principais ingredientes para que a transmissão de um sinal ocorra sem erros é que a distância mínima entre os pontos seja grande. Por isso, a análise de desempenho de uma constelação de sinais passa sempre pelo cálculo de sua distância mínima.

De maneira geral, dada uma dimensão n e um número de pontos M, queremos saber: qual o código esférico $[M, n]$ com a maior distância mínima? Este código é chamado *ótimo* . Achar um código ótimo é um problema bastante difícil. Na esfera euclidiana $S^2 \subset \mathbb{R}^3$, este problema é conhecido como o problema de Tammes. Segundo Sloane [36], Tammes foi um botânico alemão que estudou o número de poros em um grão de pólen. Seu trabalho de 1930, publicado em uma revista de botânica [37] com o título: "On the origin of number and arrangment of the places of exit on the surface of pollen-grains", procurava relações para a distância mínima entre os poros de um pólen. Configurações ótimas de pontos na $S^2 \subset \mathbb{R}^3$ são conhecidas apenas para $M \leq 12$ e $M = 24$, segundo [15]. Todas as outras são as "melhores conhecidas", sem um prova formal de que são ótimas.

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

Este capítulo está dividido da seguinte maneira: na primeira seção, mostramos como representar um conjunto de sinais contínuos como um código esférico. Na

segunda seção, há uma breve explanação da probabilidade de erro e da distância mínima de um código esférico. A terceira seção é dedicada aos limitantes para códigos esféricos, que relacionam distância mínima e cardinalidade. Na quarta, seção falamos dos códigos simplex e biortogonal e, na quinta, sobre códigos de grupo cíclico, uma classe de códigos esféricos com simetrias.

Nesta seção, mostramos como um conjunto de sinais contínuos pode ser visto como um código esférico. Antes do caso geral, abordaremos o problema para um caso especial: um conjunto de sinais com mudança de fase, o PSK.

3.2 Representação Geométrica de Sinais Contínuos

3.2.1 Um exemplo: o M-PSK

PSK é uma sigla, oriunda da língua inglesa, para *Phase-Shift Keying*, uma modulação intimamente ligada às rotações do espaço euclidiano. Suponhamos que uma informação pode ser representada binariamente, por exemplo, ligar e desligar a luz de um quarto, ou, abrir e fechar uma porta. Ligar é "0" e desligar é "1". Vamos associar cada uma destas operações a uma fase de um sinal contínuo, conforme a figura 3.1. Ao "0" associamos a fase zero e ao "1" associamos a fase π. Tais fases, por conseguinte, estão associadas a dois sinais contínuos

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

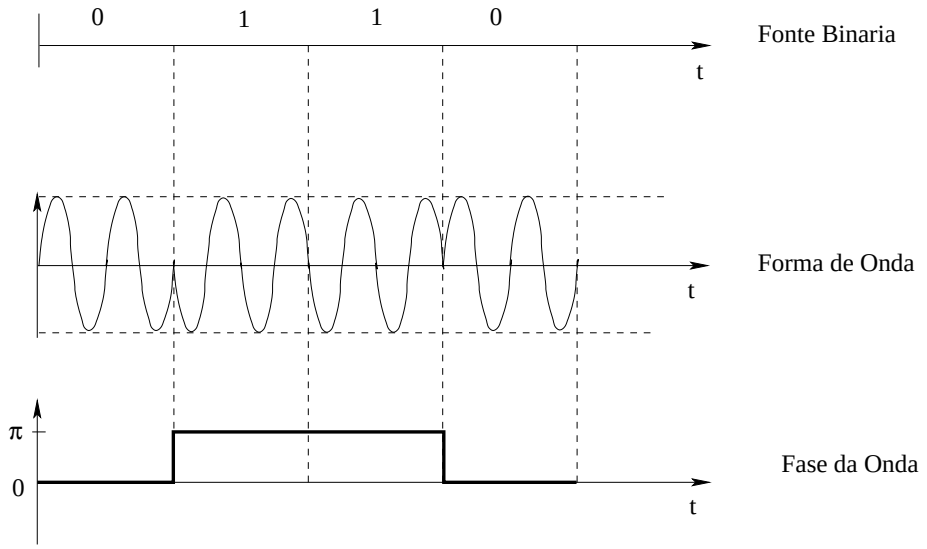


Figura 3.1: Modulação de um 2-PSK

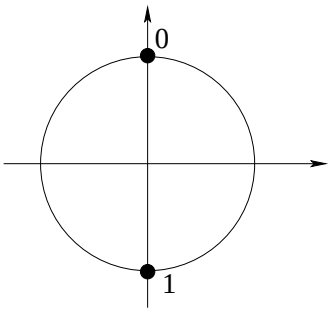


Figura 3.2: Representação geométrica de um 2-PSK

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

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

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

Assim, representamos "0" pelo ponto $(0, 1)$ e "1" pelo ponto $(0, -1)$, conforme figura 3.2.

Esta construção se generaliza para o conjunto de M sinais

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

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

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

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

3.2.2 Representação geométrica de sinais

Seja $\mathcal{S} = \{s_1(t), ..., s_M(t)\}$ um conjunto de sinais formado pelas funções reais contínuas s_i de energia finita, isto é,

$$|s_i| = \int_{-\infty}^{\infty} s_i(t)^2 dt < \infty.$$

Queremos dar uma representação geométrica para $\mathcal{S}$ da mesma maneira que demos para o M-PSK na seção anterior. Para tanto, precisaremos de alguns fatos oriundos da álgebra linear.

Considere $C^0(\mathbb{R})$, o conjunto das funções contínuas reais, e o subconjunto E de $C^0(\mathbb{R})$, formado pelas funções com energia finita. O subconjunto E, com a soma de

funções usual e a multiplicação por números reais, é um espaço vetorial que pode ser munido do produto interno $\langle \cdot, \cdot \rangle$, definido da seguinte maneira:

$$\text{se } f, g \in E, \text{ então } \langle f, g \rangle = \int_{-\infty}^{\infty} f(x)g(x)dx.$$

Deixamos a prova destes fatos nos exercícios abaixo.

Exercício 3.1. *Mostre que conjunto* $E = \{f : \mathbb{R} \to \mathbb{R}; f$ *é contínua e* $\int_{-\infty}^{\infty} f(t)^2 dt < \infty\}$ *é um espaço vetorial. Não se esqueça de demonstrar que a soma de funções pertence a E. Utilize o fato, conhecido como desigualdade de Hölder para* $p = q = 2$*, que se* f *e* g *são funções reais contínuas, então*

$$\int_{-\infty}^{\infty} |f(x)||g(x)|dx \leq \left(\int_{-\infty}^{\infty} |f(x)|^2 dx \right)^{1/2} \left(\int_{-\infty}^{\infty} |g(x)|^2 dx \right)^{1/2}.$$

Exercício 3.2. *Demonstre que o produto de funções* $\langle f, g \rangle = \int_{-\infty}^{\infty} f(x)g(x)dx$ *é um produto interno real em* $E = \{f : \mathbb{R} \to \mathbb{R}; f$ *é contínua e* $\int_{-\infty}^{\infty} f(t)^2 dt < \infty\}$.

Em particular, o espaço vetorial gerado pela constelação de sinais $\mathcal{S}$ é um espaço vetorial com produto interno de dimensão finita. Podemos, portanto, contruir um conjunto de funções ortonormais $\{\phi_i(t)\}_{i=1}^{N}$ através do processo de ortonormalização de Gram-Schmidt, de tal maneira que

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

Assim, para cada sinal contínuo $s_i(t) \in \mathcal{S}$ associamos um vetor

$$(s_{1i}, s_{2i}, s_{3i}, \ldots, s_{Ni}) \in \mathbb{R}^N.$$

Além disso, quando um dos sinais $s_i(t)$ é transmitido através de um canal AWGN[1], o vetor de onda recebido $\widehat{s_i}(t) = s_i(t) + r(t)$, onde $r(t)$ é o ruído acrescido ao sinal pelo canal, pode ser representado pela soma $s_i + r = (s_{1i} + r_1, s_{2i} + r_2, s_{3i} + r_3, \ldots, s_{Ni} + r_N)$, onde r é um vetor aleatório de erro cujas entradas satisfazem a distribuição de probabilidade gaussiana, de maneira que toda a análise de desempenho de um conjunto de sinais é feita em cima do conjunto de coordenadas $\{(s_{1i}, \ldots, s_{Ni}) \in \mathbb{R}^N; i = 1, \ldots, M\}$. Este conjunto é chamado de constelação de sinais. Para maiores detalhes sobre modulações de sinais e suas representações geométricas, veja [40].

3.3 Propriedades Importantes de uma Constelação de Sinais.

Seja $\{\xi_k\}_{k=1}^{M} \subset \mathbb{R}^N$ uma constelação de sinais. Ao transmitir ξ_k, o canal de transmissão acrescenta um erro r ao sinal ξ_k e o receptor recebe $\widehat{\xi_k} = \xi_k + r$. Para recu-

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

perar o sinal transmitido, procuramos saber em qual região de decisão ou região de Voronoy

$$R_i = \{x \in \mathbb{R}^N; ||x - \xi_i|| < ||x - \xi_k||, \text{ para todo } k \neq i\}$$

está $\widehat{\xi_k}$. Se $\widehat{\xi_k} \in R_m$, decidimos por verossimilhança que o sinal transmitido foi ξ_m. Se $m = k$, a transmissão foi um sucesso, pois o canal tinha transmitido ξ_k. Caso contrário, dizemos que houve um erro na transmissão.

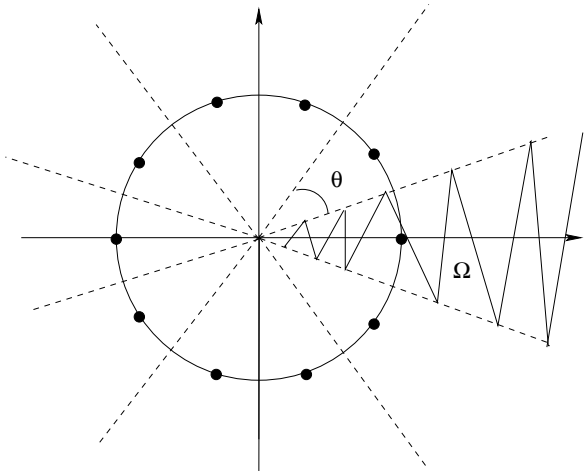


Figura 3.3: Representação geométrica de um 10-PSK e suas regiões de decisão.

O desempenho de uma constelação é medido pela probabilidade de erro na transmissão dos sinais, ou seja,

$$P(e) = P\{\widehat{\xi_k} \notin R_k\}.$$

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

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

Denote $P(c|\xi_j)$ a probabilidade de decisão correta, dado que ξ_j foi transmitido, então

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

Se R_j é a região de decisão de ξ_j, $P(c/\xi_j) = P\{\widehat{\xi_j} \in R_j\}$. Se r for um ruído gaussiano com variância $N_0/2$ e média s_j, têm-se que

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

3.3.1 O limitante de Bhattacharyya

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

Um limitante conhecido para a probabilidade de erro é o limitante de Bhattacharyya ([6], pp 190-192). Se $d_{ij} = |s_i - s_j|$, então

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

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

Boas constelações apresentam probabilidade de erro baixa mesmo quando a transmissão é ruim, ou seja, a variância N_0 do canal é grande. Equivalentemente, elas não precisam dispender muita energia média ε para compensar a transmissão ruim. Uma maneira para isto acontecer é aumentando a distância entre as palavras da constelação. Segue daí um dos primeiros objetivos na construção de uma constelação de sinais S:

$$\text{Maximizar } \; d_{min}(S) = min\{|s_i - s_j|; s_i, s_j \in S, i \neq j\},$$

para um número fixo de pontos e energia média fixada.

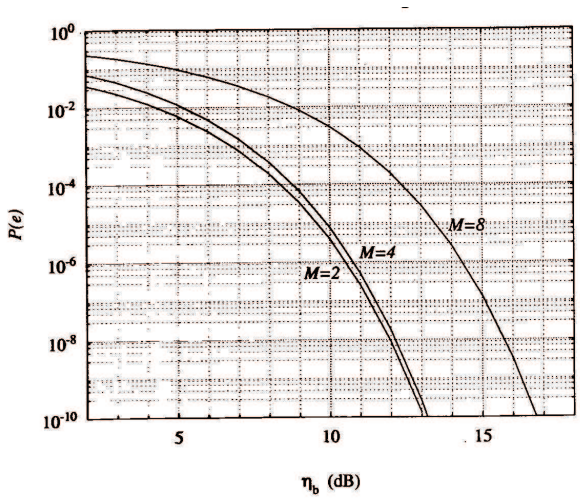


Figura 3.4: Probabilidade de Erro do M-PSK, segundo [6].

Às vezes, não basta aumentar a distância mínima, o número de pontos vizinhos também desempenha papel relevante em $P(e)$. Um exemplo deste fato pode ser encontrado no problema 4.17 de [6].

Para facilitar a procura de boas constelações de sinais, vamos supor que todos os pontos têm energia igual a um, ou seja, a constelação está sobre a esfera unitária.

Exercício 3.3. *A matriz formada pelos produtos escalares de uma constelação é chamada matriz de configuração ou matriz de Gram da constelação S. Essa matriz pode ser vista como o produto $M = a^T a$, onde a é a matriz cujas colunas são os vetores da constelação. Mostre que aumentar a distância entre as palavras de um código esférico é equivalente a diminuir o produto interno $\langle s_i, s_j \rangle$ entre as palavras. Visualize este fato em $\mathbb{R}^2$ e em $\mathbb{R}^3$.*

3.4 Limitantes para Códigos Esféricos

Dados $x, y \in S^n = \left\{x \in R^{n+1}; |x| = 1\right\}$, o ângulo entre estes pontos é $\cos^{-1}(\langle x, y \rangle)$. Se d é a distância mínima em um código esférico, então o ângulo mínimo entre os pontos é

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

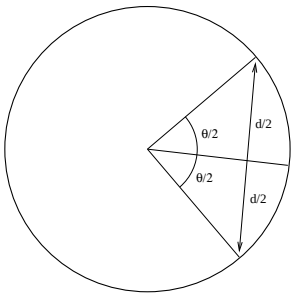


Figura 3.5: Ângulo mínimo e a distância mínima em um código esférico.

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

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

Se o ponto central do chapéu não for importante denotaremos $C(n, \phi)$. É possível demonstrar ([15]) que a área do chapéu esférico é

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

$$k_n = \begin{cases} \frac{(2\pi)^{n/2}}{(n-2)!!} & \text{, se } n = 2, 4, \ldots \\ \frac{2.(2\pi)^{(n-1)/2}}{(n-2)!!} & \text{, se } n = 3, 5, \ldots \end{cases} \quad e \tag{3.4.1}$$

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

Em particular, a área total da esfera é

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

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

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

3.4.1 O limitante da união

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

Proposição 3.1. *Limitante da União*
Seja um código esférico n-dimensional com M pontos e distância mínima $d = 2\sin\theta/2$. Então, em termos do coeficiente k_n, definido em 3.4.1, a seguinte desigualdade deve ser satisfeita:

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

3.4.2 O Limitante de Tóth, Coxeter e Böröckzy

Um dos primeiros limitantes a aparecer para códigos em $\mathbb{R}^3$ foi o de L. Fejes Tóth [39, 38], em 1943. Este limitante é alcançado por códigos com $M = 4, 6$ e 12 pontos, o tetraedro regular ($d^2_{min} = 8/3$), o octaedro ($d^2_{min} = 2$) e o icosaedro ($d^2_{min} = 2 - 2/\sqrt{5}$). Sua construção utiliza estimativas sobre a área de triângulos esféricos.

Proposição 3.2. *Limitante de Tóth*
Em $\mathbb{R}^3$, todo código esférico com M pontos tem ângulo mínimo θ satisfazendo

$$\theta \leq cos^{-1}\frac{\cot^2\frac{M\pi}{6(M-2)}}{2}.$$

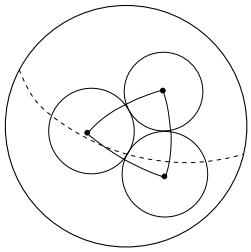


Figura 3.6: Três pontos na esfera S^2 com seus respectivos chapéus esféricos. O limitante de Tóth envolve estimativas para a área não ocupada pelos chapéus, interna ao triângulo formado pelos pontos.

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

Proposição 3.3. *Limitante de Böröckzy - Coxeter*
Todo código esférico em $\mathbb{R}^n$ tem ângulo mínimo ϕ e número de pontos M satisfazendo

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

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

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

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

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

Exercício 3.4. *Os vértices do icosaedro podem ser obtidos através dos deslocamentos cíclicos do ponto $(0, \pm\sigma, \pm 1)$, onde $\sigma = \frac{1-\sqrt{5}}{2}$, perfazendo 12 pontos. Mostre que a distância mínima ao quadrado deste código é $\frac{4\sigma^2}{1+\sigma^2}$. Mostre que este código é ótimo.*

3.4.3 O Limitante de Rankin

Em 1954, Rankin propôs alguns limitantes para códigos esféricos euclidianos que, além de fácil manipulação, possibilitaram demonstrar que duas classes de códigos

esféricos, chamadas simplex e biortogonal, são ótimas. Veremos este fato na próxima seção. Para demonstração desses limitantes, seguiremos a referência [15], além do próprio artigo do autor [32].

Proposição 3.4. *Limitante de Rankin I*
Todo código com M pontos e ângulo mínimo 2ϕ, contido na esfera $S^{n-1} = \{x \in \mathbb{R}^n; |x| = 1\}$, satisfaz as seguintes desigualdades:

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

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

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

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

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

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

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

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

Como o ângulo mínimo é 2ϕ, a distância mínima do código é $d = 2\sin\phi$. Consequentemente, a distância mínima ao quadrado, quando a quantidade de pontos é no máximo $n+1$, deve satisfazer a desigualdade

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

Exercício 3.5. *Reescrever as outras desigualdades em termos da distância mínima do código esférico.*

A seguir, demonstraremos três limitantes equivalentes aos enunciados acima.

Proposição 3.5. *Rankin I*
Qualquer código esférico $\mathcal{X}$ em $\mathbb{R}^n$ com distância mínima ao quadrado ρ e M pontos satisfaz

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

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

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

Por outro lado,

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

■

Proposição 3.6. *Rankin II*
Qualquer código esférico $\mathcal{X}$ em $\mathbb{R}^n$ com distância mínima ao quadrado ρ, satisfazendo $2 < \rho \leq 4$, e M pontos satisfaz

$$M \leq n + 1.$$

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

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

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

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

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

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

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

Proposição 3.7. *Rankin III*
Qualquer código esférico em $\mathbb{R}^n$ com distância mínima ao quadrado $\rho \geq 2$ e M pontos satisfaz

$$M \leq 2n.$$

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

Procurar por códigos esféricos com boa distância mínima e por empacotamentos de chapéus esféricos com melhores densidades são tarefas que nem sempre podem ser confundidas, apesar de suas similaridades. Uma consequência que fica implícita no proposição de Rankin é que se $n+2$ pontos podem ser colocados na esfera S_{n-1}, então $2n$ podem ser colocados com a mesma distância mínima. Isto quer dizer que apesar da densidade do código esférico aumentar, sua distância mínima se mantém constante. Os primeiros a demonstrar esse fato, para $n = 3$, segundo Rankin, foram Schüte e van der Waerden [34] em 1951. O resultado acima, além de estabelecer novos limitantes para códigos esféricos, ilustra essa sutileza entre densidade e distância mínima.

3.5 Os Códigos Simplex e Biortogonal

Duas classes de códigos ótimos geradas por matrizes são amplamente conhecidas: os códigos simplex e biortogonal. Essas classes de códigos, definidas em qualquer dimensão, são generalizações do triângulo isósceles e do quadrado, em dimensão dois, e do tetraedro e octaedro, em dimensão três (figura 3.7).

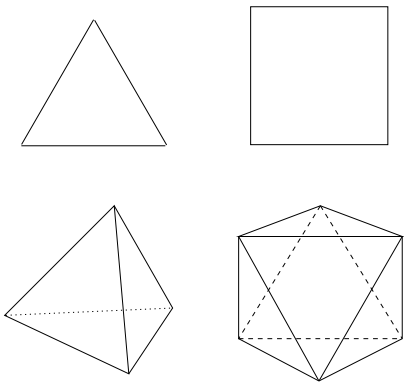


Figura 3.7: Os códigos simplex e biortogonal em dimensão dois e três.

3.5.1 O código simplex

Considere o conjunto $\mathcal{S}_n$ formado pelo ponto $(1,\ldots,1,-n)$ em $\mathbb{R}^{n+1}$ e seus deslocamentos cíclicos, ou melhor, a órbita[2] de $(1,\ldots,1,-n)$ pelo grupo gerado pela matriz

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

onde Id_n é a matriz identidade $n \times n$. Chamaremos $\mathcal{S}_n$ de código simplex.

Da sua definição, segue que, se $x = (x_1,\ldots,x_{n+1}) \in \{S^l(1,\ldots,1,-n)\}_{l=1}^{n+1}$, então

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

Logo, $\mathcal{S}_n$ é um código esférico que mora em um hiperplano de $\mathbb{R}^{n+1}$, portanto em $\mathbb{R}^n$. É de fácil demonstração que o espaço vetorial gerado $\mathcal{S}_n$ tem dimensão n, assim o simplex é um código com $M = n+1$ pontos em $\mathbb{R}^n$, com distância mínima ao quadrado $\frac{2(1+n)^2}{n^2+n} = \frac{2(1+n)}{n}$. O limitante de Rankin, proposição 3.6, assegura que, na esfera S^{n-1} em $\mathbb{R}^n$, o máximo que se consegue com distância mínima ao quadrado $\frac{2(1+n)}{n}$ é colocar $n+1$ pontos. Portanto, o código simplex é o melhor código esférico em $\mathbb{R}^n$ com $n+1$ pontos e distância mínima ao quadrado $\frac{2(1+n)}{n}$.

3.5.2 O código biortogonal

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

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

onde Id_{n-1} é a matriz identidade $(n-1)\times(n-1)$. Chamaremos esse conjunto com $2n$ pontos de *código biortogonal*.

Note que há duas distâncias ao quadrado possíveis entre os pontos de $\mathcal{B}_n$: $2 = |(1,0,\ldots,0) - (0,\ldots,0,1)|^2$ e $4 = |(1,0,\ldots,0) - (-1,0,\ldots,0)|^2$. Assim, $\mathcal{B}_n$ é um código em $\mathbb{R}^n$ com $2n$ pontos e distância mínima ao quadrado 2. Portanto, o código biortogonal satisfaz o limitante de Rankin, proposição 3.7, o que o faz um código ótimo.

[2]Seja G um grupo de matrizes $n \times n$ e $x_0 \in \mathbb{R}^n$. O conjunto $Gx_0 = \{gx_0; g \in G\}$ é chamado órbita de x_0 por G.

3.6 Códigos de Grupo Cíclico

Considere $\mathcal{B}$ uma matriz ortogonal[3] $n \times n$ tal que $\mathcal{B}^M$ é a matriz identidade para algum inteiro M. Se $x_0 \in \mathbb{R}^n$, chamaremos a constelação formada pela órbita de x_0 pelo grupo cíclico gerado por $\mathcal{B}$, $\left\{\mathcal{B}^l x_0\right\}_{l=1}^{M}$, de *código de grupo cíclico* com vetor inicial x_0. Os códigos esféricos gerados por grupos de matrizes ortogonais foram introduzidos por Slepian [35]. Como as matrizes ortogonais são as isometrias do espaço euclidiano, estes códigos são geometricamente uniformes, como definido no capítulo 1. Assim, possuem as regiões de decisão isométricas e uma distribuição de pontos homogênea, o que facilita na hora das análises de desempenho e decodificação.

Exercício 3.6. *Demonstre que, para toda matriz ortogonal $\mathcal{B}$, existe uma matriz ortogonal Q tal que $Q^T\mathcal{B}Q$ é uma matriz diagonal formada pelos blocos*

$$1, -1, \begin{pmatrix} cos(\theta) & -sen(\theta) \\ sen(\theta) & cos(\theta) \end{pmatrix}.$$

As matrizes $\mathcal{B}$ e $Q^T\mathcal{B}Q$ são chamadas similares. Segue que, em dimensão três, uma matriz ortogonal é sempre similar a uma do tipo

$$\begin{pmatrix} cos(\theta) & -sen(\theta) & 0 \\ sen(\theta) & cos(\theta) & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}.$$

Exercício 3.7. *Dois códigos esféricos $\mathcal{X}_1$ e $\mathcal{X}_2$ são equivalentes quando existir uma matriz ortogonal A tal que $\mathcal{X}_1 = A\mathcal{X}_2$. Demonstre que, dado duas matrizes similares, existem dois vetores iniciais tais que os códigos de grupo cíclico associados a eles são equivalentes.*

3.7 Códigos de Grupo Cíclico em Dimensão Três

Os códigos de grupo cíclico em dimensão três possuem propriedades geométricas bastante interessantes. Nos casos em que eles não moram em um plano, eles são anti-primas e só podem ter uma quantidade par de elementos (figura 3.8). Os anti-prismas são prismas com uma das base rotacionadas formados pela órbita de um grupo cíclico de matrizes, cujo gerador é o produto de uma rotação em torno de um eixo e da reflexão pelo plano normal ao eixo, ou seja,

$$\begin{pmatrix} Cos(\theta) & -Sen(\theta) & 0 \\ Sen(\theta) & Cos(\theta) & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

[3] Um matriz é ortogonal quando sua inversa é a sua transposta.

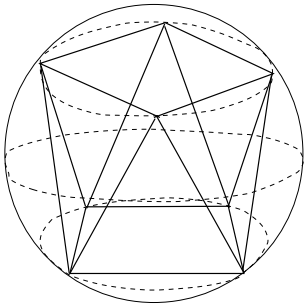


Figura 3.8: O anti-prisma de oito pontos.

Exercício 3.8. *Mostre que toda órbita de um grupo cíclico de matrizes, cujo gerador é da forma*

$$\begin{pmatrix} cos(\theta) & -sen(\theta) & 0 \\ sen(\theta) & cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

é planar.

Uma pergunta importante, proposta por Slepian [35], é: qual é o vetor inicial, para uma dado grupo de matrizes ortogonais, que maximiza a distância mínima do código gerado?

A resposta para a dimensão dois é fácil de ser encontrada. As melhores constelações nesta dimensão são as formadas pelos vértices dos polígonos regulares. Essas constelações podem ser obtidas pelas matrizes de rotação 2×2 e são conhecidas, como vimos na primeira seção, como modulação PSK. Fica claro que, se usamos matrizes de rotação, a escolha independe do vetor inicial e todas as constelações serão isométricas. Entretanto, se o grupo escolhido for o grupo das reflexões pelos eixos coordenados e as retas $y = \pm x$, veremos que a configuração dos pontos dependerá do vetor inicial (figura 3.9).

O problema do vetor inicial ótimo pode ser resolvido em dimensão três no caso dos códigos de grupo cíclico. O resultado é um anti-prisma cuja base é um poliedro regular. O conjunto de vértices deste poliedro é composto por metade dos pontos da constelação.

Seja (x_1, x_2, x_3) o vetor inicial de um código de grupo cíclico com M pontos e matriz geradora

$$\mathcal{A} = \begin{pmatrix} Cos(\frac{2\pi k}{M}) & -Sen(\frac{2\pi k}{M}) & 0 \\ Sen(\frac{2\pi k}{M}) & Cos(\frac{2\pi k}{M}) & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Note que M deve ser par, do contrário, $\mathcal{A}^M$ não seria a identidade. Podemos supor $x_2 = 0$, não alterando a configuração dos pontos da constelação. Deste modo,

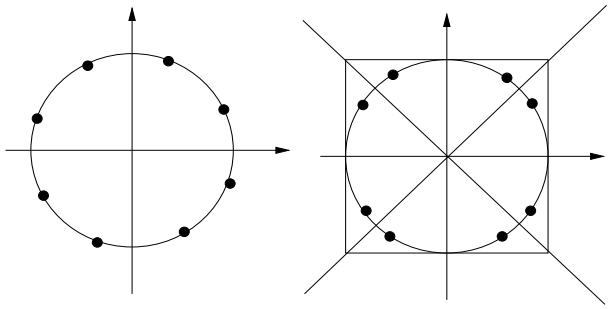


Figura 3.9: Oito pontos gerados por um grupo cíclico e um grupo de reflexões

os pontos do código são

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

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

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

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

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

$$\{2x_1^2(1 - cos(\frac{4\pi}{M})), -2x_1^2(1 + cos(\frac{2\pi}{M})) + 4\}$$

, quando $0 < x_1 < 1$.

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

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

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

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

Ao contrário do caso planar, a distância mínima de um código de grupo cíclico depende do vetor inicial. De fato, o vetor inicial ótimo $(x_1, 0, x_3)$ tem as coordenadas satisfazendo

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

Exercício 3.9. *Demonstre que não existem códigos de grupo não planares em dimensão ímpar com cardinalidade prima. Utilize o fato que todo grupo de cardinalidade prima é cíclico.*

Karlof e Downey descreveram, a menos de equivalências, todos os códigos de grupo tridimensionais que são ótimos em [20].

3.8 Exercícios Complementares

Exercício 3.10. *Construa a expressão em coordenadas do M-PSK, o polígono regular de M lados. Ele pode ser visto como um código de grupo cíclico em $\mathbb{R}^2$ com M pontos. Prove que a distância mínima de um M-PSK independe da escolha do vetor inicial. Note que estamos considerando constelações com energia constante igual a um. Você seria capaz de argumentar por que estas são as melhores constelações em $\mathbb{R}^2$, ou seja, não existe uma constelação com M pontos tal que sua distância mínima é maior que a do polígono regular de M lados?*

Exercício 3.11. *Qual a distância mínima ótima de um código de grupo cíclico em $\mathbb{R}^3$ com oitos pontos, o anti-prisma da figura 3.8? Ela é melhor que o cubo de oito pontos formado pelos pontos $\{(\pm 1, 0, 0), (0, \pm 1, 0), (0, 0, \pm 1)\}$? Faça um desenho de ambos e justifique geometricamente os resultados que você obteve.*

3.9 Leituras de Aprofundamento e Extensão

Um ótimo tratado sobre códigos esféricos é o livro [15], de Ericsson e Zinoviev. Você pode encontrar muita informação sobre o assunto também na página de Neil Sloane: http://www.research.att.com/ njas/. Esta página contém o que de mais novo existe na teoria de reticulados, empacotamentos de esferas e problemas correlatos, e uma lista dos melhores códigos esféricos conhecidos para várias dimensões e quantidade de pontos.

Pode-se encontrar mais detalhes sobre códigos de grupo esféricos na tese de doutorado de R. M. Siqueira [29]. Neste trabalho, o autor estudou códigos de grupo gerados por grupos de matrizes comutativas, procurando limitantes e códigos ótimos, tal como fizemos aqui em casos particulares. O artigo de Slepian [35] pode ser lido com algum conhecimento em álgebra linear e teoria de grupos. A maioria das perguntas fundamentais da teoria são encontradas lá.

Capítulo 4

Códigos Quânticos

4.1 Introdução

Este capítulo faz uma introdução a uma área recente da teoria de códigos: os códigos quânticos. Para tornar o texto auto-suficiente, apresentamos as ferramentas necessárias para se ter uma compreensão inicial dos problemas e dos conceitos da área.

Os postulados da mecânica quântica são apresentados de uma maneira simplificada, dando ênfase a sua estrutura matemática. Baseados neles, discutimos três códigos quânticos: o código de inversão de bit, o código de inversão de fase e o código de Shor.

4.2 Os Postulados da Mecânica Quântica

A mecânica quântica é a parte da física que descreve o comportamento de átomos e partículas. Os seus postulados foram desenvolvidos através de um longo processo de erros e suas correções. Caso você não consiga entender o real significado deles, não se preocupe. Mesmo para os especialistas, essa é uma questão não resolvida [22]. Inicialmente, aceite-os como sendo a estrutura matemática que usaremos para iniciar o estudo sobre códigos quânticos.

Postulado 1: Existe um espaço vetorial complexo, com produto interno, associado a qualquer sistema físico *fechado* (sistema que não interage com outros sistemas). Um estado desse sistema é completamente descrito por um vetor unitário, chamado *vetor de estado*.

O sistema quântico que nos interessa é o *bit quântico*, ou *q-bit*, cujo espaço vetorial associado é o $\mathbb{C}^2$, com o produto interno usual. Uma base ortonormal para esse espaço pode ser dada pelos vetores $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, que serão representados

usando a *notação de Dirac* [22]:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

e

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Existem várias maneiras para a representação física de um q-bit [22]. Entretanto, direcionaremos nosso estudo apenas sobre a sua representação matemática. Ou seja, um q-bit é um vetor unitário de $\mathbb{C}^2$. Um estado arbitrário $|\psi\rangle$ nesse sistema pode ser descrito por

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

onde α e β são números complexos. A base $\{|0\rangle, |1\rangle\}$ é chamada de *base computacional* e o vetor $|\psi\rangle$ é chamado de uma *superposição* dos vetores $|0\rangle$ e $|1\rangle$, com *amplitudes* α e β (usaremos os termos vetor e estado indistintamente).

Exercício 4.1. *Demonstre que a condição de* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ *ser unitário é equivalente a* $|\alpha|^2 + |\beta|^2 = 1$.

O nome q-bit vem do fato de que o bit quântico pode ser visto como uma generalização do bit clássico, que assume apenas 2 estados: 0 ou 1. A diferença entre eles é que um q-bit pode, além dos estados $|0\rangle$ e $|1\rangle$, assumir uma quantidade infinita de estados!

Postulado 2: A evolução de um sistema quântico fechado é descrita por um operador linear que preserva o produto interno (operador *unitário)*. Ou seja, o estado $|\psi_1\rangle$ do sistema, no tempo t_1, está relacionado ao estado $|\psi_2\rangle$, no tempo t_2, através de um operador unitário U que depende apenas de t_1 e t_2. Isto é,

$$|\psi_2\rangle = U|\psi_1\rangle.$$

Existe um operador unitário que transforma o estado $|0\rangle$ em $|1\rangle$ e o estado $|1\rangle$ em $|0\rangle$. Esse operador é denotado por X e sua representação matricial, na base computacional, é dada por

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{4.2.1}$$

Exercício 4.2. *O que acontecerá se o operador* X *for aplicado sobre um q-bit genérico?*

Outro exemplo de um operador unitário sobre um q-bit é o operador Z, cuja representação matricial, também na base computacional, é dada por

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{4.2.2}$$

Exercício 4.3. *O que acontecerá se o operador Z for aplicado sobre um q-bit genérico?*

Os operadores X e Z, quando aplicados sobre o estado $|0\rangle$, ainda retornam estados da base computacional $\{|0\rangle, |1\rangle\}$. Ou seja,

$$X|0\rangle = |1\rangle$$

e

$$Z|0\rangle = |0\rangle.$$

Entretanto, existe um operador unitário H, cuja representação matricial, na base computacional, é dada por

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

que produz uma superposição de estados, mesmo quando aplicado sobre o estado $|0\rangle$. Esse operador é chamado operador *Hadamard*.

Exercício 4.4. *Demonstre que*

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Para prosseguirmos, precisamos definir três conceitos: *dual, produto interno* e *produto externo* . O dual de um vetor $|\varphi\rangle \in \mathbb{C}^n$, denotado por $\langle\varphi|$, é o vetor transposto de $|\varphi\rangle$ com os elementos substituídos pelos seus conjugados. Ou seja,

$$\langle\varphi| = |\varphi\rangle^\dagger.$$

Dados dois vetores $|\varphi\rangle, |\psi\rangle \in \mathbb{C}^n$, o produto interno $\langle\varphi|\psi\rangle$ e o produto externo $|\varphi\rangle\langle\psi|$ são definidos, respectivamente, por

$$\langle\varphi|\psi\rangle = |\varphi\rangle^\dagger|\psi\rangle$$

e

$$|\varphi\rangle\langle\psi| = |\varphi\rangle|\psi\rangle^\dagger.$$

Note que $|\varphi\rangle, |\psi\rangle$ são vetores "coluna" e $\langle\varphi|, \langle\psi|$ são vetores "linha". Exemplos:

$$\langle 0|1\rangle = 0$$

e

$$|0\rangle\langle 1| = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

Exercício 4.5. *Considere dois q-bits $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ e $|\psi\rangle = \gamma|0\rangle + \delta|1\rangle$. Verifique que*

$$\langle\varphi|\psi\rangle = \begin{bmatrix} \alpha^* & \beta^* \end{bmatrix} \begin{bmatrix} \gamma \\ \delta \end{bmatrix} = \alpha^*\gamma + \beta^*\delta$$

e

$$|\varphi\rangle\langle\psi| = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \begin{bmatrix} \gamma^* & \delta^* \end{bmatrix} = \begin{bmatrix} \alpha\gamma^* & \alpha\delta^* \\ \beta\gamma^* & \beta\delta^* \end{bmatrix},$$

onde z^* é o conjugado de z.

A interpretação física do q-bit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, para α e β não nulos, é que ele está simultaneamente nos estados $|0\rangle$ e $|1\rangle$! Pelo postulado 2, já sabemos que, aplicando um operador unitário sobre o estado $|\psi\rangle$, o novo estado ainda será uma superposição dos estados $|0\rangle$ e $|1\rangle$. Entretanto, se fizermos uma medida sobre $|\psi\rangle$, o sistema deixará de ser fechado, pois o ato de medir provoca uma interação com o sistema. Para considerar esse fato, existe um terceiro postulado.

Postulado 3: As medidas sobre sistemas quânticos são descritas por operadores *hermitianos* M ($M^\dagger = M$), chamados *observáveis*. Pelo fato de M ser hermitiano, podemos escrever

$$M = \sum_{i=1}^{n} \lambda_i |i\rangle\langle i|,$$

onde $\{|i\rangle\}$, $i = 1, ..., n$, é uma base ortonormal de autovetores de M com os respectivos autovalores λ_i [22]. Os possíveis resultados da medida correspondem aos autovalores λ_i de M. Supondo que o resultado da medida seja "λ_i", o estado $|\psi_{\lambda_i}\rangle$, após a medida, é dado por

$$|\psi_{\lambda_i}\rangle = \frac{(|i\rangle\langle i|)|\psi\rangle}{\sqrt{p_{\lambda_i}}}, \tag{4.2.3}$$

onde $|\psi\rangle$ é o estado anterior à medida e p_{λ_i} é a probabilidade de se obter "λ_i", dada por

$$p_{\lambda_i} = \langle\psi|(|i\rangle\langle i|)|\psi\rangle. \tag{4.2.4}$$

Exercício 4.6. *Demonstre que* $(|i\rangle\langle i|)|\psi\rangle = (\langle i|\psi\rangle)\,|i\rangle$.

Exercício 4.7. *Demonstre que* $\langle\psi|(|i\rangle\langle i|)|\psi\rangle = (\langle\psi|i\rangle)(\langle i|\psi\rangle)$.

Na realidade, a medida descrita no Postulado 3, chamada *medida projetiva*, é um caso particular de uma medida mais geral [22]. Para os nossos propósitos, será perfeitamente suficiente.

Vejamos um exemplo. Façamos uma medida de um q-bit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, usando o observável Z, dado em (4.2.2), que pode ser escrito como

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

Usando (4.2.3) e (4.2.4), temos:

$$p_1 = \left(\alpha^\dagger\langle 0|0\rangle + \beta^\dagger\langle 1|0\rangle\right)\left(\alpha\langle 0|0\rangle + \beta\langle 0|1\rangle\right) = |\alpha|^2$$

e

$$|\psi_1\rangle = \frac{\alpha\langle 0|0\rangle|0\rangle + \beta\langle 0|1\rangle|0\rangle}{|\alpha|} = \frac{\alpha}{|\alpha|}|0\rangle.$$

Exercício 4.8. *Verifique todas as passagens acima.*

De forma similar, podemos obter

$$p_{-1} = |\beta|^2$$

e

$$|\psi_{-1}\rangle = \frac{\beta}{|\beta|}|1\rangle.$$

Resumindo: usando o observável Z para fazer uma medida de um q-bit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, podemos obter o estado $\frac{\alpha}{|\alpha|}|0\rangle$, com probabilidade $|\alpha|^2$, ou o estado $\frac{\beta}{|\beta|}|1\rangle$, com probabilidade $|\beta|^2$ (em termos de observação, os estados $\frac{\alpha}{|\alpha|}|0\rangle$ e $|0\rangle$ são idênticos, assim como os estados $\frac{\beta}{|\beta|}|1\rangle$ e $|1\rangle$ [22]).

Para descrever estados com mais de um q-bit, temos o postulado 4.

Postulado 4: O estado composto por n estados $|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_n\rangle$ é o *produto tensorial* $|\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$.

Para os nossos propósitos, definimos o produto tensorial $A \otimes B$, entre as matrizes $A \in \mathbb{C}^{m\times n}$ e $B \in \mathbb{C}^{p\times q}$, como sendo a matriz

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix},$$

onde A_{ij} é o elemento da linha i e da coluna j de A. Note que a dimensão da matriz $A \otimes B$ é $mp \times nq$ e que o produto tensorial não é comutativo. Por exemplo,

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

e

$$|1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Exercício 4.9. *Demonstre as seguintes propriedades do produto tensorial ($\alpha \in \mathbb{C}$; $|v\rangle, |v_1\rangle, |v_2\rangle \in \mathbb{C}^m$; $|w\rangle, |w_1\rangle, |w_2\rangle \in \mathbb{C}^n$):*

1. $\alpha(|v\rangle \otimes |w\rangle) = (\alpha|v\rangle) \otimes |w\rangle = |v\rangle \otimes (\alpha|w\rangle)$,
2. $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = (|v_1\rangle \otimes |w\rangle) + (|v_2\rangle \otimes |w\rangle)$,

3. $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = (|v\rangle \otimes |w_1\rangle) + (|v\rangle \otimes |w_2\rangle)$.

Usaremos também a notação $|v\rangle|w\rangle$ ou $|vw\rangle$ para o produto tensorial $|v\rangle \otimes |w\rangle$.

Existe uma outra formulação dos postulados da mecânica quântica em termos do *operador densidade* [22]. Essa nova formulação é útil para descrever sistemas quânticos cujos estados não são completamente conhecidos. Por exemplo, suponha que um sistema quântico esteja em um do estados $|\psi_1\rangle, ..., |\psi_n\rangle$, com as respectivas probabilidades $p_1, ..., p_n$. O operador densidade do sistema é dado por

$$\rho = \sum_{i=1}^{n} p_i |\psi_i\rangle\langle\psi_i|.$$

No nosso contexto, utilizaremos apenas o operador densidade de um sistema cujo estado está bem definido, ou seja, está no estado $|\psi\rangle$, com probabilidade 1. Nesse caso, o operador densidade é dado por

$$\rho = |\psi\rangle\langle\psi|.$$

4.3 Códigos Quânticos

A construção de códigos clássicos corretores de erros é baseada na possibilidade de copiar e observar um bit, sem que seu estado, 0 ou 1, seja alterado.

Considere um operador unitário C que copie um q-bit $|\psi\rangle$, definido por

$$C\left(|\psi\rangle|0\rangle\right) = |\psi\rangle|\psi\rangle. \tag{4.3.5}$$

Usando C para copiar outro q-bit $|\varphi\rangle$, temos:

$$C\left(|\varphi\rangle|0\rangle\right) = |\varphi\rangle|\varphi\rangle. \tag{4.3.6}$$

Calculando o produto interno entre (4.3.5) e (4.3.6), obtemos:

$$\langle\psi|\varphi\rangle = \left(\langle\psi|\varphi\rangle\right)^2 \Rightarrow \langle\psi|\varphi\rangle = 1 \text{ ou } \langle\psi|\varphi\rangle = 0.$$

Ou seja, não existe um operador unitário capaz de copiar q-bits arbitrários. Este resultado é conhecido como o Teorema da Não-Clonagem [22].

Exercício 4.10. *Verifique todas as passagens acima.*

Conclusão: além de ser impossível copiar um q-bit genérico $|\psi\rangle$, o postulado 3 diz que uma medida sobre $|\psi\rangle$ provoca uma alteração irreversível em seu estado. Entretanto, mesmo com essas "limitações", é possível contruir códigos quânticos.

4.3.1 Código de inversão de bit

Suponha que um q-bit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ seja enviado através de um canal que, com probabilidade $p > 0$, altera o estado do q-bit para $X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$ (*canal de inversão de bit*). Para definirmos o *código de inversão de bit* [22], inicialmente, codificamos o q-bit $|\psi\rangle$ em um estado de 3 q-bits, dado por $|\psi'\rangle = \alpha|000\rangle + \beta|111\rangle$. Isso pode ser feito usando o operador unitário U, definido por

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}. \tag{4.3.7}$$

Isto é,

$$U\left((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \otimes |0\rangle\right) = U\left(\alpha|000\rangle + \beta|100\rangle\right) = \alpha|000\rangle + \beta|111\rangle.$$

Em termos matriciais, temos:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ 0 \\ 0 \\ 0 \\ \beta \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \beta \end{bmatrix} = \alpha \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Exercício 4.11. *Verifique todas as passagens acima.*

Agora, cada um dos 3 q-bits do estado $|\psi'\rangle = \alpha|000\rangle + \beta|111\rangle$ é enviado por 3 canais de inversão de bit independentes onde, no máximo, apenas um dos q-bits é alterado. Em seguida, façamos duas medidas, definidas pelos observáveis $Z \otimes Z \otimes I$ e $I \otimes Z \otimes Z$, onde I é o operador identidade.

Exercício 4.12. *Demonstre que os autovalores dos observáveis $Z \otimes Z \otimes I$ e $I \otimes Z \otimes Z$ são 1 e -1.*

O observável $Z \otimes Z \otimes I$ pode ser representado por

$$Z \otimes Z \otimes I = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I.$$

Ou seja, podemos interpretar a medida $Z \otimes Z \otimes I$ como sendo uma comparação entre os dois primeiros q-bits. Se der 1, indicará que os q-bits têm o mesmo valor; se der -1, indicará que os q-bits são distintos. De forma similar, a medida

$$I \otimes Z \otimes Z = I \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|) - I \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|)$$

faz uma comparação entre os dois últimos q-bits. Novamente, se der 1, indicará que os q-bits têm o mesmo valor e, se der -1, indicará que os q-bits são distintos.

Combinando o resultado das duas medidas, podemos determinar se houve alguma alteração dos q-bits. Havendo alteração, além de identificarmos o q-bit alterado, poderemos também corrigi-lo. Representando por (m_1, m_2), o resultado das 2 medidas, respectivamente, temos quatro possibilidades:

1. $(1, 1)$ indica que não houve nenhuma alteração;
2. $(-1, 1)$ indica alteração no 1° q-bit;
3. $(-1, -1)$ indica alteração no 2° q-bit;
4. $(1, -1)$ indica alteração no 3° q-bit.

Para fazer a correção, caso necessário, bastará aplicar o operador X sobre o q-bit alterado, pois $X^{-1} = X$.

4.3.2 Código de inversão de fase

Agora, suponha que um q-bit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ seja enviado através de um canal que, com probabilidade $p > 0$, altera o estado do q-bit para $Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$ (*canal de inversão de fase*). Antes de definirmos o *código de inversão de fase* [22], apliquemos o operador Z sobre os estados $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$:

$$Z\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

e

$$Z\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Exercício 4.13. *Demonstre que os estados* $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ *e* $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ *formam uma base ortonormal de* $\mathbb{C}^2$.

Para simplificar a notação, definamos

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

e

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Dessa forma,

$$Z|+\rangle = |-\rangle$$

e

$$Z|-\rangle = |+\rangle.$$

Ou seja, na base $\{|+\rangle, |-\rangle\}$, o operador Z atua como o operador X (canal de inversão de bit).

Faremos, então, os mesmos procedimentos realizados para o canal de inversão de bit, considerando a base $\{|+\rangle, |-\rangle\}$ no lugar da base $\{|0\rangle, |1\rangle\}$. Para fazer a mudança de base, usaremos o operador H, pois

$$H|0\rangle = |+\rangle,\ H|1\rangle = |-\rangle$$

e

$$H|+\rangle = |0\rangle,\ H|-\rangle = |1\rangle.$$

Exercício 4.14. *Demonstre que* $H^{-1} = H$.

Inicialmente, codificamos o q-bit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ em um estado de 3 q-bits, dado por $|\psi'\rangle = \alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle$. Podemos fazer isso usando o operador H e o mesmo operador U, definido em (4.3.7):

$$\begin{aligned}(H \otimes H \otimes H)\,(U\,((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \otimes |0\rangle)) &= (H \otimes H \otimes H)\,(\alpha|000\rangle + \beta|111\rangle) \\ &= \alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle.\end{aligned}$$

Cada um dos 3 q-bits do estado $|\psi'\rangle = \alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle$ é enviado por 3 canais de inversão de fase independentes onde, no máximo, apenas um dos q-bits é alterado. Em seguida, façamos duas medidas, definidas pelos observáveis

$$H^{\otimes 3}\,(Z \otimes Z \otimes I)\,H^{\otimes 3}$$

e

$$H^{\otimes 3}\,(I \otimes Z \otimes Z)\,H^{\otimes 3},$$

onde $H^{\otimes 3} = H \otimes H \otimes H$.

Exercício 4.15. *Demonstre que os autovalores dos observáveis* $H^{\otimes 3}\,(Z \otimes Z \otimes I)\,H^{\otimes 3}$ *e* $H^{\otimes 3}\,(I \otimes Z \otimes Z)\,H^{\otimes 3}$ *são* 1 *e* -1.

Os observáveis $H^{\otimes 3}\,(Z \otimes Z \otimes I)\,H^{\otimes 3}$ e $H^{\otimes 3}\,(I \otimes Z \otimes Z)\,H^{\otimes 3}$ podem ser representados, respectivamente, por

$$\begin{aligned}H^{\otimes 3}\,(Z \otimes Z \otimes I)\,H^{\otimes 3} = H^{\otimes 3}((&|{+}{+}\rangle\langle{+}{+}| + |{-}{-}\rangle\langle{-}{-}|) \otimes I \\ &- (|{+}{-}\rangle\langle{+}{-}| + |{-}{+}\rangle\langle{-}{+}|) \otimes I)H^{\otimes 3}\end{aligned}$$

e

$$\begin{aligned}H^{\otimes 3}\,(I \otimes Z \otimes Z)\,H^{\otimes 3} = H^{\otimes 3}(&I \otimes (|{+}{+}\rangle\langle{+}{+}| + |{-}{-}\rangle\langle{-}{-}|) \\ &- I \otimes (|{+}{-}\rangle\langle{+}{-}| + |{-}{+}\rangle\langle{-}{+}|))H^{\otimes 3}.\end{aligned}$$

Combinando o resultado das duas medidas, da mesma forma que fizemos para o canal de inversão de bit, podemos determinar se houve alguma alteração dos q-bits. Havendo alteração, além de identificarmos o q-bit alterado, poderemos também corrigi-lo. Novamente representando por (m_1, m_2), o resultado das 2 medidas, respectivamente, temos quatro possibilidades:

1. $(1, 1)$ indica que não houve nenhuma alteração;
2. $(-1, 1)$ indica alteração no 1° q-bit;
3. $(-1, -1)$ indica alteração no 2° q-bit;
4. $(1, -1)$ indica alteração no 3° q-bit.

Para fazer a correção, caso necessário, bastará aplicar o operador HXH sobre o q-bit alterado.

4.3.3 Código de Shor

Os códigos de inversão de bit e de inversão de fase corrigem erros específicos de um q-bit. Entretanto, combinando esses dois códigos, podemos construir um novo código, chamado *código de Shor* [22], capaz de corrigir qualquer tipo de alteração de um q-bit!

Inicialmente, codificamos o q-bit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ em um estado de 3 q-bits, dado por $|\psi'\rangle = \alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle$. Em seguida, codificamos cada um desses q-bits da seguinte forma:

$$|+\rangle \rightarrow \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

e

$$|-\rangle \rightarrow \frac{|000\rangle - |111\rangle}{\sqrt{2}}.$$

O resultado será um estado de 9 q-bits dado por

$$\begin{aligned}|\psi''\rangle = \frac{1}{2\sqrt{2}}(&\alpha\left((|000\rangle + |111\rangle)\left(|000\rangle + |111\rangle\right)\left(|000\rangle + |111\rangle\right)\right)\\ &+ \beta\left((|000\rangle - |111\rangle)\left(|000\rangle - |111\rangle\right)\left(|000\rangle - |111\rangle\right)\right)).\end{aligned}$$

Exercício 4.16. *Defina um operador unitário que transforme* $|\psi\rangle$ *em* $|\psi''\rangle$.

Para descrever o código de Shor, usaremos uma ferramenta chamada *operações quânticas* [22], utilizada para tratar sistemas abertos.

Uma operação quântica ε pode ser descrita pela *representação de operador soma* [22], dada por

$$\varepsilon(\rho) = \sum_{i=1}^{n} E_i \rho E_i^{\dagger},$$

onde

$$\sum_{i=1}^{n} E_i E_i^{\dagger} = I.$$

Os operadores $\{E_i\}$, $i = 1, ..., n$, são os *elementos de operação* de ε, I é o operador identidade e ρ é o operador densidade do sistema.

Exercício 4.17. *Demonstre que os operadores unitários U, representados por*

$$\varepsilon_U(\rho) = U\rho U^\dagger,$$

e as medidas descritas pelos observáveis M, representadas por

$$\varepsilon_M(\rho) = \sum_{i=1}^{n} |i\rangle\langle i|\rho|i\rangle\langle i|,$$

onde $M = \sum_{i=1}^{n} \lambda_i |i\rangle\langle i|$, são exemplos de operações quânticas.

Além de representarem os operadores unitários, descritos no postulado 2, e as medidas, descritas no postulado 3, as operações quânticas também são utilizadas para representar as alterações provocadas pela passagem de um q-bit em um canal qualquer.

Como vimos acima, antes da passagem do q-bit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ por um canal qualquer, ele é codificado como

$$\begin{aligned}|\psi''\rangle = \frac{1}{2\sqrt{2}}(&\alpha\left((|000\rangle + |111\rangle)\left(|000\rangle + |111\rangle\right)\left(|000\rangle + |111\rangle\right)\right)\\ &+ \beta\left((|000\rangle - |111\rangle)\left(|000\rangle - |111\rangle\right)\left(|000\rangle - |111\rangle\right)\right)).\end{aligned}$$

Vamos considerar o caso em que apenas o primeiro q-bit de $|\psi''\rangle$ esteja sujeito a um ruído qualquer. O estado desse q-bit, após a passagem pelo canal, será descrito por uma operação quântica ε, dada por

$$\varepsilon(|\psi''\rangle\langle\psi''|) = \sum_{i=1}^{n} E_i|\psi''\rangle\langle\psi''|E_i^\dagger,$$

onde $\{E_i\}$, $i = 1, ..., n$, são os elementos de operação de ε.

Exercício 4.18. *Demonstre que cada operador E_i, $i = 1, ..., n$, pode ser representado como uma combinação linear dos operadores I, X, Z e XZ.*

Considerando a atuação de um operador E_i, $i = 1, ..., n$, sobre o primeiro q-bit de $|\psi''\rangle$, podemos representá-lo como uma combinação linear dos operadores I, X, Z e XZ. O estado $E_i|\psi''\rangle$ pode, então, ser escrito como uma superposição de quatro termos:

$$|\psi''\rangle,\ X|\psi''\rangle,\ Z|\psi''\rangle \text{ e } XZ|\psi''\rangle.$$

Fazendo uma medida do estado $E_i|\psi''\rangle$ (descreva essa medida), obtemos apenas um desses termos. Para recuperar o q-bit original, basta usar os códigos de inversão de bit e de inversão de fase! Casos mais gerais são considerados em [22].

Exercício 4.19. *Defina o código associado ao canal definido pelo operador XZ.*

4.4 Leituras de Aprofundamento e Extensão

Este capítulo foi baseado, principalmente, nas referências [22] e [26]. Além de conter mais detalhes do que aqui foi exposto, elas apresentam outros tópicos da área de computação e informação quântica. A referência [31] apresenta uma boa visão geral dessa área, sem a formalização matemática. Outros textos importantes são listados em [7, 21, 27].

Apêndice

Neste apêndice apresentamos de forma sucinta algumas definições e propriedades utilizadas ao longo dos quatro capítiulos deste livro com algumas referências.

Um *grupo* é um conjunto G com uma operação $*$, isto é, uma aplicação $* : G \times G \to G$, tal que

1. $(x * y) * z = x * (y * z)$
2. Existe um elemento e tal que $x * e = e * x = x$
3. Para cada $x \in G$, existe um elemento x^{-1} (o inverso de g) tal que $x * x^{-1} = x^{-1} * x = e$

Se a operação for comutativa, ou seja, $x * y = y * x$ para todo x e y em G, chamamos o grupo de *abeliano*.

Um subgrupo H de G é um subconjunto de G para o qual valem

1. e está em H.
2. Se h_1 e h_2 estão em H, então $h_1 * h_2$ também está em H.
3. Se h está em H, então h^{-1} está em H.

A ordem de G é o número de elementos de G e é denotada por $|G|$.

Proposição 4.1. *(Lagrange) Se G é um grupo finito e H é um subgrupo de G, então $|G|$ é múltiplo de $|H|$.*

Para $g \in G$, definimos $g^n = g * g * \ldots * g$ (n termos) para $n > 0$, $g^m = (g^{-1})^{-m}$ para $m < 0$, e $g^0 = e$. Esta definição permite estender várias propriedades de potências de números para potências de elementos de grupos; verifica-se facilmente, por exemplo, que $g^{m+n} = g^m * g^n$.

Dado g em G, o *subgrupo cíclico* gerado por g é o conjunto

$$< g >= \{g^n; n \in \mathbb{Z}\}$$

Pode-se mostrar que este conjunto é um subgrupo de G. Se existir um elemento g tal que $G = < g >$, diremos que G é um *grupo cíclico*. Se $< g >$ é finito e tem M elementos, então $< g >= \{e, g, g^2, \ldots, g^{M-1}\}$. Diremos que M é a ordem de g. Pela

proposição 4.1, a ordem de g é um divisor de $|G|$. No capítulo 3 vimos exemplos dos grupos cíclcicos $\mathbb{Z}_m$, dos inteiros módulo m com a operação soma.

Um *anel* (comutativo e com unidade) é um conjunto A com duas operações, soma e produto, que satisfazem:

1. $x + y = y + x$
2. $x + (y + z) = (x + y) + z$
3. Existe um elemento 0 tal que $0 + x = x + 0 = 0$
4. Para cada $x \in A$, existe um elemento $-x$ tal que $x + (-x) = (-x) + x = 0$
5. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. $x \cdot y = y \cdot x$
7. Existe um elemento $1 \neq 0$ tal que $x \cdot 1 = 1 \cdot x = x$
8. $x \cdot (y + z) = x \cdot y + x \cdot z$,

Note que as quatro primeiras dizem que A é um grupo abeliano com relação à adição. No capítulo 1, utilizamos o anel dos inteiros módulo m, $\mathbb{Z}_m$ com as operações de soma e multiplicação induzidas do anel dos inteiros $\mathbb{Z}$ Se um anel satisfizer a propriedade extra de que, para cada $x \neq 0$, existe um elemento x^{-1} tal que $x \cdot x^{-1} = 1$, este anel recebe o nome de *corpo*; neste caso, costuma-se denotá-lo por F (ou K). $\mathbb{Z}_m$ é um corpo se, e somente se, m for um número primo [18].

Boa parte do que se faz em álgebra linear sobre $\mathbb{R}$ ou $\mathbb{C}$ pode ser feita sobre qualquer corpo F; a definição geral de espaço vetorial sobre F é a mesma de espaço vetorial sobre $\mathbb{R}$ ou $\mathbb{C}$, bastando trocar o que se refere a escalares em $\mathbb{R}$ (ou $\mathbb{C}$) por escalares em F. Em especial, se F é um corpo, o conjunto

$$F^n = \{(a_1, a_2, \ldots, a_n); a_i \in F\}$$

é um espaço vetorial sobre F, do mesmo modo que $\mathbb{R}^n$ é espaço vetorial real.

Proposição 4.2. *Se F é finito, $|F| = q$ o número de elementos de um subespaço de dimesão k de F^n é q^k Referência: [Abramo]*

Uma operação elementar por colunas é uma operação onde substituimos uma coluna C_i de uma matriz pela combinação de colunas $C_i + kC_j$, ou permutamos duas colunas C_i e C_j.

Proposição 4.3. *Toda matriz $A_{n\times k}$, $k < n$, de elementos num corpo F que tenha posto k pode ser reduzida por operação elementar de colunas a uma matriz*

$$G = \begin{bmatrix} I_{k\times k} \\ B_{(n-k)\times k} \end{bmatrix}$$

Temos ainda, como consequência do fato que as operações elementares por colunas ser inversível que $A = GM$, one $M_{k\times k}$ é inversível e que os subespaço de F^n gerados pelas colunas de A e de G são os mesmos. Referências: [8], Cap. 3 e [14].

Um *produto interno* em um espaço vetorial *real* é uma aplicação $\langle , \rangle : V \times V \to \mathbb{R}$ tal que, dados $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$ em V e α em $\mathbb{R}$,

1. $\langle \mathbf{u} + \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle + \langle \mathbf{v}, \mathbf{w} \rangle$
2. $\langle \alpha\mathbf{v}, \mathbf{w} \rangle = \alpha \langle \mathbf{v}, \mathbf{w} \rangle$
3. $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle$
4. $\langle \mathbf{u}, \mathbf{u} \rangle \geq 0$, e a igualdade ocorre se e somente se $u = 0$.

Para espaços vetoriais complexos, a definição de produto interno tem uma pequena modificação.

Um *produto interno* em um espaço vetorial *complexo* é uma aplicação $\langle , \rangle : V \times V \to \mathbb{C}$ tal que

1. $\langle \mathbf{u} + \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle + \langle \mathbf{v}, \mathbf{w} \rangle$
2. $\langle \alpha\mathbf{v}, \mathbf{w} \rangle = \alpha \langle \mathbf{v}, \mathbf{w} \rangle$
3. $\langle \mathbf{u}, \mathbf{v} \rangle = \overline{\langle \mathbf{v}, \mathbf{u} \rangle}$
4. $\langle \mathbf{u}, \mathbf{u} \rangle \geq 0$, e a igualdade ocorre se e somente se $u = 0$.

O exemplo padrão é $V = \mathbb{C}^n$ e $\langle u, v \rangle = u_1\overline{v_1} + u_2\overline{v_2} + \ldots + u_n\overline{v_n}$.

Finalmente, no espaço F^n, onde F é um corpo finito, usamos o "produto interno" dado por

$$\langle (u_1, u_2, \ldots, u_n), (v_1, v_2, \ldots, v_n) \rangle = u_1v_1 + \ldots + u_nv_n$$

Esta aplicação satisfaz as três primeiras propriedades de produto interno real (tomando os escalares em F) mas, como F não é ordenado, a propriedade 4 não faz sentido. No entanto, como a expressão é a mesma do produto interno usual em $\mathbb{R}^n$, e todas as outras 3 propriedades valem, costuma-se chamar esta aplicação de produto interno também.

Bibliografia

[1] E. Bayer-Fluckiger, Lattices and Number Fields, Contemporary Mathematics, 241 (1999), 69-84.

[2] J.P. de O. Santos, "Introdução à Teoria dos Números", Coleção Matemática Universitária, IMPA, 3a. edição, 2005.

[3] E. Bayer-Fluckiger, F. Oggier, E. Viterbo, New algebraic constructions of rotated $\mathbb{Z}^n$ lattice constellations for the Rayleight fading channel, IEEE Transactions on Information Theory, 50 (2004), 702-714.

[4] J. Martinet, "Perfect Lattices in Euclidean Spaces", Springer, 2000.

[5] A.F. Beardon, "The geometry of discrete groups", Springer, 1995.

[6] S. Benedetto, E. Biglieri, "Principles of digital Transmition", Kluwer, New York, 2000.

[7] G. Benenti, G. Casati, and G. Strini, "Principles of Quantum Computation and Information", Vol. I, World Scientific, Singapore, 2004.

[8] J.L. Boldrini, S.I.R. Costa, V.L. Figueiredo e H. Wetzler, "Álgebra Linear", Harbra, 1984.

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

[10] S.I.R. Costa, M. Muniz, E. Agustini and R. Palazzo Jr., Graphs, tessellations, and perfect codes on flat tori, IEEE Transactions on Information Theory, 50 (2004), 2363-2377.

[11] S.I.R. Costa, J.E. Strapasson, M. Muniz, T.B. Carlos and R.M. Siqueira, Circulant graphs viewed as graphs on flat tori, preprint (2006).

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

[13] W. Ebeling, "Lattices and Codes", 2nd edition, Advanced Lectures in Mathematics, Vieweg, 2002.

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

[15] T. Ericson, V. Zinoviev, "Codes on Euclidian Spheres", North-Holland, 2001.

[16] G. D. Forney, Geometrically Uniform codes, IEEE Transactions on Information Theory, 37 (1991), 1241-1260.

[17] H. W. Hamming, Error detecting and error correcting, *Bell Systems Tech. J.* 29 (1950), 147-160.

[18] A. Hefez e M. A. T. Villela, "Códigos corretores de erros", IMPA, 2002.

[19] C. Heuberger, On planarity and colorability of circulant graphs, *D*iscrete Mathematics, 268 (2003), 153-169.

[20] J. Karlof and C.P. Downey, Optimal [M,3] Group Codes for the Gaussian Channel, IEEE Transaction on Information Theory, IT-24 (1976).

[21] A. Yu. Kitaev, A.H. Shen, and M.N. Vyalyi, "Classical and Quantum Computation", American Mathematical Society, Providence, Rhode Island, 2002.

[22] M.A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press, Cambridge, 2000.

[23] G. A. Jones and J. M. Jones, "Information and Coding Theory", Springer, 2000.

[24] F.J. Mac-Williams and N.J.A. Sloane, "Theory of Error Correcting Codes", North-Holland, 1977.

[25] M. Muniz and S.I.R. Costa, Labelings of Lee and Hamming Spaces, Discrete Mathematics, 260 (2003), 119-136.

[26] R. Portugal, C. Lavor, L.M. Carvalho e N. Maculan, "Uma Introdução à Computação Quântica", vol. 8 da Série Notas em Matemática Aplicada, SBMAC, São Carlos, 2004.

[27] J. Preskill, Quantum Information and Computation, Lecture Notes, California Institute of Technology, 1998.

[28] O. Pretzel, "Error Correcting Codes and Finite Fields", Oxford Univ. Press, 1992.

[29] R.M. Siqueira, "Códigos Esféricos com Simetrias Cíclicas", Tese de Doutorado, IMECC/ UNICAMP, 2006.

[30] C. E. Shannon, A Mathematical Theory of Communications, Bell Systems Tech. J., 27 (1948), 379-423, 623-656.

[31] T. Siegfried, "O Bit e o Pêndulo", Editora Campus, Rio de Janeiro, 2000.

[32] R.A. Rankin, The Closest Packing of Spherical Caps in n Dimensions, Proc. Glasgow Math. Assoc., 2 (1954), 139-144.

[33] B.F. Rice and C.O. Wilde, “Error Correcting codes”, UMAP, Modules and Monographs in Undergraduate Mathematics and Its Applications, 502-526, 1981.

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

[35] D. Slepian, Group codes for the Gaussian Channel, The Bell System Technical Journal, 47 (1968), 575-602.

[36] J.H. Conway, N.J.A. Sloane, “Sphere Packings, Lattices and Groups”, Grundlehren der mathematischen Wissenschaften, Springer, 3rd edition, 1998.

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

[38] L.F. Tóth, Über die dichteste Kugellagerung, Math. Zeitschrift, 48 (1943), 676-684.

[39] L.F. Tóth, Über eine Abschätzung des k̈rzesten Abstandes zweier Punkte eines auf einer Kugelfläche liegenden Punktsystems, Jahresbericht Deut. Math. Verein., 53 (1943),66-68.

[40] J.M. Wozencraft and I.M. Jacobs, “Principles of Communication Engineering", John Wiley and Sons, 1965.

Índice

Notas em Matemática Aplicada

1. Restauração de Imagens com Aplicações em Biologia e Engenharia

   Geraldo Cidade, Antônio Silva Neto e Nilson Costa Roberty

2. Fundamentos, Potencialidades e Aplicações de Algoritmos Evolutivos

   Leandro dos Santos Coelho

3. Modelos Matemáticos e Métodos Numéricos em Águas Subterrâneas

   Edson Wendlander

4. Métodos Numéricos para Equações Diferenciais Parciais

   Maria Cristina de Castro Cunha e Maria Amélia Novais Schleicher

5. Modelagem em Biomatematica

   Joyce da Silva Bevilacqua, Marat Rafikov e Cláudia de Lello Courtouke Guedes

6. Métodos de Otimização Randômica: algoritmos genéticos e "simulated annealing"

   Sezimária F. Pereira Saramago

7. "Matemática Aplicada à Fisiologia e Epidemiologia"

   H.M. Yang, R. Sampaio e A. Sri Ranga

8. Uma Introdução à Computação Quântica

   Renato Portugal, Carlile Campos Lavor, Luiz Mariano Carvalho e Nelson Maculan

9. Aplicações de Análise Fatorial de Correspondências para Análise de Dados

   Dr. Homero Chaib Filho, Embrapa

10. Modelos Matemáticos baseados em autômatos celulares para Geoprocessamento

    Marilton Sanchotene de Aguiar, Fábia Amorim da Costa, Graçaliz Pereira Dimuro e Antônio Carlos da Rocha Costa

11. Computabilidade: os limites da Computação
    Regivan H. N. Santiago e Benjamín R. C. Bedregal
12. Modelagem Multiescala em Materiais e Estruturas
    Fernando Rochinha e Alexandre Madureira
13. Modelagem em Biomatemática (Coraci Malta ed.)
    1 - "Modelagem matemática do comportamento elétrico de neurônios e algumas aplicações"
        Reynaldo D. Pinto
    2 - "Redes complexas e aplicações nas Ciências"
        José Carlos M. Mombach
    3 - "Possíveis níveis de complexidade na modelagem de sistemas biológicos"
        Henrique L. Lenzi, Waldemiro de Souza Romanha e Marcelo Pelajo-Machado
14. A lógica na construção dos argumentos
    Angela Cruz e José Eduardo de Almeida Moura
15. Modelagem Matemática e Simulação Numérica em Dinâmica dos Fluidos
    Valdemir G. Ferreira, Hélio A. Navarro, Magda K. Kaibara
16. Introdução ao Tratamento da Informação nos Ensinos Fundamental e Médio
    Marcilia Andrade Campos, Paulo Figueiredo Lima
17. Teoria dos Conjuntos Fuzzy com Aplicações
    Rosana Sueli da Motta Jafelice, Laércio Carvalho de Barros, Rodney Carlos Bassanezi
18. Introdução à Construção de Modelos de Otimização Linear e Inteira
    Socorro Rangel
19. Observar e Pensar, antes de Modelar
    Flavio Shigeo Yamamoto, Sérgio Alves, Edson P. Marques Filho, Amauri P. de Oliveira
20. Frações Contínuas: Propriedades e Aplicações
    Eliana Xavier Linhares de Andrade, Cleonice Fátima Bracciali