# Universidade Estadual de Campinas

Instituto de Matemática, Estatística e Computação Científica

Departamento de Matemática


**Dissertação de Mestrado**

# UM ESTUDO SOBRE CÓDIGOS CORRETORES DE ERROS EM ESPAÇOS SOBRE POSETS

por


## Donizete Ritter

Mestrado Profissional em Matemática - Campinas - SP

**Orientador: Prof. Dr. Marcelo Muniz Silva Alves**

# UM ESTUDO SOBRE CÓDIGOS CORRETORES DE ERROS EM ESPAÇOS SOBRE POSETS

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por **Donizete Ritter** e aprovada pela Comissão Julgadora.

Campinas, 27 de fevereiro de 2009.

Prof. Dr. Marcelo Muniz Silva Alves
Orientador

**Banca Examinadora:**
Prof. Dr. Luiz Antonio Ribeiro de Santana
Prof. Dr. Marcelo Firer
Prof. Dr. Marcelo Muniz Silva Alves

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para a obtenção do título de **Mestra em Matemática**.

**FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP**
Bibliotecária: Miriam Cristina Alves – CRB8a / 5094

Ritter, Donizete
R514u Um estudo sobre códigos corretores de erros em espaços sobre posets/ Donizette Ritter -- Campinas, [S.P. :s.n.], 2009.

Orientador : Marcelo Muniz Silva Alves
Dissertação (mestrado profissional) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Códigos de controle de erros (Teoria da informação). 2. Teoria dos erros. 3. Métricas sobre ordens parciais. I. Alves, Marcelo Muniz Silva. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: A study on error-correting codes in Poset Spaces.

Palavras-chave em inglês (Keywords): 1. Error-correcting codes. 2. Error theory. 3. Poset metric.

Área de concentração: Teoria dos erros

Titulação: Mestra em Matemática

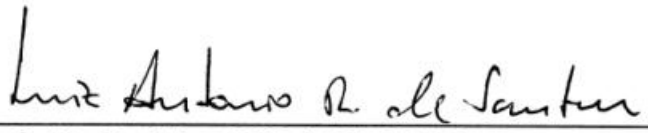
Banca examinadora: Prof. Dr. Marcelo Muniz Silva Alves (DMAT-UFPR)
Prof. Dr. Marcelo Firer (IMECC-UNICAMP)
Prof. Dr. Luiz Antônio Ribeiro de Santana (DMAT-UFPR)

Data da defesa: 27/02/2009

Programa de Pós-Graduação: Mestrado profissional em Matemática

**Dissertação de Mestrado Profissional defendida em 27 de fevereiro de 2009**
**E aprovada pela Banca Examinadora composta pelos Profs. Drs.**

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



**Prof. (a). Dr (a). LUIZ ANTONIO RIBEIRO DE SANTANA**

**Prof. (a). Dr (a). MARCELO FIRER**

*Àqueles que reconhecem que se a educação sozinha não transforma a sociedade, sem ela, tampouco, a sociedade muda.*

*"Mestre não é quem sempre ensina, mas quem de repente aprende."*
*(Guimarães Rosa)*

# Agradecimentos


- A Deus, dono do tempo e da eternidade, teu é o hoje e o amanhã, o passado e o futuro. Agradeço por tudo aquilo que recebi de Ti. Obrigada pela vida e pelo amor; pelas flores, pelo ar e pelo sol; pela alegria e pela dor; pelo que foi possível e pelo que não foi; pela experiência da vida e por poder desfrutar do amor dos meus pais, irmãos e amigos; pelo esplendor do céu azul e pela brisa da tarde; pelas nuvens rápidas e pelas constelações nas alturas; pelos oceanos imensos e pela água corrente; pelas montanhas eternas, pelas árvores frondosas e pela relva macia em que os nossos pés repousam.

- Aos meus pais: Em todos os momentos da minha vida vocês foram meus amigos e conselheiros. Obrigada por estarem sempre comigo, mesmo à distância. Amo-os indescritivelmente.

- Ao meu filho Maycon Christian Mick, por suportar minhas ausências constantes em prol de minha formação, por sua compreensão e amizade, sendo sempre um bom filho. Eu te amo e te desejo a paz e serenidade para levares a sua vida em frente, conquistando seus sonhos e alcançando seus ideais.

- Ao professor Marcelo Muniz Silva Alves, meu orientador. Sempre será para mim um exemplo e uma inspiração muito forte. Pela dedicação que tem me dispensado, pelos estímulos e cobranças.

- A todos meus amigos e parentes, muitos dos quais torceram bastante para que este momento se concretizasse. Em especial aos meus irmãos Danderlei, Deoclecio e Daiane.

- Aos idealizadores desse projeto, em especial à professora Sueli Irene Rodrigues Costa (que nunca mediu esforços para apoiar-me no decorrer do mestrado) e à professora Maria Zoraide Martins Costa Soares, por terem sonhado este sonho, contribuindo com o crescimento de muita gente, atentos ao fato de que educação se multiplica. Nós havemos de conduzir outros ao caminho libertador do conhecimento.

- Aos amigos do Mestrado Profissional em Matemática, em especial ao meu eterno amigo Lúdio. Existem pessoas que são apenas uma passagem, e outras nos marcam por serem únicas na nossa vida.
- Aos amigos Aldair, Eliane e Paulo Vicente, dentre outros igualmente queridos.

# Sumário

# Abstract

RITTER, Donizete. *A study on error-correcting codes over Poset Spaces*. Campinas - SP - Brazil: Universidade Estadual de Campinas, February 2009. Dissertation presented as a partial requisite for the title of Master in Mathematics.

In this work, we address the classical theory of error-correcting codes and the theory of codes over poset spaces, also known as poset codes, establishing comparisons between these two cases. In particular, we present the definition of alphabet, the Hamming distance, linear codes and the definition of a generating matrix for a linear code; we also present the Singleton and Hamming bounds, alongside with the Hamming codes. With respect to poset codes, we present the definitions of partial orders and of the poset metric, the counting of the number of elements in a ball in a poset space, some results on ideals in posets and the extended Hamming code; we study the chain poset case, analysing the cases of codes over a chain poset and codes over a union of two chains of the same length and, finally, we study the poset metrics that allow $m$-perfect binary codes of codimension $m$, thus characterizing these codes. Our aim is to present a text, accessible for undergraduates, that encompasses the basic theory of error-correcting codes and, nonetheless, also provides some notions on poset codes.

**Keywords:** Error-Correcting Codes, Error Theory, Poset Metric.

# Resumo

RITTER, Donizete. *Um Estudo Sobre Códigos Corretores de Erros em Espaços sobre Posets*. Campinas - SP: Universidade Estadual de Campinas, fevereiro de 2009. Dissertação apresentada como requisito parcial para obtenção do Título de Mestra em Matemática.

Neste trabalho abordamos a teoria dos Códigos Corretores de Erros clássica e também os códigos sobre ordens parciais, com algumas comparações entre os dois casos. Enfocamos, particularmente, a definição de Alfabeto, a distância de Hamming, os códigos lineares e a definição de matriz geradora de um código; o estudo dos limitantes de Singleton e de Hamming, além de tratar dos Códigos de Hamming. Em relação aos Códigos em Conjuntos Parcialmente Ordenados, apresentamos a definição de ordens parciais, métricas sobre conjuntos ordenados, contagem dos elementos da "bola", resultados sobre Ideais e o Código de Hamming Estendido; estudamos o caso da ordem cadeia ("chain poset"), analisando os códigos de uma cadeia e os códigos de duas cadeias de mesmo comprimento e, por fim, nos dedicamos ao estudo das "Métricas POSET", que admitem códigos binários perfeitos de codimensão m, caracterizando assim os Códigos Posets m-corretores de erros. Nosso objetivo é apresentar um texto, acessível a alunos de graduação, que contemple a teoria básica dos Códigos Corretores de Erros, no entanto, forneça uma noção sobre os códigos sobre ordens parciais.

**Palavras-Chave:** Códigos de Controle de Erros, Métricas sobre Ordens Parciais, Teoria do Erros.

# Introdução

Pelo que nos consta, a história dos Códigos Corretores de Erros começa na década de 50, juntamente com o advento dos computadores, que passaram a ser usados em instituições de pesquisa, gerando problemas com a transmissão e o armazenamento de informações. Mais precisamente começa-se a falar sobre os Códigos Corretores de Erros em 1948 com a publicação de um artigo pelo matemático e engenheiro Claude E. Shannon, do laboratório Bell. Inicialmente alguns dos maiores interessados nesta teoria foram os matemáticos, que a desenvolveram consideravelmente nas décadas de 50 e de 60. A partir da década de 70, com as pesquisas espaciais e a grande popularização dos computadores, essa teoria começou a interessar também aos engenheiros.

Hoje os códigos corretores de erros participam do nosso cotidiano de inúmeras formas, estando presentes, por exemplo, sempre que fazemos uso de informações digitalizadas, tais como assistir a um programa de televisão, falar ao telefone, ouvir um CD de música, assistir a um filme em DVD, mandar um recado a alguém via Pager ou navegar pela Internet. Garantem, portanto, a comunicação por internet e satélites, o bom uso de computadores, a gravação de CDs e DVDs e o posterior uso dos mesmos.

A teoria de Códigos foi criada para tentar corrigir erros que ocorrem nestas atividades. Um código corretor de erros é, basicamente, um modo organizado de acrescentar algum dado adicional a cada informação que se queira transmitir ou armazenar e que permita, ao recuperar a informação, detectar e corrigir os erros no processo de transmissão da informação. Pode-se afirmar que hoje praticamente todo sistema de envio de informações possui algum tipo de código corretor de erros. Pelo fato da motivação primária para o desenvolvimento dos códigos corretores de erros ser a resolução de problemas em comunicações, essa teoria foi enquadrada na teoria das comunicações. Isto porque, ao contrário das teorias matemáticas que surgiram nas universidades e geralmente após um longo período de tempo migraram para as aplicações práticas em tecnologia e indústrias, a teoria de Códigos Corretores de Erros surgiu nos laboratórios de empresas de telefonia e posteriormente se transformou em uma

teoria matemática completa, com aplicações em várias áreas como, por exemplo, geometria algébrica.

A Teoria da Informação preocupa-se com os aspectos quantitativos de armazenamento e transmissão de mensagens, tendo como um de seus objetivos principais garantir a integridade das informações enviadas através de algum tipo de canal. No entanto, na manipulação de mensagens dois obstáculos são encontrados: a falta de capacidade no armazenamento ou transmissão das mensagens enviadas e os ruídos na transmissão, ou seja, a introdução aleatória de erros nas mensagens enviadas. Assim, a teoria dos Códigos é um campo de pesquisa atual, muito atraente, tanto do ponto de vista científico quanto tecnológico. A teoria dos códigos é capaz de mesclar conceitos e técnicas importantes da Álgebra abstrata com aplicações imediatas da vida real, o que mostra como a sofisticação tecnológica torna cada vez mais imperceptível a relação entre a chamada matemática pura e a matemática aplicada.

Com o aumento da confiabilidade nas comunicações digitais e a emergência do computador digital como ferramenta essencial na sociedade tecnológica, os códigos corretores de erros vêm conquistando uma posição prominente. Além disso vários são os Códigos desenvolvidos. Para exemplificar a importância e variedade dos códigos corretores de erros temos: Uso do bit de paridade como um mecanismo detector de erro - é um dos esquemas mais simples e conhecidos na comunicação computacional; Armazenamento em discos - estão sendo muito utilizados devido ao aumento da densidade. Quanto maior a densidade, a probabilidade de ocorrência de erros também aumenta; Transmissão de informação pelas naves espaciais: em 1972 a nave espacial Mariner transmitiu figuras de Marte para a Terra com 64 tonalidades de cinza. Atividade solar e outras condições atmosféricas podem introduzir erros em sinais fracos vindos do espaço. O código utilizado foi o de Reed-Muller. Em 1979 a nave espacial Voyager começou a enviar imagens com 4096 tonalidades de cores. O código utilizado foi o de Golay; Áudio digital - o aumento da popularidade do áudio digital deve-se ao desenvolvimento dos códigos corretores de erros que facilita o processo de digitalização. Ao inicializar a leitura de DVD, blu-ray (Video digital) ou CD, o sistema corrige os erros produzidos por marcas de dedos, arranhões e outras imperfeições, para logo em seguida transformar em sinais sonoros. O código utilizado é o de Reed-Solomon (ver [9]).

Aplicações em problemas de comunicações são diversificadas. Dados binários são comumente transmitidos entre terminais de computadores, entre aeronaves, satélites e sondas

espaciais. Códigos corretores de erros são usados freqüentemente em aplicações militares para proteção contra interferência inimiga intencional. As transmissões entre sistemas computacionais usualmente são intolerantes até mesmo a baixas taxas de erros, porque um simples erro pode destruir um programa de computador. Códigos corretores de erros tornam-se importantes nestas aplicações. Assim, os códigos representam um papel central na maioria dos sistemas de comunicação e armazenamento de dados digitais.

O presente trabalho constitui uma breve introdução à teoria dos códigos corretores de erros clássica e também aos códigos sobre ordens parciais, com algumas comparações entre os dois casos.

No **capítulo I** desta dissertação apresentamos os elementos de um sistema de comunicações e definimos alguns conceitos básicos para podermos iniciar a compreensão de como funcionam os códigos corretores de erros, como definição de Alfabeto, a distância de Hamming, os códigos lineares e definição de matriz geradora de um código. Antes disso, fazemos ainda uma retomada ao estudo de Álgebra, com uma revisão sobre congruências, classes residuais e sua aritmética, elementos importantes para a compreensão dos conceitos abordados neste trabalho;

Já no **capítulo II** nos dedicamos ao estudo dos limitantes de Singleton e de Hamming, além de tratar dos Códigos de Hamming;

No **capítulo III** tratamos, de forma geral, dos Códigos em Conjuntos Parcialmente Ordenados ("Posets"), apresentando a definição de ordens parciais, métricas sobre conjuntos ordenados, contagem dos elementos da bola, resultados sobre Ideais e o Código de Hamming Estendido.

Já no **capítulo IV** estudamos o caso da ordem cadeia ("chain poset"), analisando os códigos de uma cadeia e os códigos de duas cadeias de mesmo comprimento;

Por sua vez, o **capítulo V** é dedicado ao estudo das Métricas "Poset" que admitem códigos binários perfeitos de codimensão $m$. Faremos algumas considerações iniciais e caracterizaremos os Códigos "Posets" $m$-corretores de erros.

Capítulo 1

# TEORIA CLÁSSICA DOS CÓDIGOS CORRETORES DE ERROS

## 1.1 Um Pouco de Álgebra

Os resultados desta seção baseiam-se principalmente nas definições encontradas no Curso de Álgebra de HEFEZ, Abramo ([8]), com o apoio de outras bibliografias sobre Álgebra, presentes nas referências bibliográficas ([3], [4] e [11]). Na verdade, estas bibliografias foram importantes no decorrer de todo o texto.

### 1.1.1 Congruência

**Definição 1.1** *Congruência é uma relação de equivalência entre números inteiros: a e b são congruentes módulo m se a − b é múltiplo de m. Escreve-se* $a \equiv b (mod\ m)$.

Pode-se provar que isso acontece se, e somente se , $a$ e $b$, ao serem divididos por $m$ (módulo) dão o mesmo resto.

Por Exemplo:

$20 \equiv 14 (\text{mod } 6)$.

$-1 \equiv 9 (\text{mod } 5)$.

$1100 \equiv 2 (\text{mod } 9)$.

e o quadrado de qualquer número ímpar é 1 côngruo 8. (Prova-se!)

Tem-se que $a \equiv b(\text{mod } m)$ se, e somente se, houver um inteiro $q$ de tal modo que $a = b + qm$. Desta forma, as conguências podem ser transformadas em igualdades com a adição de uma incógnita.

**Proposição 1.1** *Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 1$, são válidas as seguintes propriedades:*

1. *(Reflexiva) Se $a$ é qualquer inteiro, $a \equiv a(mod\ m)$.*
2. *(Simétrica) Se $a \equiv b(mod\ m)$ então $b \equiv a(mod\ m)$.*
3. *(Transitiva) Se $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$ então $a \equiv c(mod\ m)$.*

Devido a estas três propriedades sabemos que o conjunto dos números inteiros é dividido em $m$ diferentes classes de congruência módulo $m$.

**Demonstração:** 1. e 2. são imediatas.

3. Se $a \equiv b(\text{mod } m)$ e $b \equiv c(\text{mod } m)$, então $m|(a-b)$ e $m|(b-c)$, logo $m|(a-b+b-c)$, donde $m|(a-c)$ e, portanto, $a \equiv c(\text{mod } m)$. ■

**Proposição 1.2** *Se $a, b, c, d$ são inteiros quaisquer com $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então:*

1. *$a + c \equiv b + d(mod\ m)$.*
2. *$a.c \equiv b.d(mod\ m)$.*
3. *Se $a \equiv b(mod\ m)$ então $a^n \equiv b^n(mod\ m)$.*

**Demonstração:** 1. Se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, segue que $m|(a-b)$ e $m|(c-d)$; logo $m|(a-b+c-d)$, ou seja $m|(a+c)-(b+d)$ logo $a + c \equiv b + d(\text{mod } m)$.

2. Se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, segue que $m|(a-b)$ e $m|(c-d)$. Como $ac - bd = a(c-d) + d(a-b)$, segue que $m|(ac-bd)$ e, consequentemente, $a.c \equiv b.d(\text{mod } m)$.

3. Isto segue de 2., por indução sobre $n$. ■

No que segue, denotaremos o máximo divisor comum de $a$ e $b$ por mdc $(a, b)$ ou simplesmente $(a, b)$.

**Proposição 1.3** *Sejam $a, b, c, m, n \in \mathbb{Z}$ com $m > 1$ e $n > 1$.*
*i) Se $a \equiv b(mod\ m)$ e se $n|m$, então $a \equiv b(mod\ n)$;*

*ii*) $a \equiv b(mod\ m)$ *e* $a \equiv b(mod\ n)$ *se, e somente se,* $a \equiv b(mod\ mmc\ (m, n))$;
*iii*) *Se* $ac \equiv bc(mod\ m)$ *e* $(c, m) = 1$, *então* $a \equiv b(mod\ m)$;
*iv*) *Se* $d = (c, m)$, *então* $ac \equiv bc(mod\ m)$ *se, e somente se,* $a \equiv b(mod\ \frac{m}{d})$

**Demonstração:**

*i*) Se $a \equiv b(\text{mod } m)$, então $m|(a-b)$ e como $n|m$, segue que $n|(a-b)$, logo $a \equiv b(\text{mod } n)$;

*ii*) ($\Rightarrow$) Se $a \equiv b(\text{mod } m)$, então $m|(a-b)$ e se $a \equiv b(\text{mod } n)$ então $n|(a-b)$, logo, pela definição de mmc temos que mmc $(m, n)|(a-b)$ e, portanto $a \equiv b(\text{mod mmc } (m, n))$. ($\Leftarrow$) Reciprocamente, se $a \equiv b(\text{mod mmc } (m, n))$, temos de i) que $a \equiv b(\text{mod } m)$ e $a \equiv b(\text{mod } n)$ pois $m|\text{mmc } (m, n)$ e $n|\text{mmc } (m, n)$;

*iii*) Se $ac \equiv bc(\text{mod } m)$, então $m|ac - bc \Rightarrow m|[c(a-b)]$ e como $(c, m) = 1$ então $m|(a-b)$ e, portanto $a \equiv b(\text{mod } m)$;

*iv*) ($\Rightarrow$) Se $ac \equiv bc(\text{mod } m)$ segue que $m|[c(a-b)]$, donde $c(a-b) = tm$ para algum $t \in \mathbb{Z}$. Sendo $d = (c, m)$, temos que:
$\frac{c}{d}.(a-b) = t.\frac{m}{d}$ com $(\frac{c}{d}, \frac{m}{d}) = 1$ implica em $\frac{m}{d}|(a-b)$, ou seja, $a \equiv b(\text{mod } \frac{m}{d})$. ($\Leftarrow$) Reciprocamente, sejam $c_0, m_0 \in \mathbb{Z}$ tais que $c = c_0.d$ e $m = m_0.d$. Por hipótese $a \equiv b(\text{mod } m_0)$, logo $m_0|(a-b) \Rightarrow (a-b) = t.m_0$ para algum $t \in \mathbb{Z}$, portanto, $c.(a-b) = t.m_0.c = t.m_0.c_0.d = t.c_0.m \Rightarrow m|(ac-bc) \Rightarrow ac \equiv bc(\text{mod } m)$. ■

**Corolário 1.1** *Sejam* $a, b, m, m_1, \ldots, m_r \in \mathbb{Z}$ *com* $m, m_1, \ldots, m_r > 1$. *Suponha que* $m = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ *seja a decomposição de m em fatores primos distintos. Temos que:*
*i*) *Se* $a \equiv b(mod\ m_1, \ldots, a) \equiv b(mod\ mr)$, *então,* $a \equiv b\ mod\ (mmc\ (m_1, \ldots, m_r))$;
*ii*) *Se* $a \equiv b(mod\ (p_i^{\alpha_i}))$, *então,* $a \equiv b(mod\ (p_i))$.

**Teorema 1.1 O Pequeno Teorema de Fermat**: *Seja p um número primo positivo, tem-se que:*
*a*) *Se a é um inteiro qualquer, então* $a^p \equiv a(mod\ p)$;
*b*) *Se a é um inteiro não divisível por p, então* $a^{p-1} \equiv 1(mod\ p)$.

### 1.1.2 As Classes Residuais e sua Aritmética

**Definição 1.2** *Seja dado um inteiro* $m > 1$. *Define-se a classe residual módulo m do elemento a de* $\mathbb{Z}$ *como sendo o conjunto:*

$$\bar{a} = \{x \in \mathbb{Z} | x \equiv a(mod\ m)\}.$$

É imediato ver que:

$$\bar{a} = \{m.\lambda + a; \lambda \in \mathbb{Z}\}.$$

Exemplo: Seja $m = 3$. Então:

$\bar{0} = \{3.\lambda; \lambda \in \mathbb{Z}\}$

$\bar{1} = \{3.\lambda + 1; \lambda \in \mathbb{Z}\}$

$\bar{2} = \{3.\lambda + 2; \lambda \in \mathbb{Z}\}$

ou seja

$$\bar{a} = \begin{cases} \bar{0}, & \text{se a é múltiplo de 3} \\ \bar{1}, & \text{se a tem resto 1 quando dividido por 3} \\ \bar{2}, & \text{se a tem resto 2 quando dividido por 3.} \end{cases}$$

Vejamos algumas propriedades das classes residuais:

**Proposição 1.4** *Seja m um inteiro maior do que* 1. *Temos que:*

*i*) $\bar{a} = \bar{b}$ *se, e somente se,* $a \equiv b (mod\ m)$;

*ii*) *Se* $\bar{a} \cap \bar{b} \neq \varnothing$ *então* $\bar{a} = \bar{b}$;

*iii*) $\bigcup_{a \in \mathbb{Z}} \bar{a} = \mathbb{Z}$

**Demonstração:** *i*)($\Rightarrow$) Suponha que $\bar{a} = \bar{b}$, como $a \in \bar{a}$, segue que $a \in \bar{b}$, logo $a \equiv b (\text{mod } m)$. ($\Leftarrow$). Reciprocamente, suponha que $a \equiv b (\text{mod } m)$, logo $x \equiv a (\text{mod } m)$ se, e somente se, $x \equiv b (\text{mod } m)$ e, portanto $x \in \bar{a}$ se, e somente se, $x \in \bar{b}$, donde $\bar{a} = \bar{b}$.

*ii*) Suponha que $\bar{a} \cap \bar{b} \neq \varnothing$ e seja $c \in \bar{a} \cap \bar{b}$; segue que $c \equiv a (\text{mod } m)$ e $c \equiv b (\text{mod } m)$, logo $a \equiv b (\text{mod } m)$ e, pelo item *i*) segue que $\bar{a} = \bar{b}$.

*iii*) É claro que $\bigcup_{a \in \mathbb{Z}} \bar{a} \subset \mathbb{Z}$. Por outro lado seja $x \in \mathbb{Z}$, como $x \in \bar{x}$, segue que $x \in \bigcup_{a \in \mathbb{Z}} \bar{a}$ e, portanto, $\mathbb{Z} \subset \bigcup_{a \in \mathbb{Z}} \bar{a}$. Assim temos: $\mathbb{Z} \subset \bigcup_{a \in \mathbb{Z}} \bar{a} \subset \mathbb{Z} \Rightarrow \bigcup_{a \in \mathbb{Z}} \bar{a} = \mathbb{Z}$. ■

**Observação 1.1** *Um inteiro qualquer b tal que* $\bar{b} = \bar{a}$ *é dito representante da classe residual* $\bar{a}$.

**Exemplo 1.1** *Se* $m = 2$, *então qualquer inteiro par é representante da classe residual* $\bar{0}$ *e qualquer inteiro ímpar é representante da classe residual* $\bar{1}$;

**Exemplo 1.2** *Se $m = 3$, então qualquer múltiplo de 3 é representante da classe residual $\bar{0}$; qualquer número da forma $3\lambda + 1$ com $\lambda \in \mathbb{Z}$ é representante da classe residual $\bar{1}$; enquanto que qualquer número da forma $3\lambda + 2$, com $\lambda \in \mathbb{Z}$ é representante da classe residual $\bar{2}$.*

**Proposição 1.5** *Para cada $a \in \mathbb{Z}$ existe um, e somente um, $r \in \mathbb{Z}$ com $0 \leq r < m$ tal que $\bar{a} = \bar{r}$.*

**Demonstração:** Seja $a \in \mathbb{Z}$. Pela divisão euclidiana existe um único inteiro $r$ com $0 \leq r < m$ tal que $a = mq + r$ para algum $q \in \mathbb{Z}$. Portanto é único o inteiro $r$ tal que $0 \leq r < m$ e $a \equiv r(\text{mod } m)$, consequentemente, é único o inteiro $r$ tal que $0 \leq r < m$ e $\bar{a} = \bar{r}$. ■

**Corolário 1.2** *Existem exatamente $m$ classes residuais módulo $m$ distintas, a saber:* $\bar{0}, \bar{1}, \ldots, \overline{(m-1)}$.

**Demonstração:** Segue direto da proposição acima que $r$ pode assumir $m$ valores, uma vez que $0 \leq r < m$. ■

**Definição 1.3** *Um conjunto $\{a_1, \ldots, a_m\}$ é um sistema completo de resíduos módulo $m$ se para todo $a \in \mathbb{Z}$ existir um $i$, com $i = 0, \ldots, m$, tal que $a \equiv a_i (mod\ m)$.*

Em outras palavras $\{a_1, \ldots, a_m\}$ é um sistema completo de resíduos módulo $m$ se, e somente se, $\bar{a}_1, \ldots, \bar{a}_m$ são as $m$ classes residuais módulo $m$. Os conjuntos $\{0, 1, \ldots, m-1\}$ e $\{1, 2, \ldots, m\}$ são sistemas completos de resíduos módulo $m$.

Temos que $m$ inteiros formam um sistema completo de resíduos módulo $m$ se, e somente se, eles são dois a dois incongruentes módulo $m$.

O conjunto de todas as classes residuais módulo $m$ é representado por $\mathbb{Z}_m$. Ele possui $m$ elementos que podem ser representados por $\bar{0}, \bar{1}, \ldots, \overline{(m-1)}$.

A primeira vantagem das classes residuais é que transformam a congruência $a \equiv b(\text{mod } m)$ na igualdade $\bar{a} = \bar{b}$.

**Definição 1.4** *Em $\mathbb{Z}_m$ definimos as seguintes operações:*
*Adição:* $\bar{a} + \bar{b} = \overline{a + b}$;
*Multiplicação:* $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$.

Note que sendo definidas estas operações usando os representantes $a$ e $b$ para as classes residuais $\bar{a}$ e $\bar{b}$ respectivamente, temos que verificar que ao mudarmos os representantes das classes $\bar{a}$ e $\bar{b}$, não mudam os valores de $\overline{a+b}$ e de $\overline{a.b}$. Para verificar que isto acontece, basta notar que se $a \equiv a'(\text{mod } m)$ e $b \equiv b'(\text{mod } m) \Rightarrow a+b \equiv a'+b'(\text{mod } m)$ e $a.b \equiv a'.b'(\text{mod } m) \Rightarrow \overline{a+b} \equiv \overline{a'+b'}(\text{mod } m)$ e $\overline{a.b} \equiv \overline{a'.b'}(\text{mod } m)$, o que segue diretamente dos ítens 1. e 2. da Proposição 1.2.

Estas operações que acabamos de definir gozam das propriedades que definem um *anel comutativo*.

**Definição 1.5** *Um anel comutativo é um conjunto $A$ com uma operação de soma e uma operação de multiplicação satisfazendo as seguintes propriedades:*

*Propriedades da adição:*

*A1) (ASSOCIATIVIDADE):*

$$(a+b)+c = a+(b+c),\ \forall\ a,b,c \in A.$$

*A2) (COMUTATIVIDADE):*

$$a+b = b+a,\ \forall\ a,b \in A.$$

*A3) (EXISTÊNCIA DE ELEMENTO NEUTRO):*

*Existe um elemento chamado zero e denotado por* $0$*, tal que*

$$a+0 = 0+a = a,\ \forall\ a \in A.$$

*A4) (EXISTÊNCIA DE ELEMENTO INVERSO):*

*Dado $a \in A$, existe um elemento chamado simétrico de $a$ e denotado por $-a$ tal que*

$$a+(-a) = (-a)+a = 0,\ \forall\ a \in A.$$

*Propriedades da multiplicação:*

*M1) (ASSOCIATIVIDADE):*

$$(a.b).c = a.(b.c),\ \forall\ a,b,c \in A.$$

*M2) (COMUTATIVIDADE):*

$$a.b = b.a, \ \forall \ a, b \in A.$$

*M3) (EXISTÊNCIA DE ELEMENTO NEUTRO):*

*Existe um elemento chamado unidade e denotado por* $1$ *tal que*

$$a.1 = 1.a = a, \ \forall \ a \in A.$$

*Propriedade de ligação da multiplicação com a adição:*

*AM) (DISTRIBUTIVIDADE DA MULTIPLICAÇÃO COM RELAÇÃO À ADIÇÃO):*

$$a.(b + c) = a.b + a.c, \ \forall \ a, b, c \in A.$$

Em $\mathbb{Z}_m$, o zero é $\bar{0}$, o simétrico de $\bar{a}$ é $\overline{-a}$, a unidade é $\bar{1}$ e assim por diante. Assim, de fato:

$\bar{a}.(\bar{b} + \bar{c}) = \bar{a}.\overline{b + c} = \overline{a.(b + c)} = \overline{a.b + a.c} = \overline{a.b} + \overline{a.c} = \bar{a}.\bar{b} + \bar{a}.\bar{c}.$ ■

Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ também são anéis, com as operações usuais de adição e multiplicação de seus elementos.

Uma consequência do fato de $\mathbb{Z}_m$ ser anel comutativo, é que a aplicação

$$\psi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$$

$$a \longmapsto \bar{a}$$

satisfaz as seguintes propriedades:

$$\psi(a + b) = \psi(a) + \psi(b)$$

$$\psi(ab) = \psi(a)\psi(b)$$

$$\psi(1) = \overline{1}$$

Ou seja, $\psi$ é um *homomorfismo de anéis* de $\mathbb{Z}$ em $\mathbb{Z}_m$.

Este é o único homomorfismo de $\mathbb{Z}$ em $\mathbb{Z}_m$: dado um anel $A$, a aplicação natural:

$$\rho : \mathbb{Z} \longrightarrow A$$

$$n \longmapsto n1$$

é um homomorfismo de anéis, chamado de homomorfismo característico. O próximo resultado nos garante que este é o único homorfismo de $\mathbb{Z}$ em $A$.

**Proposição 1.6** *Se $A$ é um anel e $h : \mathbb{Z} \longrightarrow A$ é um homomorfismo de anéis, então $h = \rho$.*

Em álgebra, um homomorfismo é uma aplicação que preserva uma dada estrutura. As funções consideradas naturais entre duas estruturas algébricas do mesmo tipo, como os anéis, são aquelas que preservam as operações, ou seja, transformam a soma de elementos no anel domínio na soma de suas imagens e transformam um produto de elementos no anel domínio no produto de suas imagens. Essas funções são chamadas homomorfismos.

**Exemplo 1.3** *Tabelas da adição e da multiplicação em: $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$, $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ e $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$:*

$\mathbb{Z}_2$;

| $+$ | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{0}$ |

| $\cdot$ | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ |

$\mathbb{Z}_3$;

| $+$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

| $\cdot$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{1}$ |

$\mathbb{Z}_4$;

| $+$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

| $\cdot$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{0}$ | $\bar{2}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

$\mathbb{Z}_5$;

| $+$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |

| $\cdot$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{1}$ | $\bar{3}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{1}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

É interessante notar que $\mathbb{Z}_4$ não é um domínio de integridade[1], pois $\bar{2} \neq \bar{0}$ e, no entanto, $\bar{2}.\bar{2} = \bar{0}$.

Note que em $\mathbb{Z}_2$, $\mathbb{Z}_3$ e $\mathbb{Z}_5$, para cada elemento $\bar{a}$ que não é zero existe um elemento $\bar{b}$ tal que $\bar{a}.\bar{b} = \bar{1}$, isto é, todo elemento diferente de zero tem um inverso para a multiplicação. Um elemento $a$ de um anel $A$ será dito invertível se existir um elemento $b \in A$ tal que $a.b = 1$. Nesse caso dizemos que $b$ é um inverso de $a$. O elemento inverso de $A$ para a multiplicação, se existir, é único, e será denotado por $a^{-1}$. Note que se $a$ é invertível, então $a^{-1}$ é invertível com $(a^{-1})^{-1} = a$, e que o produto de elementos invertíveis é invertível. Se todo elemento $a$ de $A$ não-nulo tem inverso, dizemos que $A$ é um *corpo*. Assim, $\mathbb{Z}_2$, $\mathbb{Z}_3$ e $\mathbb{Z}_5$ são corpos, e $\mathbb{Z}_4$ não é. A seguir daremos uma caracterização dos elementos invertíveis de $\mathbb{Z}_m$.

**Observação 1.2** *Todo corpo é domínio de integridade.*

**Exemplo 1.4** *Em $\mathbb{Z}$ os únicos elementos invertíveis são 1 e -1, enquanto que em $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, todo elemento distinto de 0 é invertível. Estes anéis são corpos, ou seja, um anel onde todo elemento não nulo é invertível é chamado de corpo.*

**Observação 1.3** *Até agora, temos que $\mathbb{Z}_m$ (já definido) é um anel, para qualquer valor de m. Mas vimos também que $\mathbb{Z}_2$, $\mathbb{Z}_3$ e $\mathbb{Z}_5$ são corpos mas $\mathbb{Z}_4$ não é (pois $\bar{2}.\bar{2} = \bar{4} = \bar{0}$). Veremos a seguir para quais valores de m vale que $\mathbb{Z}_m$ é corpo.*

**Proposição 1.7** *Um elemento $\bar{a} \in \mathbb{Z}_m$ é invertível se, e somente se, $(a, m) = 1$.*

**Demonstração:** ($\Rightarrow$) Se $\bar{a}$ é invertível, então existe $\bar{b} \in \mathbb{Z}$ tal que $\bar{1} = \bar{a}.\bar{b} = \overline{a.b}$, logo $a.b \equiv 1 (\text{mod } m)$, ou seja, $m|(a.b - 1) \Rightarrow$ existe um inteiro $t$ tal que: $a.b - 1 = t.m \Rightarrow a.b - t.m = 1 \Rightarrow (a, m) = 1$ ($\Leftarrow$). Reciprocamente, se $(a, m) = 1$ existem inteiros $b$ e $t$ tais que $a.b + m.t = 1$ e, consequentemente, $\bar{1} = \overline{a.b + m.t} = \overline{a.b} + \overline{m.t} = \bar{a}.\bar{b} + \bar{0} = \bar{a}.\bar{b}$, assim sendo, $\bar{1} = \bar{a}.\bar{b}$, temos que $\bar{a}$ é invertível. ■

[1] Propriedade adicional de certos anéis, não compartilhada por todos os anéis: Um anel $A$ será chamado de domínio de integridade se possuir a seguinte propriedade:

$$\forall a, b \in A, a \neq 0 \text{ e } b \neq 0 \Rightarrow a.b \neq 0$$

que é equivalente à:

$$\forall a, b \in A, a.b = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

Os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são todos domínios de integridade.

**Corolário 1.3** *$\mathbb{Z}_m$ é um corpo se, e somente se, m é primo.*

**Demonstração: 1**

($\Rightarrow$) $\mathbb{Z}_m$ é um corpo se, e somente se, todos os elementos $\bar{1}, \bar{2}, \ldots, \overline{m-1}$ são invertíveis, o que, pela proposição acima, equivale ao fato de que $(1, m) = (2, m) = \ldots = (m-1, m) = 1$; e isso é, portanto, equivalente a $m$ ser primo. ($\Leftarrow$) Reciprocamente, seja $m$ primo, temos que, $\forall \bar{a} \in \mathbb{Z}_m$ temos que $(a, m) = 1$, logo, pela proposição acima, $\bar{a}$ é invertível. Sendo $\mathbb{Z}_m$, com $m$ primo, um anel onde todo elemento não nulo é invertível, então $\mathbb{Z}_m$ é um corpo. ■

**Demonstração: 2**

($\Rightarrow$) Se $\mathbb{Z}_m$ é um corpo e $m$ não é primo, então $m = m_1.m_2$ com $1 < m_1 < m$ e $1 < m_2 < m$, logo, $\bar{0} = \bar{m} = \overline{m_1}.\overline{m_2}$, com $\overline{m_1} \neq 0$ e $\overline{m_2} \neq 0$, contradição, pois todo corpo é domínio de integridade, ou seja, dado $m_1 \neq 0$ e $m_2 \neq 0 \Rightarrow m_1.m_2 \neq 0$. Logo $m$ é primo. ($\Leftarrow$) Reciprocamente, suponha $m$ primo. Como $(i, m) = 1$ para $i = 1, \ldots, m-1$, segue, pela proposição acima, que $\bar{1}, \bar{2}, \ldots, \overline{(m-1)}$ são invertíveis, logo $\mathbb{Z}_m$ é um corpo. ■

As próximas seções deste Capítulo são o resultado do estudo e análise principalmente do clássico texto de HEFEZ, A., VILLELA, M. L. T.: Códigos Corretores de Erros ([9]).

## 1.2 Conceitos Básicos sobre Códigos Corretores de Erros

Num sistema de informação entram dados, através de uma fonte de dados. Estes são inicialmente processados por um codificador da fonte projetado para representar os dados da fonte de maneira mais compacta. Esta representação é uma seqüência de símbolos chamada palavra código da fonte. Então, os dados são processados por um codificador de canal, que transforma a seqüência de símbolos da palavra código da fonte em outra seqüência chamada palavra código do canal.

A palavra código do canal é uma nova e longa seqüência que, geralmente, têm mais redundância que a palavra código da fonte. Depois, o modulador converte cada símbolo da palavra código do canal em um símbolo analógico correspondente de um conjunto finito de símbolos analógicos possíveis. A seqüência de símbolos analógicos é transmitida através do canal. Como o canal está sujeito a vários tipos de ruídos, distorções e interferências, os dados que saem do canal diferem dos dados que entram no canal. O demodulador converte cada sinal de saída do canal recebido na seqüência correspondente de símbolos da palavra código do canal.

Cada símbolo demodulado é a melhor estimativa do símbolo transmitido, mas o demodulador comete alguns erros devido a interferências do canal. A seqüência de símbolos demodulada é chamada de palavra recebida. Devido aos erros, os símbolos da palavra recebida nem sempre são iguais aos símbolos da palavra código do canal. O decodificador do canal usa a redundância da palavra código do canal para corrigir os erros da palavra recebida e então produzir uma estimativa da palavra código fonte. Se todos os erros são corrigidos, a palavra código fonte estimada é igual à palavra código fonte original. O decodificador da fonte executa a operação inversa do codificador da fonte e envia sua saída para o usuário.

O ponto de partida é um conjunto finito $A$ chamado de alfabeto. Seja $n$ um número natural. Um código corretor de erros é um subconjunto próprio qualquer de $A^n$. Quando $A$ é um corpo temos uma classe particularmente importante de códigos, que são os *códigos lineares*, que são subespaços vetoriais de $A^n$. Por exemplo, seja $A_2 = \{0, 1\}$ e vamos considerar $A_2^n$ (alfabeto binário). Um código corretor de erros sobre $A_2^3$ poderia ser: (000), (010), (100), (110). A quantidade de palavras do código, ou seja, a cardinalidade do código é menor ou igual a cardinalidade do conjunto $A^n$. No exemplo acima, a cardinalidade é 4 (poderia ser no máximo $8 = 2^3$).

Durante a transmissão dessas palavras por um canal físico, a informação é freqüentemente distorcida pelos ruídos. Para manejar essa indesejável mas inevitável situação, alguma forma de redundância deve ser incorporada à mensagem original. Com essa redundância, mesmo se alguns erros são introduzidos (em um nível tolerável), a informação original pode ser recuperada, ou pelo menos a presença desses erros pode ser detectada. Consideraremos nos próximos exemplos o código $C = (00), (01), (10), (11)$. Introduzindo redundância nas palavras do código, transformaremos as palavras de 2 bits para 5 bits, usando a seguinte correspondência:

00 - 00000

01 - 01011

10 - 10110

11 - 11101

Observa-se que os dois primeiros bits da informação com redundância correspondem à mensagem original, ou seja, nessa recodificação, as duas primeiras posições reproduzem o código da fonte, enquanto que as três posições restantes são redundâncias introduzidas. O novo código introduzido na recodificação é chamado de código do canal. Define-se $k$ como

sendo o tamanho da palavra original e $n$ o tamanho da palavra com redundância, no exemplo acima $k = 2$ e $n = 5$.

Define-se taxa de informação R como sendo:

$$R = \frac{k}{n}$$

ou seja, a relação entre a informação original pela informação enviada.

Suponhamos que temos um robô que se move sobre um tabuleiro quadriculado, de modo que, ao darmos um dos comandos (para frente, para trás, para direita ou para esquerda), o robô se desloca do centro de uma casa para o centro de outra casa adjacente indicada pelo comando. Os quatro comandos acima podem ser codificados como elementos de $\{0, 1\} \times \{0, 1\}$, como se segue:

Para frente $\rightarrow$ 00

Para direita $\rightarrow$ 10

Para trás $\rightarrow$ 01

Para esquerda $\rightarrow$ 11

O código acima é chamado de código da fonte. Suponhamos, agora, que esses pares ordenados devam ser transmitidos via rádio e que o sinal no caminho sofra interferências. Imaginemos que a mensagem 00 possa, na chegada ser recebida como 01, o que faria com que o robô, em vez de ir para frente, fosse para trás. O que se faz, então, é recodificar as palavras, de modo a introduzir redundâncias que permitam detectar e corrigir erros. Podemos, por exemplo, modificar o nosso código da fonte como já fizemos anteriormente.

Suponhamos que se tenha introduzido um erro ao transmitirmos, por exemplo, a palavra 01011, de modo que a mensagem recebida seja 11011. Comparando essa mensagem com as palavras do código, notamos que não lhe pertence e, portanto, detectamos erros. A palavra do código mais próxima da referida mensagem (a que tem menor número de componentes diferentes) é 01011, que é precisamente a palavra transmitida.

Para a introdução da redundância, no caso linear, utiliza-se uma matriz $k \times n$, cujas linhas formam um base para o código $C$. Essa matriz é denominada matriz geradora. Através de operações elementares nas linhas e colunas (permutação de duas linhas, multiplicação de uma linha por um escalar não nulo, adição de um múltiplo escalar de uma linha a outra,

permutação de duas colunas e multiplicação de uma coluna por um escalar não nulo), pode-se colocar a matriz geradora $G$ na forma padrão:

$$G = [I_d A]$$

onde $I_d$ representa a matriz identidade de ordem $k$ e $A$ uma matriz $k \times (n-k)$. Assim, a informação original estará nas primeiras $k$ posições da palavra com redundância.

Um Código Corretor de Erros, portanto, detecta e corrige erros na palavra recebida e, depois de corrigidos os erros, relaciona à palavra transmitida e transforma a palavra transmitida em código fonte para o usuário. Mas será que um Código detecta todos os erros de uma palavra recebida? E se detecta, pode corrigir todos eles? Estas respostas dependem do código que se está usando? Tenho certeza que perguntas como estas não querem calar.

Para começar a pensar sobre isso, lembremos do exemplo que demos anteriormente: recebendo a palavra 11011, comparamos essa mensagem com as palavras do código e notamos que ela não lhe pertence e, portanto, detectamos erros. Verificamos que a palavra do código mais próxima da referida mensagem (a que tem menor número de componentes diferentes) é 01011, que é precisamente a palavra transmitida, ou seja, detectou-se e corrigiu-se um erro. No entanto, digamos que a palavra recebida fosse 01110. Comparando esta mensagem com o código verificamos que ela não lhe pertence, no entanto, ao verificar qual a palavra do código mais próxima desta, encontramos duas com as mesmas chances: 01011 e 10110 (uma vez que estas duas palavras possuem dois componentes diferentes da palavra recebida). Nesse caso, não é possível estimar qual foi a palavra código transmitida.

## 1.3 Alfabeto

Para iniciar a construção de um código corretor de erros é necessário, primeiramente, definir o alfabeto $\mathbb{F}_q$, que é um corpo finito de $q$ elementos. Pode-se provar que existe um corpo de $q$ elementos se, e somente se, $q = p^m$, onde $p$ é um primo e $m$ é um natural, $m \geq 1$. No caso dos códigos binários $\mathbb{F}_2 = \{0, 1\}$. Um código corretor de erros é um subconjunto próprio qualquer de $\mathbb{F}_q^n = \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \times \ldots \times \mathbb{F}_q$, para algum número natural $n$. O número de elementos de um conjunto $\mathbb{F}_q$ será denotado por $|\mathbb{F}_q|$.

O código do robô é um subconjunto próprio de $\mathbb{F}_2^5$ , com $\mathbb{F}_2 = \{0, 1\}$, onde $\mathbb{F}_2^5 = \{(00000); (00001); (00010); (00100); \ldots; (11111)\}$ e $|\mathbb{F}_2^5| = 2^5 = 32$.

A fim de que possamos identificar as palavras mais próximas de uma dada palavra recebida com erro e estimar qual foi a palavra do código transmitida, vamos apresentar, mais a frente, um modo de medir a "distância" entre palavras em $\mathbb{F}_q^n$.

**Definição 1.6** *Um alfabeto finito é um corpo finito $\mathbb{F}_q$, onde $q = p^m$, $p$ primo e $m \geq 1$.*

**Definição 1.7** *Diremos que $C$ é um código de comprimento $n$ (sobre $\mathbb{F}_q$) se $C \subset \mathbb{F}_q^n$.*

**Observação 1.4** *Assim, $C$ é dito um código $q$-ário. Desse modo, tem-se códigos binários ($q = 2$), ternários ($q = 3$), etc.*

Caso você sinta-se inseguro com estas definições, pense em $\mathbb{F}_q$ como o conjunto dos símbolos $\{\bar{0}, \bar{1}, \ldots, \overline{q-1}\}$ com duas operações, a soma e o produto (valendo lembrar aqui que $q$ precisa ser primo para isso funcionar, ou seja, se $q = p$, $p$ primo, então $\mathbb{F}_p = \mathbb{Z}_p$ e são válidas as propriedades trabalhadas na seção 1.1). Para somarmos $\bar{x}$ e $\bar{y}$, fazemos a soma usual $x+y$, dividimos esta pelo primo $q$ e obtemos um resto inteiro $r$ entre 0 e $q-1$. Dizemos então que $\bar{r} = \bar{x} + \bar{y}$. O produto $\bar{x}.\bar{y}$ é definido de modo similar: fazemos o produto usual $x.y$, dividimos por $q$, obtemos um resto $r$ e definimos $\bar{r} = \bar{x}.\bar{y}$. Para maior esclarecimento, vamos apresentar as tabelas com a soma e o produto em $\mathbb{F}_2$ e $\mathbb{F}_3$.

$\mathbb{F}_2$;

| + | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{0}$ |

| · | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ |

$\mathbb{F}_3$;

| + | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

| · | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{1}$ |

## 1.4 Distância de Hamming

Para se identificar as palavras mais próximas de uma dada palavra recebida com erro e estimar qual foi a palavra código transmitida, apresentaremos um modo de "medir" a distância entre palavras de $\mathbb{F}_q^n$.

**Definição 1.8** *A distância de Hamming entre* $x, y \in \mathbb{F}_q^n$ *é dada por:*

$$d(x, y) = |\{i : x_i \neq y_i, 1 \leq i \leq n\}|.$$

Por exemplo, seja $\mathbb{F}_2$ e considerarmos $\mathbb{F}_2^3 = (\{0, 1\}^3)$, temos:

$$d(001, 111) = 2$$

$$d(000, 111) = 3$$

$$d(100, 110) = 1$$

**Proposição 1.8** *A Distância de Hamming é uma métrica, ou seja, dados* $x, y, z \in \mathbb{F}_q^n$*, valem as seguintes propriedades:*

(1) *Positividade:* $d(x, y) \geq 0$*, valendo a igualdade se, e somente se,* $x = y$*;*

(2) *Simetria:* $d(x, y) = d(y, x), \forall x, y \in \mathbb{F}_q^n$*;*

(3) *Desigualdade Triangular:* $d(x, y) \leq d(x, z) + d(z, y), \forall x, y, z \in \mathbb{F}_q^n$*;*

**Demonstração:** (1) Temos por definição que:

$d(x, y) = |\{i, x_i \neq y_i, 1 \leq i \leq n\}| \geq 0$

($\Rightarrow$) Caso $d(x, y) = 0$, temos que $x_i = y_i$ para $i = 1, 2, \ldots, n$ e daí $x = y$.

($\Leftarrow$) Se $x = y$, temos $x_j = y_j$, para $1 \leq j \leq n$ e, consequentemente $d(x, y) = 0$.

(2) Pela definição de distância de Hamming temos que $d(x, y) = |\{i, x_i \neq y_i, 1 \leq i \leq n\}| = |\{i, y_i \neq x_i, 1 \leq i \leq n\}| = d(y, x)$.

(3) Sejam:

$x = (x_1, x_2, x_3, \ldots, x_i)$

$y = (y_1, y_2, y_3, \ldots, y_i)$

$z = (z_1, z_2, z_3, \ldots, z_i)$

A cada $i$-ésima dupla de coordenadas iguais que tivermos em $x$ e $y$ contabilizamos 0, já a cada $i$-ésima dupla de coordenadas diferentes que tivermos em $x$ e $y$ contabilizamos 1.

Logo poderemos ter:

1º caso: $x_i = y_i \Rightarrow$ contribuição 0 (zero); portanto a soma $d(x, z) + d(z, y)$ da $i$-ésima coordenada pode ser zero ou dois, atendendo assim a desigualdade;

$2^o$ caso: $x_i \neq y_i \Rightarrow$ contribuição 1 (um); portanto não podemos ter $x_i = z_i$ e $z_i = y_i$, logo a soma $d(x,z)+d(z,y)$ da $i$-ésima coordenada deve ser um, atendendo assim a desigualdade;

■

As propriedades (1), (2) e (3) caracterizam o que se costuma, em matemática, chamar de métrica. Por isso, a distância de Hamming entre elementos de $\mathbb{F}^n$ é também chamada de métrica de Hamming.

**Definição 1.9** *Dados um elemento $a \in \mathbb{F}_q^n$ e um número real $r > 0$, definimos a* bola *e a* esfera *de centro em $a$ e raio $r$ como sendo respectivamente os conjuntos:*

$B(a,r) = \{x \in \mathbb{F}_q^n : d(x,a) \leq r\}$

$S(a,r) = \{x \in \mathbb{F}_q^n : d(x,a) = r\}$

**Definição 1.10** *Seja $C \subset \mathbb{F}_q^n$ um código. A* **distância mínima** *de $C$ é o número:*

$$d = min\,\{d(x,y) : x,y \in C \text{ e } x \neq y\}.$$

Por exemplo, se $C$ é o código do robô, temos que $d = 3$.

**Proposição 1.9** *Seja $C$ um código com distância mínima $d$. Se $c$ e $c'$ são palavras distintas de $C$, então $B(c,t) \cap B(c',t) = \varnothing$, onde $t = [\frac{d-1}{2}]$ sendo que $[*]$ representa a parte inteira de um número real $*$.*

**Demonstração:** De fato, se $x$ pertencesse à $B(c,t) \cap B(c',t)$ , teríamos $d(x,c) \leq t$ e $d(x,c') \leq t$ e, portanto, pela simetria, pela desigualdade triangular e pela definição de $t$ teríamos:

$d(c,c') \leq d(c,x) + d(x,c') \leq t + t = 2t \leq d - 1$ (Absurdo).

Como $d$ é a distância mínima de $C$, temos, necessariamente, $d(c,c') \geq d$.

Portanto $x \notin B(c,t) \cap B(c',t)$.

Logo $B(c,t) \cap B(c',t) = \varnothing$. ■

**Teorema 1.2** *Seja $C$ um código com distância mínima $d$ . Então $C$ pode corrigir até $[\frac{d-1}{2}]$ erros. Se $d$ é par, o código pode simultaneamente corrigir $\frac{d-2}{2}$ erros e detectar até $\frac{d}{2}$ erros.*

**Demonstração:**

Se ao transmitirmos uma palavra $c$ do código cometemos $s$ erros com $s \leq t$, recebendo a palavra $r$, então $d(r,c) = s \leq t$.

Como $B(c,t) \cap B(c',t) = \varnothing$, temos que $d(r,c') > t$, para toda palavra $c' \in C$, com $c' \neq c$ e, portanto, a decodificação pela vizinhança mais próxima vai corrigir este erro, pois $c$ está univocamente determinado a partir de $r$.

Agora, se $d$ for par, então $[\frac{d-1}{2}] = \frac{d-2}{2}$. Consequentemente $C$ pode corrigir $\frac{d-2}{2}$ erros. Mas se $\frac{d}{2}$ ocorreu, isso significa que a palavra recebida $r$ tem $d(c,r) = \frac{d}{2}$. Se existe alguma palavra $c \in C$ tal que $d(c,c') = d$, teremos que $r$ pode estar no "ponto médio" entre $c$ e $c'$. Neste caso $d(c',r) = \frac{d}{2}$ e o decodificador pode detectar que $\frac{d}{2}$ erros ocorreram, mas não pode corrigí-los pois existem duas possibilidades distintas $c$ e $c'$ para efetuar a decodificação pela vizinhança mais próxima.

Por outro lado, se mais de $\frac{d}{2}$ erros ocorrem, a palavra recebida $r$ pode estar mais próxima de outra palavra do código que não a correta.

Nesse caso, a decodificação de $r$ determinará $c'$ incorretamente. ■

Isso é chamado erro de decodificação. Em um código eficiente, isto raramente ocorre. No entanto, o fato de ocorrer erro de decodificação não é algo que tenha a ver apenas com o código; isso depende do canal também. Isto é, o código pode ser muito eficiente, no sentido de atingir um dos limitantes (Hamming ou Singleton) e mesmo assim não ser bom para o canal.

Por exemplo em um código com $d = 4$, é possível corrigir até $t = [\frac{4-1}{2}] = 1$ erro e detectar até $\frac{4}{2} = 2$ erros.

Note que pelo teorema anterior, um código terá maior capacidade de correção de erros quanto maior for a sua distância mínima. Portanto, é fundamental, para a Teoria de Códigos, poder calcular $d$, ou pelo menos determinar uma cota inferior para ele.

Vamos considerar agora dois exemplos de códigos de $\mathbb{F}_2$ com dimensão $k = 1$.

**Exemplo 1.5** *Consideremos* $\mathbb{F}_2^4$*:*

$$C_1 = \{(0,0,0,0);(1,1,1,1)\}.$$

*Obtemos então* $d = 4$ *e* $t = [\frac{4-1}{2}] = 1$ *(código de parâmetros* $[4,1,4]$*). Temos então as bolas disjuntas:*

$$B_1 = B((0,0,0,0),1) = \{(0,0,0,0),(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}$$

$$B_2 = B((1,1,1,1),1) = \{(1,1,1,1),(0,1,1,1),(1,0,1,1),(1,1,0,1),(1,1,1,0)\}$$

*Observe que ambas as bolas são disjuntas e contém, cada uma delas cinco pontos de* $\mathbb{F}_2^4$*. Temos então* $6 = 2^4 - 2 \cdot 5$ *pontos os quais não são cobertos por qualquer uma das bolas, pontos para os quais não sabemos decidir o que fazer.*

**Exemplo 1.6** *Consideremos* $\mathbb{F}_2^3$*:*

$$C_2 = \{(0,0,0);(1,1,1)\}.$$

*Obtemos então* $d = 3$ *e* $t = [\frac{3-1}{2}] = 1$ *(código de parâmetros* $[3,1,3]$*). Temos então as bolas disjuntas:*

$$B_1 = B((0,0,0),1) = \{(0,0,0),(1,0,0),(0,1,0),(0,0,1)\}$$

$$B_2 = B((1,1,1),1) = \{(1,1,1),(0,1,1),(1,0,1),(1,1,0)\}$$

*Temos agora que cada uma das bolas contém* 4 *pontos e* $B_1((0,0,0)) \cup B_2((1,1,1)) = \mathbb{F}_2^3$*. Em outras palavras, podemos escrever o espaço ambiente* $\mathbb{F}_2^3$ *como união disjunta de bolas centradas em pontos do código.*

Esta situação, do ponto de vista de códigos, é ideal, pois não importa qual a mensagem recebida $y$, saberemos sempre o que fazer com ela: se necessário trocamos $y$ pelo centro da única bola (desta família) que o contém.

É por este motivo que códigos com esta propriedade são ditos códigos perfeitos.

**Definição 1.11** *Seja* $C \subset \mathbb{F}_q^n$ *um código com distância mínima* $d$ *e seja* $t = [\frac{d-1}{2}]$*. O código* $C$ *será dito perfeito se:*

$$\bigcup_{c \in C} B(c,t) = \mathbb{F}_q^n.$$

Assim:

**Exemplo 1.7** *O código do Robô, em que* $d = 3$*, não é perfeito, pois ele é um código* $C \subset \mathbb{F}_2^5$*, onde*

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

*e, além disso*

$$\bigcup_{c \in C} B(c,1) \neq \mathbb{F}_2^5.$$

**Proposição 1.10** *Todo código $C$, $C \subset \mathbb{F}_2^n$, com dimensão 1, distância mínima igual ao comprimento ($n = d$), ou seja: $C = \{(0,0,\ldots,0),(1,1,\ldots,1)\}$, é perfeito se, e somente se, $n$ for ímpar.*

**Demonstração:** ($\Leftarrow$) Seja $n = d$, para $n$ par temos $d$ par, logo podemos fazer $d = 2a$, assim, para $d$ par:

$$t = \left[\frac{d-1}{2}\right] = \frac{d-2}{2} = \frac{2a-2}{2} = a-1$$

Assim, como podemos receber um vetor $r$ com metade das coordenadas iguais à 1 e metade igual à zero, este vetor não é coberto por nenhuma das bolas, logo qualquer $C \subset \mathbb{F}_2^n$ com $n$ par não é perfeito.

($\Rightarrow$) Seja $n = d$, para $n$ ímpar temos $d$ ímpar, logo podemos fazer $d = 2a+1$, assim, para $d$ ímpar:

$$t = \left[\frac{d-1}{2}\right] = \frac{d-1}{2} = \frac{2a+1-1}{2} = a$$

Assim, qualquer vetor recebido terá necessariamente mais coordenadas $1's$ do que $0's$ ou vice-versa, assim, sempre será coberto por uma das bolas, logo, qualquer código $C \subset \mathbb{F}_2^n$ com $n$ ímpar é perfeito. ■

**Observação 1.5** *É facil observar que os códigos de que tratam essa proposição são todos MDS ("Maximum Distance Separable"), ou seja, vale a igualdade: $d = n - k + 1$.*

**Lema 1.1**

$$|B(0,r)| = |B(c,r)|, \forall c \in \mathbb{F}_q^n.$$

**Demonstração:** É fácil contarmos o número de pontos em uma bola fechada. Examinemos as bolas centradas na origem, isto é, no ponto $(0,0,\ldots,0)$. Não perdemos qualquer generalidade, pois podemos sempre transladar as bolas para a origem, ou seja, para qualquer $x \in \mathbb{F}_q^n$ e qualquer positivo $r \geq 0$, temos que $y \in B(x,r)$ se, e somente se, $y - x \in B(0,r)$.

Portanto, há uma bijeção:

$$\psi : B(0,r) \longrightarrow B(c,r)$$

$$u \longmapsto u + c$$

onde:

*i*) $u \in B(0,r) \Rightarrow \psi(u) \in B(c,r)$.

De fato, tem-se que $d(\psi(u), c) = d(u+c, c) = w(u+c-c) = w(u)$.

*ii*) A função

$$\phi : B(c,r) \longrightarrow B(0,r)$$

$$v \longmapsto v - c$$

é a inversa, pois:

$\psi(\phi(v)) = \phi(v) - c = (v+c) - c = v, \ \forall \ v \in B(c,r)$

e, analogamente,

$\phi(\psi(u)) = u, \ \forall \ u \in B(0,r)$.

**Lema 1.2** *Para todo $c \in \mathbb{F}_q^n$ e todo número natural $r > 0$, temos que:*

$$|B(c,r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

**Demonstração:** Daremos, a seguir, uma idéia da demonstração. Para isso vamos estudar alguns casos em particular:

**Observação 1.6** *Nos exemplos a seguir, $*$ indica um elemento de $\mathbb{F}_q$ diferente de zero, ou seja, para cada lugar ocupado por $*$ nos vetores temos $(q-1)$ possibilidades.*

1. Supondo $n = 3, q > 1, r = 1, c =$ origem, temos:

   $|B(0,1)| = |S(0,0)| + |S(0,1)| \Rightarrow$

   $$(0,0,0) + \begin{cases} (*,0,0) \\ (0,*,0) \\ (0,0,*) \end{cases}$$

2. Supondo $n = 3, q > 1, r = 2, c =$ origem, temos:

   $|B(0,2)| = |S(0,0)| + |S(0,1)| + |S(0,2)| \Rightarrow$

$$(0,0,0) + \begin{Bmatrix} (*,0,0) \\ (0,*,0) \\ (0,0,*) \end{Bmatrix} + \begin{Bmatrix} (*,*,0) \\ (*,0,*) \\ (0,*,*) \end{Bmatrix}$$

3. Supondo $n = 4$, $q > 1$, $r = 2$, $c =$ origem, temos:

   $|B(0,2)| = |S(0,0)| + |S(0,1)| + |S(0,2)| \Rightarrow$

$$(0,0,0,0) + \begin{Bmatrix} (*,0,0,0) \\ (0,*,0,0) \\ (0,0,*,0) \\ (0,0,0,*) \end{Bmatrix} + \begin{Bmatrix} (*,*,0,0) \\ (*,0,*,0) \\ (*,0,0,*) \\ (0,*,*,0) \\ (0,*,0,*) \\ (0,0,*,*) \end{Bmatrix}$$

Em cada vetor pertencente à esfera de raio $i$ escolhemos $i$ coordenadas, dentre $n$ coordenadas para serem diferentes de zero, ou seja, temos uma combinação de $n$ elementos tomados $i$ a $i$, ou seja:

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}$$

Deste modo, a esfera de raio $i$ tem

$$\binom{n}{i}(q-1)^i$$

vetores. Assim, nos casos estudados, temos:

1. $$|B(c,1)| = \binom{3}{0}(q-1)^0 + \binom{3}{1}(q-1)^1 = \sum_{i=0}^{1}\binom{3}{i}(q-1)^i$$

2. $$|B(c,2)| = \binom{3}{0}(q-1)^0 + \binom{3}{1}(q-1)^1 + \binom{3}{2}(q-1)^2 = \sum_{i=0}^{2}\binom{3}{i}(q-1)^i$$

3.
$$|B(c,2)| = \binom{4}{0}(q-1)^0 + \binom{4}{1}(q-1)^1 + \binom{4}{2}(q-1)^2 = \sum_{i=0}^{2}\binom{4}{i}(q-1)^i$$

Assim, dados $n > 1$, $q > 1$, $r \in \mathbb{N}$ e $c \in \mathbb{F}_q^n$ (uma vez que $d_h = w_h$), temos que:

$$|B(c,r)| = |S(c,0)| + |S(c,1)| + \cdots + |S(c,r)| = \sum_{i=0}^{r}\binom{n}{i}(q-1)^i$$

■

## 1.5 Códigos Lineares

A classe de códigos mais utilizada na prática é a chamada classe dos códigos lineares.

**Definição 1.12** *Um código $C \subset \mathbb{F}_q^n$ será chamado de* **código linear** *se for um sub-espaço vetorial de $\mathbb{F}_q^n$.*

Desse modo, $C$ é por definição um espaço vetorial de dimensão finita. Denotaremos por $k$ a dimensão do código $C$. Conseqüentemente, todo elemento de $C$ se escreve de modo único da seguinte maneira:

$$(*)\ \alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_k u_k, \alpha_i \in \mathbb{F}_q,$$

onde $i = 1, 2, \ldots, k$; em que $\{u_1, u_2, \ldots, u_k\}$ é uma base de $C$. Como $\alpha_i \in \mathbb{F}_q$, $i = 1, 2, \ldots, k$; existem $q$ possibilidades para cada um dos $\alpha_i$ em $(*)$. Logo, existem $q^k$ elementos em $C$, isto é,

$$M = |C| = q^k,$$

e, consequentemente,

$$\dim C = k \log_q q = \log_q q^k = \log_q M.$$

**Definição 1.13** *Dado $u \in \mathbb{F}_q^n$, define-se o* **peso** *de $u$ como sendo o número inteiro:*

$$w(u) := |\{i, u_i \neq 0\}|,$$

*ou seja: $w(u) = d(u, 0)$, em que $0$ é o vetor nulo de $\mathbb{F}_q^n$.*

**Definição 1.14** *O peso de um código linear $C$, é o inteiro $w(C) = \min\{w(u) : u \in C - \{0\}\}$.*

**Proposição 1.11** *Seja $C \subset \mathbb{F}_q^n$ um código linear com distância mínima $d$. Temos que:*

*i)* $\forall u, v \in \mathbb{F}_q^n; d(u, v) = w(u - v)$;

*ii)* $d = w(C)$.

**Demonstração:**

*i)* $d(u, v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}| = |\{i : u_i - v_i \neq 0, 1 \leq i \leq n\}| = w(u - v)$;

*ii)* Para todo par de elementos $u, v \in C$ com $u \neq v$, temos que $z = u - v \in C$ (Note que todo vetor pode ser escrito como uma diferença entre ele e o vetor nulo). Daí $d(u, v) = w(z)$. Portanto, o conjunto $\{w(z) : z \in C - \{0\}\}$ é igual ao conjunto $\{d(u, v) : u, v \in C \text{ e } u \neq v\}$.

Assim: $d = \min\{d(u, v) : u, v \in C \text{ e } u \neq v\} = \min\{w(z) : z \in C - \{0\}\} = w(C)$. ■

Em virtude desta proposição, a distância mínima de um código linear $C$ será também chamada de peso do código $C$.

Em álgebra linear, se conhecem essencialmente duas maneiras de se descrever subespaços vetoriais $C$ de um espaço vetorial $\mathbb{F}_q^n$, uma como imagem, e outra como núcleo de transformação linear.

Vamos obter a representação de $C$ como imagem de uma transformação linear. Escolha uma base $\{v_1, v_2, \ldots, v_k\}$ de $C$ e considere a aplicação linear:

$$T : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$$

$$(a_1, a_2, \ldots, a_k) \longmapsto a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$$

Temos que $T$ é uma transformação linear injetora, pois o $\ker(T) = 0$, tal que $\text{Im}\ (T) = C$.

Portanto, dar um código $C \subset \mathbb{F}_q^n$ de dimensão $k$ é equivalente a dar uma transformação linear injetora $T : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$ e definir $C = \text{Im}\ (T)$

**Exemplo 1.8** *Considere a transformação linear:*

$$T : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^5$$

$$(x_1, x_2) \longmapsto (x_1, x_2, x_1, x_1 + x_2, x_2)$$

*Temos que:*

$$T(x_1, x_2) = (0, 0, 0, 0, 0), \text{ se } (x_1, x_2, x_1, x_1 + x_2, x_2) = (0, 0, 0, 0, 0),$$

*ou seja,* $x_1 = x_2 = 0$. *Logo* $\ker(T) = \{(0, 0)\}$. *Portanto,* $T$ *é injetora e daí* $Im\,(T) = C$ *(a imagem de* $T$ *é um código* $C$*). Como* $x_1, x_2 \in \mathbb{F}_2$, *temos* $|C| = 2^2 = 4$ *e*

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

*Além disso,* $w(C) = 3$ *e* $C$ *corrige* $t = [\frac{d-1}{2}] = 1$ *erro.*

## 1.6 Matriz Geradora e Matriz Teste de um Código

Dado um código linear $C \subset \mathbb{F}_q^n$, chamaremos de parâmetros do código linear $C$ os inteiros $[n, k, d]$, onde $k$ é a dimensão de $C$ sobre $\mathbb{F}_q$, $d$ representa a distância mínima de $C$ e $n$ é denominado o comprimento do código $C$.

Seja o código linear $C = [u_1, u_2, \ldots, u_k]$ com $B = \{u_1, u_2, \ldots, u_k\}$ base de $C$, com $u_i = (u_{i1}, u_{i2}, \ldots, u_{in})$. A matriz:

$$G_{k\times n} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{pmatrix} = \begin{pmatrix} u_{11} & u_{12} & \ldots & u_{1n} \\ u_{21} & u_{22} & \ldots & u_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ u_{k1} & u_{k2} & \ldots & u_{kn} \end{pmatrix}$$

é chamada de matriz geradora de $C$ associada à base:

$$B = \{u_1, u_2, \ldots, u_k\}$$

**Exemplo 1.9** *No exemplo anterior,* $B = \{(1, 0, 1, 1, 0); (0, 1, 0, 1, 1)\}$ *é uma base de* $C$ *e:*

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

*é uma matriz geradora do código linear* $C$. *De fato,*

$$(0,0)\cdot G = (0,0)\cdot \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (0,0,0,0,0),$$

$$(0,1)\cdot G = (0,1)\cdot \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (0,1,0,1,1),$$

$$(1,0)\cdot G = (1,0)\cdot \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (1,0,1,1,0),$$

$$(1,1)\cdot G = (1,1)\cdot \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (1,1,1,0,1),$$

De maneira geral, consideramos a transformação linear definida por:

$$T : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$$

$$x \longmapsto xG$$

Se $x = (x_1, x_2, \ldots, x_k)$, temos $T(x) = xG = x_1u_1 + x_2u_2 + \ldots + x_ku_k$, ou seja, $T\left(\mathbb{F}_q^k\right) = C$. Podemos, então, considerar $\mathbb{F}_q^k$ como sendo um código da fonte, $C$ o código do canal e a transformação $T$, uma codificação.

Além disso, devemos ressaltar que a matriz geradora $G$ não é única, pois ela depende da base $B$. Portanto, mudando para uma base $\bar{B}$, teremos uma outra matriz geradora $\bar{G}$ para o mesmo código $C$. Da Álgebra Linear, sabemos que $\bar{G}$ pode ser obtida de $G$ através de operações elementares (permutação de duas linhas; multiplicação de uma linha por um escalar não nulo e adição de um múltiplo escalar de uma linha a outra) com as linhas de $G$ e vice versa.

Podemos também fazer o inverso, ou seja, construir códigos a partir de matrizes geradoras $G$. Para isto, basta tomar uma matriz cujas linhas sejam Linearmente Independentes e definir um código como sendo a imagem da transformação linear:

$$T : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$$

$$x \longmapsto xG$$

Seguindo o exemplo dado anteriormente, a partir da matriz geradora $G$, podemos construir uma matriz de teste de paridade $H$ utilizada para decodificação das palavras. Com a matriz $H$, pode-se determinar se uma palavra pertence ou não ao código.

Uma matriz teste de $C$ é uma matriz $H$, de posto $n-k$, tal que:

$$v \in C \iff H \cdot v^t = \vec{0}.$$

Temos que, se:

$$G = [Id_k|A]$$

é geradora de $C$, então

$$H = [A^t|Id_{n-k}]$$

é matriz teste de $C$.

Assim, seja a matriz $G$ do exemplo dado anteriormente,

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

temos

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

Dessa forma, temos a matriz $H$ do exemplo:

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

Para saber se a palavra pertence ao código, basta multiplicar a palavra recebida $v$ pela matriz teste de paridade. Se o resultado for o vetor nulo,

$$H \cdot v^t = \vec{0}$$

a palavra pertence ao código. Qualquer outro vetor não nulo como resultado significa que a palavra recebida contém erro(s).

Suponhamos que a palavra recebida seja $v_1 = (1, 0, 1, 1, 0)$,

$$H \cdot v_1^t = \vec{0}$$

isto é, $v_1$ é uma palavra do nosso código.

Seja a palavra $v_2 = (0, 1, 0, 1, 0)$,

$$H \cdot v_2^t = (0, 0, 1)$$

então a palavra contém erro(s).

Capítulo 2

# CÓDIGOS DE HAMMING E LIMITANTES

Neste capítulo nos dedicamos aos limitantes de Singleton e de Hamming, além de tratar dos Códigos de Hamming. Para isso, nos valemos do estudo, principalmente, de [1], além de [2] e [6].

## 2.1 Limitante de Singleton

Através da matriz teste de paridade podemos fazer uma interpretação do problema da distância mínima. Veja que se as colunas da matriz $H$ são $h_1, h_2, \ldots, h_n$, e $c = (c_1, c_2, \ldots, c_n)$ é um vetor de $\mathbb{F}^n$, então:

$$H.c^T = [h_1^T h_2^T \ldots h_n^T].c = c_1.h_1^T + c_2.h_2^T + \ldots + c_n.h_n^T.$$

Assim, cada palavra $c$ do código $C$ (definido por $H$) fornece uma combinação linear entre vetores-coluna de $H$. Reciprocamente, se os escalares $c_1, c_2, \ldots, c_n$ dão origem a uma combinação linear:

$$c_1.h_1^T + c_2.h_2^T + \ldots + c_n.h_n^T = 0,$$

então o vetor $c = (c_1, c_2, \ldots, c_n)$ está em $C$. Note também que, olhando apenas as coordenadas não-nulas, obtemos uma dependência linear entre $w(c)$ colunas, onde $w(c)$ é o peso do vetor $c$. Este argumento prova o seguinte resultado:

**Lema 2.1** *Seja $C$ código em $\mathbb{F}_q^n$ e seja $H$ uma matriz teste para $C$:*

*1) Se todo conjunto de $d-1$ colunas de $h$ é linearmente independente, a distância mínima de $C$ é pelo menos $d$.*

*2) O código $C$ tem distância mínima igual a $d$ se e somente se todo conjunto de $d-1$ colunas é linearmente independente, e existe um conjunto de $d$ colunas que é linearmente dependente.*

**Demonstração:**

1) Suponhamos que cada conjunto de $d-1$ colunas de $H$ é linearmente independente. Seja $c = (c_1, c_2, \ldots, c_n)$ uma palavra não nula de $C$ e sejam $h_1, h_2, \ldots, h_n$ as colunas de $H$. Como $H.c^T = 0$, temos que:

$$0 = H.c^T = \sum c_i h_i \ (*).$$

Visto que $w(c)$ é o número de componentes não nulos de $c$, segue que se $w(c) \leq d-1$, teríamos, por $(*)$, uma combinação nula de um número $t$, com $1 \leq t \leq d-1$, de colunas de $H$, o que é contraditório. Logo, $w(c) \geq d$ e, portanto, $w(C) \geq d$.

Reciprocamente, suponhamos que $w(C) \geq d$. Suponhamos também, por absurdo, que $H$ tenha $d-1$ colunas linearmente independentes, digamos $h_{i_1}, h_{i_2}, \ldots, h_{i_{d-1}}$. Logo, existiriam $c_{i_1}, c_{i_2}, \ldots, c_{i_{d-1}}$, no corpo, nem todos nulos, tais que:

$$c_{i_1}.h_{i_1} + c_{i_2}.h_{i_2} +, \ldots, + c_{i_{d-1}}.h_{i_{d-1}} = 0.$$

Portanto, $c = (o, \ldots, c_{i_1}, 0, \ldots, c_{i_{d-1}}, 0, \ldots, 0) \in C$ e, consequentemente $w(c) \leq d-1 < d$, o que seria um absurdo.

2) Admitamos $w(C) = d$, logo todo conjunto de $d-1$ colunas de $H$ é linearmente independente. Se não existir pelo menos um conjunto com $d$ colunas de $H$ linearmente dependentes, ter-se ia, por 1) que $w(C) \geq d+1$, o que é uma contradição. Portanto, existe pelo menos um conjunto com $d$ colunas de $H$ que são linearmente dependentes.

Reciprocamente, admitamos que todo conjunto de $d-1$ colunas de $H$ é linearmente independente e existe um conjunto com $d$ colunas de $H$ que é linearmente dependente.

Por 1) tem-se que $w(C) \geq d$. Mas $w(C)$ não pode ser maior que $d$, pois neste caso, por 1) todo conjunto com $d$ colunas de $H$ seria linearmente dependente, o que é uma contradição. Portanto $w(C) = d$. ■

Agora já podemos aplicar isso a alguns casos específicos.

**Corolário 2.1** *Seja $C$ um código binário e seja $H$ uma matriz teste para $C$. Se todas as colunas de $H$ são não nulas e distintas, então a distância mínima de $C$ é pelos menos* 3.

**Demonstração:** De fato, sobre $\mathbb{F}_2$, dois vetores não nulos são linearmente dependentes (L.D.) apenas se são iguais. Logo, se todas as colunas são distintas, então todos os conjuntos de duas colunas são linearmente independentes (L.I.), e a distância mínima é maior ou igual à 3. ■

**Observação 2.1** *Os códigos de Hamming, $\mathcal{H}_m$, de que trataremos adiante possuem matrizes $H$ com estas características, logo $d \geq 3$ nesses códigos. Veremos que, na verdade, $d = 3$.*

Recordemos que o posto de $H$ é a dimensão da imagem de $H$, que é o número máximo de colunas L.I. de $H$. Prova-se que o posto de $H$ é igual ao de $H^T$ e, portanto, que é igual ao número máximo de linhas L.I. Assim, se $H$ é uma matriz $k \times n$, posto $(H) \leq k$ e posto $(H) \leq n$.

**Proposição 2.1** *(Limitante de Singleton)*

*Se $C$ é um código $[n, k, d]$ então:*

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

*Este é um dos limitantes que envolve os três parâmetros fundamentais. Quando ocorre a igualdade o código é MDS ("Maximum Distance Separable"). Alguns dos códigos mais utilizados atualmente são deste tipo. Faremos a seguir duas provas desta proposição.*

**Demonstração:** (1)

O "Teorema do Núcleo e Imagem", traduzido para nossa situação, afirma que:

$$\text{posto } (H) + \dim(C) = n$$

Assim, seja um código $C$, de parâmetros $[n, k, d]$ e sua matriz teste $H$. Pelo Lema 2.1, todo conjunto de $d-1$ vetores é L.I, em particular, posto $(H) \geq d-1$. Por outro lado, o "Teorema do Núcleo e Imagem" diz que posto $(H) = n-k$; logo, temos: $n-k \geq d-1 \Rightarrow d \leq n-k+1$. ■

**Demonstração:** (2)

Seja $H$ uma matriz de verificação de paridade de um código linear $C$, com parâmetros $[n, k, d]$. Então o posto de $H$ é $n-k$, pois a mesma é uma matriz de ordem $(n-k) \times n$, isto é, $n-k$ linhas linearmente independentes.

Logo, cada coluna de $H$ tem $n-k$ entradas, ou seja, comprimento $n-k$, ou ainda, estão em $\mathbb{F}_q^{n-k}$. Pelo Lema 2.1, quaisquer $d-1$ colunas de $H$ são linearmente independentes.

Como um conjunto de vetores de $\mathbb{F}_q^{n-k}$ que é L.I. tem no máximo $n-k$ vetores, então:

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

Daí:

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

■

## 2.2 Limitante de Hamming

A importância dos códigos de Hamming, dos quais trataremos na próxima seção, vem do Limitante de Hamming, o qual é geométrico-combinatório, tendo um estilo totalmente diferente do Limitante de Singleton.

Seja $C$ um código $[n, k, d]$, $t = [\frac{d-1}{2}]$ e $u$ e $v$ dois elementos distintos de $C$, recordemos que:

$$B(u, t) \cap B(v, t) = \varnothing$$

Logo, se tomarmos a união de todas as bolas de raio $t$ centradas em elementos de $C$ não teremos sobreposição em nenhuma delas, e assim:

$$|\bigcup_{c \in C} B(c, t)| = \sum_{c \in C} |B(c, t)|$$

Como temos $q^n$ vetores em $\mathbb{F}_q^n$, já concluímos que:

$$q^n \geq \sum_{c \in C} |B(c,t)|$$

Para melhorar o termo à direita vamos usar o fato de que cada uma destas bolas tem o mesmo número de elementos. De fato basta ver que a aplicação $v \longmapsto v + c$ estabelece uma bijeção entre $B(0,t)$ e $B(c,t)$, para qualquer $c$, como já mostrado no Capítulo 1. Assim, basta calcular quantos elementos temos em $B(0,t)$.

**Proposição 2.2** *Seja $V = \mathbb{F}_2^n$:*

*1) O número de elementos de peso igual à $r$ em $V$ é $\binom{n}{r}$.*

*2) O número de elementos de $B(0,t)$ em $V$ é:*

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}.$$

**Demonstração:** $w(v) = r$ se, e somente se $v$ tem $r$ coordenadas iguais à 1 (e $n-r$ nulas). Assim, para listar todos os vetores com peso $r$, precisamos escolher $r$ posições para colocar 1, o que dá $\binom{n}{r}$ escolhas e $\binom{n}{r}$ vetores.

Como $B(0,r)$ consiste dos vetores que tem peso $r$ ou menos, se chamarmos de $S(0,r)$ a esfera dos vetores de peso $r$, temos:

$$B(0,r) = S(0,0) \cup S(0,1) \cup \ldots \cup S(0,r)$$

e como $S(0,i) \cap S(0,j) = \varnothing$ se $i \neq j$, temos o resultado. ■

Com isso podemos obter, finalmente, o limitante:

**Teorema 2.1** *Limitante de Hamming*

*Seja $C$ um código $[n,k,d]$ em $\mathbb{F}_q^n$ e seja $t = [\frac{d-1}{2}]$. Então:*

$$q^{n-k} \geq \binom{n}{0}(q-1)^0 + \binom{n}{1}(q-1)^1 + \cdots + \binom{n}{t}(q-1)^t.$$

Os códigos que atingem a igualdade na expressão acima são chamados de *perfeitos*.

**Definição 2.1** *Seja $C$ um código $[n, k, d]$ em $\mathbb{F}_2^n$ e seja $t = [\frac{d-1}{2}]$. O código $C$ é perfeito se*

$$2^{n-k} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t},$$

*ou seja, se*

$$\mathbb{F}_2^n = \bigcup_{c \in C} B(c, t)$$

**Observação 2.2** *Ao contrário dos MDS, não existem muitos códigos perfeitos e todos os lineares já estão classificados: eles são, a menos de equivalência, os códigos triviais de $2t+1$ repetições, os códigos de Hamming, que apresentaremos a seguir, e os dois códigos de Golay (um binário e outro ternário). Prova-se também que os códigos não-lineares perfeitos têm os mesmos parâmetros dos códigos de Hamming. No entanto, existem outras métricas em uso, como a métrica de Lee e as métricas de tipo "Poset", onde a classificação dos códigos perfeitos ainda está por ser feita. Destas últimas trataremos nos demais capítulos deste trabalho.*

## 2.3 Códigos de Hamming

Um código de Hamming de ordem $m$ sobre $\mathbb{F}_2$ é um código com matriz teste de paridade $H_m$ de ordem $m \times n$, cujas colunas são os elementos de $\mathbb{F}_2^m - \{0\}$ numa ordem qualquer. Essa definição de $H_m$ determina o código $C$ a menos da equivalência.

Temos, portanto, que o comprimento ($n$) de um código de Hamming de ordem $m$ é igual à $2^m - 1$.

Pela definição de $H_m$ e pela observação acima temos que o posto $m = n-k \Rightarrow k = n-m$, ou seja, a dimensão de um código de Hamming de ordem $m$ é dado por:

$$k = n - m = 2^m - m - 1.$$

A matriz $H_m$ não tem nenhuma coluna nula e nenhuma coluna repetida. Pelo teorema acima, verificamos facilmente que $d = 3$, independente de $m$, pois em $H_m$ é fácil achar três colunas linearmente dependentes. Assim, um código $\mathcal{H}_m$ detecta até dois erros e corrige até um erro.

**Proposição 2.3** *Todo código de Hamming é perfeito.*

**Demonstração:** Como $d = 3$, temos $t = [\frac{d-1}{2}] = 1$.

Dado $c$ em $\mathbb{F}_2^n$ temos que $|B(c,1)| = 1 + n$.

Portanto:

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

e, consequentemente:

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

■

**Observação 2.3** *Verifica-se facilmente que um código de Hamming de ordem m é MDS se, e somente se, $m = 2$. Basta usar $k = n - m$.*

**Observação 2.4** *O fato de $\mathcal{H}_m$ ser um código perfeito, ou seja, todo elemento de $\mathbb{F}_2^{2^m-1}$ está à uma distância de no máximo um de uma palavra do código, retrata uma distribuição muito uniforme do código no espaço de dimensão maior. Por exemplo, em $\mathcal{H}_3$ teremos as $2^4 = 16$ palavras do código muito bem distribuídas nos $2^7 = 128$ elementos de $\mathbb{F}_2^7$, de forma que nenhum deste dista mais que um de alguma destas palavras.*

**Observação 2.5** *Os códigos de Hamming surgiram com Richard Hamming, considerado por muitos o primeiro teórico de códigos da história, e o primeiro código que apresentou foi o $H_3$, que já é um código muito bom.*

*Posteriormente, Hamming generalizou este código para outras dimensões e Marcel Golay construiu códigos semelhantes para quaisquer corpos finitos. Aqui apresentamos apenas a família binária dos códigos de Hamming.*

Capítulo 3

# INTRODUÇÃO AOS CÓDIGOS EM CONJUNTOS PARCIALMENTE ORDENADOS ("POSETS")

Grande parte dos resultados deste capítulo foram alcançados através do estudo da primeira seção do artigo "Codes with a poset metric" de Brualdi, Graves e Lawrence ([5]) e do texto "Códigos e Métricas" de Firer e Panek ([6]).

## 3.1 Definição da Métrica

Nesta seção introduziremos as métricas ponderadas (*poset-metric* em inglês). O conceito de métricas ponderadas por ordens parciais foi introduzido, em [5], por Richard A. Brualdi, Janine Smolin Graves e K. Mark Lawrence em 1995. No entanto, alguns anos antes Harald Niderreiter, ([13]), falou sobre um caso particular dessas métricas, que trata da união disjunta de cadeias de mesmo comprimento. A partir de 2003, diversos trabalhos tem aprofundado o conhecimento sobre estes espaços.

Considere um conjunto finito com $n$ elementos. Sem perda de generalidade vamos assumir que este é o conjunto que contém os números naturais $1, 2, 3, \ldots n$ e denotá-los por $[n] := \{1, 2, 3, \ldots n\}$.

**Definição 3.1** *Uma ordem parcial $P$ em um conjunto $X$ é um subconjunto $R \subset X \times X$ satisfazendo as seguintes condições:*

*(i)* $(x, x) \in R, \forall x \in X$;

*(ii) Dados* $x, y \in X$, *se* $(x, y) \in R$ *e* $(y, x) \in R$, *então* $x = y$;

*(iii) Se* $(x, y) \in R$ *e* $(y, z) \in R$, *então* $(x, z) \in R, \forall x, y, z \in X$.

Neste caso dizemos que $X$ é ordenado por $R$. Por analogia com a ordem usual da reta real, dada uma ordem parcial em $X$ nós dizemos que $x \leq y$ se $(x, y) \in R$, e escrevemos $P = (X, \leq)$. Além disso, usaremos tanto "conjunto ordenado" quanto "poset" (de "partially-ordered set") neste texto.

Um *ideal* em uma ordem $P = (X, \leq)$ é um conjunto $I \subset X$ que contém todos os elementos de $X$ menores que algum elemento de $I$, ou seja, se $x \in X, y \in I$ e $x \leq y$, então $x \in I$. Dado $J = \{x_1, x_2, \ldots, x_n\} \subset X$, chamamos de *ideal gerado por* $J$ o menor ideal de $X$ contendo $J$, usando qualquer uma das notações $\langle J \rangle$ ou $\langle x_1, x_2, \ldots, x_n \rangle$. Como $X$ é um ideal contendo $J$ e a intersecção de ideais é um ideal, temos que o ideal gerado por um conjunto sempre existe e:

$$\langle J \rangle = \bigcap_{\text{I é ideal ; J} \subset \text{I}} I.$$

Seja $P$ um poset arbitrário de cardinalidade $n$. Se $A \subseteq P$ então $\langle A \rangle$ denota o menor ideal de $P$ que contém $A$ (uma vez que a intersecção de ideais é um ideal, $\langle A \rangle$ é a intersecção de todos os ideais de $P$ contendo $A$).

Considere o vetor espaço $\mathbb{F}_q^n$ de n-uplas de $\mathbb{F}_q$. Sem perda de generalidade, assumimos que $P = [n]$ e, assim, as coordenadas positivas de $\mathbb{F}_q^n$ estão em correspondência uma a uma com os elementos de $P$. Seja $x = (x_1, x_2, \ldots, x_n)$ um vetor de $\mathbb{F}_q^n$. Definimos o *$P$-peso* ponderado de $x$ como sendo a cardinalidade

$$w_P(x) = |\langle \operatorname{supp}(x) \rangle|$$

do menor ideal de $P$ contendo o suporte de $x$, onde:

$$\operatorname{supp}(x) = \{i : x_i \neq 0\}.$$

Note que se $x'$ é obtido a partir de $x$ alterando uma ou mais coordenadas não nulas para zero, então é possível que $w_P(x') = w_P(x)$. Se $x$ e $y$ são dois vetores de $\mathbb{F}_q^n$, então definimos a *métrica ponderada* (por $P$), denominada *$P$-distância* por:

$$d_P(x, y) := w_P(x - y)$$

**Lema 3.1** *Se $P$ é uma ordem em $[n]$, então $P$-distância $d_P(\cdot, \cdot)$ é uma métrica sobre $\mathbb{F}_q^n$.*

**Demonstração:** Claramente, a $P$-distância é simétrica e positiva definida. Para provar que $d_P(x, y) \leq d_P(x, z) + d_P(z, y)$ para todo $x, y, z \in \mathbb{F}_q^n$ basta mostrar que $w_P(x - y) \leq w_P(x - z) + w_P(z - y)$.

Fazendo $(x - z) = u$ e $(z - y) = v$ temos que $(x - y) = (x - z) + (z - y) = (u + v)$, assim, basta mostrar que:

$$w_P(u + v) \leq w_P(u) + w_P(v),$$

para quaisquer $u, v \in \mathbb{F}_q^n$. Visto que $\text{supp}\,(u + v) \subset \text{supp}\,(u) \cup \text{supp}\,(v)$ e uma vez que a união de dois ideais também é um ideal; $\langle I \cup J \rangle = \langle I \rangle \cup \langle J \rangle$, temos que:

$$\begin{aligned} w_P(u + v) &= |\langle \text{supp}\,(u + v) \rangle| \\ &\leq^* |\langle \text{supp}\,(u) \rangle \cup \langle \text{supp}\,(v) \rangle| \\ &\leq |\langle \text{supp}\,(u) \rangle| + |\langle \text{supp}\,(v) \rangle| \\ &\leq w_P(u) + w_P(v). \end{aligned}$$

■

**Observação 3.1** *Na demonstração acima, o sinal $\leq$ marcado com $*$, explica-se porque na soma das coordenadas de vetores podemos ter coordenadas anuladas, o que justifica o $\leq$:*

$$w_P(u + v) = |\langle supp\,(u + v) \rangle| \leq |\langle supp\,(u) \rangle \cup \langle supp\,(v) \rangle|$$

Sendo $d_P$ uma métrica, todos os conceitos referentes à métrica, como bolas, esferas, distância mínima e outros, são denotados como o uso do sub-índice $P$ ($B_P(x, r)$, $S_P(x, r)$ e $d_P(C)$ respectivamente), a menos que a falta dos índices não cause confusão.

**Definição 3.2** *Um elemento é maximal em um ideal se não há nenhum elemento maior do que ele no ideal, ou seja, um elemento $x$ é maximal em um ideal $I$ se não há nenhum elemento maior do que $x$ em $I$.*

Se $\mathbb{F}_q^n$ é dotado de uma métrica ponderada, então chamamos um subconjunto $C$ de $\mathbb{F}_q^n$ de Código Parcialmente Ordenado (*poset-code* em inglês). Se a métrica ponderada corresponde a uma ordem parcial $P$, então $C$ é um *$P$-código*. Segue a notação usual da teoria do códigos. Assim, se $C$ é linear, então $C$ é um subespaço sobre $\mathbb{F}_q^n$ de dimensão $k$, logo $C$ é um *poset-code* $[n, k]$. Se $d_P$ é a mínima $P$-distância entre distintos vetores do código $C$ (se $C$ é linear, então é o mesmo que o mínimo $P$-peso de vetores não nulos), então $C$ tem parâmetros $[n, k, d_P]$.

Seja $x$ um vetor em $\mathbb{F}_q^n$ e seja $r$ um inteiro não negativo. A $P$-bola com centro $x$ e raio $r$ é o conjunto:

$$B_P(x, r) = \{y \in \mathbb{F}_q^n : d_P(x, y) \leq r\},$$

de todos os vetores em $\mathbb{F}_q^n$ cuja $P$-distância à $x$ é, no máximo, igual à $r$. Já a $P$-esfera com centro $x$ e raio $r$ é o conjunto:

$$S_P(x, r) = \{y \in \mathbb{F}_q^n : d_P(x, y) = r\},$$

de todos os vetores em $\mathbb{F}_q^n$ cuja $P$-distância à $x$ é, exatamente, igual à $r$.

O número de vetores em $\mathbb{F}_q^n$ cuja distância ao vetor nulo é exatamente igual à $i$ é:

$$\begin{cases} 1, & \text{se i = 0,} \\ \sum_{j=1}^{i} (q-1)^j \cdot q^{i-j} \cdot \Omega_j(i), & \text{se i > 0} \end{cases}$$

onde $\Omega_j(i)$ é igual ao número de ideais de $P$ com cardinalidade $i$ que tem exatamente $j$ elementos maximais. Essa afirmação será provada mais adiante.

Visto que $d_P(x, y) = d_P(0, y - x)$, segue que o número de vetores na bola de raio $r$ não depende de seu centro (pois podemos sempre transladar as bolas para a origem, ou seja,

para qualquer $x \in \mathbb{F}_q^n$ e qualquer positivo $r \geq 0$, temos que $y \in B_P(x, r)$ se, e somente se, $y - x \in B_P(0, r)$) e é igual a:

$$1 + \sum_{i=1}^{r} \sum_{j=1}^{i} (q-1)^j \cdot q^{i-j} \cdot \Omega_j(i).$$

Em particular, se $q = 2$, o número de vetores na bola de raio $r$ é:

$$1 + \sum_{i=1}^{r} \sum_{j=1}^{i} 2^{i-j} \cdot \Omega_j(i).$$

**Definição 3.3** *Diremos que um código linear $C \subset \mathbb{F}_q^n$, é um $r$-código $P$-perfeito (ou simplesmente perfeito se $d_P$ é a métrica de Hamming) se existir $r \in \mathbb{N}$ tal que a união de todas as bolas de raio $r$ centradas nos elementos de $C$ é igual à $\mathbb{F}_q^n$ sendo esta união disjunta. Em outras palavras, $C$ é perfeito se:*

$$\bigcup_{u \in C} B_P(u, r) = \mathbb{F}_q^n$$

$$B_P(u, r) \cap B_P(v, r) = \varnothing$$

*qualquer que seja $u, v \in C$ com $u \neq v$.*

Fixada uma métrica $d$ em $\mathbb{F}_q^n$ e dado um número $r > 0$, um problema central de teoria de códigos clássica, é descobrir quais códigos (se existem) são $r$-perfeitos em $(\mathbb{F}_q^n, d)$. No caso das métricas poset consideramos um problema "inverso": dados um código $C$ em $\mathbb{F}_q^n$, que não é perfeito com a métrica de Hamming, e um número $r > 0$, quais são (se existem) as métricas poset que tornam este código $r$-perfeito? Ou seja, um problema interessante em relação às $P$-métricas, dado $r > 0$ é o de classificar as ordens parciais $P$ que tornam um determinado código não perfeito $C \subseteq \mathbb{F}_q^n$ um $r$-código $P$-perfeito.

**Observação 3.2** *As métricas ponderadas abrangem a métrica de Hamming, pois quando $P$ é uma ordem anti-cadeia ($x \not\leq y$ para todo $x \neq y \in [n]$), ou seja, cada elemento é comparável apenas consigo próprio, então $P$-peso e $P$-distância são, respectivamente, peso de Hamming e distância de Hamming da clássica teoria dos códigos.*

**Observação 3.3** *Se $P$ é união disjunta de cadeias de mesmo comprimento, a métrica $d_P$ coincide com a métrica de Rosenbloom-Tsfasman apresentada em [15], que foi definida independentemente da teoria de $P$-códigos.*

## 3.2 Código de Hamming Estendido

Qualquer código $[n, k]$ pode ser **estendido**, isto é, a partir da matriz de paridade H de $[n, k]$ a matriz $H_E$ é obtida de H conforme segue:

$$H_E = \left(\begin{array}{ccc|c} 1 & \dots & 1 & 1 \\ \hline & & & 0 \\ & H & & \dots \\ & & & 0 \end{array}\right).$$

Demonstra-se que a distância mínima de Hamming de um código estendido é igual à distância mínima do código não-estendido acrescido de 1 (convém lembrar que a distância aumenta de um se for ímpar; se for par, ela não muda), isto é, $d_{\min}E = d_{\min} + 1$.

Assim, dado o código de Hamming $\mathcal{H}_m$ com matriz de verificação de paridade $H_m$, acrescentamos a esta uma linha com todas as entradas iguais a 1 e completamos a última coluna com 0's:

$$\hat{H}_m = \left(\begin{array}{ccc|c} 1 & \dots & 1 & 1 \\ \hline & & & 0 \\ & H_m & & \dots \\ & & & 0 \end{array}\right).$$

O *código de Hamming estendido* $\hat{\mathcal{H}}_m$ é definido como o código linear que tem $\hat{H}_m$ como matriz de paridade:

$$\hat{\mathcal{H}}_m = \{x \in \mathbb{F}_2^{2^m} : \hat{H}_m \cdot x = 0\}.$$

Sendo que $H_m$ é uma matriz com $2^m - 1$ colunas e um máximo de $m$ linhas Linearmente Independentes, temos que $\hat{H}_m$ tem $2^m$ colunas e $m + 1$ linhas L.I., de modo que $\hat{\mathcal{H}}_m$ é um $[2; 2^m; 2^m - m - 1]$ código linear.

Considerando-se a métrica de Hamming, é possível demonstrar que a distância mínima de $\hat{\mathcal{H}}_m$ é $d(\hat{\mathcal{H}}_m) = 4$, de modo que o raio de empacotamento é $R_e(\hat{\mathcal{H}}_m) = [\frac{4-1}{2}] = 1$.

Em um $\mathbb{F}_q^n$, considerando-se a métrica de Hamming, temos que $|B_H(0, 1)| = n(q-1)+1$. Assim, considerando $\hat{\mathcal{H}}_m \subset \mathbb{F}_2^{2^m}$ temos que $|B_H(0, 1)| = 2^m + 1$. Observe ainda que $\hat{\mathcal{H}}_m$ tem dimensão $2^m - m - 1$, de modo que possui $2^{2^m-m-1}$ elementos. As bolas de raio 1 centradas

nestes pontos são disjuntas mas a união destas tem $(2^m + 1) \cdot (2^{2^m - m - 1})$ pontos e como $2^m + 1$ é ímpar, temos que:

$$|B_H(u, 1)| \cdot |\hat{\mathcal{H}}_m| = (2^m + 1) \cdot (2^{2^m - m - 1}) < 2^{2^m} = |\mathbb{F}_2^{2^m}|,$$

ou seja, estas bolas não cobrem o espaço $\mathbb{F}_2^{2^m}$ e, considerando-se a métrica de Hamming, $\hat{\mathcal{H}}_m$ não é perfeito.

A seguir mostraremos que, considerando-se uma métrica $d_P$ ponderada por uma ordem parcial, $\hat{\mathcal{H}}_m$ torna-se perfeito. Além disso, a capacidade de correção de $\hat{\mathcal{H}}_m$ aumenta para 2.

Seja $[2^m] = \{1, 2, \ldots, 2^m\}$ munido com a ordem onde as únicas relações existentes são $i \leq i$ e $1 \leq i$ para $i = 1, 2, 3, \ldots, 2^m$. Esta ordem é conhecida como *ordem* $[1, 2^m]$*-semi-fraca*.

**Teorema 3.1** *Para cada inteiro positivo n, $P_n$ denota o conjunto parcialmente ordenado com elementos $\{1, 2, \ldots, n\}$ tal que $1 < i$ para cada $i = 2, 3, \ldots, n$ e estas são as únicas estritas comparações. Assim, para cada inteiro positivo m, o código binário de Hamming estendido $\hat{\mathcal{H}}_m$, com parâmetros $[n = 2^m, 2^m - m - 1, 4]$, é um $P_n$-código perfeito.*

**Demonstração:**

A prova que $\hat{\mathcal{H}}_m$ é um $P_n$-código perfeito segue do fato das bolas de raio 2 sobre as $2^{2^m - m - 1}$ "palavras" do código serem duas a duas dinjuntas e cobrirem perfeitamente $\mathbb{F}_2^{2^m}$. Dessa forma, para mostrar que $\hat{\mathcal{H}}_m$ é perfeito quando é considerado um $P$-código, devemos determinar inicialmente a cardinalidade das $P$-bolas em $\mathbb{F}_2^{2^m}$ e para isto basta determinar $|B_P(0, r)|$.

Seja $[2^m] = \{1, 2, \ldots, 2^m\}$. Seja $x \in B_P(0, r)$. Então $w_P(x) = i$ com $i \leq r$. Se $i = 0$ ou 1, temos exatamente um vetor em $\mathbb{F}_2^{2^m}$ com peso 0 ou 1 respectivamente, a saber $(0, 0, \ldots, 0)$ e $(1, 0, \ldots, 0)$. Se $i > 0$, então temos em $[2^m]$ um total de $\begin{pmatrix} 2^m - 1 \\ i - 1 \end{pmatrix}$ ideais com cardinalidade $i$, determinados pela escolha de $i - 1$ elementos diferentes de 1 que são elementos maximais.

Em $\mathbb{F}_2^{2^m}$ cada coordenada associada a um dos $i - 1$ elementos maximais escolhidos em $[2^m]$ deve ser igual à 1, e as outras iguais à 0 (associadas aos outros elementos maximais), já a primeira coordenada pode ser 0 ou 1.

Assim, para $i > 1$, temos:

$$2 \cdot |S_P(0,i)| = 2 \cdot \begin{pmatrix} 2^m - 1 \\ i - 1 \end{pmatrix}$$

possibilidades para $x$.

Portanto:

$$|B_P(0,r)| = 1 + 1 + \sum_{i=2}^{r} 2 \cdot \begin{pmatrix} 2^m - 1 \\ i - 1 \end{pmatrix}.$$

A distância mínima em $\hat{\mathcal{H}}_m$ é 4.

Afirmamos que bolas de raio 2 centradas em pontos de $\hat{\mathcal{H}}_m$ cobrem o espaço $\mathbb{F}_2^{2^m}$ e são duas a duas disjuntas, ou seja, com $P$-métrica $\hat{\mathcal{H}}_m$ é perfeito e o raio de empacotamento $R_e = 2$ (na métrica de Hamming $R_e$ de $\hat{\mathcal{H}}_m$ é 1).

Para mostrar que $B_P(u,2) \cap B_P(v,2) = \varnothing$ para todo $u, v \in \hat{\mathcal{H}}_m$, com $u \neq v$, é suficiente mostrar que:

$$B_P(0,2) \cap B_P(u,2) = \varnothing \text{ para todo } u \in \hat{\mathcal{H}}_m - \{0\}.$$

Seja $u \in \hat{\mathcal{H}}_m$ e suponha que exista $x \in \mathbb{F}_2^{2^m}$ tal que:

$$x \in B_P(0,2) \cap B_P(u,2).$$

Podemos fazer as seguintes observações:

- Com peso 1 temos só o vetor $(1, 0, \ldots, 0)$;
- Com peso 2: os vetores possuem uma coordenada não nula a partir da segunda;
- $w_P(u) \geq 4 \Rightarrow u$ tem ao menos 3 posições entre $2, 3, \ldots, 2^m$ iguais à 1;
- $x$ tem no máximo uma destas posições não nulas.

Além disso, $u - x$ tem no mínimo duas dentre estas posições não nulas, mais a primeira coordenada não nula, de modo que: $d_P(x,u) = w_P(u-x) \geq 3$, o que contradiz a hipótese de termos $x \in B_P(0,2)$ e, assim, temos que:

$$B_P(0,2) \cap B_P(u,2) = \varnothing \text{ para todo } u \in \hat{\mathcal{H}}_m - \{0\}.$$

Mas cada bola de raio 2 tem:

$$|B_P(0,2)| = 1 + 1 + 2 \cdot (2^m - 1) = 2^{m+1}$$

elementos. (Veja que $\begin{pmatrix} 2^m - 1 \\ i - 1 \end{pmatrix}$ para $i = 2$ é igual à $(2^m - 1)$).

Além disso, $\hat{\mathcal{H}}_m$ tem $2^{2^m - m - 1}$ elementos, logo temos que:

$$|B_P(u,2)| \cdot |\hat{\mathcal{H}}_m| = (2^{m+1}) \cdot (2^{2^m - m - 1}) = 2^{2^m} = |\mathbb{F}_2^{2^m}|,$$

donde segue que $\hat{\mathcal{H}}_m$ é um $P_n$-código perfeito. ■

## 3.3 Resultados sobre Ideais e Contagem dos Elementos da Bola

A Proposição seguinte nos ajudará à provar o próximo Lema.

**Proposição 3.1** *Seja $P$ poset e $I$ um ideal de $P$.*

1. *Se $X$ e $Y$ são subconjuntos de $P$ tais que $X \subset Y$, então $\langle X \rangle \subset \langle Y \rangle$.*
2. *Se $I$ é um ideal de $I$, então $\langle I \rangle = I$.*
3. *Se $M(I) = \{i_1, i_2, \ldots, i_m\}$ é o conjunto de maximais de $I$, então $I = \langle M(I) \rangle$.*

**Demonstração:**

1. Seja $J$ um ideal de $P$. Se $X \subset Y$ e $J \supset Y$ então $J \supset X$.

   Por definição temos que o ideal gerado por um conjunto sempre existe e:

   $$\langle Y \rangle = \bigcap_{\text{J é ideal}; J \supset Y} J \supset X.$$

   Assim $X \subset \langle Y \rangle$.

Da teoria de conjuntos, temos que o conjunto intersecção está contido em cada um dos conjuntos da intersecção, ou seja:

$$\bigcap_{j=1}^{n} A_j \subset A_i; i = 1, \ldots, n.$$

Assim:

$$\langle X \rangle = \bigcap_{\text{J é ideal}; J \supset X} J \subset \langle Y \rangle.$$

2. Por definição

$$\langle I \rangle = \bigcap_{\text{J é ideal}; J \supset I} J.$$

Ou seja, dado $I = \{x_1, \ldots, x_r\} \subset X$, o ideal gerado por $I$ é o menor ideal de $X$ contendo $I$. No entanto, $I$ é ideal, assim temos que algum $J$ ideal é igual à $I$, além disso todos os ideais $J'$s contém $I$ ($J_i \supset I$):

$J_1 \cap J_2 \cap I \cap \ldots \cap J_i \supset I$, logo:

$$\langle I \rangle = \bigcap_{J \supset I} J = I.$$

3. Devemos mostrar que:

$I \subset \langle M(I) \rangle$ $(*)$ e $\langle M(I) \rangle \subset I$:

Temos $\langle M(I) \rangle = \bigcap_{J \supset M(I)} J$ (definição).

$(*)$ Agora:

$J \supset M(I) \Rightarrow J \supset I$

Portanto:

$\langle M(I) \rangle = \bigcap_{J \supset M(I)} J \supset I$

Por definição temos que $M(I) \subseteq P$, então $\langle M(I) \rangle$ denota o menor ideal de $P$ que contém $M(I)$. ($\langle M(I) \rangle$ é a intersecção de todos os ideais de $P$ contendo $M(I)$).

$I \subset X$ contém todos os elementos de $X$ menores que algum elemento de $I$, ou seja, se $x \in X, y \in I$ e $x \leq y$, então $x \in I$, assim $I \subset \langle M(I) \rangle$, pois todo elemento de $I$:

- ou é maximal, logo pertence ao conjunto $M(I)$;
- ou, se não é maximal, é menor que algum maximal, logo pertence ao ideal gerado por $M(I)$.

Como $X$ é um ideal contendo $J$ e a intersecção de ideais é um ideal, temos que o ideal gerado por um conjunto sempre existe e:

$$\langle M(I)\rangle = \bigcap_{J\supset M(I)} J,$$

$J \supset M(I) \Rightarrow J \supset I$, portanto $\langle M(I)\rangle = \bigcap_{J\supset M(I)} J \supset I$

$X \in I$, então:

- $x \in M(I)$, ou
- $x \notin M(I) \Rightarrow \exists$ i maximal $(i \in M(I))$, tal que $x < i (i \in J$ pois $j \subset M(I)) \Rightarrow x \in J$

Assim:

$$I \subset \langle M(I)\rangle \text{ e } \langle M(I)\rangle \subset I \Rightarrow I = \langle M(I)\rangle.$$

■

**Lema 3.2** *Dado $X \subset P$, seja $I$ ideal de $P$ e $M(I) = \{i_1, i_2, \ldots, i_m\}$ o conjunto de maximais de $I$, então:*

$$\langle X\rangle = I \textit{ se, e somente se, } M(I) \subset X \subset I$$

**Demonstração:** Usaremos os ítens (1), (2) e (3) da Proposição 3.1.

($\Leftarrow$) Temos:

$$M(I) \subset X \subset I \Rightarrow \text{ por (1)}$$

$$\langle M(I)\rangle \subset \langle X\rangle \subset \langle I\rangle \Rightarrow \text{ por (2) e (3)}$$

$$I \subset \langle X\rangle \subset I \Rightarrow$$

$$\langle X\rangle = I$$

($\Rightarrow$) $\langle X\rangle = I \Rightarrow$ por (3), $\langle X\rangle = \langle M(I)\rangle$.

Temos que, dado $x \in I$, ou $x \in M(I)$ ou $x$ é menor do que algum elemento que pertence à $M(I)$. Assim, a cardinalidade $|M(I)|$ é a menor dentre os conjuntos $X$, tal que $\langle X \rangle = I$, e todo elemento de $M(I)$ está em $X$, assim sendo:

$$M(I) \subset X.$$

Ainda temos que:

$$\langle X \rangle = I \Rightarrow \text{ por (2), } \langle X \rangle = \langle I \rangle.$$

Temos que a cardinalidade, $|X|$, de qualquer conjunto $X$ tal que $\langle X \rangle = I$ é menor ou igual à $|I|$ e todo $x \in X$ está no ideal, logo $x \in I$, assim:

$$X \subset I.$$

Logo temos

$$M(I) \subset X \subset I,$$

concluindo assim a demonstração de que:

$$\langle X \rangle = I \text{ se, e somente se, } M(I) \subset X \subset I.$$

■

**Corolário 3.1** *$I$ ideal de $P$, $v \in \mathbb{F}_q^n$:*

$$\langle supp\ (v) \rangle = I \iff M(I) \subset supp\ (v) \subset I$$

Voltemos agora, através do teorema seguinte, aos resultados da contagem dos elementos de uma bola de raio $r$, já enunciadas mas não provadas anteriormente.

**Teorema 3.2** *O número de vetores em $\mathbb{F}_q^n$ cuja distância ao vetor nulo é exatamente igual a $i$ é:*

$$\begin{cases} 1, & \text{se } i = 0, \\ \sum_{j=1}^{i} (q-1)^j \cdot q^{i-j} \cdot \Omega_j(i), & \text{se } i > 0 \end{cases}$$

*onde $\Omega_j(i)$ é igual ao número de ideais de $P$ com cardinalidade $i$ que tem exatamente $j$ elementos maximais.*

**Demonstração:** De fato, se $i = 0$, temos apenas um vetor, o próprio vetor nulo que está à uma distância zero dele mesmo.

Para $i > 0$, seja $v \in S_P(0, i)$, $\langle \text{supp } (v) \rangle$ é um ideal de $i$ elementos maximais, ou seja, $1 \leq j \leq i$ ($I$ tem no máximo $i$ maximais, que é o caso em que todos os elementos do Ideal são maximais). Dado um Ideal $I$ de $i$ elementos, vamos determinar quantos vetores $v$ satisfazem $\langle \text{supp } (v) \rangle = I$.

Assim, seja $v$ em $\mathbb{F}_q^n$ e $v \in S_P(0, i)$, podemos escrever:

$$v = \sum_{i \in M(I)} a_i e_i + \sum_{i \in I - M(I)} b_i e_i + \sum_{i \notin I} c_i e_i$$

onde $e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$, ou seja, a $i$-ésima coordenada é igual à 1 e as demais são nulas.

Seja $v \in S_P(0, i)$ e seja $I = \langle \text{supp } (v) \rangle$, então, pelo Corolário 3.1, $M(I) \subset \text{ supp } (v) \subset I$. Assim, temos, para cada $v$, que cada coordenada ($a_i$) que é maximal ($j$ coordenadas) não pode ser 0, logo restam $(q-1)$ valores a escolher para cada coordenada, ou seja, $(q-1)^j$ escolhas.

Por sua vez, para as coordenadas ($b_i$) que pertencem ao ideal mas não são maximais, $(i-j)$ coordenadas, podemos, para cada uma delas, escolher entre $q$ valores, uma vez que não há restrições, assim temos $q^{i-j}$ escolhas.

Por fim, as coordenadas ($c_i$) do vetor que não pertencem ao ideal , $(n-i)$ são, necessariamente, nulas, ou seja, há apenas uma possibilidade.

Assim, se:

$$v \in S_P(0, i) \iff |\langle \text{supp } (v) \rangle| = i.$$

Dado $i$, teremos ideais com diferentes número de maximais, assim podemos ter ideais da seguinte forma:

$J_1^1, \ldots J_{m_1}^1$ (ideais com $i$ elementos dos quais 1 é maximal);

$J_1^2, \ldots J_{m_2}^2$ (ideais com $i$ elementos dos quais 2 são maximais);

$\vdots$

$J_1^i, \ldots J_{m_i}^i$ (ideais com $i$ elementos dos quais $i$ são maximais);

Pelo Corolário 3.1

$$|A_l^j| = |\{v \in \mathbb{F}_q^n; \langle \text{supp } (v)\rangle = J_l^j\}| \Longleftrightarrow M(J_l^j) \subset \text{supp } (v) \subset J_l^j.$$

Assim, temos:

$$|S_P(0,i)| = \sum_{j=1}^{i} \left( \sum_{l=1}^{m_j} A_l^j \right).$$

Como a contagem dos ideais de $P$ com $i$ elementos, que tem exatamente $j$ maximais depende de cada conjunto ordenado, ou seja, de como é a ordem do conjunto, chamaremos essa contagem de $\Omega_j(i)$.

Em cada ideal desses temos $[(q-1)^j \cdot q^{i-j}]$ vetores, como já mostramos, logo temos que:

$$|S_P(0,i)| = \sum_{j=1}^{i} (q-1)^j \cdot q^{i-j} \cdot \Omega_j(i), \text{ se } i > 0,$$

o que conclui a demonstração. ■

**Corolário 3.2** *Seja $x$ um vetor em $\mathbb{F}_q^n$ e seja $r$ um inteiro não negativo. O número de vetores na P-bola com centro $x$ e raio $r$ é igual a:*

$$1 + \sum_{i=1}^{r} \sum_{j=1}^{i} (q-1)^j \cdot q^{i-j} \cdot \Omega_j(i).$$

**Demonstração:** De fato, visto que $d_P(x,y) = d_P(0, y-x)$, segue que o número de vetores na bola de raio $r$ não depende de seu centro (pois podemos sempre transladar as bolas para a origem, ou seja, para qualquer $x \in \mathbb{F}_q^n$ e qualquer positivo $r \geq 0$, temos que $y \in B_P(x,r)$ se, e somente se, $y - x \in B_P(0,r)$). Assim, basta contar o número de vetores na bola centrada no vetor nulo, ou seja, os vetores cuja distância ao vetor nulo é menor ou igual à $r$. Pelo Teorema 3.2 o número de vetores em $\mathbb{F}_q^n$ cuja distância ao vetor nulo é exatamente igual a $i$ é:

$$\begin{cases} 1, & \text{se i = 0,} \\ \displaystyle\sum_{j=1}^{i} (q-1)^j \cdot q^{i-j} \cdot \Omega_j(i), & \text{se i > 0} \end{cases}$$

onde $\Omega_j(i)$ é igual ao número de ideais de $P$ com cardinalidade $i$ que tem exatamente $j$ elementos maximais.

Temos ainda que a $P$-bola com centro no vetor nulo e raio $r$ é igual a união do vetor nulo com as esferas de raio $i$, com $1 \leq i \leq r$, ou seja:

$$B_P(0,r) = \{\vec{0}\} \cup S_P(0,1) \cup \ldots \cup S_P(0,r)$$

Assim, temos que o número de vetores na $P$-bola com centro $x$ e raio $r$ é igual a:

$$1 + \sum_{i=1}^{r} \sum_{j=1}^{i} (q-1)^j \cdot q^{i-j} \cdot \Omega_j(i).$$

Em particular, se $q = 2$, o número de vetores na bola de raio $r$ é:

$$1 + \sum_{i=1}^{r} \sum_{j=1}^{i} 2^{i-j} \cdot \Omega_j(i).$$

■

Capítulo 4

# CÓDIGOS EM CONJUNTOS PARCIALMENTE ORDENADOS DE UMA E DUAS CADEIAS

Neste capítulo, grande parte dos resultados foram alcançados através do estudo da segunda seção do artigo "Codes with a poset metric" de Brualdi, Graves e Lawrence ([5]) e do texto "Códigos e Métricas" de Firer e Panek ([6]). Além disso, para compreender o "Princípio da Casa dos Pombos", necessário para mostrar alguns resultados, recorremos à "Introdução à Análise Combinatória", de J. Plínio de O., M. P. Mello e I. T. C. Murari ([16]).

## 4.1 Códigos Perfeitos e Raio de Empacotamento

Os resultados desta seção podem ser encontrados em [6].

Dado um código $C$ com raio de empacotamento $R_e(C)$, consideramos todas as bolas de raio $R_e$ centradas nos pontos do código. Quando uma mensagem é recebida e constata-se a existência de erro, verifica-se em qual destas bolas a mensagem recebida se encontra e corrigimos o erro assumindo que a mensagem enviada é a mais próxima da recebida, ou seja, o centro da bola em questão. No entanto, encontramos problema para a correção de erros, por exemplo, quando a mensagem recebida não pertence à nenhuma destas bolas. Em

um código perfeito isto nunca ocorre, pois toda mensagem recebida pertence à alguma bola centrada em um ponto do código.

Segue, no caso particular de trabalharmos com um código $C \subset \mathbb{F}_q^n$ que, independente da métrica em questão:

$$\left[\frac{d_P - 1}{2}\right] \leq R_e(C) \leq d_P - 1.$$

Veremos que a segunda das desigualdades não é estrita, ou seja, exibiremos um código $C$ e uma ordem $P$ tais que $R_e(C) = d_P(C) - 1$.

**Exemplo 4.1** *Seja $P = ([3], R)$, a ordem total $1 \leq 2 \leq 3$. Afirmamos que $R_e(C) = 2$, sendo $C = \{000, 101\}$, que coincide com $d_P(C) - 1$, já que $w_P(101) = 3 = d_P(C)$.*

*De fato as bolas de raio 2 centradas nos elementos de C são disjuntas:*

$$B_P(000, 2) = \{000, 010, 110\}$$

*e*

$$B_P(101, 2) = \{101, 001, 011, 111\}$$

*O mesmo não acontece se aumentarmos o raio das bolas:* 001 *pertence à intersecção $B_P(000, 3) \cap B_P(101, 3)$. Concluímos então que $R_e(C) = 2$.*

Este exemplo pode ser estendido para dimensões arbitrárias, o que será feito auxiliado pelo próximo lema:

**Lema 4.1** *Seja $[n] = \{1, 2, \ldots, n\}$ munido com a ordem total $1 \leq 2 \leq \ldots \leq n$ (cadeia). Se $u \in B_P(v, r)$ e $w_P(v) > r$, então:*

$$\langle supp\ (u)\rangle = \langle supp\ (v)\rangle,$$

*ou seja,* $\max\{supp\ (u)\} = \max\{supp\ (v)\}$.

**Demonstração:**

Seja $u \in B_P(v, r)$. Suponha que $\langle \text{supp } (u)\rangle \subset \langle \text{supp } (v)\rangle$, com $\langle \text{supp } (u)\rangle \neq \langle \text{supp } (v)\rangle$, então $\langle \text{supp } (v)\rangle = \langle \text{supp } (v-u)\rangle$. Daí segue que $d_P(u, v) = w_P(v-u) = w_P(u) > r$, assim $u \notin B_P(v, r)$, contradizendo a hipótese.

Suponha agora que $\langle \text{supp}\ (u)\rangle \supset \langle \text{supp}\ (v)\rangle$, com $\langle \text{supp}\ (u)\rangle \neq \langle \text{supp}\ (v)\rangle$. Então $\langle \text{supp}\ (u)\rangle = \langle \text{supp}\ (v-u)\rangle$. Donde segue que $d_P(u,v) = w_P(v-u) = w_P(u)$. Como $\langle \text{supp}\ (u)\rangle \supset \langle \text{supp}\ (v)\rangle$ e, por hipótese $w_P(v) > r$, segue que $w_P(u) > r$. Logo $d_P(u,v) > r$, o que contradiz o fato de que $u \in B_P(v,r)$.

Como em $P$ as únicas possibilidades são $\langle i\rangle \subset \langle j\rangle$, $\langle i\rangle \supset \langle j\rangle$ ou $\langle i\rangle = \langle j\rangle$, concluímos que:

$$\langle \text{supp}\ (u)\rangle = \langle \text{supp}\ (v)\rangle$$

■

Agora sim podemos mostrar que nas ordens totais o raio de empacotamento é sempre o máximo possível ($d_P - 1$), o que permite abundância de códigos perfeitos.

**Teorema 4.1** *Seja $[n] = \{1, 2, \ldots, n\}$ totalmente ordenado, $1 \leq 2 \leq \ldots \leq n$. Se $C \subset \mathbb{F}_q^n$ é um código com distância mínima igual à $d_P$, então $C$ tem a capacidade de corrigir $d_P - 1$ erros.*

**Demonstração:** Queremos provar que

$$B_P(0, d_P - 1) \cap B_P(v, d_P - 1) = \varnothing$$

para todo $v \in C - \{0\}$. Se $u \in B_P(0, d_P - 1) \cap B_P(v, d_P - 1)$, com $w_P(v) \geq d_P$, segue do Lema 4.1 que:

$$\langle \text{supp}\ (u)\rangle = \langle \text{supp}\ (v)\rangle,$$

já que $u \in B_P(v, d_P - 1)$. Daí tem-se $w_P(u) = w_P(v) \geq d_P$, o que é um absurdo, pois $u \in B_P(0, d_P - 1)$, ou seja, $w_P(u) \leq d_P - 1$. Portanto $B_P(0, d_P - 1) \cap B_P(v, d_P - 1) = \varnothing$. ■

## 4.2 Códigos de uma Cadeia

Seja $P$ um conjunto parcialmente ordenado com elementos $\{1, 2, \ldots, n\}$, e seja $C$ um código em $\mathbb{F}_q^n$ cujas coordenadas são indexadas por elementos de $P$.

Primeiramente caracterizaremos códigos $P$-perfeitos no caso em que $P$ é uma cadeia.

**Teorema 4.2** *Seja $P$ um Poset com elementos $\{1, 2, \ldots, n\}$ onde $1 < 2 < \ldots < n$, e seja $C$ um código em $\mathbb{F}_q^n$.*

*Então $C$ é um P-código perfeito se, e somente se, existir um inteiro $k$, com $0 \leq k \leq n$ tal que $|C| = q^k$ e o conjunto de todos os vetores $(x_{n-k+1}, \ldots, x_n) \in \mathbb{F}_q^k$ tal que*

$$(x_1, \ldots, x_{n-k}, x_{n-k+1}, \ldots, x_n) \in C$$

*para algum*

$$(x_1, \ldots, x_{n-k}) \in \mathbb{F}_q^{n-k}$$

*é igual à $\mathbb{F}_q^k$.*

*Em particular, o código linear $C_k$ de dimensão $k$ formado por todos os vetores*

$$(0, 0, \ldots, 0, a_{n-k+1}, \ldots, a_n) \text{ em } \mathbb{F}_q^n$$

*cujas primeiras $n-k$ coordenadas são iguais à zero é um P-código perfeito com P-distância mínima igual à $n-k+1$.*

Antes de provar este Teorema, provaremos um Lema sobre os códigos de uma cadeia e, como consequência deste, um Corolário sobre os códigos perfeitos de uma cadeia.

**Lema 4.2** *Sejam $C \subseteq \mathbb{F}_q^n$, $P$ cadeia. A distância mínima de $C$ é pelo menos $d_P$ se, e somente se, para cada*

$$(x_d, x_{d+1} \ldots, x_n) \in \mathbb{F}_q^{n-d+1}$$

*existe, no máximo, um vetor em $C$ com estas $n-d+1$ coordenadas.*

**Demonstração:** ($\Rightarrow$) Seja $d$ a distância mínima $C \subseteq \mathbb{F}_q^n$ e sejam

$$u = (\ldots, x_d, u_{d+1}, \ldots, u_n) \text{ e } v = (\ldots, x_d, v_{d+1}, \ldots, v_n)$$

dois vetores de $C$ cujas últimas $n-d+1$ coordenadas são iguais, assim, temos $d(u,v) = w(u-v) < d$, contradição, pois, por hipótese, $d$ é a distância mínima.

($\Leftarrow$) Sejam $x = (x_1, \ldots, x_d, x_{d+1}, \ldots, x_n)$ e $y = (y_1, \ldots, y_d, y_{d+1}, \ldots, y_n)$ vetores distintos de $C$. Por hipótese, $x$ é o único vetor de $C$ que tem as últimas $n-d+1$ coordenadas iguais a $(x_d, x_{d+1}, \ldots, x_n)$. Assim, temos que $x_i \neq y_i$ para algum $i$, com $d \leq i \leq n$. Logo:

$$d_P(x,y) = w_P(x-y) \geq d$$

e a distância mínima de $C$ é pelo menos $d$. ■

**Corolário 4.1** *Nos P-códigos de uma cadeia, perfeitos, existe exatamente um vetor em C, como descrito acima.*

**Demonstração:** Se a distância mínima é $d$, pelo Lema 4.2, dado $u \in \mathbb{F}_q^{n-d+1}$, existe no máximo uma palavra $c \in C$ cujas últimas $n-d+1$ coordenadas são as coordenadas de $u$. Portanto, $C$ tem no máximo tantos elementos quanto há em $F^{n-d+1}$, ou seja, $|C| \leq q^{n-d+1}$.

Por outro lado, se $C$ é perfeito e tem distância mínima $d$ então o raio de empacotamento de $C$ é $d-1$ e, pelo "vínculo das bolas",

$$|\mathbb{F}_q^n| = |C| \cdot |B_P(0, d-1)| = |C| \cdot (q^{d-1}),$$

o que implica

$$|C| = \frac{q^n}{q^{d-1}} = q^{n-d+1},$$

e isso só ocorre se para cada $u \in \mathbb{F}_q^{n-d+1}$ existir exatamente um vetor correspondente em $C$ como descrito acima. ■

**Demonstração:** do Teorema 4.2:

($\Rightarrow$) Primeiramente vamos mostrar que os códigos especificados no teorema são perfeitos.

Pela definição dos mesmos, temos que esses códigos tem cardinalidade $q^k$. Pelo Lema 4.2 e pelo Corolário 4.1, segue que a $P$-distância mínima é $n-k+1$ e que existe um único vetor do código com determinadas $k$ últimas coordenadas. Assim, cada vetor $(y_1, \ldots, y_n)$ em $\mathbb{F}_q^n$ está contido na $P$-bola de raio $(n-k)$ com centro em algum vetor do código, da forma $(x_1, \ldots, x_{n-k}, y_{n-k+1}, \ldots, y_n)$, mas não é contido na $P$-bola de raio $(n-k+1)$ com centro em qualquer outro vetor do código. Daí $C_k$ é um $P$-código perfeito.

($\Leftarrow$) Reciprocamente, assumimos que $C$ é $P$-código perfeito. Seja $r$ um inteiro, de tal modo que, para qualquer $x, y \in C$, temos:

$$B_P(x, r) \cap B_P(y, r) = \varnothing,$$

e

$$\bigcup_{x \in C} B_P(x, r) = \mathbb{F}_q^n.$$

As $P$-bolas de raio $r$ tem cardinalidade $q^r$, assim:

$$q^n = |C| \cdot |B_P(x, r)| \Rightarrow |C| = \frac{q^n}{q^r} \Rightarrow |C| = q^{n-r}.$$

Seja $y = (y_1, \ldots, y_n)$ um vetor de $\mathbb{F}_q^n$. Então, existe um vetor $c$ tal que $y \in B_P(c, r)$ e, assim, o vetor $c$ é da forma $c = (c_1, \ldots, c_r, y_{r+1}, \ldots, y_n)$, logo $C$ tem a forma indicada no teorema com $r = n - k$ (ou seja, $r = d_P - 1$, veja o Teorema 4.1). ■

## 4.3 Códigos de duas Cadeias de mesmo Comprimento

**Teorema 4.3** *Sejam $n = 2l$, inteiros positivos. Seja $P$ o conjunto de ordem parcial consistindo de duas cadeias disjuntas $N$ e $N'$ de mesmo comprimento $l$. Então, os únicos $P$-códigos perfeitos $C$ em $\mathbb{F}_q^n = \mathbb{F}_q^{2l}$ são os códigos triviais, $C = \mathbb{F}_q^{2l}$ e $C = \{x\}$ para cada $x$ em $\mathbb{F}_q^n$.*

**Demonstração:** Claramente os códigos $C = \mathbb{F}_q^{2l}$ e $C = \{x\}$ são perfeitos. Agora mostraremos que não existem outros $P$-códigos perfeitos. Sejam os elementos de $N$

$$N = \{1, 2, \ldots, l\}, \text{ onde } 1 < 2 < \ldots < l,$$

e sejam os elementos de $N'$

$$N' = \{1', 2', \ldots, l'\}, \text{ onde } 1' < 2' < \ldots < l'.$$

Note que se $x = (x_1, \ldots, x_l, x_{1'}, \ldots, x_{l'}) \in \mathbb{F}_q^{2l}$ então $w_P(x) = s + s'$, onde $x_s$ é a última coordenada não-nula entre 1 e $s$, e $x_{s'}$ é a última coordenada não-nula entre $1'$ e $s'$.

Suponha que, ao contrário, $C$ é um $P$-código perfeito onde $1 < |C| < q^{2l}$. Seja $r$ um inteiro de tal modo que as $P$-esferas de raio $r$ com centro nas palavras de $C$ são duas a duas disjuntas e cobrem $\mathbb{F}_q^{2l}$, ou seja:

$$B_P(x, r) \cap B_P(y, r) = \varnothing, \forall x, y \in C \text{ com } x \neq y \text{ e}$$

$$\bigcup_{x \in C} B_P(x, r) = \mathbb{F}_q^{2l}$$

Então $1 \leq r \leq 2l - 1$.

Primeiro assumiremos que $r \geq l$.

Sejam

$$x = (x_1, \ldots, x_l, x_{1'}, \ldots, x_{l'}) \text{ e } y = (y_1, \ldots, y_l, y_{1'}, \ldots, y_{l'}) \in \mathbb{F}_q^{2l}.$$

Então,

$$v = (x_1, \ldots, x_l, y_{1'}, \ldots, y_{l'}) \subset B_P(x, r) \cap B_P(y, r).$$

Em particular, as $P$-esferas de raio $r$ sobre quaisquer duas palavras do código se interceptam. Como $|C| \geq 2$, isto contradiz a suposição de que $C$ é perfeito.

Agora assumiremos que $1 \leq r < l$.

Primeiro calculamos a cardinalidade das $P$-bolas de raio $r$. Seja $i$ um inteiro com $1 \leq i \leq l$.

Decorre de

$$\begin{cases} 1, & \text{se i = 0,} \\ \sum_{j=1}^{i} (q-1)^j \cdot q^{i-j} \cdot \Omega_j(i), & \text{se i > 0} \end{cases}$$

e do fato de que a quantidade de maximais ($j$) para este tipo de ordem só pode ser 1 ou 2 ($1 \leq j \leq 2$), que o número de vetores cuja distância de um determinado vetor $x$ em $\mathbb{F}_q^n$ é igual à $i$, é:

$$\alpha_i = \sum_{j=1}^{2} (q-1)^j \cdot q^{i-j} \cdot \Omega_j(i) \Rightarrow$$

$$\alpha_i = (q-1)^1 \cdot q^{i-1} \cdot \Omega_1(i) + (q-1)^2 \cdot q^{i-2} \cdot \Omega_2(i).$$

Temos:

- Ideais que tem exatamente 1 maximal: $\Omega_1(i) = 2$;
- Ideais que tem exatamente 2 maximais: $\Omega_2(i) = i + 1 - 2 = i - 1$;

Assim temos o cálculo de elementos em cada esfera de raio $i$:

$$\alpha_i = (q-1)^1 \cdot q^{i-1} \cdot 2 + (q-1)^2 \cdot q^{i-2} \cdot (i-1)$$

$$= (q-1) \cdot q^{i-2}[2q^1 + (i-1) \cdot (q-1)]$$

$$= (q-1)\cdot q^{i-2}[2q + iq - i - q + 1]$$

$$= (q-1)\cdot q^{i-2}[q + iq - i + 1]$$

$$= (q-1)\cdot q^{i-2}[(i+1)\cdot q - i + 1].$$

Assim, para cada vetor $x$, temos:

$$|B_P(x,r)| = 1 + \sum_{i=1}^{r} \alpha_i.$$

Por indução, temos que:

$$|B_P(x,r)| = q^{r-1}[r(q-1) + q].$$

De fato, para $r = 1$ temos:

$$|B_P(x,1)| = 1 + \{(q-1)\cdot q^{1-2}[(1+1)q - 1 + 1]\} = 1 + \{(1-q^{-1})\cdot 2q\} = 1 + 2q - 2 = 2q - 1$$

e

$$q^{1-1}[1(q-1) + q] = 2q - 1$$

Supondo que vale para $r$, ou seja:

$$|B_P(x,r)| = 1 + \sum_{i=1}^{r}\{(q-1)\cdot q^{i-2}[(i+1)q - i + 1]\} = q^{r-1}[r(q-1) + q].$$

Mostraremos que vale para $r+1$, ou seja, que $|B_P(x,r)| = q^r[(r+1)(q-1) + q]$. Assim:

$$|B_P(x,r)| = 1 + \sum_{i=1}^{r+1}\{(q-1)\cdot q^{i-2}[(i+1)q - i + 1]\} =$$

$$= 1 + \sum_{i=1}^{r}\{(q-1)\cdot q^{i-2}[(i+1)q - i + 1]\} + \{(q-1)\cdot q^{r+1-2}[(r+1+1)q - r - 1 + 1]\}$$

$$= q^{r-1}[r(q-1) + q] + \{(q-1)\cdot q^{r-1}[(r+2)q - r]\}$$

$$= q^{r-1}[r(q-1)+q] + \{(q-1)\cdot q^{r-1}[rq+2q-r]\}$$

$$= q^{r-1}[rq-r+q] + \{(q-1)[q^r r + 2q^r - q^{r-1}r]\}$$

$$= q^r r - q^{r-1}r + q^r + q^{r+1}r + 2q^{r+1} - q^r r - q^r r - 2q^r + q^{r-1}r$$

$$= q^{r+1}r + 2q^{r+1} - q^r r - q^r$$

$$= q^r[qr + 2q - r - 1]$$

$$= q^r[qr + q - r - 1 + q]$$

$$= q^r[(r+1)(q-1)+q]$$

Assim

$$|B_P(x,r)| = q^{r-1}[r(q-1)+q].$$

Como $C$ é perfeito, $q^{2l} = |C||B_P(x,r)|$

Assim existe $j$, inteiro positivo, tal que:

$$r(q-1)+q = q^j \text{ e, portanto, } r = \frac{q^j - q}{q-1}(*).$$

Assim

$$|B_P(x,r)| = q^{r-1}\cdot q^j = q^{r+j-1}.$$

e temos:

$$|C| = \frac{q^{2l}}{|B_P(x,r)|} = q^{2l-r-j+1} = q^{2(l-r)+r-(j-1)},$$

Desde que $r \geq 1$, por $(*)$ temos $j \geq 2$.

Assim

$$r = \frac{q^j - q}{q-1} = q(1 + q + \ldots + q^{j-2}) \geq 2(j-1) \geq j.$$

e como $r > j-1$, segue que

$$|C| > q^{2(l-r)} = \frac{q^{2l}}{q^{2r}}.$$

Pelo "Princípio da Casa dos Pombos", existem palavras distintas do código:

$$x = (x_1, \ldots, x_l, x_{1'}, \ldots, x_{l'}) \text{ e } y = (y_1, \ldots, y_l, y_{1'}, \ldots, y_{l'}) \in \mathbb{F}_q^{2l}.$$

tal que $x_i = y_i$ e $x_{i'} = y_{i'}$ para $i = r+1, \ldots, l$.

Desde que o vetor

$$v = (x_1, \ldots, x_l, y_{1'}, \ldots, y_{l'}) \subset B_P(x, r) \cap B_P(y, r),$$

as $P$-bolas de raio $r$ sobre as palavras $x$ e $y$ se interceptam, novamente contradizendo o pressuposto de que $C$ é perfeito, logo $C$ não é perfeito. Assim os únicos $P$-códigos perfeitos $C$ em $\mathbb{F}_q^n = \mathbb{F}_q^{2l}$ são $C = \mathbb{F}_q^{2l}$ e $C = \{x\}$ para cada $x$ em $\mathbb{F}_q^n$. ■

**Observação 4.1** *Seja $P = N \cup N'$, $|N| = |N'| = l$ então,*

$$|B_P(x, r)| = q^{r-1}[r(q-1) + q].$$

**Observação 4.2** *Seja $P = N \cup N'$, $|N| = |N'| = l$. Se $x, y \in \mathbb{F}_q^{2l}$ e $r \geq l$, então:*

$$B_P(x, r) \cap B_P(y, r) \neq \varnothing$$

**Observação 4.3** *Um código de duas cadeias de mesmo comprimento teria no máximo $\frac{q^{2l}}{q^{2r}} = q^{2(l-r)}$ palavras distintas, uma vez que seja*

$$x = (\underbrace{x_1, \ldots, x_r}_{r}, x_{r+1}, \ldots, x_l, \underbrace{x_{1'}, \ldots, x_{r'}}_{r}, x_{r+1'}, \ldots, x_{l'}) \in \mathbb{F}_q^{2l},$$

*ao trocarmos estas $2r$ coordenadas, o vetor continua pertencendo à mesma bola $B_P(x, r)$.*

*No entanto, na demonstração acima, chegamos em $|C| > q^{2(l-r)} = \frac{q^{2l}}{q^{2r}}$, supondo $C$ perfeito. Logo, se temos no máximo $q^{2(l-r)}$ "palavras", para colocar em mais de $q^{2(l-r)}$ "lugares" (o que justifica o uso do "Princípio Fundamental da Casa do Pombos"), teremos "lugares" sobrando. Assim, o código $C$ não é perfeito porque não cobre o espaço todo, ou seja*

$$\bigcup_{x \in C} B_P(x, r) \neq \mathbb{F}_q^{2l}$$

**Exemplo 4.2** *Seja $C \in \mathbb{F}_2^n$ e seja $n = 2l = 2 \cdot 5 = 10$.*

*$N = \{1, 2, 3, 4, 5\}$ onde $1 < 2 < 3 < 4 < 5$;*

*$N' = \{6, 7, 8, 9, 10\}$ onde $6 < 7 < 8 < 9 < 10$.*

*Suponha $C$ perfeito com $1 < |C| < 2^{10}$*

*Seja* $r \in \mathbb{N}$, *suponha que* $B_P(u,r) \cap B_P(v,r) = \varnothing, \forall u, v \in C$ *com* $u \neq v$ *e* $\bigcup_{u \in C} B_P(u,r) = \mathbb{F}_q^{2l}$.

*Para* $r \geq l$, *digamos* $r = l = 5$.

*Seja* $x = (0, \ldots, 0, 0, \ldots, 0)$ *e* $y = (1, \ldots, 1, 1, \ldots, 1)$.

*Seja* $v = (0, \ldots, 0, 1, \ldots, 1) \in B_P(x,5) \cap B_P(y,5) \Rightarrow C$ *não é perfeito.*

*Para* $1 \leq r < l$.

*Seja* $r = 3$ *e*

$x = (0,0,0,\underbrace{1,1},1,1,1,\underbrace{0,0})$;

$y = (1,1,1,\underbrace{1,1},0,0,0,\underbrace{0,0})$.

*Temos* $x_i = y_i$ *e* $x_{i'} = y_{i'}$ *para* $i = r+1, \ldots, l$.

*Seja* $v = (0,0,0,1,1,0,0,0,0,0)$, *v está à mesma distância de x e y:*

$d_P(y,v) = w_P(y-v) = w_P(1,1,1,0,0,0,0,0,0,0) = 3$;

$d_P(x,v) = w_P(x-v) = w_P(0,0,0,0,0,1,1,1,0,0) = 3$.

*Logo* $v \in B_P(x,3) \cap B_P(y,3)$.

Capítulo 5

# MÉTRICAS POSET QUE ADMITEM CÓDIGOS BINÁRIOS PERFEITOS DE CODIMENSÃO M

## 5.1 Considerações Iniciais

Este capítulo é dedicado ao problema da existência de códigos perfeitos em espaços métricos de conjuntos parcialmente ordenados (posets), que são uma generalização do espaço métrico de Hamming. Muitos artigos tratam da existência de códigos em conjuntos parcialmente ordenados, corretores de 1, 2 ou 3 erros. Inversamente, neste texto classificaremos posets que admitem a existência de códigos perfeitos corretores da maior quantidade possível de erros com respeito ao comprimento e dimensão do código, ou seja, quando o número de erros é ligado à codimensão do código.

Os códigos posets binários de codimensão $m$ (de cardinalidade $2^{n-m}$, onde $n$ é o comprimento do código) podem corrigir, no máximo, $m$ erros. Em [10], KIM e KROTOV descrevem todas as possíveis métricas poset que permitem códigos de codimensão $m$ serem $m$, $(m-1)$ ou $(m-2)$-perfeitos. Nos limitaremos aqui a caracterizar os $m$-perfeitos.

Como provaremos pelo Lema 5.1 adiante, a codimensão $m$ do código $(n, 2^{n-m})$ corretor de $r$ erros não pode ser inferior a $r$. E os conjuntos parcialmente ordenados, que admitem códigos

posets binários de codimensão $m$ que são $m$-perfeitos podem ser simplesmente caracterizados. (Teorema 5.1)

Seja $P = ([n], \leq)$ um poset, onde $[n] = \{1, 2, \ldots, n\}$. O subconjunto $I$ de $[n]$, como já definido anteriormente, é chamado um ideal em $P$, se para cada $a \in I$, a relação $b \leq a$ significar $b \in I$.

Para $a_1, \ldots, a_i \in P$ denote por $\langle a_1, \ldots, a_i \rangle$ ou $\langle \{a_1, \ldots, a_i\} \rangle$ o menor ideal que contém $a_1, \ldots, a_i$.

Denotamos por $\mathcal{I}_p^r \subset 2^{[n]}$ (onde $2^{[n]} = \mathbb{F}^n$), o conjunto de todos os $r$-ideais (ou seja, ideais de cardinalidade $r$) de $P$, onde $r \in \{0, 1, \ldots, n\}$.

Se $x \in \mathbb{F}^n$, então o $P$-peso $w_P(x)$ de $x$ é a cardinalidade de $\langle \text{supp } x \rangle$. Agora, para dois elementos $x, y \in \mathbb{F}^n$, podemos definir a $P$-distância $d_P(x, y) = w_P(x - y)$.

Para $r \in \{0, \ldots, n\}$ denota-se, como de costume, por $B_P(0, r) = \{x \in \mathbb{F}^n | w_P(x) \leq r\}$, a bola de raio $r$ com centro no vetor nulo.

Subconjuntos $C$ de $\mathbb{F}^n$ são chamados de $P$-códigos corretores de $r$ erros se cada vetor $x \in \mathbb{F}^n$ tem no máximo uma representação $x = u + v$, onde $u \in C$ e $v \in B_P(0, r)$. Em outras palavras, as bolas de raio $r$ centradas em palavras de um $P$-código $C$ corretor de $r$ erros são mutuamente disjuntas.

Se os subconjuntos acima descritos tiverem exatamente uma representação como descrito, eles são chamados $P$-códigos $r$-perfeitos. Em um $P$-código $r$-perfeito as bolas de raio $r$ centradas em palavras do código, além de serem mutuamente disjuntas, cobrem todo o espaço $\mathbb{F}^n$.

Como consequência,

$$|C| \leq \frac{|\mathbb{F}^n|}{|B_P(0, r)|} (\text{vínculo das bolas})$$

onde a igualdade é equivalente à $r$-perfeição de $C$.

## 5.2 Caracterização de Códigos Posets m-Corretores de Erros

Começaremos com vários resultados simples.

**Proposição 5.1** *a) Seja $0 \leq r \leq r' \leq n$ e $I \in \mathcal{I}_p^r$; então existe $I' \in \mathcal{I}_p^{r'}$ tal que $I \subseteq I'$.*

*b) Seja* $0 \leq r' \leq r \leq n$ *e* $I \in \mathcal{I}_p^r$*; então existe* $I' \in \mathcal{I}_p^r$ *tal que* $I' \subseteq I$*.*

**Demonstração:**

Se $r = r'$ então $I' = I$ em ambos os casos, satifazendo assim as condições.

a) No caso $r' = r + 1$, seja $j$ um elemento minimal de $P - I$, então $I' \doteq I \cup \{j\}$ satisfaz a condição.

b) No caso $r' = r - 1$, seja $j$ um elemento maximal de $I$, então $I \doteq I - \{j\}$ satisfaz a condição.

Os casos gerais $r' = r + t$ e $r' = r - t$ são provados por indução, ou seja, já mostramos que a) é válida para $r' = r + 1$ e b) é válida para $r' = r - 1$. Supondo que a) e b) sejam válidas para $r' = r + t$ e $r' = r - t$, respectivamente, mostraremos que a) é válida para $r' = r + t + 1$ e que b) é válida para $r' = r - t - 1$;

a) No caso $r' = r + t + 1$ fazemos $r + t = s$, temos então $r' = s + 1$. Por hipótese, temos que a) é válida para $r' = r + t = s$ e já mostramos no início que se a) é válida para $r' = r$ então é válida para $r' = r + 1$, logo a) é válida para $r' = s + 1$.

b) No caso $r' = r - t - 1$ fazemos $r - t = s$, temos então $r' = s - 1$. Por hipótese, temos que b) é válida para $r' = r - t = s$ e já mostramos no início que se b) é válida para $r' = r$ então é válida para $r' = r - 1$, logo b) é válida para $r' = s - 1$. ■

A esta hora o leitor deve estar se perguntando como usamos de forma tão direta em a), $I \cup \{j\} = I'$, ou seja, a união de um ideal com o elemento $j$ é igual à outro ideal. De fato, temos que a união de ideais é um ideal, assim poderíamos ter definido $I' = I \cup \langle j \rangle$. No entanto, por definição, $j$ é o elemento minimal de $P - I$, assim, não há nenhum elemento $h \in P - I$, tal que $j > h$, logo, se $j > h \Rightarrow h \in I$. Por conta disso temos:

$$I \cup \langle j \rangle = I \cup \{j\} = I'$$

De modo análogo, em b) $j$ é definido como elemento maximal de $I$, logo temos que $I - \{j\}$ é um ideal.

**Corolário 5.1** *Para cada* $r$ *de* 0 *a* $n$*, o conjunto* $\mathcal{I}_p^r$ *é não vazio.*

**Demonstração:**

Atribuindo $r = 0$ e $I = \varnothing$ na Proposição 5.1, teremos pelo menos um ideal em $\mathcal{I}_p^r$, para cada $r$ entre 0 e $n$. Para $r = 1$, por exemplo, podemos tomar um $j$ minimal em $P$ e daí $j \in \mathcal{I}_p^1$. ■

**Proposição 5.2**

$$B_P(0,r) = \bigcup_{I \in \mathcal{I}_p^r} \{v \in \mathbb{F}_2^n | supp\ (v) \subset I\}$$

**Demonstração:** ($\Rightarrow$) Seja $v \in B_P(0,r)$, ou seja, $w_P(v) = |\langle \text{supp } (v)\rangle| \leq r$. Pela Proposição 5.1, existe um ideal $I \in \mathcal{I}_p^r$ tal que $\langle \text{supp } (v)\rangle \subseteq I$. Assim, temos supp $(v) \subseteq \langle \text{supp } (v)\rangle \subseteq I$, ou seja, supp $(v) \subset I$.

($\Leftarrow$) Inversamente, se $v \in \mathbb{F}^n$ e supp $(v) \subset I$ para algum $I \in \mathcal{I}_p^r$, então, $\langle \text{supp } (v)\rangle \subseteq I$ e $w_P = |\langle \text{supp } (v)\rangle| \leq |I| = r$. Logo, se $w_P(v) \leq r$ então $v \in B_P(0,r)$. ■

Sendo $|\mathcal{I}_p^r| \geq 1$, pelo Corolário 5.1, obtemos imediatamente o seguinte:

**Corolário 5.2** *Seja $P$ poset, $d_P$ a métrica associada e $r$ um número natural. Então:*

$$|B_P(0,r)| \geq 2^r$$

O lema seguinte é simples consequência do "Vínculo das bolas" e Corolário 5.2.

**Lema 5.1** *Se um $P$-código $[n, 2^{n-m}]$, $C \subset \mathbb{F}^n$, é corretor de $r$ erros, então $r \leq m$.*

**Demonstração:**

De fato: $|\mathbb{F}^n| \geq |C|.|B_P(0,r)| \Rightarrow |B_P(0,r)| \leq \frac{|\mathbb{F}^n|}{|C|} \Rightarrow |B_P(0,r)| \leq \frac{2^n}{2^{n-m}} \Rightarrow |B_P(0,r)| \leq 2^m$. Disso e do Corolário 5.2, temos que:

$$2^r \leq |B_P(0,r)| \leq 2^m \Rightarrow r \leq m$$

■

Antes de caracterizar os códigos posets corretores de $m$ erros (teorema seguinte), vamos enunciar um lema que será de grande valia para provar que esses códigos são perfeitos. Para auxiliar nos próximos resultados, além do artigo citado no início deste capítulo, recorremos também a alguns conceitos básicos de "Álgebra Linear" encontrados no texto [11], de LIMA, Elon Lages.

**Lema 5.2** *Para qualquer $X \subset P$, $X \neq \varnothing$ e $X \neq P$, com:*

$V_X = \{v \in \mathbb{F}^n; supp\ (v) \subset X\}$ *e*

$V_{P-X} = \{v \in \mathbb{F}^n; supp\ (v) \subset P - X\}$.

*Temos que:* $\mathbb{F}^n = V_X \oplus V_{P-X}$

**Demonstração:** Sejam $V_X$ e $V_{P-X}$ subconjuntos de $\mathbb{F}^n$, dizemos que $\mathbb{F}^n = V_X \oplus V_{P-X}$, ou seja, $V_X + V_{P-X}$ é uma soma direta e, além disso, gera $\mathbb{F}^n$. Logo, temos que mostrar que:

i) $V_X \cap V_{P-X} = \{0\}$ e

ii) $\mathbb{F}^n = V_X + V_{P-X}$.

De fato:

i) Seja $X \subset P$, o conjunto $P - X$ chama-se complementar de $X$ em relação à $P$ e é dado por:

$$P - X = \{x \in P | x \notin X\}$$

Assim, temos:

$$(P - X) \cap X = \varnothing \ (*)$$

Supondo que existe $v$, diferente do vetor nulo, tal que $v \in V_X \cap V_{P-X}$, assim, por definição, temos que: supp $(v) \subset X$ e supp $(v) \subset P - X$, contradição, pois, por $(*)$ temos que $P - X \cap X = \varnothing$, logo $V_X \cap V_{P-X} = \{0\}$.

ii) Pela definição de $P - X$ dada em i) temos ainda que:

$$(P - X) \cup X = P \ (**)$$

Dado $v \in \mathbb{F}^n$, podemos escrever:

$v = \sum_{i=1}^{n} a_i.e_i$ onde $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, ou seja, $e_i$ é o vetor pertencente à $\mathbb{F}^n$, cuja $i$-ésima coordenada é igual à 1 e as demais são nulas.

Assim, $v$ pode ser escrito também da seguinte forma:

$$v = \sum_{i \in X} a_i.e_i + \sum_{i \in P-X} a_i.e_i$$

com $\sum_{i \in X} a_i.e_i \in V_X$ e $\sum_{i \in P-X} a_i.e_i \in V_{P-X}$.

Portanto, todo vetor $v$ de $\mathbb{F}^n$ é da forma $v = u + w$, com $u \in V_X$ e $w \in V_{P-X}$.

De i) obtemos que a interseção de $V_X$ e $V_{P-X}$ é o subespaço nulo, e de ii) temos que $\mathbb{F}^n = V_X + V_{P-X}$, logo temos que $\mathbb{F}^n = V_X \oplus V_{P-X}$. ■

**Teorema 5.1** *Caracterização dos códigos Posets corretores de m erros.*

*Um $[n, 2^{n-m}]$ código $C$ é um $P$-código corretor de $m$ erros se, e somente se, atender às duas condições seguintes:*

*a) $\mathcal{I}_p^m$ contém exatamente um ideal $I$;*

*b) Existe uma função $f : V_{P-I} \longrightarrow V_I$ tal que $C = \{v + f(v); v \in V_{P-I}\}$ ou seja, o código $C$ é sistemático com $P - I$ símbolos de informação e $I$ símbolos de verificação.*

*Cada $P$-código corretor de $m$ erros é um $P$-código $m$-perfeito.*

**Demonstração:**

($\Rightarrow$) Mostramos primeiramente que a) e b) são válidas para qualquer $P$-código $C$, corretor de $m$ erros.

a) Sendo $B_P$ uma bola de raio $m$, temos $[2^n = |\mathbb{F}^n| \geq |C| \cdot |B_P| = 2^{n-m} \cdot |B_P|]$ e daí $2^m \geq |B_P|$. Como $|B_P| = 2^m$ temos $|\mathcal{I}_p^m| = 1$.

b) Fazendo $X = I$, pelo Lema 5.2, temos que:

$$\mathbb{F}^n = V_I \oplus V_{P-I}$$

Uma vez definida a função, temos que os vetores do código tem a forma $v + f(v)$, com $v \in V_{P-I}$ e $f(v) \in V_I$, e como a soma $V_I + V_{P-I}$ é direta e igual a $\mathbb{F}^n$. Assim, não existem duas palavras $u$ e $v$ do código coincidindo em $P - I$, pois aí coincidiriam em $I$ também, logo $u = v$.

Mostraremos que que se duas palavras coincidem em $P - I$ então são a mesma palavra. De fato, se $u, v \in C$ são distintas e coincidem em $P - I$, então $u + v \in V_I$ e $d_P(u, v) = |\langle u + v \rangle| \leq |I| = m$. Assim, $d_P(u, v) \leq m$ e $C$ não é corretor de $m$ erros, contradição. Segue que para cada elemento $u$ de $V_{P-I}$ há no máximo uma palavra $v$ correspondente em $C$ tal que $\text{supp}(v) \cap P - I = u$. Como $|P - I| = 2^{n-m} = |C|$, para cada elemento $v$ de $V_{P-I}$ há um elemento $v' \in V_I$ tal que $v + v' \in C$. Isso define uma função $f : V_{P-I} \longrightarrow V_I$, $f(v) = v'$, de modo que $C = \{v + f(v); v \in V_{P-I}\}$.

($\Leftarrow$) Assumindo a) e b) válidas. Mostraremos que $C$ é um código $m$-perfeito.

Precisamos verificar que para cada $u \in \mathbb{F}^n$ existe um único $v \in C$ tal que $d_P(v, u) \leq m$.

Seja $u \in \mathbb{F}^n$ e $\mathbb{F}^n = V_I \oplus V_{P-I}$ temos $u = u_1 + u_2$, onde $u_1 \in V_{P-I}$ e $u_2 \in V_I$.

$v := u_1 + f(u_1)$

Assim temos $d_P(v, u) = w_P(v - u) = w_P(u_1 + f(u_1)) - (u_1 + u_2) = w_P(f(u_1) - u_2)$.

Temos, por definição, que $f(u_1) \in V_I$ e $u_2 \in V_I$, logo, temos que $n - m$ coordenadas do vetor $(f(u_1) + u_2)$ se anulam, logo temos que $d_P(v, u) \leq m$, o que prova a existência.

Assim, mostramos que $v$ é um vetor do código, pela definição de $f$; e que $d_P(v, u) \leq m$ porque supp $(v + u) \subset I$.

Se não há unicidade então existem $v, v' \in C$ tais que $B_P(v, m) \cap B_P(v', m) \neq \varnothing$. Então

$$\left[ |\bigcup_{c \in C} B_P(c, m)| < \sum_{c \in C} |B_P(c, m)| \right],$$

pois a união não é disjunta. Por outro lado, como cada vetor de $\mathbb{F}^n$ está em alguma bola de raio $m$ centrada em uma palavra do código, $\mathbb{F}^n = \bigcup_{c \in C} B_P(c, m)$ e

$$\left[ 2^n = |\mathbb{F}^n| = |\bigcup_{c \in C} B_P(c, m)| < \sum_{c \in C} |B_P(c, m)| = |C| \cdot |B_P(0, m)| = 2^{n-m} \cdot 2^m = 2^n \right],$$

absurdo.

Ou seja, a unicidade está implícita pela cardinalidade do código:

$$|C| = 2^{n-m} = \frac{|\mathbb{F}^n|}{|B_P(0, r)|} = \frac{2^n}{2^m}.$$

■

**Exemplo 5.1** *Seja $P = ([n], \leq)$ um poset onde $[n] = \{1, 2, \ldots, n\}$ com $1 < 2 < \ldots < n$ (ordem cadeia) e seja $I$ um ideal de $P$ com cardinalidade 3.*

*Seja $u \in \mathbb{F}^n$; $u = (a_1, a_2, a_3, a_4, \ldots, a_n)$ temos:*

$u = (a_1, a_2, a_3, 0, \ldots, 0) + (0, 0, 0, a_4, a_5, \ldots, a_n)$

$\downarrow \qquad\qquad \downarrow$

$V_I \qquad\qquad V_{P-I}$

*Seja $v \in C$, temos que, pela definição de $f : V_{P-I} \longrightarrow V_I$,*

$v = (0, 0, 0, a_4, \ldots, a_n) + f(0, 0, 0, a_4, \ldots, a_n)$

$v = (0, 0, 0, a_4, \ldots, a_n) + (b_1, b_2, b_3, 0, \ldots, 0) = (b_1, b_2, b_3, a_4, \ldots, a_n)$

*Assim:*

$d_P(u, v) = w_P(u - v) = (a_1 - b_1, a_2 - b_2, a_3 - b_3, 0, \ldots, 0) \leq 3 = |I| = m$

# Considerações Finais

O presente trabalho constituiu uma breve introdução à teoria dos códigos corretores de erros clássica e também aos códigos sobre ordens parciais, com algumas comparações entre os dois casos. Primeiramente enfocamos conceitos básicos da teoria clássica dos códigos corretores de erros, como a definição de Alfabeto, a distância de Hamming, os códigos lineares e a definição de matriz geradora de um código; o estudo dos limitantes de Singleton e de Hamming, além de tratar dos Códigos de Hamming. No entanto, nosso objetivo maior neste trabalho foi em relação aos Códigos em Conjuntos Parcialmente Ordenados, uma vez que pouquíssimos textos se encontram publicados ainda, principalmente em português, sobre este assunto.

Um dos principais problemas da teoria dos códigos, dado $\mathbb{F}_q$ um corpo finito, $\mathbb{F}_q^n$ o espaço vetorial das $n$-uplas sobre $\mathbb{F}_q$ e $k < n$, é determinar os subconjuntos $C \subseteq \mathbb{F}_q^n$ de cardinalidade $q^k$ com maior distância mínima de Hamming possível. Ou seja, determinar os códigos de cardinalidade $q^k$ em $\mathbb{F}_q^n$ com maior capacidade de correção de erros.

Como comentamos no texto, em 1991 Harald Niederreiter [13] generalizou esse problema considerando uma métrica mais geral que a métrica de Hamming. Posteriormente, em 1995, Brualdi, Graves e Lawrence [5] observaram que a métrica de Niederreiter era um caso particular de uma métrica ponderada por uma ordem parcial (no caso de Niederreiter, união disjunta de cadeias de mesmo comprimento) e passaram a considerar essa métrica sobre uma ordem parcial arbitrária.

Dado $r > 0$ dizemos que um código $C \subseteq \mathbb{F}_q^n$ é um $r$-código $P$-perfeito (ou simplesmente perfeito se $d_P$ é a métrica de Hamming) se as bolas de raio $r$ centradas nos elementos de $C$ são duas a duas disjuntas e cobrem todo o espaço $\mathbb{F}_q^n$. Um problema interessante em relação às $P$-métricas, dado $r > 0$, é o de classificar as ordens parciais $P$ que tornam um determinado código não perfeito $C \subseteq \mathbb{F}_q^n$ um $r$-código $P$-perfeito.

Fizemos isto no Capítulo 3, quando tratamos do código de Hamming estendido $\hat{\mathcal{H}}_m$. Considerando-se a métrica de Hamming, é possível demonstrar que a distância mínima de

$\hat{\mathcal{H}}_m$ é $d(\hat{\mathcal{H}}_m) = 4$, de modo que o raio de empacotamento é $R_e(\hat{\mathcal{H}}_m) = [\frac{4-1}{2}] = 1$. As bolas de raio 1 centradas nestes pontos são disjuntas mas estas bolas não cobrem o espaço $\mathbb{F}_2^{2^m}$ e, considerando-se a métrica de Hamming, $\hat{\mathcal{H}}_m$ não é perfeito. No entanto, considerando-se uma métrica $d_P$ ponderada por uma ordem parcial que apresentamos, $\hat{\mathcal{H}}_m$ torna-se perfeito. Além disso, a capacidade de correção de $\hat{\mathcal{H}}_m$ aumenta para 2.

No decorrer do texto, apresentamos ainda a definição de ordens parciais, métricas sobre conjuntos ordenados, contagem dos elementos da bola, resultados sobre Ideais; estudamos o caso da ordem cadeia ("chain poset"), analisando os códigos de uma cadeia e os códigos de duas cadeias de mesmo comprimento e, por fim, nos dedicamos ao estudo das Métricas POSET que admitem códigos binários perfeitos de codimensão $m$, caracterizando assim os Códigos Posets $m$-corretores de erros.

De maneira geral, o trabalho apresenta e desenvolve os fundamentos matemáticos da Teoria dos Códigos Clássica e dos Códigos sobre Ordens Parciais. E, por estarmos tratando de um vasto campo, tendo várias ramificações em diversas áreas da matemática, nos concentramos nos aspectos de natureza algébrica, sem nos atermos muito à maneira com essas teorias são aplicadas, tanto que não falamos sequer sobre decodificação.

Por fim, é natural algumas expectativas para estudos futuros. Por exemplo, como dissemos no Capítulo 5, muitos artigos tratam da existência de códigos em conjuntos parcialmente ordenados, corretores de 1, 2 ou 3 erros. Os códigos posets binários de codimensão $m$ (de cardinalidade $2^{n-m}$, onde $n$ é o comprimento do código) podem corrigir, no máximo, $m$ erros. Em [10], Kim e Krotov descrevem todas as possíveis métricas poset que permitem códigos de codimensão $m$ serem $m$, $(m-1)$ ou $(m-2)$-perfeitos. No entanto, neste trabalho nos limitamos à caracterizar os $m$-perfeitos. Assim, gostaríamos de investigar mais profundamente as outras possibilidades existentes. Além disso, há inúmeras outras sugestões de estudos a serem feitos, dado a dimensão do campo de estudo sobre códigos corretores de erros.

# Referências Bibliográficas


[1] ALVES, Marcelo Muniz Silva: *Minicurso 01 - Códigos Corretores de Erros*. UFPR - XI ERMAC. Curitiba - PR, 2007.

[2] ALVES, M. M. S.; COSTA, S. I. R.; LAVOR, C. C.; SIQUEIRA, R. M.: *Uma Introdução à Teoria de Códigos*. Sociedade Brasileira de Matemática Aplicada e Computacional. XXIX CNMAC. São Carlos - SP, 2006.

[3] ANTON, H., RORRES, C.: *Álgebra Linear com Aplicações*. 8. ed., Porto Alegre: Bookman, 2001.

[4] BOLDRINI, J. L., COSTA, S. I. R., FIGUEIREDO, V. L., WETZLER, H. G.: *Álgebra Linear*. 3. ed., São Paulo: Harbra, 1986.

[5] BRUALDI, R. A.; GRAVES, J. S.; LAWRENCE, K. M.: *Codes with a poset metric*. Discrete Mathematics, 147 (1995) 57-72.

[6] FIRER, Marcelo; PANEK, Luciano: *Códigos e Métricas*. Congresso de Matemática e suas Aplicações. Foz do Iguaçu - PR, 2006.

[7] FIRER, Marcelo: *Loterias Esportivas e Códigos*. IMECC - UNICAMP. Bol. Soc. Paran. Mat. (3s.) v. 23 1-2 (2005): 151-162.

[8] HEFEZ, Abramo: *Curso de Álgebra*. volume 1. 3. ed., Rio de Janeiro: IMPA, 2002.

[9] HEFEZ, A., VILLELA, M. L. T.: *Códigos Corretores de Erros*. 1. ed., Rio de Janeiro: IMPA, 2002.

[10] KIM, Hyun Kwang; KROTOV, Denis S.: *The Poset Metrics That Allow Binary Codes of Codimension m to be m -, $(m-1)$-, or $(m-2)$-Perfect*. IEEE Transactions on Information Theory, 54(11) 2008, 5241-5246.

[11] LIMA, Elon Lages: *Álgebra Linear*. 7. ed., Rio de Janeiro: IMPA, 2006.

[12] MAC WILLIAMS, F. J.; SLOANE, N. J. A.: *The theory of error-correcting codes*. North-Holland, 1996.

[13] NIEDERREITER, Harald, LIDL, Rudolf.: *Introduction to Finite Fields and Their Applications*. Cambridge University Press.

[14] PANEK, Luciano: *Código de Golay Estendido e Métricas Poset*. UFPR - Simpósio de Álgebra e Aplicações. Curitiba - PR, 2008.

[15] ROSENBLOOM, M. Yu. and TSFASMAN, M. A.: *Coding Theory: Codes for m-Metric*, Problems of Information Transmission, Vol. 33, No. 1, 1997.

[16] SANTOS, J. P. de O., MELLO, M. P., MURARI, I. T. C.: *Introdução à Análise Combinatória*. 3. ed. rev., Campinas, SP: Editora da UNICAMP, 2002.