**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**
**Pró-Reitoria de Pesquisa e Pós-Graduação**
**Departamento de Matemática Pura e Aplicada - CCENS**

RELATÓRIO DE INICIAÇÃO CIENTÍFICA

# *Códigos Corretores de Erros sob o Ponto de Vista Algébrico*

Discente: *Juliana Gavinho Sanção*
Orientador: *Prof. Dr. Victor do Nascimento Martins (DMPA - UFES)*

AGOSTO/2019

# SUMÁRIO

**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**
**Pró-Reitoria de Pesquisa e Pós-Graduação**
**Departamento de Matemática Pura e Aplicada - CCENS**

## RESUMO

# CÓDIGOS CORRETORES DE ERROS SOB O PONTO DE VISTA ALGÉBRICO

*Este trabalho tem como objetivo ampliar o conhecimento, em geral, na área de Álgebra, aprofundando o estudo na teoria dos códigos lineares, mesclando assim conceitos da Matemática Pura, mais especificamente os da Álgebra Abstrata, e da Matemática Aplicada, com foco em alguns desenvolvimentos da Teoria de Códigos Corretores de Erros. A fim de motivar o estudo da teoria dos códigos, são abordados conceitos básicos da teoria, como o que é um código, a métrica de Hamming, códigos equivalentes e por fim códigos lineares. Para a compreensão destes conceitos será importante o estudo de alguns resultados sobre as estruturas algébricas de anéis, corpos e de tópicos de Álgebra Linear.*

**Palavras chaves:** Códigos Lineares, Álgebra, Matriz Geradora, Anéis e Corpos.

# INTRODUÇÃO

Várias pesquisas têm sido desenvolvidas sobre a Teoria de Códigos Corretores de Erros nas últimas décadas. Esta teoria tem como grandes pioneiros Marcel J. E. Golay, Richard W. Hamming e C. E. Shannon. e, sendo assim, iremos apresentar algumas das ideias desenvolvidas por estes pesquisadores.

Hamming, em meados de 1947, era motivado pela ideia de que se um computador podia detectar erros de digitação , por que não podíamos localizar a posição de um erro e corrigí-lo? Com esta ideia ele desenvolveu um código capaz de detectar até dois erros e corrigir um erro, se ele for único. À medida que sua pesquisa evoluía surgiu uma questão relacionada a possibilidade de criar códigos mais eficientes do que aquele proposto inicialmente. Em 1948, Shannon respondeu a questão indiretamente e com isto, ele deu início a dois novos campos de pesquisa em matemática: a teoria de códigos e a Teoria da Informação. Mais adiante, Golay extendeu um dos resultados dados no artigo de Shannon em 1948 e desenvolveu vários códigos importantes na teoria. A partir das décadas de 50 e 60 muitos matemáticos se interessaram pelo estudo da Teoria de Códigos e a partir da década de 70, devido as pesquisas espaciais e a grande popularização dos computadores, os engenheiros também começaram a manifestar interesse nesta área de estudo.

Atualmente, os códigos corretores de erros são utilizados sempre que se deseja transmitir ou armazenar dados, garantindo, assim, sua confiabilidade. Conforme [1], na transmissão de dados, na vida real, podem ocorrer alguns problemas que façam com que a mensagem recebida seja diferente daquela que foi enviada, por isso, o objetivo da teoria é desenvolver métodos para a detecção e a correção de erros. Com isso, baseado em [1], iremos apresentar os principais conceitos e resultados básicos para o desenvolvimento deste estudo e de descrever uma das classes mais utilizadas de códigos corretores de erros: os códigos lineares. Para o desenvolvimento desta etapa, é necessário entender como se dá a construção de um código

corretor de erros.

Este trabalho é dividio em três capítulos. No primeiro capítulo procuramos fazer um estudo suscinto sobre alguns tópicos algébricos essenciais para um entendimento maior sobre os Códigos Corretores de Erros, usando como base [1], [2] e [3]. Estudaremos alguns conceitos sobre anéis e corpos e com um pouco mais de detalhes abordaremos o anel dos números inteiros. Por fim revisaremos conceitos relacionados a estrutura dos espaços vetoriais. Além disso, procuramos neste capítulo, estabelecer as notações que serão utilizadas no decorrer do trabalho.

O objetivo do segundo capítulo, é abordar conceitos básicos da teoria de códigos apresentados em [1]. Essencialmente procuramos neste momento conceituar formalmente o que é um código, analisando sua estrutura e detalhando como é o processo de envio e recebimento de uma "mensagem". Falaremos de alguns tipos de códigos,como por exemplo daqueles ditos "perfeitos", isto é que satisfazem a condição

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

Iremos definir uma das métricas mais utilizadas na teoria, a métrica de Hamming.

Por fim, no Capítulo 3 apresentamos os Códigos Lineares, estudando os conceitos de Matriz Geradora de um Código, os Códigos Duais e por fim falaremos sobre Decodificação e apresentaremos alguns exemplos de códigos.

O projeto de Pesquisa no qual este Subprojeto está vinculado tem por objetivo estudar certos tipos de representações de Álgebras de Lie, sendo assim este projeto procurou munir a estudante de uma base em tópicos de álgebra, principalmente fazendo uso de tópicos de álgebra linear, propriciando assim que a estudante esteja apta a aprofundar seus estudos em estruturas algébricas, como por exemplo as Álgebras de Lie.

# CAPÍTULO 1

# ESTRUTURAS ALGÉBRICAS

## 1.1 Anéis e Corpos

### 1.1.1 Anéis

Um **anel** é um conjunto não vazio $A$ com duas operações, adição e multiplicação, respectivamente

$$+ : \begin{array}{ccc} A \text{ x } A & \longrightarrow & A \\ (a,b) & \longmapsto & a+b \end{array} \quad e \quad \cdot : \begin{array}{ccc} A \text{ x } A & \longrightarrow & A \\ (a,b) & \longmapsto & a \cdot b \end{array},$$

satisfazendo as seguintes propriedades:

A1) Associatividade da adição:

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

A2) Existência do elemento neutro na adição:
Existe um elemento chamado *zero*, denotado por 0, tal que

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

A3) Existência do elemento inverso na adição:
Dado $a \in A$, existe um elemento chamado simétrico de $a$ e denotado por $(-a)$, tal que

$$a+(-a) = -a+a = 0.$$

A4) Comutatividade da adição:

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

M1) Associatividade da multiplicação:

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

M2) Existência do elemento neutro na multiplicação:
Existe um elemento chamado *unidade*, denotado por 1, tal que

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

M3) Comutatividade da multiplicação:

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

M4) Distributividade da multiplicação com relação a adição:

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

**Observação 1.1** *A multiplicação de $a$ e $b$ será denotada por $a \cdot b$ ou $ab$.*

**Exemplo 1.1** *O conjunto dos números inteiros $\mathbb{Z}$, racionais $\mathbb{Q}$, reais $\mathbb{R}$ e complexos $\mathbb{C}$ são exemplos de anéis.*

**Exemplo 1.2** *O conjunto dos números naturais $\mathbb{N}$ não é um anel. De fato, se $a \in \mathbb{N}$ é não nulo, então $a$ não possui simétrico em $\mathbb{N}$.*

**Proposição 1.1** *Seja $A$ um anel. Para todo $a \in A$ temos que $a \cdot 0 = 0$.*

**Demonstração:** Considere as igualdades:

$$a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$$

Somando $-(a \cdot 0)$ nos dois lados da igualdade, temos

$$-(a \cdot 0) + (a \cdot 0) = -(a \cdot 0) + (a \cdot 0 + a \cdot 0)$$

daí

$$0 = (-(a \cdot 0) + a \cdot 0) + a \cdot 0 = 0 + a \cdot 0 = a \cdot 0.$$

■

**Proposição 1.2** *Seja $A$ um conjunto munido de uma operação $*$ com elemento neutro $e$.*

i) O elemento neutro é único.

ii) Se a operação $*$ é associativa e um elemento $a$ de $A$ possui um elemento inverso, esse inverso é único.

**Demonstração:**

i) Suponha $e'$ outro elemento neutro. Daí $e$ e $e'$ são elementos neutros, então

$$e' = e * e' = e' * e \qquad e \qquad e = e' * e = e * e'$$

segue que $e = e'$.

ii) Suponha que dado $a$, existam $b$ e $b'$, tais que

$$b * a = a * b = e \qquad e \qquad a * b' = b' * a = e.$$

então, temos

$$b' = b' * e = b' * (a * b) = (b' * a) * b = e * b = b$$

Com isso, mostramos que os elemento neutro da adição e multiplicação são únicos. E através disso definimos uma nova operação, chamada subtração, como segue:

$$a - b = a + (-b).$$

■

**Definição 1.1** *Um anel $A$ será chamado* ***domínio de integridade*** *se possuir a seguinte propriedade*

$$\forall\ a, b \in A, \quad a \neq 0\ e\ b \neq 0 \Longrightarrow a \cdot b \neq 0.$$

A propriedade acima é equivalente a:

$$\forall\ a, b \in A, \quad a \cdot b = 0 \Longrightarrow a = 0\ ou\ b = 0.$$

**Observação 1.2** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *e* $\mathbb{C}$ *são* ***domínio de integridade****.*

**Definição 1.2** *Um elemento de um anel $A$ será dito* ***invertível*** *se existir um elemento $b \in A$ com $a.b = 1$. Daí dizemos que $b$ é um* ***inverso*** *de $a$*

O elemento inverso de $a$ para a multiplicação, caso exista, é único e será denotado por $a^{-1}$. Se $a$ é invertível, então $a^{-1}$ é invertível com $(a^{-1})^{-1} = a$, lembrando que o produto de elementos invertíveis é invertível.

**Observação 1.3** *Os únicos elementos invertíveis de* $\mathbb{Z}$ *são* $1$ *e* $-1$ *pois, por exemplo,* $2$ *tem seu inverso como* $\frac{1}{2}$ *e ele não pertence a* $\mathbb{Z}$.

**Definição 1.3** *Um anel onde todo elemento não nulo é invertível é chamado de* ***corpo***.

Um exemplo de corpo é o chamado **corpo de Galois**, é o conjunto $A = \{0, 1\}$ munido das seguintes operações:

| $+$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $1$ |
| $1$ | $1$ | $0$ |

e

| $\cdot$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ |

Note que todo corpo é um domínio de integridade. De fato, se $a \cdot b = 0$, com $a \neq 0$, então eiste $a^{-1}$, e temos que

$$b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

**Proposição 1.3** *(Lei do Cancelamento) Seja* $A$ *um* ***domínio de integridade****. Suponhamos que os elementos* $a, b, c \in A$ *sejam tais que* $c \neq 0$ *e* $a \cdot c = b \cdot c$*, então* $a = b$.

**Demonstração:**
Se $a \cdot c = b \cdot c$, segue que $(a - b) \cdot c = 0$. Como $A$ é um domínio de integridade e $c \neq 0$, que $a = b$.

Seja $A$ um domínio de integridade, Define-se o **corpo de frações** de $A$ como sendo o conjunto

$$Q(A) = \left\{ \frac{\alpha}{\beta};\ \alpha, \beta \in A \ e\ \beta \neq 0 \right\},$$

onde identificam-se $\dfrac{\alpha}{\beta}$ e $\dfrac{\gamma}{\delta}$ sempre que $\alpha\delta = \beta\gamma$, munido com as operações de adição e multiplicação:

$$\frac{\alpha}{\beta} + \frac{\gamma}{\delta} = \frac{\alpha\delta + \beta\gamma}{\beta\delta},$$

e

$$\frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} = \frac{\alpha\gamma}{\beta\delta},$$

respectivamente.

Note que estas operações em $Q(A)$ estão bem definidas, pois $\beta\delta \neq 0$ e independem da representação escolhida para os elementos de $Q(A)$, De fato, se

$$\frac{\alpha}{\beta} = \frac{\alpha'}{\beta'} \; e \; \frac{\gamma}{\delta} = \frac{\gamma'}{\delta'},$$

é fácil verificar que

$$(\alpha\delta + \beta\gamma)\beta'\delta' = (\alpha'\delta' + \beta'\gamma')\beta\delta,$$

e

$$(\alpha\gamma)\beta'\delta' = (\alpha'\gamma')\beta\delta.$$

Portanto,

$$\frac{\alpha}{\beta} + \frac{\gamma}{\delta} = \frac{\alpha\delta + \beta\gamma}{\beta\delta} = \frac{\alpha'\delta' + \beta'\gamma'}{\beta'\delta'} = \frac{\alpha'}{\beta'} + \frac{\gamma'}{\delta'}$$

e

$$\frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} = \frac{\alpha\gamma}{\beta\delta} = \frac{\alpha'\gamma'}{\beta'\delta'} = \frac{\alpha'}{\beta'} \cdot \frac{\gamma'}{\delta'}.$$

■

Uma série de verificações diretas mostram que $Q(A)$ é um corpo, onde $\frac{0}{1}$ e $\frac{1}{1}$ são respectivamente os elementos neutros da adição e da multiplicação, e o inverso de $\frac{\alpha}{\beta} \neq \frac{0}{1}$ é $\frac{\beta}{\alpha}$. Pelo fato de todo elemento $a \in A$ poder ser escrito de modo único na forma $\frac{\alpha}{1}$, temos que

$$A \hookrightarrow Q(A).$$

Com esta construção temos que

$$Q(\mathbb{Z}) = \mathbb{Q}.$$

Sejam $A$ um anel, $a \in A$ e $m \in \mathbb{Z}$. Definimos $ma$ como sendo o elemento de A dado por

$$ma = \begin{cases} a + a + \ldots + a \; (m \; vezes) & se \; m > 1 \\ a & se \; m = 1 \\ 0 & se \; m = 0 \\ (-m)(-a) & se \; m < 0. \end{cases}$$

**Proposição 1.4** *Sejam $a, b \in A$ e $m, n \in \mathbb{Z}$. Temos que*

i) $na = -(-n)a = (-n)(-a) = -n(-a)$ e $na = (n1) \cdot a$.

ii) $n(ma) = (nm)a$.

iii) $n(a + b) = na + nb$ e $n(a - b) = na - nb$.

iv) $(n+m)a = na + ma$ e $(n-m)a = na - ma$.

De modo análogo, para $a \in A$ e $m \in \mathbb{N} \cup \{0\}$, podemos definir

$$a^m = \begin{cases} a \cdot a \cdot \ldots \cdot a \ (m \ vezes) & se \ m > 1 \\ a & se \ m = 1 \\ 1 & se \ m = 0 \ e \ a \neq 0. \end{cases}$$

**Proposição 1.5** *Sejam $a, b \in A$ e $m, n \in \mathbb{N}$. Temos que*

*i)* $(a^m)^n = a^{mn}$

*ii)* $(ab)^n = a^n b^n$

*iii)* $a^{n+m} = a^n a^m$

### 1.1.2 Os Inteiros

Um dos maiores pensadores da história da ciência matemática, Euclides é o autor de *Os Elementos*, escrito por volta de 300 a.C., e provavelmente, um dos livros matemáticos mais marcantes de todos os tempos. Essa obra possui treze volumes (cada um denominado "Livro") onde Euclides conseguiu incorporar praticamente todo o conhecimento matemático acumulado por seus antecessores. Porém iremos nos concentrar em um ponto da obra de Euclides responsável por ter construído sua fama internacional: a divisão euclidiana.

A palavra número significa o que hoje denominamos número natural e nesses livros cada número é representado por um segmento de reta. Assim, Euclides se refere ao número como $AB$ e usa expressões como "é medido por"ou "mede", diferente de como é dito na atualidade "é múltiplo de"ou "é dividido por", respectivamente.

**Exemplo 1.3** *O número 7 era entendido como o segmento $AB$ e $u$ a unidade de medida escolhida arbitrariamente, como na figura abaixo.*


Uma característica dos números inteiros é que nem sempre um número divide o outro, e Euclides se interessava particularmente pelo estudo dessa relação, ou seja, pela teoria da divisibilidade.

Dados dois segmentos de reta $AB$ e $CD$, podemos comparar seus comprimentos e talvez possamos utilizar um deles para medir o outro. Daí, o segmento $AB$ possa estar contido um número exato de vezes no segmento $CD$, ou seja, o segmento $CD$ pode ser obtido através da justaposição do segmento $AB$ um certo número de vezes.

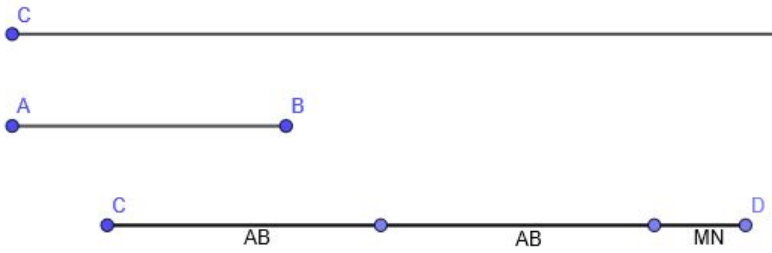
**Exemplo 1.4**


Assim, $CD = AB + AB + AB = 3AB$, no qual a soma é a soma do número natural representado por $AB$. A partir disso obtemos a definição de múltiplo.

**Definição 1.4** *Dados os números naturais $a$ e $b$, dizemos que $a$ é **múltiplo** de $b$, se existe um número natural $n$ tal que $a = nb$.*

Se o segmento $AB$ não for uma parte exata do segmento $CD$, podemos considerar o número máximo de segmentos do tamanho de $AB$ que cabe em $CD$ e obter assim um segmento restante, que denotaremos por $MN$, o qual possui comprimento menos do que o segmento $AB$.

**Exemplo 1.5**




Portanto, se $CD$ e $AB$ representam os números naturais $a$ e $b$, respectivamente, temos que $a = nb + r$, no qual $r < b$ é o número natural que representa o segmento $MN$ e $n$ é o número máximo de segmentos do tamanho de $AB$ que cabe em $CD$.

Agora iremos repetir o processo acima, porém com uma linguagem mais abstrata. Sejam $a$ e $b$ números naturais. Dispondo os números naturais sobre uma semireta e destacando os múltiplos de $b$, obtemos uma divisão dessa em intervalos de comprimento $b$


e então vemos que existem somente duas possibilidades:

i) $a$ é múltiplo de $b$, ou seja, $a = qb$, em que $q \in \mathbb{N}$.

ii) $a$ está compreendido entre dois múltiplos consecutivos de $b$:


E ainda temos que a distância de $a$ a $qb$ é menor do que a distância entre dois múltiplos consecutivos de $b$. Logo, $a = qb + r$, em que $0 < r < b$.

**Observação 1.4** *Até agora consideramos que o "1" é o primeiro número natural. A seguir, no Lema de Euclides, iremos considerar o "0" como o primeiro número natural.*

**Lema 1.1** *(Lema da Divisão de Euclides) Sejam $a$ e $b$ números naturais, com $b > 0$. Então existem números naturais $q$ e $r$, com $0 \leq r < b$, de modo que $a = qb + r$.*

**Demonstração:**

Faremos a demonstração por indução. Se $a = 0$, escolhemos $q = 0$ e $r = 0$, obtendo $0 = 0 \cdot b + 0$. Nesse caso, o resultado está demonstrado.

Seja $a > 0$ e menor do que $b$. Daí suponhamos, por indução, que o resultado seja válido para o número natural $(a - 1)$: existem $r'$ e $q' \in \mathbb{N}$, tais que

$$(a - 1) = q'b + r', \quad \textit{em que} \quad 0 \leq r' < b.$$

Logo,

$$a = q'b + (r' + 1) \quad \textit{com} \quad 1 \leq r' + 1 \leq b.$$

Se $r' + 1 < b$, tomamos $q = q'$ e $r = r' + 1$, o que mostra o resultado. Se, por outro lado, $r'+1 = b$, temos que $a = q'b+b = (q'+1)b$, e daí basta tomar $q = q'+1$ e $r = 0$, para este caso.

Portanto, o Lema da Divisão de Euclides nos garante que, dados $a, b \in \mathbb{N}$, com $b > 0$, sempre podemos achar o quociente $q$ e o resto $r$ da divisão de $a$ por $b$.

Iremos agora demonstrar a unicidade da divisão de $a$ por $b$, e para tal, iremos supor que $(q', r')$ e $(q'', r'')$ sejam dois pares de números naturais tais que

$$a = q'b + r', \quad a = q''b + r'', \quad com \quad 0 \leq r' < b \quad e \quad 0 \leq r'' < b.$$

Queremos concluir que $q' = q''$ e $r' = r''$.

Se tivéssemos $q' > q''$, obteríamos $(q' - q'')b = r'' - r'$, e como $q' - q''$ é um número natural não-nulo, $q' - q'' \geq 1$ e, portanto, $(q' - q'')b \geq b$. Logo, obteríamos $r'' - r' \geq b$, o que é absurdo, já que $0 \leq r' < b$ e $0 \leq r'' < b$. Assim, não podemos ter $q' > q''$. Analogamente, não podemos ter $q'' > q'$ e, portanto, $q' = q''$. Mas então $r' = a - q'b = a - q''b = r''$. Provando assim a unicidade no Lema da Divisão de Euclides.

■

Iremos agora estender o Lema de Euclides para o conjunto dos inteiros $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

**Definição 1.5** *O* ***valor absoluto*** *de um número inteiro $b$, denotado por $|b|$, é*

$$|b| = \begin{cases} b, & se \quad b \geq 0, \\ -b, & se \quad b < q0 \end{cases}$$

**Observação 1.5** *Para todo $b \in \mathbb{Z}$, $|b|$ é um número natural. Além disso, $|b| = |-b|$.*

**Definição 1.6** *Dados dois inteiros $a$ e $b$, dizemos que $a$ é* ***múltiplo*** *de $b$, se existe um inteiro $q$ tal que $a = qb$.*

**Exemplo 1.6** *Claramente 6 é múltiplo de 3, pois $6 = 2 \cdot 3$. 6 é múltiplo de $-3$, pois $6 = (-2) \cdot (-3)$. $-6$ é múltiplo de 3 e de $-3$, pois $-6 = (-2)3 = 2(-3)$.*

Dado um inteiro $b \neq 0$, destacando na reta os múltiplos deste, temos que, para todo inteiro $a$, ou $a$ é múltiplo de $b$ ou $a$ está entre dois múltiplos consecutivos de $b$:


Esta informação pode ser expressa de duas maneiras:

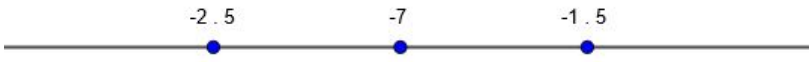
$$a = q|b| + r, \quad \text{com} \quad 0 \leq r < |b|$$

ou

$$a = (q+1)|b| + r, \quad \text{com} \quad -|b| < r < 0.$$

Iremos escolher sempre a primeira forma.

**Exemplo 1.7** *Para $a = -7$ e $b = 5$ temos $q = -2$:*




*ou seja:*

$$-7 = \underbrace{-2}_{q} \cdot 5 + \underbrace{3}_{r_1},\ 0 < r_1 < |5|$$

*ou*

$$-7 = \underbrace{-1}_{q+1} \cdot 5 - \underbrace{2}_{r_2},\ -|5| < r_2 < 0.$$

Desta maneira, assim como no caso dos naturais, vamos provar que temos dois inteiros: $q$ (quociente) e $r$ (resto), que serão unicamente determinados desde que escolhamos o resto para ser não negativo.

Chegamos ao seguinte enunciado para os números inteiros.

**Teorema 1.1** *(Lema da Divisão de Euclides) Sejam $a$ e $b$ inteiros, com $b \neq 0$. Então existem inteiros $q$ e $r$, com $0 \leq r < |b|$, tais que $a = qb + r$. Além disso, são únicos os inteiros $q$ e $r$ satisfazendo essas condições.*

**Demonstração:**

A prova da existência de $q$ e $r$ será feita considerando os quatro casos possíveis abaixo:

Caso 1: $a \geq 0$ e $b > 0$.
Caso 2: $a \geq 0$ e $b < 0$.
Caso 3: $a < 0$ e $b > 0$.
Caso 4: $a < 0$ e $b < 0$.

Claramente não é necessário provar o caso 1 pois este é exatamente o Lema da Divisão de Euclides para os naturais.

Para o caso 2, observamos que $|b| = -b > 0$ e recorremos novamente ao Lema da Divisão de Euclides. Deste modo, existem naturais $q_1$ e $r_1$ tais que:

$$a = (-b)q_1 + r_1, \quad \textit{onde} \quad 0 \leq r_1 < -b.$$

Tomamos $r = r_1$ e $q = -q_1$, obtemos $a = bq + r$ dentro das condições exigidas, ou seja, $0 \leq r < |b|$.

No caso 3 temos $-a > 0$ e assim:

$$-a = bq_1 + r_1, \quad com \quad 0 \leq r_1 < b.$$

Logo, $a = -bq_1 - r_1$ e deste modo, se $r_1 = 0$, tomamos $r = 0$ e $q = -q_1$. Mas se $0 < r_1 < b$ então $0 < b - r_1 < b$. Tomamos $r = b - r_1$ e $q = -q_1 - 1$ pois, deste modo,

$$a = -bq_1 - r_1 + b - b = b(-q_1 - 1) + (b - r_1) = bq + r, \ onde \ 0 \leq r < |b|.$$

Para o caso 4, temos $|a| = -a > 0$ e $|b| = -b > 0$ e, assim, ao usar o Lema da Divisão de Euclides, sabemos que existem naturais $q_1$ e $r_1$ tais que:

$$-a = (-b)q_1 + r1, \quad onde \quad 0 \leq r_1 < -b$$

e portanto $a = bq_1 - r_1$. Novamente, se $r_1 = 0$ tomamos $r = 0$ e $q = q_1$. Mas se $0 < r_1 < -b$ então $0 < -b - r_1 < -b$. Deste modo, tomamos $r = -b - r_1$ e $q = q_1 + 1$ pois com isso temos

$$a = bq_1 - r_1 - b + b = b(q_1 + 1) + (-b - r_1) = bq + r, \quad onde \quad 0 \leq r < |b|.$$

Após garantir a existência do quociente e do resto na divisão euclidiana, vamos garantir a unicidade supondo que podemos escrever

$$a = |b|q_1 + r_1 \quad e \quad a = |b|q_2 + r_2, \quad com \quad 0 \leq r_1, r_2 < |b|.$$

Primeiramente, como $r_1$ e $r_2$ são ambos $\geq 0$, note que

$$|r_1 - r_2| < |r_1| = r_1 < |b|.$$

Por outro lado, temos $|b|q_1 + r_1 = |b|q_2 + r_2$ e assim, $r_1 - r_2 = |b|(q_2 - q_1)$. Portanto

$$|r_1 - r_2| = |b||q_2 - q_1|.$$

Mas assim, $|r_1 - r_2|$ é um múltiplo de $|b|$ e é menor que $|b|$, consequentemente $|r_1 - r_2| = 0$. Logo $r_1 = r_2$ e $q_1 = q_2$, como queríamos mostrar.

■

**Observação 1.6** *Se $a \in \mathbb{Z}$, então $a = 2q + r$, em que $q, r \in \mathbb{Z}$ e $0 \leq r < 2$. Assim, $a = 2q$ ou $a = 2q + 1$. Os números da primeira forma são chamados **pares** e os da segunda forma **ímpares**.*

**Observação 1.7** *O quadrado de um inteiro qualquer é da forma $3k$ ou $3k + 1$, com $k \in \mathbb{N}$. Com efeito, pelo Lema da Divisão de Euclides, qualquer inteiro a pode ser escrito como*

$$a = 3q + r, \quad em \ que \quad r \in \{0, 1, 2\}.$$

*Portanto, $a^2 = 9q^2 + 6qr + r^2 = 3(3q^2 + 2qr) + r^2$.*
*Logo, temos as seguintes possibilidades:*

- *se* $r = 0$, *então* $a^2 = 3(3q^2 + 2qr) = 3k$, *em que* $k = 3q^2 + 2qr$.
- *se* $r = 1$, *então* $a^2 = 3(3q^2 + 2qr) + 1 = 3k + 1$, *em que* $k = 3q^2 + 2qr$.
- *se* $r = 2$, *então* $a^2 = 3(3q^2+2qr)+4 = 3(3q^2+2qr+1) = 3k+1$, *em que* $k = 3q^2+2qr+1$.

Iremos estudar agora o caso em que a divisão euclidiana é exata e demonstraremos alguns resultados.

Se $a$ for múltiplo de $b$, dizemos também que $b$ **divide** $a$ ou que $b$ é **divisor** de $a$ e denotamos $b \mid a$. Se $b$ não divide $a$, denotamos $b \nmid a$.

**Proposição 1.6** *Sejam* $a$ *e* $b$ *inteiros quaisquer. Então vale:*

*i)* $a \mid b$, *então* $a \mid (-b)$.

*ii)* $a \mid b$ *e* $a \mid c$, *então* $a \mid (b + c)$.

*iii)* $a \mid b$ *e* $a \mid (b + c)$, *então* $a \mid c$.

*iv)* $a \mid b$ *e* $b \mid a$, *então* $a = \pm b$.

*v)* $a \mid b$ *e* $a \mid c$, *então* $a \mid (bx + cy)$ *para quaisquer* $x, y \in \mathbb{Z}$.

*vi)* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

**Observação 1.8** *Vimos que se* $a \mid b$ *e se* $a \mid c$, *então* $a \mid (b + c)$. *Isso é muito diferente da afirmação: se* $a \mid (b + c)$, *então* $a \mid b$ *e* $a \mid c$.

No Livro VII de *Os Elementos* de Euclides encontra-se a definição de números primos. Claramente, dado qualquer número inteiro $n$, os números $1$, $n$, $-1$ e $-n$ são divisores inteiros de $n$. Vamos nos preocupar apenas com os divisores positivos de $n$. A pergunta é se existem outros além de $1$ e $n$.

**Definição 1.7** *Um número inteiro* $n > 1$ *é* ***primo*** *se seus únicos divisores positivos são 1 e n.*
*Assim:*

$$n \text{ é } \textbf{\textit{primo}} \iff \text{se } a \mid n,\ a > 0 \text{ então } a = 1 \text{ ou } a = n.$$

*Caso o número* $n > 1$ *não seja primo, dizemos que ele é* ***composto****, ou seja,*

$$n \text{ é } \textbf{\textit{composto}} \iff \text{existe } a \mid n,\ a > 0 \text{ tal que } a \neq 1 \text{ e } a \neq n.$$

*Neste caso,* $n = ab$, *onde* $a$ *e* $b$ *são inteiros e* $1 < a,\ b < n$.

Note que o número 1 não é classificado nem como primo, nem como composto. Claro que 2 é um número primo e é o único primo que é par. Não é difícil dar outros exemplos de números primos, podemos listar os iniciais $2, 3, 5, 7, 11, 13, 17, 19, \ldots$.

**Lema 1.2** *Se $n \geq 2$ for um número natural então $n$ possui um divisor que é um número primo.*

**Demonstração:**

Para provar este resultado, usaremos a segunda forma do Princípio de Indução Matemática. Se $n = 2$, é claro que o resultado vale. Suponhamos $k > 2$ e que o resultado vale para $2 \leq m < k$, ou seja, dado qualquer natural $m$ entre 2 e $k$, $m$ possui um divisor primo.

Vamos provar que vale para $n = k$. Se $k$ for primo, não temos nada a fazer. Caso contrário, $k$ tem um divisor $d$ tal que $1 < d < k$. Deste modo, usando a hipótese de indução, $d$ possui um divisor primo e como este será tambem divisor primo de $k$, o resultado está demonstrado.

■

**Proposição 1.7** *Se $n$ for um número natural composto, então $n$ possui (pelo menos) um divisor primo $p \leq \sqrt{n}$.*

**Demonstração:**

Para um número composto $n$ existem divisores $1 < a, b < n$ tais que $n = ab$. Além disso, não podemos ter simultaneamente $a > \sqrt{n}$ e $b > \sqrt{n}$ (caso contrário $n = ab > \sqrt{n}\sqrt{n} = n$, o que é absurdo). Logo, pelo menos um dos divisores (digamos que seja $a$) tem que ser $\leq \sqrt{n}$. Mas, pela proposição anterior, $a$ possui um divisor primo e assim concluímos que $n$ possui um divisor primo $\leq \sqrt{n}$.

■

Desta forma, o resultado anterior nos informa que para um dado número natural $n \geq 2$, se constatarmos que todos os primos $p \leq \sqrt{n}$ não são divisores de $n$, então podemos concluir que $n$ é primo.

O inconveniente do teste acima é que se o número for muito grande, determinar todos os primos anteriores a ele pode ser uma tarefa extremamente difícil.

**Teorema 1.2** *Existem infinitos números primos.*

**Demonstração:**

Uma simples demonstração pode ser dada por absurdo, considerando que temos um número finito de números primos e que $p_1, p_2, \ldots, p_k$ sejam todos os primos existentes.

O inteiro $m = p_1 \cdot p_2 \ldots p_k + 1$ não é primo pois não é igual a nenhum dos listados. Portanto, possui um divisor primo. Porém, este divisor não é nenhum dos primos já considerados, pois caso seja algum dos $p_i$ temos $p_i \mid p_1 \cdot p_2 \ldots pk + 1$ mas como $p_i \mid p_1 \cdot p_2 \ldots p_k$ chegaríamos ao absurdo que $p_i \mid 1$. Com este argumento, garantimos que existem infinitos números primos.

■

Muitas questões interessantes sobre números primos não foram respondidas até hoje. Por exemplo, dizemos que dois números primos são **gêmeos** se eles são números ímpares consecutivos. Assim, 3 e 5, 7 e 9, 11 e 13 são números primos gêmeos. Um antigo problema, é se existe ou não um número infinito de primos gêmeos.

**Proposição 1.8** *Para todo número natural $n > 2$ existem $n$ números compostos consecutivos.*

**Demonstração:**

A sequência $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$ é formada apenas por números compostos, pois $i \mid (n+1)! + i$ para todo $i$ tal que $2 \leq i \leq n+1$. O que prova a afirmação.

■

Os gregos foram os primeiros a perceber que qualquer número natural, exceto o 0 e o 1, pode ser gerado pela multiplicação de números primos, os chamados "blocos de construção". Ou seja, um número natural $n \geq 2$ pode ser escrito como um produto de primos e, é claro, a ordenação dos primos neste produto não modifica o resultado.

A demonstração deste fato foi dada por Euclides, que provou apenas a existência da fatoração de um natural em primos. Acredita-se que Euclides conhecesse a unicidade desta fatoração e que não fez sua demonstração pela dificuldade em estabelecer uma notação adequada. No próximo teorema, provaremos a existência e a unicidade da fatoração de um natural em primos utilizando o Princípio de Indução Matemática.

**Teorema 1.3** *(Teorema Fundamental da Aritmética - TFA) Dado um número natural $n \geq 2$, existem primos distintos $p_1, p_2, \ldots, p_k$ tais que*

$$n = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \ldots p_k^{\alpha k},$$

*onde os expoentes $\alpha_i$ são naturais, $1 \leq i \leq k$. Além disso, se $n = q_1^{\beta 1} \cdot q_2^{\beta 2} \ldots q_t^{\beta t}$ , onde $q_j$ são primos distintos, $1 \leq j \leq t$, então $t = k$ e todo $q_j$ é igual a algum $p_i$.*

**Demonstração:**

Usaremos a segunda forma de indução para garantir a existência da fatoração. Para $n = 2$ existe uma decomposição trivial em números primos, já que 2 já é um número primo. Consideremos $k > 2$ e suponhamos que existe uma fatoração para todo natural $m$ tal que $2 \leq m \leq k$.

Mostraremos agora que também vale para $k + 1$ e, como consequência, teremos que o resultado vale para todo $n \geq 2$.

Se $k+1$ for primo, admite a decomposição trivial. Caso contrário, $k+1$ pode ser escrito como

$$k + 1 = ab, \quad \text{onde} \quad 1 < a < k + 1 \quad e \quad 1 < b < k + 1.$$

Assim, $2 \leq a \leq k$ e $2 \leq b \leq k$, e pela hipótese de indução $a$ e $b$ podem ser escritos como produtos de primos. Logo, o resultado também vale para $k + 1$.

Para provar a unicidade, devemos garantir que um natural $n \geq 2$ não admite mais de uma fatoração em produto de fatores primos. Esta demonstração também será feita usando a segunda forma de indução.

Claro que $n = 2$ possui uma única fatoração. Vamos considerar $k > 2$ e assumir que qualquer natural $m$ tal que $2 \leq m \leq k$ tem uma fatoração única como produto de primos. Agora suponhamos que $k + 1$ tenha duas fatorações distintas como produto de primos (os primos não são necessariamente distintos):

$$k + 1 = p_1 \dots p_r = q_1 \dots q_s.$$

Reordenando os primos, se necessário, podemos supor que

$$p_1 \leq \dots \leq p_r \quad e \quad q_1 \leq \dots \leq q_s.$$

Note que $p_1 \neq q_1$ pois se tivéssemos $p_1 = q_1$ então o natural $\frac{k+1}{p_1} \leq k$ teria duas fatorações distintas com produto de primos, contrariando a hipótese de indução.
Se assumimos, sem perda de generalidade, que $p_1 < q_1$ e considerarmos o inteiro

$$m = (k + 1) - (p_1 \cdot q_2 \dots q_s),$$

então $m < k + 1$ temos que $m$ se escreve como

$$m = p_1 \cdot p_2 \dots p_r - p_1 \cdot q_2 \dots q_s$$

e também como

$$m = q_1 \cdot q_2 \dots q_s - p_1 \cdot q_2 \dots q_s.$$

Deste modo:

$$m = p_1(p_2 \dots p_r - q_2 \dots q_s)$$

e

$$m = (q_1 - p_1)(q_2 \dots q_s).$$

Por $m = p_1(p_2 \dots p_r - q_2 \dots q_s)$, temos $m \geq 2$ pois $p_1 \mid m$ e assim já que $2 \leq m \leq k$, por hipótese de indução, $m$ tem fatoração única em primos.
Deste modo, o primo $p_1$ deve estar presente no produto em $m = (q_1 - p_1)(q_2 \dots q_s)$ (pois está presente em $m = p_1(p_2 \dots p_r - q_2 \dots q_s)$) e como $p_1 < q_1 \leq \dots \leq q_s$, devemos ter $p_1$ como fator de $q_1 - p_1$, ou seja, $p_1 \mid q_1 - p_1$. Portanto, existe $c \in \mathbb{Z}$ tal que

$$q_1 - p_1 = cp_1$$

e, com isso, $q_1 = (c+1)p_1$, o que é absurdo pois $p_1$ e $q_1$ são primos distintos. Com esta contradição, concluímos que $k+1$ não possui duas fatorações distintas como produto de primos, o que mostra que qualquer natural $n \geq 2$ tem uma fatoração única como produto de primos.

■

**Exemplo 1.8** *Vamos mostrar que não existe um primo cujo dobro seja igual a um quadrado perfeito menos 1.*

*Para resolver, suponhamos que exista um primo $p$ tal que $2p = n^2 - 1$. Mas então $2p = (n-1)(n+1)$ e, assim, usando o TFA:*

$$\underbrace{n+1 = 2 \text{ e } n-1 = p}_{(1)} \quad \text{ou} \quad \underbrace{n-1 = 2 \text{ e } n+1 = p}_{(2)}$$

*Se (1) ocorre então $n = 1$ e $p = 0$, o que é um absurdo. Se (2) ocorre, então $n = 3$ e, assim, $p = 4$, o que é igualmente um absurdo. Logo tal primo não existe.*

O próximo resultado é uma consequência imediata do Teorema Fundamental da Aritmética.

**Corolário 1.1** *Todo número inteiro não-nulo diferente de $\pm 1$ pode ser escrito como $\pm 1$ vezes o produto de números primos. Essa expressão é única, exceto pela ordem na qual os fatores primos aparecem.*

**Definição 1.8** *Um número negativo $q$ cujo simétrico $-q$ é um número natural primo é chamado número* ***primo negativo****.*

**Exemplo 1.9** *Temos então que $2, 3$ e $5$ são números primos, enquanto que $-2, -3$ e $-5$ são primos negativos.*

**Observação 1.9** *Observamos que, na fatoração de um número inteiro $a$, o mesmo primo $p$ pode aparecer várias vezes. Agrupando esses primos, podemos escrever a decomposição de $a$ como:*

$$a = (\pm 1)p_1^{r_1} \cdot p_2^{r_2} \dots p_n^{r_n},$$

*em que $0 < p_1 < p_2 < \ldots < p_n$ e $r_i > 0$ para $i = 1, 2, \ldots, n$.*

Quando nos referimos a uma decomposição (ou fatoração) de um número inteiro em números primos, estaremos nos referindo a essa decomposição, em que os primos são todos positivos.

**Exemplo 1.10** *Aceitamos as decomposições do tipo:*

$$40 = 2^3 \cdot 5 \qquad e \qquad -12 = -(2^2 \cdot 3),$$

*mas não aceitamos as decomposições do tipo:*

$$40 = (-2^3) \cdot (-5) \qquad e \qquad -12 = 2^2 \cdot (-3).$$

**Corolário 1.2** *Sejam $a, b \in \mathbb{Z}$ e $p$ um número primo. Se $p$ for um fator de $ab$, então $p$ é um fator de $a$ ou $p$ é um fator de $b$.*

**Demonstração:**

Já sabemos que $m \mid n$ se, e somente se, $m \mid -(n)$, portanto é suficiente mostrar esse resultado para $a$ e $b$ números naturais.

Se $p$ não fosse um fator de $a$ e nem de $b$, então as fatorações de $a$ e $b$ em produtos de primos levaria a uma fatoração de $ab$. Por outro lado como, por hipótese, $p$ é um fator de $ab$, existiria um $q \in \mathbb{N}$ tal que $pq = ab$. Então, o produto de $p$ por uma fatoração de $q$ daria uma fatoração de $ab$ em primos contendo $p$, contrariando a unicidade da decomposição de $ab$ em primos. ■

Quando temos dois inteiros $a$ e $b$, podemos nos perguntar sobre seus divisores e múltiplos comuns, ou seja, divisores simultâneos de $a$ e $b$ e múltiplos simultâneos de $a$ e $b$.

Claro que 1 é um divisor comum de $a$ e $b$, a questão é se existem outros e qual é o maior destes divisores. Também podemos notar que $ab$ é um múltiplo comum de $a$ e $b$ e novamente nos perguntamos qual é o menor destes múltiplos.

Foi no Livro VII de *Os Elementos* que Euclides definiu o máximo divisor comum de dois inteiros, conforme abaixo.

**Definição 1.9** *Dados dois inteiros $a$ e $b$, não simultaneamente nulos, dizemos que um inteiro $d$ é* ***máximo divisor comum*** *de $a$ e $b$, se $d$ satisfaz:*

*i)* $d \mid a$ *e* $d \mid b$.

*ii) Se* $c \in \mathbb{Z}$ *for tal que* $c \mid a$ *e* $c \mid b$, *então* $c \leq d$.

Se $d$ for máximo divisor comum de $a$ e $b$ , escrevemos $d = mdc(a, b)$ ou simplesmente $d = (a, b)$, quando não houver dúvidas quanto a notação.

**Observação 1.10** *Na notação $d = mdc(a, b)$, estamos antecipando a unicidade do máximo divisor comum de $a$ e $b$.*

Para o caso particular em que o máximo divisor comum é a unidade, definimos

**Definição 1.10** *Dizemos que dois números inteiros são* ***primos entre si****, se o máximo divisor comum deles for igual a* 1.

**Observação 1.11** *O leitor deve observar que, na definição de máximo divisor comum, exigimos $a$ e $b$ não simultaneamente nulos porque, caso contrário, qualquer inteiro $c$ seria um divisor comum de $a$ e $b$, o que tornaria impossível tomar o maior desses números.*

**Proposição 1.9** *Sejam $a$ e $b$ inteiros não simultaneamente nulos. Então:*

*i)* $mdc(a, b) > 0$.

*ii) se* $a \neq 0$ *e* $b \neq 0$, *então* $mdc(a, b) \leq min\{|a|, |b|\}$.

*iii) é único o* $mdc(a, b)$.

*iv)* $mdc(a, b) = mdc(b, a)$.

*v)* $mdc(a, b) = mdc(|a|, |b|)$.

*vi) se* $a \neq 0$, $mdc(a, 0) = |a|$.

**Demonstração:** Ver demonstração em [2]. ∎

Então, vimos algumas propriedades do $mdc(a, b)$. Porém a seguinte pergunta ainda não foi respondida: o máximo divisor comum de $a$ e $b$ sempre existe? Para responder a pergunta, notamos: o conjunto de divisores positivos de $a$ e $b$é não-vazio (pois 1 divide tanto $a$ quanto $b$) e limitado superiormente.

**Exemplo 1.11** *Vamos obter o máximo divisor comum de* 24 *e* $-18$. *Como* $D_{-18} = \{\pm 18, \pm 9, \pm 6, \pm 3, \pm 2, \pm 1\}$ *e* $D_{24} = \{\pm 24, \pm 12, \pm 8, \pm 6, \pm 4, \pm 3, \pm 2, \pm 1\}$ *são, respectivamente, os conjunto dos divisores de* $-18$ *e* 24*, então o conjunto dos divisores comuns de* 24 *e* $-18$ *é:*

$$D_{-18} \cap D_{-24} = \{\pm 6, \pm 4, \pm 3, \pm 2, \pm 1\}$$

*e portanto,* $mdc(-18, 24) = 6$.

Sejam dados dois segmentos $a$ e $b$. Se o menor, digamos $b$, é parte exata do maior, $a$, então $b$ é a maior medida comum procurada. Ou seja, se $a$ e $b$ forem inteiros positivos e $b \mid a$, então $mdc(a, b) = b$.

No caso de $b$ não medir $a$, ainda assim podemos subtrair $b$ de $a$ um número inteiro de vezes, de tal maneira que o segmento restante $r_0$ possua medida menor do que $b$. Observe ainda que esse é o conteúdo do Lema da Divisão de Euclides, no caso em que a divisão não é exata:

$$a = qb + r_0, \quad com \quad 0 < r_0 < b.$$

Se $r_0$ medir $b$, então $r_0$ é a maior medida comum de $a$ e $b$. Caso contrário, subtraímos $r_0$ um número inteiro de vezes de $b$, de modo que reste um segmento $r_1$ de comprimento menor do que $r_0$.

Se $r_1$ medir $r_0$ então $r_1$ é a maior medida comum de $a$ e $b$. Se não, continuamos o processo: subtraímos $r_1$ número inteiro de vezes de $r_0$ de modo que sobre um segmento de comprimento $r_2$ com $r_2 < r_1$, e assim sucessivamente.

**Exemplo 1.12** *Sejam* $a$ *e* $b$ *segmentos de* 15 *e* 4 *unidades, respectivamente. Nesse caso,* $b$ *não mede* $a$*, se subtrairmos* $b$ *três vezes de* $a$*, obteremos um segmento* $r_0$ *de comprimento* 3*, que não mede* $b$.

*Se subtraírmos* $r_0$ *de* $b$*, obtemos um segmento* $r_1$ *de comprimento* 1.

*Como* $r_1$ *mede* $r_0$*, temos que a maior medida comum de* $a$ *e* $b$ *é a unidade.*

*Trocando a palavra segmentos por números, e a palavra mede por divide no processo descrito por Euclides, obteremos o algoritmo com o qual estamos acostumados a calcular o máximo divisor comum de dois números. Temos:*

$$\begin{aligned} 15 &= 3 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

*Portanto, $mdc(a,b) = 1$, que é o último resto não-nulo obtido nas divisões sucessivas.*

**Lema 1.3** *Se $b$ for não-nulo e $a = qb + r$, então $mdc(a,b) = mdc(b,r)$.*

**Demonstração:**
Suponhamos que $d = mdc(a,b)$. Queremos mostrar que $d = mdc(b,r)$. Usando a definição de mdc, já temos que $d \mid a$ e $d \mid b$. Desta forma, como $r = a - bq$, vamos ter $d \mid r$. Logo, já concluímos que $d$ é um divisor comum de $b$ e $r$, precisamos garantir agora que ele seja o maior de todos os divisores.

Se $c$ é um outro divisor de $b$ e $r$, temos $c \mid b$ e $c \mid r$. Mas então, como $a = bq + r$ teremos que $c \mid a$. Assim, $c$ é um divisor comum de $a$ e $b$ e portanto deve ser menor ou igual a $mdc(a,b)$, ou seja, $c \leq d$.

■

**Teorema 1.4** *(Máximo Divisor Comum - Algoritmo de Eulides)*

*Sejam $a$ e $b$ naturais não nulos, com $a \geq b$. Dividindo sucessivamente, obtemos:*

$$\begin{aligned}
a = bq_1 + r_1, 0 < r_1 < b &\Longrightarrow mdc(a,b) = mdc(b,r_1)\\
b = r_1q_2 + r_2, 0 < r_2 < r_1 &\Longrightarrow mdc(b,r_1) = mdc(r_1,r_2)\\
r_1 = r_2q_3 + r_3, 0 < r_3 < r_2 &\Longrightarrow mdc(r_1,r_2) = mdc(r_2,r_3)\\
&\vdots\\
r_{n-2} = r_{n-1}q_n + r_n, 0 < r_n < r_{n-1} &\Longrightarrow mdc(r_{n-2},r_{n-1}) = mdc(r_{n-1},r_n)\\
r_{n-1} = r_nq_{n+1} &\Longrightarrow mdc(r_{n-1},r_n) = r_n.
\end{aligned}$$

*Portanto, $mdc(a,b) = r_n$, ou seja, é o último resto não nulo encontrado no processo de divisões sucessivas. Claro que se $r_1 = 0$ então $mdc(a,b) = b$.*

**Demonstração:**
Como $a$ e $b$ são naturais, é claro que se $a = bq_1$ então $mdc(a,b) = b > 0$. Portanto, vamos considerar o caso geral e provar que podemos calcular o $mdc$ usando indução sobre o número de passos do algoritmo de Euclides (AE).

Para isto, o que queremos provar é que a seguinte afirmação é verdadeira: se, ao aplicarmos o AE a dois naturais $a$ e $b$, obtivermos o primeiro resto nulo após $n+1$ passos, então $mdc(a,b)$ é igual ao último resto não nulo obtido, ou seja, o resto obtido no passo $n$.

É claro que para $n = 1$ a afirmação é verdadeira, pois se o primeiro resto nulo é obtido no passo 2 então

$$a = bq_1 + r_1,\ 0 < r_1 < b$$

$$b = r_1q_2,$$

assim, temos $mdc(a,b) = mdc(b,r_1) = r_1$ e, neste caso, o $mdc$ é o resto obtido no passo $n = 1$.

Agora suponhamos que a afirmativa seja verdadeira para $n = k$, ou seja, para obter o primeiro resto nulo precisamos de $k+1$ passos.

Vamos ver que a afirmativa também é verdadeira para $n = k+1$, ou seja, quando precisarmos de $k+2$ passos para chegar no primeiro resto nulo:

$$\begin{gathered} a = bq_1 + r_1, 0 < r_1 < b \\ b = r_1q_2 + r_2, 0 < r_2 < r_1 \\ \vdots \\ r_{k?2} = r_{k?1}q_k + r_k, 0 < r_k < r_{k?1} \\ r_{k?1} = r_kq_{k+1} + r_{k+1} \\ r_k = r_{k+1}q_{k+2}. \end{gathered}$$

Queremos mostrar que $mdc(a,b) = r_{k+1}$, ou seja, o resto não nulo obtido no passo $k+1$. Mas note que ao aplicarmos o AE aos números $b$ e $r_1$, o primeiro resto nulo foi encontrado após $k+1$ passos e então, por hipótese de indução, $mdc(b,r_1) = r_{k+1}$. Mas, temos

$$mdc(a,b) = mdc(b,r_1) = r_{k+1},$$

o que garante o resultado.

■

**Observação 1.12** *Como $mdc(a,b) = mdc(|a|,|b|)$, podemos também utilizar o algoritmo dado para calcular o máximo divisor comum de inteiros negativos.*

**Exemplo 1.13** *Vamos calcular o $mdc(726,-275)$. Como $mdc(726,-275)$ é igual ao $mdc(726,275)$, podemos aplicar o algoritmo de Euclides a $mdc(726,275)$:*

$$\begin{gathered} 726 = 2 \cdot 275 + 176 \\ 275 = 1 \cdot 176 + 99 \\ 176 = 1 \cdot 99 + 77 \\ 99 = 1 \cdot 77 + 22 \\ 77 = 3 \cdot 22 + 11 \\ 22 = 2 \cdot 11, \end{gathered}$$

*portanto, $mdc(726,-275) = 11$.*

**Proposição 1.10** *Se $a$ e $b$ forem naturais e $d = mdc(a,b)$, então existem inteiros $x$ e $y$ tais que $d = ax + by$.*

**Demonstração:**

Inicialmente notamos que se $b \mid a$ então:

$$mdc(a,b) = b = \underbrace{0}_{x} \cdot a + \underbrace{1}_{y} \cdot b.$$

Portanto, vamos considerar o caso em que $b$ não divide $a$. Neste caso, calculamos $d = mdc(a,b)$ e vamos mostrar que $d$ é uma combinação linear inteira de $a$ e $b$ usando indução sobre o número de passos do algoritmo de Euclides. É claro que, se são necessários $n = 2$ passos para calcularmos o $mdc$ então

$$a = bq_1 + r_1, 0 < r_1 < b$$

$$b = r_1 q_2,$$

ou seja, temos $mdc(a,b) = mdc(b,r_1) = r_1 = a - bq_1$ e, neste caso, $x = 1$ e $y = -q_1$. Agora suponhamos que a afirmativa seja verdadeira sempre que necessitarmos de $n = k$ passos para o cálculo do $mdc$ (ou seja, para obter o primeiro resto nulo no processo de divisões sucessivas). Vamos ver que também é verdadeira quando precisarmos de $n = k + 1$ passos:

$$\begin{gathered} a = bq_1 + r_1, 0 < r_1 < b \\ b = r_1 q_2 + r_2, 0 < r_2 < r_1 \\ r_1 = r_2 q_3 + r_3, 0 < r_3 < r_2 \\ \vdots \\ r_{k-2} = r_{k-1} q_k + r_k, 0 < r_k < r_{k-1} \\ r_{k-1} = r_k q_{k+1}, \end{gathered}$$

ou seja, o que temos aqui é que $mdc(a,b) = r_k$, obtido após $k+1$ passos. Mas note que $mdc(b,r_1) = r_k$ e necessitamos de $k$ passos para obtê-lo. Logo, por hipótese de indução, existem inteiros $x'$ e $y'$ tais que

$$r_k = bx' + r_1 y'.$$

Mas como $a = bq_1 + r_1$ temos $r_1 = a - bq_1$ e, portanto,

$$mdc(a,b) = r_k = bx' + (a - bq_1)y' = a \underbrace{y'}_{x} + b \underbrace{(x' - q_1 y')}_{y}$$

e isto finaliza a demonstração.

■

**Corolário 1.3** *Seja $p$ um número primo. Se $p \mid ab$ e $p \nmid a$, então $p \mid b$.*

**Demonstração:**

Como $mdc(a,p) = 1$, existem inteiros $x$ e $y$ tais que $xa + yp = 1$. Multiplicando essa igualdade por $b$ obtemos:

$$xab + ypb = b.$$

Como $p \mid ab$ e $p \mid ypb$, concluímos que $p \mid b$.

■

**Proposição 1.11** *Sejam $a$ e $b$ dois inteiros não simultaneamente nulos. O inteiro $d$ é o máximo divisor comum de $a$ e $b$ se, e somente se, $d$ satisfaz as propriedades abaixo:*

*i)* $d > 0$.

*ii)* $d \mid a$ *e* $d \mid b$.

*iii) se* $c \in \mathbb{Z}$ *for tal que* $c \mid a$ *e* $c \mid b$, *então* $c \mid d$.

**Demonstração:**

Se $d = mdc(a,b)$ então claramente $d$ satisfaz as propriedades $(i)$ e $(ii)$ do enunciado. Agora, temos que mostrar que também satisfaz $(iii)$. Para isto, considere $c$ um inteiro tal que $c \mid a$ e $c \mid b$. Daí escrevemos $d = ax + by$, com $x, y \in \mathbb{Z}$ e, portanto, $c \mid d$.

Para mostrar a recíproca, consideramos $d$ um inteiro satisfazendo os itens $(i), (ii)$ e $(iii)$ acima. Vamos mostrar que de fato, $d$ é o máximo divisor comum de $a$ e $b$. Claro que só temos que mostrar o último item e, para fazer isto, tomamos um inteiro $c$ tal que $c \mid a$ e $c \mid b$. Pelo item $(iii)$ acima, temos $c \mid d$ e, assim, existe $c \in \mathbb{Z}$ tal que $d = cq = |c||q|$, pois $d > 0$. Logo, $c \leq |c| \leq d$, como queríamos mostrar.

■

**Proposição 1.12** *Sejam $a, b, c, d$ inteiros não-nulos. Então vale:*

*i) se* $a \mid bc$ *e* $mdc(a,b) = 1$, *então* $a \mid c$.

*ii) se* $mdc(a,c) = mdc(b,c) = 1$, *então* $mdc(ab,c) = 1$.

*iii) se* $mdc(a,b) = d$ *então,* $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

*iv) se* $a \mid c$ *e* $b \mid c$, *então* $\left.\frac{ab}{mdc(a,b)}\right| c$.

*v) se* $a \mid c$, $b \mid c$ *e* $mdc(a,b) = 1$, *então* $ab \mid c$.

**Proposição 1.13** *Sejam $a$ e $b$ inteiros positivos não simultaneamente nulos, com decomposição em fatores primos dadas por*

$$a = p_1^{m_1} \dots p_s^{m_s} q_1^{k_1} \dots q_t^{k_t},$$

$$b = p_1^{n_1} \dots p_s^{n_s} r_1^{l_1} \dots r_t^{l_u},$$

*em que os primos $p_i$, $q_j$, $r_k$ são todos distintos ($i \in \{1, \dots, s\}, j \in \{1, \dots, t\}$ e $k \in \{1, \dots, u\}$) e todos os expoentes são positivos. Então*

$$mdc(a, b) = p_1^{x_1} \dots p_s^{x_s},$$

*em que $x_i = min\{m_i, n_i\}$, para $i = 1, \dots, s$.*

**Demonstração:**

Seja $d = p_1^{x_1} \dots p_s^{x_s}$.
Vamos mostrar que $d$ satisfaz as seguintes condições:

i) Claramente $d > 0$.

ii) Como $x_i \leq m_i$ e $x_i \leq n_i$ (para $i = 1, \dots, s$), temos que

$$a = a_1 d, \quad em\ que \quad a_1 = p_1^{m_1 - x_1} \dots p_s^{m_s - x_s} q_1^{k_1} \dots q_t^{k_t}$$

e

$$b = b_1 d, \quad em\ que \quad b_1 = p_1^{n_1 - x_1} \dots p_s^{n_s - x_s} r_1^{l_1} \dots r_t^{l_u},$$

mostrando que $d \mid a$ e $d \mid b$.

iii) Se $c \mid a$ e $c \mid b$ temos, pelo Teorema Fundamental da Aritmética, que $c$ pode ser escrito como

$$c = p_1^{e_1} \dots p_s^{e_s}$$

em que $0 \leq e_i \leq min\{m_i, n_i\}$, *para* $i = 1, \dots, s$. Como $e_i \leq x_i$ (para $i = 1, \dots, s$), temos que

$$d = p_1^{x_1} \dots p_s^{x_s} = (p_1^{e_1} \dots p_s^{e_s})(p_1^{x_1 - e_1} \dots p_s^{x_s - e_s}) = c(p_1^{x_1 - e_1} \dots p_s^{x_s - e_s}).$$

ou seja, $c \mid d$. Isso conclui a demonstração.

■

### 1.1.3 Classes Residuais de Inteiros

Iremos agora estudar as classes residuais de $\mathbb{Z}$ módulo um inteiro $m > 1$. A primeira observação a ser feita é que

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$$

e que, se $i, j = 0, \ldots, m-1$ com $i \neq j$, então $[i] \neq [j]$.

De fato, dado $a \in \mathbb{Z}$, pelo algoritmo da divisão euclidiana, temos que existem inteiros $q$ e $r$ univocamente determinados pelas condições $a = mq + r$ e $0 \leq r \leq m-1$. Portanto, há um único inteiro $r$ com $0 \leq r \leq m-1$, tal que $[a] = [r]$.
Logo, $\mathbb{Z}_m$ é um anel finito com exatamente $m$ elementos.

**Exemplo 1.14** *Seja $m = 2$. Logo, $\mathbb{Z}_2 = \{[0], [1]\}$ com as operações*

| $+$ | $[0]$ | $[1]$ |
|---|---|---|
| $[0]$ | $[0]$ | $[1]$ |
| $[1]$ | $[1]$ | $[0]$ |

*e*

| $\cdot$ | $[0]$ | $[1]$ |
|---|---|---|
| $[0]$ | $[0]$ | $[0]$ |
| $[1]$ | $[0]$ | $[1]$ |

*é um anel. Como $[1]$ é o único elemento não nulo de $\mathbb{Z}_2$ e é invertível, segue que $\mathbb{Z}_2$ é um corpo. E observe ainda que, a menos de identificarmos $[0]$ com 0 e $[1]$ com 1, esse é o corpo de Galois que já apareceu no início deste capítulo.*

**Exemplo 1.15** *Seja $m = 3$. Considere $\mathbb{Z}_3 = \{[0], [1], [2]\}$ com adição e multiplicação dadas pelas tábuas*

| $+$ | $[0]$ | $[1]$ | $[2]$ |
|---|---|---|---|
| $[0]$ | $[0]$ | $[1]$ | $[2]$ |
| $[1]$ | $[1]$ | $[2]$ | $[0]$ |
| $[2]$ | $[2]$ | $[0]$ | $[1]$ |

*e*

| $\cdot$ | $[0]$ | $[1]$ | $[2]$ |
|---|---|---|---|
| $[0]$ | $[0]$ | $[0]$ | $[0]$ |
| $[1]$ | $[0]$ | $[1]$ | $[2]$ |
| $[2]$ | $[0]$ | $[2]$ | $[1]$ |

*Como $[1]$ e $[2]$ são invertíveis (com inversos respectivamente $[1]$ e $[2]$), temos que $\mathbb{Z}_3$ é um corpo.*

**Exemplo 1.16** *Seja $m = 4$. Considere $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ com adição e multiplicação dadas pelas tábuas abaixo*

| $+$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
|---|---|---|---|---|
| $[0]$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
| $[1]$ | $[1]$ | $[2]$ | $[3]$ | $[0]$ |
| $[2]$ | $[2]$ | $[3]$ | $[0]$ | $[1]$ |
| $[3]$ | $[3]$ | $[0]$ | $[1]$ | $[2]$ |

*e*

| $\cdot$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
|---|---|---|---|---|
| $[0]$ | $[0]$ | $[0]$ | $[0]$ | $[0]$ |
| $[1]$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
| $[2]$ | $[0]$ | $[2]$ | $[0]$ | $[2]$ |
| $[3]$ | $[0]$ | $[3]$ | $[2]$ | $[1]$ |

*Como $[2]$ não é invertível, temos que $\mathbb{Z}_4$ não é um corpo. Como $[2] \cdot [2] = [4] = [0]$, temos que esse anel não é um domínio de integridade.*

A fim de determinar quais são os $\mathbb{Z}^m$ que são corpos, vamos inicialmente caracterizar os elementos invertíveis desses anéis.

**Proposição 1.14** $[a] \in \mathbb{Z}_m$ *é* ***invertível*** *se, e somente se,* $mdc(a, m) = 1$.

**Demonstração:**

Suponhamos que $[a]$ seja invertível. Daí, existe $b \in \mathbb{Z}$ tal que $[a] \cdot [b] = [1]$. Logo, $[a \cdot b] = [1]$ e, portanto, $a \cdot b \equiv 1 \ mod \ m$. Isso implica que existe um inteiro $s$ tal que $a \cdot b + s \cdot m = 1$, que implica que $mdc(a, m) = 1$.

Reciprocamente, suponhamos que $mdc(a, m) = 1$. Logo, existem inteiros $b$ e $c$ tais que $b \cdot a + c \cdot m = 1$. Logo, $b \cdot a \equiv 1 \ mod \ m$. Daí, $[a] \cdot [b] = [a \cdot b] = 1$ e, portanto, $[a]$ é invertível. ■

Com a proposição acima temos um método para calcular o inverso de um elemento $[a]$ de $\mathbb{Z}_m$ quando o mesmo é invertível. De fato, pelo algoritmo de Euclides, determina-se o $mdc$ $d$ de $a$ e $m$, e inteiros $\lambda$ e $\mu$ tais que $d = \lambda \cdot a + \mu \cdot m$. O elemento $a$ é invertível se, e somente se, $d = 1$ e nesse caso, $[a]^{-1} = [\lambda]$.

**Teorema 1.5** *O anel* $\mathbb{Z}_m$ *é um corpo se, e somente se,* $m$ *é um número primo.*

**Demonstração:**

$\mathbb{Z}_m$ só é um corpo se, e somente se, todos os seus elementos $[1], [2], \ldots, [m-1]$ são invertíveis e equivale ao fato de que $mdc(1, m) = mdc(2, m) = \ldots = mdc(m-1, m) = 1$ e, portanto, isso é equivalente a $m$ ser primo.

■

### 1.1.4 Corpos Finitos

Sejam $A$ e $B$ dois anéis (ou corpos). Uma função $f : A \longrightarrow B$ será chamada **homomorfismo** se, para todos os elementos $a$ e $b$ em $A$, vale que

(i) $f(a + b) = f(a) + f(b)$,

(ii) $f(a \cdot b) = f(a) \cdot f(b)$,

(iii) $f(1) = 1$.

**Proposição 1.15** *Seja* $f : A \longrightarrow B$ *um homomorfismo entre os anéis* $A$ *e* $B$ *e sejam* $a, b \in A$. *Temos que*

*i)* $f(0) = 0$.

*ii)* $f(-a) = -f(a)$.

*iii)* $f(a-b) = f(a) - f(b)$.

*iv) Se* $a \in A$ *é invertível, então* $f(a)$ *é invertível e* $f(a^{-1}) = (f(a))^{-1}$.

*v) Se* $f$ *é bijetora, então a função* $f^{-1}$*, inversa de* $f$*, é um homomorfismo.*

*vi) Se* $A$ *e* $B$ *são corpos, então a função* $f$ *é injetora e* $f(A)$ *é um subcorpo de* $B$.

**Demonstração:**

i) Note que $f(0) = f(0+0) = f(0) + f(0)$, subtraindo $f(0)$ em ambos os lados da igualdade teremos que $0 = f(0)$.

ii) Note que $0 = f(0) = f(a+(-a)) = f(a) + f(-a)$, somando $-f(a)$ em ambos os lados da igualdade teremos que $-f(a) = f(-a)$.

iii) Note que $0 = f(0) = f((a-b)+(-a+b)) = f(a-b)+f(-a+b) = f(a-b)-f(a)+f(b)$, somando $f(a)-f(b)$ em ambos os lados da igualdade teremos que $f(a-b) = f(a)-f(b)$.

iv) Se $a$ é invertível, temos que $(f(a))^{-1} = f(a^{-1})$, pois $1 = f(1) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$.

v) Se $f$ é um homomorfismo bijetor, segue que $f^{-1}(1) = 1$, pois, $f(1) = 1$, por definição. Sejam $c, d \in B$, $a = f^{-1}(c)$ e $b = f^{-1}(d)$, temos que

$$f^{-1}(c+d) = f^{-1}(f(a) + f(b)) = f^{-1}(f(a+b)) = a + b = f^{-1}(c) + f^{-1}(d),$$

e

$$f^{-1}(c \cdot d) = f^{-1}(f(a) \cdot f(b)) = f^{-1}(f(a \cdot b)) = a \cdot b = f^{-1}(c) \cdot f^{-1}(d).$$

vi) Suponhamos que $A$ e $B$ sejam corpos. Se $f(a) = f(b)$, por (iii), segue que $f(a-b) = f(a)-f(b) = 0$. Se $a \neq b$, então $a-b$ seria invertível. Por (iv), $f(a-b)$ seria invertível, e portanto, não nulo, o que seria um absurdo. Consequentemente, $a = b$ e, portanto, $f$ é injetora.

Para provar que $f(A)$ é um subcorpo de $B$, temos que mostrar apenas que, se $\alpha, \beta \in f(A)$ com $\beta \neq 0$, então $\alpha - \beta \in f(A)$ e $\frac{\alpha}{\beta} \in f(A)$. Daí, suponhamos então que $\alpha = f(a)$ e $\beta = f(b)$, temos que

$$\alpha - \beta = f(a) - f(b) = f(a-b) \in f(A),$$

e

$$\frac{\alpha}{\beta} = \frac{f(a)}{f(b)} = f(a \cdot b^{-1}) \in f(A).$$

■

**Definição 1.11** *Um homomorfismo bijetor de corpos será chamado de* ***isomorfismo****. Dois corpos serão ditos* ***isomorfos*** *se existir um isomorfismo entre eles. Dois corpos isomorfos são considerados idênticos.*

*Seja $K$ um corpo finito com elemento unidade 1. Considere o conjunto*

$$\Lambda_K = \{n \in \mathbb{N};\ n1 = 0\} \subset \mathbb{N}.$$

*Pelo fato de $K$ ser finito, temos que existem dois inteiros $n_1 < n_2$ tais que $n_1 1 = n_2 1$. Logo, $(n_2 - n_1)1 = 0$ com $n_2 - n_1 > 0$ e, portanto, $\Lambda_K \neq \emptyset$.*

**Definição 1.12** *Define-se a* ***característica*** *de um corpo finito $K$, como sendo o inteiro positivo*

$$car(K) = min\Lambda_K = min\{n \in \mathbb{N};\ n1 = 0\}.$$

*Se um corpo $F$ é subcorpo de um corpo $K$, então $car(K) = car(F)$, pois $\Lambda_F = \Lambda_K$. Além disso, temos que $K$ é um espaço vetorial sobre $F$.*

**Proposição 1.16** *Seja $K$ um corpo finito, então $car(K)$ é um número primo.*

**Demonstração:**

Seja $m = car(K)$ e suponhamos que $m$ não seja primo. Logo, $m = m_1 \cdot m_2$, onde $m_1$ e $m_2$ são inteiros maiores do que 1 e menores do que $m$. Logo

$$0 = m1 = (m_1 \cdot m_2)1 = m_1(m_2 1) = (m_1 1) \cdot (m_2 1).$$

Como $K$ é um domínio, temos que $m_1 1 = 0$ ou $m_2 1 = 0$, o que condradiz a minimalidade de $m$.

■

**Proposição 1.17** *Seja $K$ um corpo finito com $car(K) = p$. Se para $m \in \mathbb{Z}$ e $a \in K$ tem-se $ma = 0$, então mé um múltiplo de $p$ ou $a = 0$.*

**Demonstração:**

Suponhamos que $ma = 0$, logo, $(m1) \cdot a = 0$. E sabemos que $K$ é um corpo, então temos que $m1 = 0$ ou $a = 0$. Agora basta mostrar que, se $m1 = 0$, então $m$ é um múltiplo de $p$. De fato, suponhamos que $m1 = 0$. Pelo algoritmo da divisão, temos que $m = \lambda p + r$, onde $0 \leq r < p$. Logo,

$$0 = m1 = (\lambda p + r)1 = \lambda(p1) + r1 = \lambda 0 + r1 = r1,$$

e como $p$ é o menor inteiro positivo tal que $p1 = 0$, segue que $r = 0$. Portanto, $m$ é múltiplo de $p$.

■

**Teorema 1.6** *Seja $K$ um corpo finito com $car(K) = p$, onde $p$ é um número primo. Então, $K$ contém um subcorpo isomorfo a $\mathbb{Z}_p$. Em particular, $K$ tem $p^n$ elementos para algum número natural $n$.*

**Demonstração:**

Iremos considerar a aplicação

$$\begin{array}{rccc} \varphi: & \mathbb{Z}_p & \longrightarrow & K \\ & [n] & \longmapsto & n1 \end{array}$$

Primeiramente, iremos mostrar que essa definição é bem posta. De fato, se $[n] = [m]$, onde $m$ e $n$ são dois inteiros, então existe um inteiro $\alpha$ tal que $n = m + \alpha p$. Logo,

$$n1 = (m + \alpha p)1 = m1 + (\alpha p)1 = m1 + \alpha(p1) = m1 + \alpha 0 = m1 + 0 = m1.$$

É imediato verificar que $\varphi$ é um homomorfismo. Logo, temos que $\varphi(\mathbb{Z}_p)$ é um subcorpo de $K$, isomorfo a $\mathbb{Z}_p$.

Portanto, temos que $K$ é um espaço vetorial sobre $\mathbb{Z}_p$ e como $K$ é finito, então tem dimensão finita sobre $\mathbb{Z}_p$. Daí, seja $\beta_1, \beta_2, \ldots, \beta_n$ uma base de $K$ sobre $\mathbb{Z}_p$. Então, todo elemento de $K$ se escreve de modo único na forma

$$\alpha_1\beta_1 + \alpha_2\beta_2 + \ldots + \alpha_n\beta_n,$$

com os $\alpha_i \in \mathbb{Z}_p,\ i = 1, 2, \ldots, n$. Contando esses elementos, segue que $|K| = p^n$.

■

## 1.2 Espaços Vetoriais

**Definição 1.13** *Sejam dados um corpo $K$, cujos elementos serão chamados de escalares, e um conjunto $V$, cujos elementos serão chamados de vetores. Diremos que $V$ é um **espaço vetorial** sobre $K$, ou um $K$-**espaço vetorial** se exitirem uma operação de adição em $V$*

$$\begin{array}{rccc} +: & V \text{ x } V & \longrightarrow & V \\ & (v, w) & \longmapsto & v + w \end{array}$$

e uma multiplicação dos elementos de $V$ por escalares,

$$\begin{array}{rccc} \cdot : & K \text{ x } V & \longrightarrow & V \\ & (\lambda, v) & \longmapsto & \lambda \cdot v \end{array} .$$

possuindo as seguintes propriedades:

1) A adição é associativa
$$(u + v) + w = u + (v + w).$$

2) A adição é comutativa
$$u + v = v + u.$$

3) Existência de elemento neutro: existe um elemento 0 em $V$ tal que
$$u + 0 = u.$$

4) Existência do elemento inverso: dado um elemento $u \in V$, existe um elemento $-u$, chamado simétrico de $u$, tal que
$$u + (-u) = 0.$$

5) Dados $\lambda, \mu \in K$ e $u \in V$, vale
$$(\lambda + \mu) \cdot u = \lambda \cdot u + \mu \cdot u.$$

6) Dados $\lambda \in K$ e $u, v \in V$, vale
$$\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v.$$

7) Dados $\lambda, \mu \in V$, vale
$$(\lambda \cdot \mu) \cdot u = \lambda \cdot (\mu \cdot u).$$

8) Para todo $u \in V$, $1 \cdot u = u$, onde 1 é a unidade de $K$.

Os exemplos mais comuns de espaços vetoriais são os $\mathbb{R}$-espaços vetoriais $\mathbb{R}^n$ e os $\mathbb{C}$-espaços vetoriais $\mathbb{C}^n$. Esses são casos particulares de uma classe mais geral de espaços vetoriais, a dos $K$-espaços vetoriais $K^n$, onde $K$ é um corpo arbitrário.
Denotaremos os elementos do tipo $\lambda \cdot v$ como $\lambda v$.

Um **subespaço vetorial** de um $K$-espaço vetorial $V$ é um subconjunto não vazio $W$ de $V$, que, com as operações de adição e multiplicação por escalares em $V$, é também um $K$-espaço vetorial.

Para que um subconjunto não vazio $W$ de um espaço vetorial V seja um subespaço vetorial, basta cumprir com a seguinte condição:

$$\forall u, v \in W,\ \forall \lambda \in K,\ u + \lambda v \in W.$$

Dizemos que $v_1, v_2, \ldots v_n \in V$ são **linearmente independentes**, se e somente se, toda vez em que houver uma relação do tipo

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n = 0,$$

com $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$, seguir que

$$\lambda_1 = \ldots = \lambda_n = 0.$$

Dizemos que $v_1, v_2, \ldots v_n \in V$ são **linearmente dependentes**, quando existem escalares $\lambda_1, \lambda_2, \ldots, \lambda_n$ que não sejam todos nulos tais que

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n = 0,$$

Iremos dizer que um subconjunto $B \subset V$ **gera** $V$ quando todo elemento de $V$ puder ser escrito da forma

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n,$$

com $v_1, v_2, \ldots, v_n \in B$ e $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$.

Além disso, quando os elementos de qualquer subconjunto finito de $B$ forem linearmente independentes sobre $K$ e $B$ gerar $V$, diremos que $B$ é uma **base** de $V$. Nos cursos de álgebra linear prova-se que todo espaço vetorial possui uma base e duas bases têm sempre o mesmo número de elementos. O número de elementos de uma base será chamado de **dimensão** de $V$ sobre $K$ e denotado por $dim_K V$.

Um espaço vetorial que possui uma base finita será dito de **dimensão finita**. Um conjunto de elementos linearmente independentes de um espaço vetorial de dimensão finita $V$ que tem o mesmo número de elementos de uma base é, ele mesmo, uma base de $V$.

Sejam $V$ e $W$ dois $K$-espaços vetoriais. Diremos que uma função $T : V \longrightarrow W$ é uma **transformação linear** quando for verificada a condição

$$\forall u, v \in V,\ \forall \lambda \in K,\ T(u + \lambda \cdot v) = T(u) + \lambda \cdot T(v).$$

Seja $T : V \longrightarrow W$ uma transformação linear. O **núcleo** de $T$ é o $K$-subespaço vetorial de $V$ definido por

$$KerT = \{v \in V;\ T(v) = 0\}.$$

A **imagem** de $T$ é o subespaço vetorial de $W$ definido por

$$ImT = \{T(v);\ v \in V\}.$$

Suponhamos que seja de conhecimento do leitor o **Teorema do Núcleo e da Imagem**, o qual afirma que, se $T : V \longrightarrow W$ é uma transformação linear entre espaços vetoriais de dimensão finita sobre um corpo $K$, então

$$dim_K KerT + dim_K ImT = dim_K V.$$

Uma transformação linear $T : V \longrightarrow W$ entre espaços vetoriais de dimensão finita possui uma representação matricial. Mais precisamente, dadas uma base $v_1, v_2, \ldots, v_n$ de $V$ e uma base $w_1, w_2, \ldots, w_m$ de $W$, temos que

$$T(v_i) = \lambda_{i1}w_1 + \lambda_{i2}w_2 + \ldots + \lambda_{im}w_m,\ i = 1, 2, \ldots, n.$$

Se $v = x_1v_1 + x_2v_2 + \ldots + x_nv_n$, então $(x_1, x_2, \ldots, x_n)$ são as **coordenadas** de $v$ na base $v_1, v_2, \ldots, v_n$. Segue que as coordenadas de $w = T(v)$, na base $w_1, w_2, \ldots, w_m$ de $W$, são dadas pelo produto matricial

$$(x_1, x_2, \ldots, x_n) \begin{pmatrix} \lambda_{11} & \lambda_{12} & \ldots & \lambda_{1m} \\ \lambda_{21} & \lambda_{22} & \ldots & \lambda_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_{n1} & \lambda_{n2} & \ldots & \lambda_{nm} \end{pmatrix}.$$

# CAPÍTULO 2

# CÓDIGOS CORRETORES DE ERROS

Muitas vezes na transmissão de dados ocorrem problemas, como interferências eletromagnéticas ou erros humanos (por exemplo, erros de digitação) que chamamos de ruído e que fazem com que a mensagem recebida seja diferente daquela que foi enviada. O objetivo da teoria é desenvolver métodos que permitam detectar e corrigir estes erros.

## 2.1 Códigos

Pode-se dizer que a construção de códigos inspira-se nos mais comuns códigos utilizados pelos seres humanos: os idiomas. Na língua portuguesa, por exemplo, usamos um alfabeto de 23 letras e as palavras nada mais são do que sequências de letras. É claro que a língua não é composta por todas as "palavras" possíveis formadas a partir das letras. Nós reconhecemos algumas delas como fazendo parte da língua e outras como alheias à língua. Se, por exemplo, ao escrevermos uma palavra, produzimos a sequência de letras "gadanhoto", como esta não é uma palavra da língua portuguesa, percebe-se imediatamente que houve um erro, e, nesse caso, a correção é possível, pois a palavra da língua portuguesa que mais se assemelha a "gadanhoto" é "gafanhoto".

**Exemplo 2.1** *Suponhamos que tenhamos um protótipo de um carro controlado via aparelho digital e que vá em quatro direções diferentes a saber: Frente, Direita, Esquerda e Trás. As quatro direções podem ser codificadas como elementos de* $\{0,1\} \times \{0,1\}$*, da seguinte forma:*

**Frente** - *00* **Direita** - *01* **Esquerda** - *10* **Trás** - *11*

*O código acima* $\{00, 01, 10, 11\}$ *é o que chamamos de* **código da fonte**. *Suponhamos que ao transmitirmos essa codificação o sinal no caminho sofra interferências. Por exemplo, a mensagem 00 foi recebida como 01, ou seja, ao invés do carro ir para FRENTE, ele vai para DIREITA. A teoria de Códigos Corretores de Erros trata de recodificar as palavras, de modo a introduzir redundâncias que permitam detectar e/ou corrigir erros como este. Assim, podemos modificar o código para:*

**Frente** - *00000* **Direita** - *01011* **Esquerda** - *10110* **Trás** - *11101*

*O novo código produzido na recodificação é chamado* **código de canal**. *Suponhamos que ao tentarmos transmitir a palavra 00000 tenhamos introduzido um erro e a mensagem recebida seja 00010. Como esta palavra não pertence ao código detectamos o erro e daí procuramos a palavra do código "mais próxima" da recebida, que é a palavra: 00000.*

| | | | | | | |
|---|---|---|---|---|---|---|
| Fonte | → | Codificador da fonte | → | Codificador de canal | ↓ | |
| Usuário | ← | Decodificador da fonte | ← | Decodificador de canal | | |

Os fatos, a seguir, servem como ilustração de aplicações importantes da Teoria dos Códigos.

A teoria dos códigos vem sendo utilizada com sucesso na nossa história recente. Em 1965, a nave espacial Mariner 4 enviou 22 fotos em preto e branco de Marte com 64 tons de cinza para cada um de seus 200 x 200 pontos, que é um elemento de $\{0,1\}^6$. A esses vetores não acrescentavam-se informaçõoes adicionais, pois a transmissão era muito lenta, demorando em torno de 8 horas para transmitir cada foto.

Em 1972, a nave espacial Mariner 9 transmitiu imagens de Marte com uma resolução de 700 x 832 pontos. Como a velocidade da transmissão era maior, o código foi recodificado através de uma função injetora $\varphi$ de $\{0,1\}^6$ em $\{0,1\}^{32}$ para acrescentar o código de canal que permite detectar e corrigir até sete erros. O dado recebido era corrigido e decodificado através de uma transformação $\varphi^{-1}$ , obtendo-se o elemento de $\{0,1\}^6$ que representa o tom de cinza correspondente. Esse código pertence à família de códigos chamados de Códigos de Reed-Muller.

Em 1979, a nave espacial Voyager transmitiu imagens coloridas de Júpiter. Cada elemento de imagem de uma cor foi representado por uma das 4096 $(= 2^{12})$ tonalidades. O codificador da fonte usava 12 bits binários e o codificador de canal usava 24 bits. Esse era chamado código de Golay que permitia corrigir até três erros.

## 2.2 Métrica de Hamming

A distância de Hamming é assim chamada em homenagem a Richard Hamming, que introduziu o conceito em um artigo fundamental sobre códigos de Hamming Error detecting and error correcting codes em 1950. Ela é utilizada, principalmente, para sinalizar erros na transmissão de palavras binárias de comprimento fixo entre um emissor e um receptor, e por isso é algumas vezes chamada de "distância do sinal". Esta forma de análise de bits é usada em várias disciplinas incluindo a teoria da informação, a teoria de códigos e a criptografia.

Primeiramente iremos considerar um conjunto finito $\mathbf{A}$ qualquer, que será chamado de **alfabeto**. A cardinalidade de $\mathbf{A}$ será denotada por $|\mathbf{A}| = q$ e os elementos deste conjunto serão chamados de **letras** ou **dígitos**. Uma **palavra** é uma sequência de elementos (letras ou dígitos) de $\mathbf{A}$ e o **comprimento** dessa palavra é o número de letras que a compõe.

Iremos considerar o conjunto $\mathbf{A}^n = \{(c_0,...,c_{n-1}) : c_i \in \mathbf{A},\ 0 \leq i \leq n-1\}$.

**Observação 2.1** *: Um código corretor de erros é um subconjunto próprio de $\mathbf{A}^n$, para algum número natural $n$.*

**Definição 2.1** *Dados dois elementos $x = (x_1, x_2, ..., x_n)$ e $y = (y_1, y_2, ..., y_n)$ de um espaço $\mathbf{A}^n$, chama-se distância de Hamming de $x$ a $y$ ao número de coordenadas em que estes elementos são diferentes, ou seja:*

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

**Exemplo 2.2** *Em $\{0,1\}^3$, temos*

$$d(001,111) = 2$$
$$d(000,111) = 3$$
$$d(100,110) = 1$$

**Proposição 2.1** *Dados $u, v, w \in \boldsymbol{A}^n$, valem as seguintes propriedades:*

i) Positividade: $d(u, v) \geq 0$, valendo a igualdade se, e somente se, $u = v$.

ii) Simetria: $d(u, v) = d(v, u)$.

iii) Desigualdade Triangular: $d(u, v) \leq d(u, w) + d(w, v)$.

**Demonstração:**

i) Pela definição $d(u,v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}| \geq 0$. Se $d(u,v) = 0$ temos que $u_i = v_i \ \forall \ i \ \in \{0,1,2,...,n\}$ portanto $u = v$. E se $u = v$, temos que $u_j = v_j$ para $1 \leq j \leq n$ e daí $d(u,v) = 0$.

ii) Já vem da definição, ao compararmos entrada por entrada de cada palavra, e sabemos que a igualdade é uma relação simétrica.

iii) Dados $u, v \in \mathbf{A}^n$ e sejam $u_i, v_i$ as $i$-ésimas coordenadas de $u$ e $v$. Daí temos dois casos:

1) Se $u_i = v_i$ nada acrescentaremos a $d(u,v)$ devido a essa coordenada (se $u_i = v_i$, $\forall i$ $d(u,v) = 0$ e isso ja foi provado). No entanto em $(d(u,w) + d(w,v))$ podemos ter o acréscimo de zero (se $u = v = w$) ou dois (se $u_i = v_i \neq w_i$).

2)Se $u_i \neq v_i$ não podemos ter $u_i = w_i$ e $w_i = v_i$, simultaneamente. Daí a contribuição das $i$-ésimas coordenadas a $(d(u,w) + d(w,v))$ é maior ou igual a 1, já que $u_i \neq w_i$ ou $v_i \neq w_i$.

■

**Definição 2.2** *Dados um elemento $a \in \mathbf{A}^n$ e um número real $t \geq 0$, definimos o* ***disco*** *e a* ***esfera*** *de centro em $a$ e raio $t$ como sendo os conjuntos:*

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

$$\text{Esfera: } S(a,t) = \{u \in \mathbf{A}^n \ ; \ d(u,a) = t\}$$

**Lema 2.1** *Para todo $a \in \mathbf{A}^n$ e todo número natural $r > 0$, temos que*

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

**Definição 2.3** *Seja $C$ um código. A* ***distância mínima*** *de $C$ é o número*

$$d = \min\{d(\mathbf{u},\mathbf{v}) \ ; \ \mathbf{u},\mathbf{v} \in C \text{ e } \mathbf{u} \neq \mathbf{v}\}.$$

Dado um código com distância mínima $d$, define-se

$$k = \left[ \ \frac{d-1}{2} \ \right],$$

onde $[t]$ representa a parte inteira de um número real $t$.

**Lema 2.2** *Seja $C$ um código com distância mínima $d$. Se $c$ e $c'$ são palavras distintas de $C$, então:*

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

**Demonstração:**
Suponha que $x \in D(c,k) \cap D(c',k)$.

$$\begin{aligned} x \in D(c,k) \cap D(c',k) \Rightarrow & x \in D(c,k) \Rightarrow d(x,c) \leq k \\ & x \in D(c',k) \Rightarrow d(x,c') \leq k \end{aligned}$$

$$\Rightarrow \qquad d(x,c) + d(x,c') \leq 2k \leq d-1. \qquad (\mathbf{1})$$

Mas pela desigualdade triangular $d(c,c') \leq d(x,c) + d(x,c')$. $\qquad (\mathbf{2})$

De $(\mathbf{1})$ e $(\mathbf{2})$, temos $d(c,c') \leq d-1$, mas $d(c,c') \geq d$, pois é a distância mínima do código. Daí temos uma contradição. Portanto, $D(c,k) \cap D(c',k) = \varnothing$

■

**Teorema 2.1** *Seja $C$ um código com distância mínima $d$. Então $C$ pode corrigir até $k = \left[ \ \frac{d-1}{2} \ \right]$ erros e detectar até $d-1$.*

**Demonstração:**

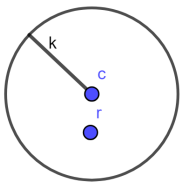
Suponha que ao transmitirmos uma palavra $c$ do código cometemos $t$ erros com $t \leq k$, recebendo uma palavra $r$, então $d(r,c) = t \leq k$. A distância de $r$ a qualquer outra palavra do código é maior do que $k$. Isso determina $c$ univocamente a partir de $r$, corrigindo a palavra recebida e substituindo-a por $c$. Por outro lado, dada uma palavra do código, podemos nela introduzir até $d-1$ erros sem encontrar outra palavra do código, e assim, a deteção do erro será possível. ■

**Definição 2.4** *Seja $C \subset \boldsymbol{A}^n$ um código com distância mínima $d$ e seja $k = \left[ \frac{d-1}{2} \right]$. O código $C$ será dito* ***perfeito*** *se*

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

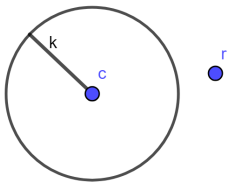
Quando se recebe uma palavra $r$, uma das seguintes situações é verificada:

- A palavra $r$ encontra-se num disco de raio $k$ em torno de uma palavra $c$ do código (palavra única).




  Como $c$ é uma palavra única, $r$ é substituído por $c$.

- A palavra $r$ não se encontra em nenhum disco de raio $k$ em torno de uma palavra $c$ do código. Não é possível decodificar $r$ com uma boa margem de segurança.




  Como $r$ está fora do disco, $r$ não pode ser substituído por $c$.

Existem 3 parâmetros fundamentais de um código $C \subset \mathbf{A}^n$.

- n: comprimento do código.
- M: o número de elementos.
- d: a distância mínima de $C$.

## 2.3 Equivalência de Códigos

**Definição 2.5** *Sejam $\boldsymbol{A}$ um conjunto finito e $n$ um número natural. Diremos que uma aplicação $F : \boldsymbol{A}^n \to \boldsymbol{A}^n$ é uma **isometria de Hamming**, ou uma **isometria** de $\boldsymbol{A}^n$, se preserva a distância de Hamming em $\boldsymbol{A}^n$. Em símbolos,*

$$d(F(x), F(y)) = d(x, y); \quad \forall\ x, y \in \boldsymbol{A}^n$$

Como $d(x, y) = 0$ se, e somente se $x = y$ é claro que uma isometria é injetora. E ainda, como toda aplicação injetora de um conjunto finito nele próprio é sobrejetora. Segue que toda isometria de $\mathbf{A}^n$ é uma aplicação bijetora.

A próxima proposição segue diretamente da definição de isometria.

**Proposição 2.2**

1. *A função identidade de $\boldsymbol{A}^n$ é uma isometria.*
2. *Se $F$ é uma isometria de $\boldsymbol{A}^n$, então $F^{-1}$ é uma isometria de $\boldsymbol{A}^n$.*
3. *Se $F$ e $G$ são isometrias de $\boldsymbol{A}^n$, então $F \circ G$ é uma isometria de $\boldsymbol{A}^n$.*

**Demonstração:**

1. $F : \mathbf{A}^n \to \mathbf{A}^n$ então $d(F(x), F(y)) = d(x, y)\ \forall\ x, y \in \mathbf{A}^n$, pois $F(x) = x$ e $F(y) = y$.
2. Se $F$ é uma isometria, exite $F^{-1}$ pois $F$ é sobrejetora. Como $F$ é uma isometria, segue que:

   $$d(F^{-1}(x), F^{-1}(y)) = d(F(F^{-1}(x)), F(F^{-1}(y))) = d(x, y)$$

   E por isso $F^{-1}$ é isometria.
3. Sejam $x, y \in \mathbf{A}^n$, usando que $F$ e $G$ são isometrias, vemos que:

   $$d(F(G(x)), F(G(y))) = d(G(x), G(y)) = d(x, y).$$

■

**Definição 2.6** *Dados dois códigos $C$ e $C'$ em $\boldsymbol{A}^n$, diremos que $C'$ é equivalente a $C$ se existir uma isometria $F$ de $\boldsymbol{A}^n$ tal que $F(C) = C'$.*

**Observação 2.2** *A equivalência de códigos é uma relação de equivalência, ou seja, possui as propriedades a seguir:*

- Reflexiva.
- Simétrica.
- Transitiva.

**Exemplo 2.3** *Se $f : A \to A$ é uma bijeção, e $i$ é um número inteiro tal que $1 \leq i \leq n$, a aplicação*

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

*é uma isometria.*

Vamos considerar, na distância de Hamming, apenas a contribuição da $i$-ésima coordenada das palavras de $\mathbf{A}^n$. Sejam $a = (a_1, ..., a_n), b = (b_1, ..., b_n) \in \mathbf{A}^n$, então

$$d(T_f^i(a_1, ..., a_i, ..., a_n), T_f^i(b_1, ..., b_i, ..., b_n)) = d((a_1, ..., f(a_i), ..., a_n), (b_1, ..., f(b_i), ..., b_n)) \ .$$

Se $a_i = b_i$, então a contribuição é nula para a distância entre as duas palavras, pois $f(a_i) = f(b_i)$, já que f é bijeção. Se $a_i \neq b_i$, então $f(a_i) \neq f(b_i)$ e teremos uma contribuição para a distância entre as palavras. Com isso, $d(a, b) = d(T_f^i(a), T_f^i(b))$ e $T_f^i$ é uma isometria.

**Exemplo 2.4** *Se $\pi$ é uma bijeção do conjunto $\{1, ..., n\}$ nele próprio, também chamada de permutação de $\{1, ..., n\}$, a aplicação permutação de coordenadas*

$$\begin{array}{rccc} T_\pi : & \boldsymbol{A}^n & \longrightarrow & \boldsymbol{A}^n \\ & (a_1, ..., a_n) & \longmapsto & (a_{\pi(1)}, ..., a_{\pi(n)}) \end{array}$$

*é uma isometria.*

Vamos considerar, na distância de Hamming, apenas a contribuição da $i$-ésima coordenada das palavras de $\mathbf{A}^n$. Sejam $a = (a_1, ..., a_n), b = (b_1, ..., b_n) \in \mathbf{A}^n$, então

$$d(T_\pi(a_1, ..., a_n), T_\pi(b_1, ..., b_n)) = d((a_{\pi(1)}, ..., a_{\pi(n)}), (b_{\pi(1)}, ..., b_{\pi(n)})) \ .$$

Se $a_i \neq b_i$, então a contribuição é nula para a distância entre as duas palavras, pois $a_{\pi(i)} \neq b_{\pi(i)}$, já que f é bijeção. Se $a_i = b_i$, então $a_{\pi(i)} = b_{\pi(i)}$ e teremos uma contribuição para a distância entre as palavras. Com isso, $d(a,b) = d(T_\pi(a), T_\pi(b))$ e $T_\pi$ é uma isometria.

**Teorema 2.2** *Seja $F : \boldsymbol{A}^n \to \boldsymbol{A}^n$ uma isometria, então existem uma permutação $\pi$ de $\{1,...,n\}$ e bijeções $f_i$ de $A$, $i = 1,...,n$, tais que*

$$F = T_\pi \circ T^1_{f1} \circ ... \circ T^n_{fn}$$

.

**Corolário 2.1** *Sejam $C$ e $C'$ dois códigos em $\boldsymbol{A}^n$. Temos que $C$ e $C'$ são equivalentes se, e somente se, existem uma permutação $\pi$ de $\{1,...,n\}$ e bijeções $f_1,...,f_n$ de $A$ tais que*

$$C' = \{(f_{\pi(1)}(x_{\pi(1)}),...,f_{\pi(n)}(x_{\pi(n)}));\ (x_1,...,x_n) \in C\}.$$

Portanto dois códigos de comprimento $n$ sobre um alfabeto $A$ (cujos elementos chamaremos de letras) são equivalentes se, e somente se, um pode ser obtido do outro mediante uma sequência de operações do tipo:

(i) Substituição das letras numa dada posição fixa em todas as palavras do código por meio de uma bijeção de $A$.

(ii) Permutação das posições das letras em todas as palavras do código, mediante uma permutação fixa de $\{1,...,n\}$.

## 2.4 Mudança de Alfabeto

É possível trocar o alfabeto de um código por outro alfabeto qualquer com o mesmo número de elementos sem alterar os parâmetros do código.

Sejam $A$ e $B$ dois conjuntos finitos e seja

$$f : A \longrightarrow B$$

uma bijeção. A partir de $f$, podemos definir a função

$$\begin{array}{rccc} \phi : & \mathbf{A}^n & \longrightarrow & \mathbf{B}^n \\ & (x_1,...,x_n) & \longmapsto & (f(x_1),...,f(x_n)). \end{array}$$

Essa função preserva as distâncias de Hamming e é bijetora.

Seja $C \subset \mathbf{A}^n$ um código com $M$ elementos e distância mínima $d$, a sua imagem $C' = \phi(C) \subset \mathbf{B}^n$ é um código sobre o alfabeto $B$ com parâmetros iguais aos de $C$. Assim, dado um código $C$ sobre um alfabeto qualquer $A$ com $m$ elementos, podemos, mediante uma bijeção dada $f : A \to \mathbb{Z}_m$, obter um código $C'$ sobre o anel $\mathbb{Z}_m$ com os mesmos parâmetros de $C$. Uma das vantagens disso é que temos mais estrutura sobre o alfabeto, o que nos permite usar mais ferramentas matemáticas. Em particular, se tem a noção de peso $\omega(u)$ de um elemento $u \in \mathbb{Z}_m$, definido como

$$\omega(u) = |\{i;\ u_i \neq 0\}|$$

ou seja, o número de coordenadas não nulas de $u$. E se o código $C'$ é fechado para a subtração, isto é, se

$$\forall\ u, v \in C', u - v \in C',$$

então vale a seguinte igualdade para a distância mínima $d$ de $C'$

$$d = min\{\omega(u);\ u \in C', u \neq 0\}.$$

# CAPÍTULO 3

# CÓDIGOS LINEARES

Na prática a classe de códigos mais utilizada é a classe dos Códigos Lineares. Assim, segue abaixo alguns resultados envolvendo essa importante classe de códigos.

Denotaremos por $K$ um corpo finito com $q$ elementos tomado como alfabeto. Da Álgebra Linear, sabemos que, para cada número natural $n$, $K^n$ é um $K$-espaço vetorial de dimensão $n$.

**Definição 3.1** *Um código $C \subset K^n$ será chamado de **código linear** se for um subespaço vetorial de $K^n$.*

Denotamos por $\mathbb{F}_n$ um corpo que possui $n$ elementos e por $\mathbb{F}_n^m$ o espaço vetorial sobre $\mathbb{F}_n$, onde cada elemento possui $m$ coordenadas.

Observemos que o Código do carro é um exemplo de código linear, onde o alfabeto $A = \mathbb{F}_2$ e o código é o subespaço vetorial de $\mathbb{F}_2^5$, imagem da transformação linear

$$\begin{array}{rccc} T & : & \mathbb{F}_2^2 & \longrightarrow & \mathbb{F}_2^5 \\ & & (x_1, x_2) & \longmapsto & (x_1, x_2, x_1, x_1 + x_2, x_2) \end{array}$$

Temos que todo código linear é por definição um espaço vetorial de dimensão finita. Seja $k$ a dimensão do código $C$ e seja $\mathbf{v}_1, \ldots, \mathbf{v}_k$ uma de suas bases. Portanto, todo elemento $\mathbf{v}$ de $C$ é combinação linear dos elementos da base de $C$, ou seja, existem únicos $\lambda_i \in K$, $i = 1, \ldots, k$, tais que

$$\mathbf{v} = \lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 + \ldots + \lambda_k \mathbf{v}_k.$$

Como para cada $\lambda_i \in K$, $i = 1, \ldots, k$ existem $q$ possibilidades, obtemos:

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

A partir disto, podemos, ao descrever o Código, citar apenas a sua dimensão.

Além disso, obtemos:

$$dim_K C = k = log_q q^k = log_q M.$$

Vimos que conhecendo a dimensão do código linear $C$, podemos obter o valor do parâmetro $M$. Assim, podemos determinar um código $q$-ário através dos parâmetros $n, k$ e $d$, ou seja, podemos definir o código como um $(n, k, d)$-código.

A seguir definimos peso de um código linear, e relacionamos com a definição de distância mínima.

**Definição 3.2** *Dado $\mathbf{x} \in K^n$, define-se o **peso** de $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ como sendo o número inteiro*

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

*Em outras palavras,temos que,*

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

*onde $d$ representa a métrica de Hamming.*

**Definição 3.3** *O **peso** de um código linear $C$ é o inteiro*

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

**Proposição 3.1** *Seja $C \subset K^n$ um código linear com distância mínima $d$. Temos que*

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

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

**Demonstração:**

O item i) segue imediatamente das definições da métrica de Hamming e da de peso de um código. O item ii) decorre do fato que, para todo par de elementos $\mathbf{x}, \mathbf{y}$ em $C$ com $\mathbf{x} \neq \mathbf{y}$, tem-se $\mathbf{z} = \mathbf{x} - \mathbf{y} \in C\ 0$ e $d(\mathbf{x}, \mathbf{y}) = \omega(\mathbf{z})$.

■

Note que a proposição acima nos mostra que, em códigos lineares com $M$ elementos, podemos calcular a distância mínima $d$ a partir de $M - 1$ cálculos de distâncias, em vez dos cálculos anteriormente requeridos. Na prática, em códigos grandes, esse método para o cálculo de $d$ é inviável por representar um custo computacional muito elevado, teremos,

portanto, que desenvolver outros métodos para determinar a distância mínima de um código.

Temos que a Proposição acima relaciona peso com distância a fim de encontrar a distância mínima de maneira mais eficiente. Com isso podemos chamar a distância mínima de um código $C$ como o **peso do código** C.

Em Álgebra Linear conhecemos essencialmente duas maneiras de descrever subespaços vetoriais $C$ de um espaço vetorial $K^n$, são elas: núcleo de uma transformação e imagem de uma transformação.

Vejamos como se obtém a representação de $C$ como imagem de uma transformação linear. Escolha uma base $\mathbf{v}_1, \ldots, \mathbf{v}_k$ de $C$ e considere a aplicação linear

$$\begin{array}{rccc} T & : & K^k & \longrightarrow & K^n \\ & & \mathbf{x} = (x_1, \ldots, x_k) & \longmapsto & (x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \ldots + x_k\mathbf{v}_k) \end{array}$$

Observemos que $T$ é uma transformação linear injetora,

$$Im(T) = C.$$

Portanto, dar um código $C \subset K^n$ de dimensão $k$ é equivalente a dar uma transformação linear injetora

$$T : K^k \longrightarrow K^n$$

e definir $C = Im(T)$. Essa é a forma paramétrica do subespaço $C$, pois os elementos de $C$ são parametrizados pelos elementos $\mathbf{x}$ de $K^k$ através de $T$, o que torna fácil gerar todos os elemento de $C$. Note que nessa representação é, porém, díficil decidir se um dado elemento $\mathbf{v}$ de $K^n$ pertence ou não a $C$, pois, para tal, é necessário resolver o sistema de $n$ equações nas $k$ incógnitas $x_1, \ldots, x_k$ abaixo

$$x_1\mathbf{v}_1, \ldots, x_k\mathbf{v}_k = \mathbf{v}.$$

Essa solução, em geral, representa um custo computacional muito elevado.

A outra maneira de descrevermos um código $C$ é através do núcleo de uma transformação linear. Sendo assim, tome um subespaço $C'$ de $K^n$ complementar de $C$, isto é,

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

e considere a aplicação linear

$$\begin{array}{rccc} H & : & C \oplus C' & \longrightarrow & K^{n-k} \\ & & \mathbf{u} \oplus \mathbf{v} & \longmapsto & \mathbf{v} \end{array}$$

cujo núcleo é precisamente $C$. Computacionalmente, é muito mais simples determinar se um certo elemento $\mathbf{v} \in K^n$ pertence ou não a $C$; para isto, basta verificar se $H(\mathbf{v})$ é ou não o vetor nulo de $K^{n-k}$, o que tem um custo bem pequeno.

**Exemplo 3.1** *Considere o corpo finito com três elementos* $\mathbb{F}_3 = \{0, 1, 2\}$ *e seja* $C \subset \mathbb{F}_3^4$ *o código gerado pelos vetores* $\mathbf{v_1} = \mathbf{1011}$ *e* $\mathbf{v_2} = \mathbf{0112}$. *Esse código possui* 9 $(= q^k = 3^2)$ *elementos, pois tem dimensão* 2 *sobre um corpo de 3 elementos. Uma respresentação paramétrica de* $C$ *é dada por*

$$x_1\mathbf{v_1} + x_2\mathbf{v_2}$$

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

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

**Definição 3.4** *Seja* $K$ *um corpo finito. Dois códigos lineares* $C$ *e* $C'$ *são* ***linearmente equivalentes*** *se existir uma isometria linear* $T : K^n \longrightarrow K^n$ *tal que* $T(C) = C'$.

Se $\pi$ é uma permutação de $\{1, \ldots n\}$, então $T_\pi$, é linear. Temos também que, se $f_i : K \longrightarrow K$, $i = 1, ..., n$ são bijeções, então $T_\pi \circ T^1_{f_1} \circ \ldots \circ T^n_{f_n}$ é linear se, e somente, se cada $f_i$ é linear. Sabemos também que uma função $f : K \longrightarrow K$ é linear se, e somente se, existe um elemento $c \in K$ tal que $f(x) = cx \quad \forall\, x \in K$.

Das observações acima segue que dois códigos lineares $C$ e $C'$ em $K^n$ são linearmente equivalentes se, e somente se, existem uma permutação $\pi$ de $\{1, \ldots, n\}$ e elementos $c_1, \ldots, c_n$ de $K$ $\{0\}$ tais que,

$$C' = \{(c_1 x_{\pi(1)}, \ldots, c_n x_{\pi(n)}) : (x_1, \ldots, x_n) \in C\}.$$

O resultado abaixo nos mostra como encontrar códigos lineares equivalentes.

Dois códigos lineares são linearmente equivalentes se, e somente se, cada um deles pode ser obtido do outro mediante uma sequência de operações do tipo:

i) Multiplicação dos elementos numa dada posição fixa por um escalar não nulo em todas as palavras.

ii) Permutação das posições de todas as palavras do código, mediante uma permutação fixa de $\{1, \ldots, n\}$.

## 3.1 Matriz Geradora de um Código

Sejam $K$ o corpo finito com $q$ elementos e $C \subset K^n$ um código linear. Chamaremos de *parâmetros do código linear* $C$ à terna de inteiros $(n, k, d)$ onde $k$ é a dimensão de $C$ sobre $K$, e $d$ representa a distância mínima de $C$, que é também igual ao peso de $\omega(C)$ do código $C$. Note que o número de elementos $M$ de $C$ é igual a $q^k$.
Seja $\beta = v_1, \ldots, v_k$ uma base ordenada de $C$ e considere a matriz $G$, cujas linhas são vetores $v_i = (v_{i1}, \ldots, v_{in})$, $i = 1, \ldots, k$, isto é,

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

A matriz $G$ é chamada de *matriz geradora* de $C$ associada à base $\beta$.
Considere a transformação linear definida por

$$\begin{array}{rccc} T & : & K^k & \longrightarrow & K^n \\ & & \mathrm{x} & \longmapsto & \mathrm{x}G \end{array}$$

Se $\mathrm{x} = (x_1, \ldots, x_k)$, temos que

$$T(\mathrm{x}) = \mathrm{x}G = x_1 v_1 + \ldots + x_k v_k,$$

logo $T(K^k) = C$. Podemos, então, considerar $K^k$ como sendo o código da fonte, $C$, o código de canal e a transformação $T$, uma codificação.
Note que a matriz $G$ não é univocamente determinada por $C$, pois ela depende da escolha da base $\beta$. Recorde, ainda, que uma base de um espaço vetorial pode ser obtidas uma outra qualquer através de sequências de operações do tipo:

- Permutação de dois elementos da base;
- Multiplicação de um elemento da base por ele mesmo somado a um múltiplo escalar de outro vetor da base;
- Substituição de um vetor da base por ele mesmo somado com um múltiplo escalar de outro vetor da base.

Então, a partir disso, temos que duas matrizes geradoras de um mesmo código $C$ podem ser obtidas uma da outra por um sequência de operações do tipo:

(L1) Permutação de duas linhas.

(L2) Multiplicação de uma linha por um escalar não nulo.

(L3) Adição de um múltiplo escalar de uma linha a outra.

De forma inversa podemos construir códigos a partir de matrizes geradoras $G$. Com isso, basta tomar uma matriz cujas linhas são l.i e definir um código sendo a imagem da transformação linear

$$\begin{array}{rccc} T & : & K^k & \longrightarrow & K^n \\ & & \mathrm{x} & \longmapsto & \mathrm{x}G \end{array}$$

**Exemplo 3.2** *Tome* $K = \mathbb{F}^2$ *e seja*

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

Considerando a transformação linear

$$\begin{array}{rccc} T & : & \mathbb{F}_2^3 & \longrightarrow & \mathbb{F}_2^5 \\ & & \mathrm{x} & \longmapsto & \mathrm{x}G \end{array}$$

obtemos um código $C$ em $\mathbb{F}_2^5$, imagem de $T$. A palavra 101 do código da fonte, por exemplo, é codificada como 01010.
Suponhamos agora que seja dada a palavra 10101 do código, e que queiramos decodificá-las, ou seja, achar a palavra x de $\mathbb{F}_2^3$ da qual ela se origina por meio de $T$. Teríamos, então, que resolver o sistema:

$$(x_1\ x_2\ x_3)G = (10101),$$

ou seja,

$$\begin{cases} x_1 + x_2 + x_3 &= 1 \\ x_2 + x_3 &= 0 \\ x_1 + x_3 &= 1 \\ x_2 + x_3 &= 0 \\ x_1 + x_3 &= 1 \end{cases}$$

cuja solução é $x_1 = 1$, $x_2 = 0$ e $x_3 = 0$.
Nesse sistema em particular foi fácil de resolver, mas dada uma matriz $G$ mais complexa, a resolução do sistema de equações associado pode ser bem trabalhoso.
No entanto, observamos que efetuando operações sobre as linhas de $G$ do tipo $(L1)$, $(L2)$ e $(L3)$, podemos colocar $G$ na forma

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

Note ainda que

$$\mathrm{x}G' = (x_1\ x_2\ x_3\ x_2\ x_3)$$

portanto, se obtém o vetor x tomando apenas as três primeiras componentes do vetor a ser decodificado. Logo, a palavra (10101) é facilmente decodificada como (101).

**Definição 3.5** *Diremos que uma matriz geradora $G$ de um código $C$ está na* ***forma padrão*** *se tivermos*

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

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

Dado um código $C$, nem sempre é possível achar uma matriz geradora de $C$ na forma padrão. Como, por exemplo, o código em $\mathbb{F}_2^5$ de matriz geradora

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

nunca poderá ter uma matriz geradora na forma padrão.
No entanto, efetuando também permutações das colunas de $G$, podemos obter a matriz

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

que é a matriz geradora na forma padrão de um código $C'$ equivalente a $C$.
De modo mais geral, efetuando também sequências de operações sobre a matriz geradora $G$ de um código linear $C$, do tipo:

(C1) permutação de duas colunas,

(C2) multiplicação de uma coluna por um escalar não nulo,

obtemos uma matriz $G'$ de um código $C'$ equivalente a $C$. (Observe que efetuar as operações acima numa base de $C$ implica efetuá-las em todas as palavras de $C$.)
Permitindo-se a utilização de operações do tipo (C1) acima, temos o seguinte resultado:

**Teorema 3.1** *Dado um código $C$, existe um código equivalente $C'$ com matriz geradora na forma padrão.*

**Demonstração:**

Seja $G$ uma matriz geradora de $C$. Mostraremos que com uma sequência de operações do tipo (L1), (L2), (L3) e (C1) podemos colocar $G$ na forma padrão.
Suponhamos

$$G = \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1n} \\ \vdots & \vdots & & \vdots \\ g_{k1} & g_{k2} & \dots & g_{kn} \end{pmatrix}.$$

Como a primeira linha de $G$ não é nula (os vetores linhas de $G$ são l.i.), por meio de (C1), podemos supor $g_{11} \neq 0$. Agora, multiplicando a primeira linha por $g_{11}^{-1}$, podemos colocar 1 no lugar de $g_{11}$ (operação (L2)).
Somando à segunda, terceira, etc. linhas, respectivamente, a primeira linha multiplicada respectivamente por $(-1)g_{21}$,$(-1)g_{31}$, etc. (operações (L3)), obtemos uma matriz

$$\begin{pmatrix} 1 & b_{12} & \dots & b_{1n} \\ 0 & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & b_{k2} & \dots & b_{kn} \end{pmatrix}.$$

Agora, na segunda linha dessa matriz, temos certamente um elemento não nulo que, por meio de uma operação (C1) pode ser colocado na segunda linha e segunda coluna. Multiplicando a segunda linha pelo inverso desse elemento, a matriz se transforma em

$$\begin{pmatrix} 1 & c_{12} & c_{13} & \dots & c_{1n} \\ 0 & 1 & c_{23} & \dots & c_{2n} \\ 0 & c_{32} & c_{33} & \dots & c_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & c_{k2} & c_{k3} & \dots & c_{kn} \end{pmatrix}.$$

Novamente, usando as operações (L3), obtemos a matriz

$$\begin{pmatrix} 1 & 0 & d_{13} & \dots & d_{1n} \\ 0 & 1 & d_{23} & \dots & d_{2n} \\ 0 & 0 & d_{33} & \dots & d_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & d_{k3} & \dots & d_{kn} \end{pmatrix},$$

e assim sucessivamente, até encontrarmos uma matriz na forma padrão

$$G' = (Id_k \mid A).$$

■

## 3.2 Códigos Duais

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

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

Essa operação possui as propriedades usuais de um produto interno, ou seja, é simétrica

$$\langle u, v\rangle = \langle v, u\rangle$$

e bilinear

$$\langle u + \lambda w, v\rangle = \langle u, v\rangle + \lambda\langle w, v\rangle$$

para todo $\lambda \in \mathbb{K}$.
Seja $C \subset K^n$ um código linear, define-se

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

**Lema 3.1** *Se $C \subset K^n$ é um código linear, com matriz geradora $G$, então*

*i) $C^{\perp}$ é um subespaço vetorial de $K^n$;*

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

**Demonstração:**

i) Sejam dados $u, v \in C^{\perp}$ e $\lambda \in K$. Temos, para todo $\mathrm{x} \in C$, que

$$\langle u + \lambda v, \mathrm{x}\rangle = \langle u, \mathrm{x}\rangle + \lambda\langle v, \mathrm{x}\rangle = 0,$$

e, portanto, $u + \lambda v \in C$, provando que $C^{\perp}$ é um subespaço vetorial de $K^n$.

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

■

O subespaço vetorial $C^{\perp}$ de $K^n$, ortogonal a $C$, é também um código linear que será chamado de **código dual** de $C$.

**Proposição 3.2** *Seja $C \subset K^n$ um código de dimensão $k$ com matriz geradora $G = (Id_k \mid A)$, na forma padrão. Então*

*i) $dim C^{\perp} = n - k$.*

*ii) ) $H = (-A^t | Id_{n-k})$ é uma matriz geradora de $C^{\perp}$.*

**Demonstração:**

i) Temos que x $= (x_1, \ldots, x_n)$ pertence a $C^\perp$ se, e somente se, $G\mathrm{x}^t = 0$. Como $G$ está na forma padrão, isto equivale a ter

$$\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = -A \begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix}$$

Portanto $C^\perp$ possui $q^{n-k}$ elementos, que são justamente as possíveis escolhas arbitrárias de $x_{k+1}, \ldots, x_n$. Logo, $C^\perp$ tem dimensão $n-k$.

ii) As linhas de $H$ são linearmente independentes (por causa do bloco $Id_{n-k}$), e portanto, geram um subespaço vetorial de dimensão $n-k$. Como as linhas de $H$ são ortogonais as linhas de $G$, isto é, $HG^t = 0$, temos que o espaço gerado pelas linhas de $H$ está contido em $C^\perp$; e como esses dois subespaços tem mesma dimensão, eles coincidem, provando assim que $H = (-A^t | Id_{n-k})$ é uma matriz geradora de $C^\perp$.

■

O próximo lema nos dirá como se relaciona a dualidade com a equivalência de códigos lineares.

**Lema 3.2** *Seja $C$ um código linear em $K^n$. Para toda permutação $\sigma$ de $1, \ldots, n$, para todo $c \in K^*$ e para todo $j = 1, \ldots, n$ temos que*

*i)* $(T_\sigma(C))^\perp = T_\sigma(C^\perp)$.

*ii)* $(T_c^j(C))^\perp = T_{c^{-1}}^j(C^\perp)$.

**Proposição 3.3** *Sejam $C$ e $D$ dois códigos lineares em $K^n$. Se $C$ e $D$ são linearmente equivalentes, então $C^\perp$ e $D^\perp$ são linearmente equivalentes.*

**Demonstração:**

Se $C$ e $D$ são linearmente equivalentes, segue que existe uma permutação $\sigma$ de $\{1, \ldots, n\}$ e elementos $c_1, \ldots, c_n \in K^*$ tais que

$$D = T_\sigma \circ T_{c_1}^1 \circ \ldots \circ T_{c_n}^n(C).$$

Daí, se segue o resultado, pois

$$D^\perp = (T_\sigma \circ T_{c_1}^1 \circ \ldots \circ T_{c_n}^n(C))^\perp = T_\sigma \circ T_{c_1^{-1}}^1 \circ \ldots \circ T_{c_n^{-1}}^n(C^\perp).$$

■

**Corolário 3.1** *Se $D$ é um código linear em $K^n$ de dimensão $k$, então $D^\perp$ é um código de dimensão $n-k$.*

**Demonstração:**

Temos que o código $D$ é equivalente a um código $C$, também de dimensão $k$, com matriz geradora na forma padrão e, portanto, segue que $dim C^\perp = n-k$. Daí, temos que $D^\perp$ é equivalente a $C^\perp$ e, portanto, também tem dimensão $n-k$.

■

**Lema 3.3** *Suponha que $C$ seja um código de dimensão $k$ em $K^n$ com matriz geradora $G$. Uma matriz $H$ de ordem $(n-k)\times n$, com coeficientes em $K$ e com linhas linearmente independentes, é uma matriz geradora de $C^\perp$ se, e somente se, $G.H^t = 0$.*

**Demonstração:**

As linhas de $H$ geram um subespaço vetorial de $K^n$ de dimensão $n-k$, portanto, igual a dimensão de $C^\perp$. Por outro lado, representando por $h_1, \ldots, h_{n-k}$ e por $g_1, \ldots, g_k$, respectivamente, as linhas de $H$ e de $G$, temos que

$$(G.H^t)i, j = \langle g_i, h_j \rangle.$$

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

$$(G.H^t) = 0 \Leftrightarrow C^\perp \textit{ gerado pelas linhas de } H.$$

■

**Corolário 3.2** $(C^\perp)^\perp = C$.

**Demonstração:**

Sejam $G$ e $H$ respectivamente matrizes geradoras de $C$ e $C^\perp$. Logo, $(G.H^t) = 0$. Tomando transpostas nessa última igualdade, temos que $H.G^t = 0$, logo, $G$ é matriz geradora de $(C^\perp)^\perp$, daí seguindo o resultado.

■

**Proposição 3.4** *Seja $C$ um código linear e suponhamos que $H$ seja uma matriz geradora de $C^\perp$. Temos então que*

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

**Demonstração:**
Temos que $v \in C$ se, e somente, $v \in (C^\perp)^\perp$ se, e somente se, $Hv^t = 0$. Com isso finalizamos a demonstração.

■

A Proposição acima nos permite caracterizar os elementos de um código $C$ por uma condição de anulamento. A matriz geradora $H$ de $C^{\perp}$ é chamada de **matriz teste de paridade** de C.

Observe que, para verificarmos se um elemento $v \in K^n$ pertence ou não a $C$ com matriz geradora $G$, basta verificar se

$$\mathrm{x}G = v,$$

admite solução. Em geral, é bastante custoso computacionalmente encontrar essa solução, pois esse sistema possui $n$ equações com $k$ incógnitas $\mathrm{x} = (x_1, \ldots, x_k)$.
Para evitar esse custo, trabalhamos com a matriz teste de paridade, pois a solução pode ser encontrada mais facilmente. Basta verificar se $Hv^t = 0$.
Dados um código $C$ com matriz teste de paridade $H$ e um vetor $\mathrm{v} \in K^n$ , chamamos o vetor $Hv^t$ de **síndrome** de $v$

**Exemplo 3.3** *Seja $C$ o código binário gerado pela matriz*

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

*e verifique se $v = (100110)$ e $v' = (010101)$, pertencem a $C$.*

*Para verificarmos se $v = (100110)$ e $v' = (010101)$, pertencem a $C$, precisamos encontrar a matriz teste de paridade, para isto, $G$ precisa estar na forma padrão.*
*Segue abaixo $G$ na forma padrão:*

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

*Logo, obtemos a matriz teste de paridade:*

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

*Agora verifiquemos se $v = (100110)$ e $v' = (010101)$, pertencem a $C$.*

$$Hv^t = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

*e*

$$Hv'^t = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

*Portanto* $v \in C$ *e* $v' \in C$

**Proposição 3.5** *Seja* $H$ *a matriz teste de paridade de um código* $C$*. Temos que o peso de* $C$ *é maior do que ou igual a* $s$ *se, e somente se, quaisquer* $s-1$ *colunas de* $H$ *são linearmente independentes.*

**Demonstração:**

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

$$0 = Hc^t = \sum c_i h^i.$$

Visto que $\omega(c)$ é o número de componentes não nulas de $c$, segue que se $\omega(c) \leq s-1$, teríamos uma combinação nula de um número $t$, com $1 \leq t \leq s-1$, de colunas de $H$, o que é contraditório. Logo, $\omega(C) \geq s$. Reciprocamente, suponhamos que $\omega(C) \geq s$. Suponhamos também, por absurdo, que $H$ tenha $s-1$ colunas linearmente dependentes, digamos $h^{i_1}, h^{i_2}, \ldots, h^{i_{s-1}}$. Logo, existiriam $c_{i_1}, \ldots, c_{i_{s-1}}$, no corpo, nem todos nulos, tais que

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

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

■

**Teorema 3.2** *Seja* $H$ *a matriz teste de paridade de um código* $C$*. Temos que o peso de* $C$ *é igual a* $s$ *se, e somente, quaisquer* $s-1$ *colunas de* $H$ *são linearmente independentes e existem* $s$ *colunas de* $H$ *linearmente dependentes.*

**Demonstração:**

De fato, suponhamos que $\omega(C) = s$, logo todo conjunto de $s-1$ colunas de $H$ é linearmente independente. Por outro lado, existem $s$ colunas de $H$ linearmente dependentes, pois, caso contrário, teríamos $\omega(C) \geq s+1$.
Reciprocamente, suponhamos que todo conjunto de $s-1$ vetores colunas de $H$ é linearmente independente e existem $s$ colunas linearmente dependentes. Logo, temos que $\omega(C) \geq s$. Mas $\omega(c)$ não pode ser maior do que $s$, pois, neste caso, teríamos que todo conjunto com $s$ colunas de $H$ é linearmente independente, o que é uma contradição.

■

**Corolário 3.3** *(Cota de Singleton). Os parâmetros $(n, d, k)$ de um código linear satisfazem à desigualdade*

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

**Demonstração:**

Se $H$ é uma matriz teste de paridade, ela tem posto $n - k$. Como, $d - 1$ é menor ou igual ao posto de $H$, segue a desigualdade.

■

Um código será chamado de **MDS (Maximum Distance Separable)** se valer a igualdade $d = n - k + 1$.

## 3.3 Decodificação

Chama-se decodificação ao procedimento de detecção e correção de erros num determinado código. O método geral de decodificação para códigos lineares que usaremos é um aperfeiçoamento de um método desenvolvido por $D$. Slepian do Laborátorio de Bell na década de 60. O método original Slepian tinha um custo computacional muito elevado e os aperfeiçoamentos tinham como objetivo reduzir esse custo.
Inicialmente, define-se o vetor erro $\mathbf{e}$ como sendo a diferença entre o vetor recebido $\mathbf{r}$ e o vetor transmitido $\mathbf{c}$, isto é,

$$\mathbf{e} = \mathbf{r} - \mathbf{c}.$$

Por exemplo, se, num dado código sobre $\mathbb{F}^2$, tenhamos transmitido a palavra (010011) e a palavra recebida tenha sido (101011) então

$$\mathbf{e} = (101011) - (010011) = (111000).$$

Note que o peso do vetor erro $\mathbf{e}$ corresponde ao número de erros cometidos numa palavra entre a transmissão e a recepção.
Seja $H$ a matriz teste de paridade do código. Como $H\mathbf{c}^t = 0$, temos que

$$H\mathbf{e}^t = H(\mathbf{r}^t - \mathbf{c}^t) = H\mathbf{r}^t - H\mathbf{c}^t = H\mathbf{r}^t.$$

Portanto a palavra recebida e o vetor erro tem a mesma síndrome. Denotemos por $h^i$ a i-ésima coluna de $H$. Se $\mathbf{e} = (\alpha_1 \dots \alpha_n)$, então

$$\sum_{i=1}^{n} \alpha_i h^i = H\mathbf{e}^t = H\mathbf{r}^t.$$

**Lema 3.4** *Seja $C$ um código linear em $K^n$ com capacidade de correção $k$. Se $\boldsymbol{r} \in K^n$ e $\boldsymbol{c} \in C$ são tais que $d(\boldsymbol{c}, \boldsymbol{r}) \leq k$, então existe um único vetor $\boldsymbol{e}$ com $\omega(\boldsymbol{e}) \leq k$, cuja síndrome é igual à síndrome de $\boldsymbol{r}$ e tal que $\boldsymbol{c} = \boldsymbol{r} - \boldsymbol{e}$.*

**Demonstração:**

De fato, $\mathbf{e} = \mathbf{r} - \mathbf{c}$ satisfaz a propriedade $\omega(\mathbf{e}) = \omega(\mathbf{r} - \mathbf{c}) = d(\mathbf{c}, \mathbf{r}) \leq k$ e temos que $\mathbf{e}$ possui a mesma síndrome de $\mathbf{r}$. Para provar a unicidade, suponhamos que $\mathbf{e} = (\alpha_1, \ldots, \alpha_n)$ e $\mathbf{e}' = (\alpha'_1, \ldots, \alpha'_n)$ sejam tais que $\omega(\mathbf{e}) \leq k$ e $\omega(\mathbf{e}') \leq k$ e tenham a mesma síndrome que $\mathbf{r}$. Então, se $H$ é uma matriz teste de paridade de $C$, temos

$$H\mathbf{e}^t = H\mathbf{e}'^t \Longrightarrow \sum_{i=1}^{n} \alpha_i h^i = \sum_{i=1}^{n} \alpha'_i h^i.$$

o que nos dá uma relação de dependência linear entre $2k(\leq d-1)$ colunas de $H$. Como quaisquer $d-1$ colunas de $H$ são linearmente independentes, temos que $\alpha_i = \alpha'_i$ para todo $i$, logo $\mathbf{e} = \mathbf{e}'$.

■

O problema que se coloca, então, é como determinar esse único vetor $\mathbf{e}$ a partir de $H\mathbf{r}^t$.

**Exemplo 3.4** *Determinação de $\boldsymbol{e}$ quando $\omega(\boldsymbol{e}) \leq 1$.*
*Suponhamos que o código $C$ tenha distância mínima $d \geq 3$ e que o vetor erro $\boldsymbol{e}$, introduzido entre a palavra transmitida $\boldsymbol{c}$ e a palavra recebida $\boldsymbol{r}$, seja tal que $\omega(\boldsymbol{e}) \leq 1$. Isto é, o canal introduziu no máximo um erro.*

*Se $H\boldsymbol{e}^t = 0$, então $\boldsymbol{r} \in C$ e se toma $\boldsymbol{c} = \boldsymbol{r}$.*

*Suponhamos $H\boldsymbol{e}^t \neq 0$. Então $\omega(\boldsymbol{e}) = 1$ e, portanto, $\boldsymbol{e}$ tem apenas uma coordenada não nula. Nesse caso, consideremos que $\boldsymbol{e} = (0, \ldots, \alpha, \ldots, 0)$ com $\alpha \neq 0$ na $i$-ésima posição. Logo,*

$$H\boldsymbol{e}^t = \alpha h^i,$$

*onde $h^i$ é a $i$-ésima coluna de $H$. Portanto, não conhecendo $\boldsymbol{e}$, mas conhecendo*

$$H\boldsymbol{e}^t = H\boldsymbol{r}^t = \alpha h^i,$$

*podemos determinar $\boldsymbol{e}$ como sendo o vetor com todas as componentes nulas exceto a $i$-ésima componente que é $\alpha$. Note que $i$ acima é bem determinado, pois $d \geq 3$.*

**Exemplo 3.5** *Seja $C$ o Código do carro. Esse código tem matriz teste de paridade*

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

*Seja* $\boldsymbol{r} = (10100)$ *uma palavra recebida, logo,*

$$H\boldsymbol{e}^t = H\boldsymbol{r}^t = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 1 \cdot h^4.$$

*Portanto,* $\boldsymbol{e} = (00010)$ *e, consequentemente,*

$$\boldsymbol{c} = \boldsymbol{r} - \boldsymbol{e} = (10110).$$

Com isso, estabelecemos um algoritmo de decodificação em códigos corretores de um erro.

Seja $H$ a matriz teste de paridade do código $C$ e seja $\mathbf{r}$ um vetor recebido. (Suponha $d \geq 3$).

i) Calcule $H\mathbf{r}^t$.

ii) Se $H\mathbf{r}^t = 0$, aceite $\mathbf{r}$ como sendo a palavra transmitida.

iii) Se $H\mathbf{r}^t = s^t \neq 0$, compare $s^t$ com as colunas de $H$.

iv) Se existirem $i$ e $\alpha$ tais que $s^t = \alpha h^i$, para $\alpha \in K$, então $\mathbf{e}$ é a n-upla com $\alpha$ na posição $i$ e zeros nas outras posições. Corrija $\mathbf{r}$ pondo $\mathbf{c} = \mathbf{r} - \mathbf{e}$.

v) Se o contrário de (iv) ocorrer, então mais de um erro foi cometido.

Esse algoritmo pode ser aplicado no caso dos códigos de Hamming como segue. Ordene os vetores colunas de $H_m$ do seguinte modo: se $\mathbf{v} \in \mathbb{F}_2^m \ \{0\}$. Logo, $\mathbf{v} = (v_1, \ldots, v_m)$ com $\mathbf{v}_i = 0, 1$, então coloque o vetor $\mathbf{v}$ em $H_m$ na coluna de ordem

$$i = v_1 + v_2 2^1 + v_3 2^2 + \ldots + v_m 2^{m-1}.$$

Note que, na condição (iv) em códigos binários, $\alpha$ é necessariamente igual a 1. Suponhamos, agora, que $H_m\mathbf{r}^t \neq 0$, logo $H_m\mathbf{r}^t = s^t$ é a coluna de $H_m$ de ordem

$$j = s_1 + s_2 2^1 + s_3 2^2 + \ldots + s_m 2^{m-1}$$

e, portanto, o vetor erro correspondente é:

$$\mathbf{e} = \mathbf{e}_j = (0, \ldots, 0, 1, 0, \ldots, 0)$$

com 1 na j-ésima componente.

**Exemplo 3.6** *No código de Hamming de ordem 3, tomemos a matriz teste de paridade*

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

*Se* $\boldsymbol{r} = (1010011)$*, então*

$$H_3 \boldsymbol{r}^t = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix},$$

*logo,* $j = 1 + 2 = 3$ *e, portanto,* $\boldsymbol{e} = (0010000)$ *e* $\boldsymbol{c} = (1000011)$.

Voltemos agora ao caso geral. Seja $C \subset K^n$ um código corretor de erros com matriz teste de paridade $H$. Sejam $d$ a distância mínima de $C$ e $k = [\frac{d-1}{2}]$. Recorde que $\mathbf{e}$ e $\mathbf{r}$ tem a mesma síndrome e, se $\omega(\mathbf{e}) = d(\mathbf{r}, \mathbf{c}) \leq k$, então $\mathbf{e}$ é univocamente determinado por $\mathbf{r}$.

Seja $\mathbf{v} \in K^n$. Defina

$$\mathbf{v} + C = \{\mathbf{v} + \mathbf{c} : \mathbf{c} \in C\}.$$

**Lema 3.5** *Os vetores* $\mathbf{u}$ *e* $\mathbf{v}$ *de* $K^n$ *tem a mesma síndrome se, e somente se,* $\mathbf{u} \in \mathbf{v} + C$

**Demonstração:**

$$H\mathbf{u}^t = H\mathbf{v}^t \Leftrightarrow H(\mathbf{u} - \mathbf{v})^t = 0 \Leftrightarrow \mathbf{u} - \mathbf{v} \in C \Leftrightarrow \mathbf{u} \in \mathbf{v} + C.$$

■

**Proposição 3.6** *Seja* $C$ *um* $(n, k)$*-código linear e* $\mathbf{v}, \mathbf{v}' \in K^n$*. Temos que*

*i)* $\mathbf{v} + C = \mathbf{v}' + C \Leftrightarrow \mathbf{v} - \mathbf{v}' \in C$.

*ii)* $(\mathbf{v} + C) \cap (\mathbf{v}' + C) \neq \emptyset \Longrightarrow \mathbf{v} + C = \mathbf{v}' + C$.

*iii)* $\cup_{\mathbf{v} \in \mathbf{K^n}} (\mathbf{v} + C) = K^n$.

*iv)* $|(\mathbf{v} + C)| = |C| = q^k$.

Cada conjunto da forma $\mathbf{v}+C$ é chamada de **classe lateral** de $\mathbf{v}$ segundo $C$. Note que

$$\mathbf{v}+C=C \Leftrightarrow \mathbf{v}\in C.$$

Segue imediatamente de (ii)-(iv) acima que o número de classes laterias segundo $C$ é

$$\frac{q^n}{q^k}=q^{n-k}.$$

**Exemplo 3.7** *Seja $C$ o $(4,2)$-código gerado sobre $\mathbb{F}_2$ pela matriz*

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

*Logo,*

$$C=\{0000,1011,0101,1110\},$$

*e as classes laterais segundo $C$ são*

$$\begin{aligned}0000+C&=\{0000,1011,0101,1110\}\\1000+C&=\{1000,0011,1101,0110\}\\0100+C&=\{0100,1111,0001,1010\}\\0010+C&=\{0010,1001,0111,1100\}\end{aligned}$$

*Note que temos uma correspondência 1 a 1 entre classes laterais e síndromes. Todos os elementos de uma classe lateral tem a mesma síndrome, e elementos de classes laterais distintas possuem síndromes distintas.*

**Definição 3.6** *Um vetor de peso mínimo numa classe lateral é chamado de* ***elemento líder*** *dessa classe.*

*No código do exemplo acima, temos que:* $0000$ *é líder de* $C$, $1000$ *é líder de* $1000+C$, $0100$ *e* $0001$ *são líderes de* $0100+C$, *e* $0010$ *é líder de* $0010+C$.
*Segue abaixo uma proposição de suma importância, pois irá nos ajudar quando formos decodificar uma mensagem.*

**Proposição 3.7** *Seja $C$ um código linear em $K^n$ com distância mínima $d$. Se $\mathbf{u}\in K^n$ é tal que*

$$\omega(\mathbf{u})\leq\left[\tfrac{d-1}{2}\right]=k,$$

*então $\mathbf{u}$ é o único elemento líder de sua classe.*

**Demonstração:**

Suponhamos que $\mathbf{u}$, $\mathbf{v} \in K^n$ com $\omega(\mathbf{u}) \leq [\frac{d-1}{2}]$ e $\omega(\mathbf{v}) \leq [\frac{d-1}{2}]$.

Se $\mathbf{u} - \mathbf{v} \in C$, então

$$(\mathbf{u} - \mathbf{v}) \leq \omega(\mathbf{u}) + \omega(\mathbf{v}) \leq \left[\frac{d-1}{2}\right] + \left[\frac{d-1}{2}\right] \leq d - 1$$

logo, $\mathbf{u} - \mathbf{v} = 0$ e, portanto, $\mathbf{u} = \mathbf{v}$.

■

Para achar líderes de classes, tomamos os elementos $\mathbf{u}$ tais que $\omega(\mathbf{u}) \leq [\frac{d-1}{2}]$. Cada um desses elementos é líder de uma e somente uma classe. Esses líderes são todos aqueles de peso $\leq [\frac{d-1}{2}]$.

Vamos agora discutir um algoritmo de correção de mensagens que tenham sofrido um número de erros menor ou igual à capacidade de correção do código, que é $k = [\frac{d-1}{2}]$.

**Preparação**: Determine todos os elementos $\mathbf{u} \in K^n$, tal que $\omega(\mathbf{u}) \leq k$. Em seguida, calcule as síndromes desses elementos e coloque esse dados numa tabela. Seja $\mathbf{r}$ uma palavra recebida. Aplique o seguinte Algoritmo de Decodificação:

**O Algoritmo de Decodificação**

(1) Calcule a síndrome $s^t = H\mathbf{r}^t$.

(2) Se $s$ está na tabela, seja $l$ o elemento líder da classe determinada por $s$; troque $\mathbf{r}$ por $\mathbf{r} - l$.

(3) Se $s$ não está na tabela, então na mensagem recebida foram cometidos mais do que $k$ erros.

**Justificativa**: Dado $\mathbf{r}$, sejam $\mathbf{c}$ e $\mathbf{e}$, respectivamente, a mensagem transmitida e o vetor erro. Como $H\mathbf{e}^t = H\mathbf{r}^t$, temos que a classe lateral onde e se encontra está determinada pela síndrome de $\mathbf{r}$. Se $\omega(\mathbf{e}) \leq k$, temos que $\mathbf{e}$ é o único elemento líder $l$ de sua classe e, portanto, é conhecido e se encontra na tabela. Consequentemente, $\mathbf{c} = \mathbf{r} - \mathbf{e} = \mathbf{r} - l$ é determinado.

**Exemplo 3.8** *Considere o* $(6, 3)$*-código linear definido sobre* $\mathbb{F}_2$ *com matriz teste de paridade*

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

*Nesse caso* $d = 3$ *e, portanto,* $k = [\frac{d-1}{2}] = 1$.

*Os vetores de peso* $\leq 1$ *com as suas respectivas síndromes estão relacionados na tabela abaixo:*

| *líder* | *síndrome* |
|---|---|
| *000000* | *000* |
| *000001* | *101* |
| *000010* | *011* |
| *000100* | *110* |
| *001000* | *001* |
| *010000* | *010* |
| *100000* | *100* |

*Suponhamos, agora, que a palavra recebida seja*

(*a*) $\boldsymbol{r} = (100011)$. *Neste caso,* $H\boldsymbol{r}^t = (010)^t$ *e, portanto,* $\boldsymbol{e} = (010000)$. *Consequentemente,* $\boldsymbol{c} = \boldsymbol{r} - \boldsymbol{e} = (110011)$.

(*b*) $\boldsymbol{r} = (111111)$. *Neste caso,* $H\boldsymbol{r}^t = (111)^t$, *que não se encontra na tabela. Sendo assim, foi cometido mais do que* 1 *erro na mensagem* $\boldsymbol{r}$.

# REFERÊNCIAS BIBLIOGRÁFICAS


[1] A. Hefez e M. L. T. Vilela, *Códigos Corretores de Erros*. Rio de Janeiro, IMPA, 2002.

[2] A. Vidigal, D. Avritzer, et al., *Fundamentos de Álgebra*. Editora UFMG, 2005.

[3] F. U. Coelho, e M. L. Lourenço, *Um Curso de Álgebra Linear*. 2ª edição. São Paulo: Ed USP, 2005.3.