
Goiânia, 07 a 10 de outubro

**Mini Curso**

# Códigos Corretores de Erros

Prof. Dr. Mário José de Souza - IME/UFG

# CÓDIGOS CORRETORES DE ERROS

SOUZA,M.J.

## 1. Introdução

Existem várias maneiras de ocorrência dos corretores de erros em nosso dia-a-dia. Por exemplo, quando assistimos televisão, falamos ao telefone, ouvimos a gravação musical em um CD, ou simplesmente navegando pela INTERNET. Um código corretor de erros é, basicamente, uma forma organizada de acrescentar algum dado a cada informação que precise ser transmitida ou armazenada, de modo que permita, ao recuperar a informação, detectar e corrigir os erros no processo de transmissão da informação. A teoria dos códigos é um campo de pesquisa atual, muito atraente, tanto do ponto de vista científico quanto tecnológico. A teoria dos códigos mistura conceitos e técnicas importantes da Álgebra abstrata com aplicações imediatas da cotidiano, mostrando que sofisticação tecnológica torna cada vez mais imperceptível a relação entre a chamada matemática pura e a matemática aplicada. Este minicurso tem por objetivo apresentar e desenvolver os fundamentos matemáticos dessa teoria. Como trata-se de um assunto com várias ramificações dentro da matemática, nos ocuparemos com aspectos de natureza algébrica.

## 2. Códigos Corretores de Erros

Todo canal corrompe o sinal transmitido, devido ao ruído inerente. Isto faz com que ocorram erros e, assim, a mensagem originalmente transmitida não pode ser reconstruída no receptor. Para tanto, o codificador de canal faz a adição controlada de redundância, para que a mesma possa ser explorada no decodificador de canal, a fim de corrigir erros, se possível. As técnicas de correção de erros podem ser classificadas em dois grupos: FEC (Forward Error Correction), onde se utilizam códigos corretores de erro para fazer a correção no receptor (daí o forward), e ARQ (Automatic Repeat reQuest), que, na ocorrência de um erro, detectado por um código detetor de erro, emite um pedido de retransmissão da mensagem, ou de parte dela. O melhor desempenho do sistema é atingido utilizando-se ambas as técnicas. Caso não houvesse os códigos corretores de erro, o número de pedidos de retransmissão poderia ser alto, fazendo com que o vazão do sistema caísse demais. Com o uso de códigos corretores de erro, é possível fazer com que a taxa de erro caia a patamares pequenos, de tal forma que o número de retransmissões atinja um ponto aceitável. Contudo, podemos pensar em usar um código bem poderoso para que a taxa de erro caia a valores suficientemente baixos, de forma a tornar praticamente inexistentes os pedidos de retransmissão. Contudo, códigos poderosos exigem uma redundância elevada e, portanto, a taxa de transmissão de dados cai excessivamente. Assim, existe um compromisso entre correção de erro e taxa de retransmissão. No presente capítulo, temos a intenção de fazer uma breve introdução à Teoria de Codificação de Canal, que é uma vasta área de intensa pesquisa e desenvolvimento de técnicas

que objetivam adicionar o mínimo de redundância e obter o máximo de proteção contra erros, buscando ficar dentro de certos limites de recursos computacionais no processo de decodificação. Os códigos corretores de erro podem ser divididos em dois grandes grupos: códigos de bloco e códigos convolucionais. Dentro de cada grupo existe uma vastidão de tipos de códigos, para as mais diversas situações.

2.1. **Códigos de Bloco.** Os códigos de bloco operam sobre sistemas algébricos chamados corpos algé-
bricos. Simplificadamente, um corpo é um conjunto de elementos nos quais podem-se realizar as operações de adição, subtração, multiplicação e divisão sem sair do conjunto. A adição e a multiplicação devem satisfazer as propriedades comutativa, associativa e distributiva. Quando assumimos um conjunto de números inteiros 0,1,2,...,p-1, onde p é um número primo, e usamos as operações de adição módulo-p e multiplicação módulo-p, obtemos um conjunto que obedece às condições para ser um corpo, ao qual se dá o nome de corpo primo, ou Galois Field (GF), em homenagem ao seu descobridor. Este corpo é representado por GF(p) e pode ser estendido, sendo sua extensão denominada de GF($p^m$), onde m é um número natural. Nos sistemas de comunicação e armazenamento de dados, os corpos GF($2^m$) são amplamente usados. Todas as operações sobre os códigos são feitos sobre GF.

A codificação é feita utilizando-se uma matriz G de um código C(n,k). Essa matriz possui dimensão k x n, com k linhas independentes.

2.2. **Códigos Convolucionais.** Os códigos convolucionais foram introduzidos primeiramente por Elias [3] em 1955 como uma alternativa aos códigos de bloco. Em 1961, Wozencraft [11] propõe o processo de decodificação diferencial como uma forma eficaz de se fazer a decodificação. Dois anos depois, Massey em 1963 propõe uma técnica chamada de decodificação por limiar, que é menos eficiente mas mais simples. Isto tornou possível a implementação prática destes códigos em sistemas de comunicação com e sem fio. Então em 1967, Viterbi [10] propõe um esquema de decodificação por seqüência de máxima verossimilhança, também conhecido por decodificação de Viterbi, que tinha uma implementação relativamente simples para códigos com pouca memória. Essa técnica, juntamente com uma versão aprimorada do processo de decodificação diferencial, fez com que os códigos convolucionais fossem utilizados em sistemas de comunicação via satélite e comunicação de espaço profundo já no começo da década de 70. Os códigos convolucionais costumam ser mais comuns que os códigos de bloco, por terem implementação mais simples. Seu desempenho é igual, quando não é maior, ao dos bons códigos de bloco. Tal desempenho é atribuído usualmente à possibilidade de implementação prática do processo de decodificação suave, que também existe para códigos de bloco, mas tem altíssimo custo computacional. O processo de codificação é feito por meio de deslocadores de registro, que também é utilizado em códigos de bloco (códigos cíclicos). Além disso, com auxílio do método de puncionamento [1], que consiste em se excluir periodicamente algumas saídas do equalizador, a fim de aumentar a taxa do codificador, é possível utilizar um mesmo decodificador para trabalhar com diferentes taxas. É claro que o aumento da taxa tem sua contrapartida pois, ao se excluir algumas saídas do codificador, perde-se em proteção contra erros. Da mesma forma que os códigos de bloco, os códigos convolucionais também possuem uma representação matricial.

## 3. Preliminares

Nesta secção são introduzidos os conceitos básicos da teoria de códigos e algumas propriedades são apresentadas. Um estudo mais detalhado pode ser encontrado em [6],[4]e[8].

Algumas notações:

· $\mathbb{F}_q$ denotará um corpo finito com $q$ elementos.

· $(\mathbb{F}_q)^n = \{\mathbf{x} = (x_1, x_2, ..., x_n) : x_i \in \mathbb{F}_q\}$

### 3.1. **ALFABETO.**

**Definição 3.1.** *Um alfabeto finito é simplesmente um conjunto finito* $\mathbb{F}_q$.

**Definição 3.2.** *Diremos que* $\mathbf{C}$ *é um código de comprimento* $n$ *(sobre* $\mathbb{F}_q$*) se* $\mathbf{C} \subset (\mathbb{F}_q)^n$.

**Observação 3.3.** *Assim,* $\mathbf{C}$ *é dito um código* $q-$*ário. Desse modo, tem-se códigos binários* $(q = 2)$*, ternário* $(q = 3)$*, etc.*

### 3.2. **DISTÂNCIA DE HAMMING.**

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

**Definição 3.4.** *A* ***distância de Hamming*** *entre* $\boldsymbol{x,y} \in (\mathbb{F}_q)^n$ *é dada por:* $d(\mathbf{x}, \mathbf{y}) = \#\{i : x_i \neq y_i\}$.

**Exemplo 3.5.** *Seja* $\mathbb{F}_2$ *e consideremos* $(\mathbb{F}_2)^3$.

$$d((0,0,1),(1,1,1)) = 2$$
$$d((0,0,0),(1,1,1)) = 3$$
$$d((1,0,0),(1,1,0)) = 1.$$

**Proposição 3.6.** *A distância de Hamming é uma métrica, ou seja:*

**(a):** $d(\mathbf{x}, \mathbf{y}) = 0 \Longleftrightarrow \boldsymbol{x=y}$;
**(b):** $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$, $\forall \boldsymbol{x,y} \in (\mathbb{F}_q)^n$;
**(c):** $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$, $\forall \boldsymbol{x,y,z} \in (\mathbb{F}_q)^n$

*Demonstração.* Exercício. □

**Definição 3.7.** *A* ***bola de centro a*** *e raio* $\boldsymbol{r}$ *é definida por* $B_{\mathbf{r}}(\mathbf{a}) = \{\mathbf{x} \in (\mathbb{F}_q)^n : d(\mathbf{x}, \mathbf{a}) \leq$

### 3.3. **Distância mínima de um código.**

**Definição 3.8.** *A distância mínima de um código* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *é*

$$d_{\min}(\mathbf{C}) = \min\{d(\mathbf{x}, \mathbf{x}') : \mathbf{x}, \mathbf{x}' \in C : \mathbf{x} \neq \mathbf{x}'\}$$

.

**Exemplo 3.9.**

*Seja* $\mathbf{C} = \{(0,0,0,0,0),(0,1,0,1,1),(1,0,1,1,0),(1,1,1,0,1)\} \subset (\mathbb{F}_2)^5$.

$\dim(\mathbf{C}) = 3$.

**Proposição 3.10.** *Seja* $\mathbf{C}$ *um código com distância mínima d. Se* $\boldsymbol{c}$ *e* $\boldsymbol{c'}$ *são palavras distintas de* $\mathbf{C}$*, então* $B_{\mathbf{t}}(\mathbf{c}) \cap B_{\mathbf{t}}(\mathbf{c\prime}) = \varnothing$*, em que* $t = \left[\frac{d-1}{2}\right]$.

**Observação 3.11.** $[*]$ : *parte inteira do número* $*$.

*Demonstração.* Exercício. □

**Teorema 3.12.** *Seja* $\mathbf{C}$ *um código com distância mínima d. Então* $\mathbf{C}$ *pode corrigir até* $t = \left[\frac{d-1}{2}\right]$ *erros. Se d é par, o código pode simultaneamente corrigir* $\frac{d-2}{2}$ *erros e detectar até* $\frac{d}{2}$ *erros.*

*Demonstração.* Exercício. □

**Definição 3.13.** *Seja* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *um código com distância mínima d e seja* $t = \left[\frac{d-1}{2}\right]$*. O código* $\mathbf{C}$ *será dito perfeito se* $\bigcup_{\mathbf{x}\in\mathbf{C}} \mathbf{B}_t(\mathbf{x}) = (\mathbb{F}_q)^n$.

**1.:** O código do **Exemplo 3.9** não é perfeito, pois trata-se de um código $\mathbf{C} \subset (\mathbb{F}_2)^5$ e $\bigcup_{\mathbf{c}\in\mathbf{C}} B_t(\mathbf{c}) \neq (\mathbb{F}_2)^5$

## 4. CÓDIGOS LINEARES

Na prática, a classe de códigos mais utilizada é a denominada classe dos códigos lineares.

**Definição 4.1.** *Um código* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *é chamado de código linear se for um subespaço vetorial de* $(\mathbb{F}_q)^n$.

**Notação 4.1.** *Assim,* $\mathbf{C}$ *é um espaço vetorial de dimensão finita. Sendo k a dimensão do código* $\mathbf{C}$*, todo elemento de* $\mathbf{C}$ *pode ser escrito de modo único da seguinte maneira:*$(*)$ $\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_k u_k, \alpha_i \in \mathbb{F}_q$, $i = 1, 2, ..., k$; *em que* $\{u_1, u_2, \cdots, u_k\}$ *é uma base de* $\mathbf{C}$*. Como* $\alpha_i \in \mathbb{F}_q$, $i = 1, 2, ..., k$; *existem q possibilidades para cada um dos* $\alpha_i$ *em* $(*)$*. Logo existem* $q^k$ *elementos em* $\mathbf{C}$*, isto é,* $M = |\mathbf{C}| = q^k$ *e consequentemente dim*$\mathbf{C} = k \log_q^q = \log_q^{q^k} = \log_q^M$.

**Definição 4.2.** *Dado u*$\in (\mathbb{F}_q)^n$*, o peso de u é o número inteiro:* $W(u) = \#\{i : u_i \neq 0\}$*. Ou seja, W(u)=d(u,o)=0, em que o é o vetor nulo de* $(\mathbb{F}_q)^n$.

**Definição 4.3.** *O peso de um código linear* $\mathbf{C}$*, é o inteiro*

$$W(\mathbf{C}) = min\{W(u) : u \in \mathbf{C} \subset (\mathbb{F}_q)^n\}$$

.

**Proposição 4.4.** *Dado um código linear* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *com distância mínima d, temos que:*

**(i):** $\forall u, v \in (\mathbb{F}_q)^n$, $d(u, v) = W(u - v)$
**(ii):** $d =$W($\mathbf{C}$).

**Notação 4.2.** *Em virtude desta proposição, a distância mínima de um código linear* $\mathbf{C}$ *será também chamada de peso do código* $\mathbf{C}$.

# 5. CONSTRUINDO CÓDIGOS LINEARES

É sabido, em Álgebra Linear, que existem duas maneiras de se escrever sub-espaços vetoriais $\mathbf{C}$ do espaço vetorial $(\mathbb{F}_q)^n$. Uma como imagem e a outra como núcleo de uma transforamação linear.

Obteremos a representação de $\mathbf{C}$ como imagem de uma imagem de uma transformação linear:

$$\begin{array}{rccc} T & : & (\mathbb{F}_q)^k & \longrightarrow & (\mathbb{F}_q)^n \\ & & \mathbf{x} & \longmapsto & \mathbf{u} \end{array}$$

em que $\mathbf{x} = (x_1, x_2, ..., x_n)$ e $\mathbf{u} = x_1u_1 + x_2u_2 + \cdots + x_ku_k$. $T$ é uma transformação linear injetora. Assim, dar um código $\mathbf{C} \subset (\mathbb{F}_q)^n$ de dimensão $k$ é equivalente a dar uma transformação linear injetora $T : (\mathbb{F}_q)^k \longrightarrow (\mathbb{F}_q)^n$ e definir $\mathbf{C} = \mathrm{Im}(\mathbf{T})$.

**Exemplo 5.1.** *Considere a 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*

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

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

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

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

## 5.1. **Matriz Geradora de um Código.**

**Definição 5.2.** *Dado um código linear* $\mathbf{C} \subset (\mathbb{F}_q)^n$, *chamaremos de parâmetros do código linear* $\mathbf{C}$ *os inteiros (n,k,d), em que k é a dimensão de* $\mathbf{C}$ *sobre* $\mathbb{F}_q$, *d representa a distância mínima de* $\mathbf{C}$ *e n é denominado o comprimento do código* $\mathbf{C}$.

Seja o código linear $\mathbf{C} = [\mathrm{u}_1, \mathbf{u}_2, ..., \mathbf{u}_k]$ com $B = \{\mathrm{u}_1, \mathbf{u}_2, ..., \mathbf{u}_k\}$ base de $\mathbf{C}$. A matriz

$$\mathbf{G}_{k\times n} = \begin{pmatrix} - & \mathrm{u}_1 & - \\ - & \mathbf{u}_2 & - \\ \vdots & \vdots & \vdots \\ - & \mathbf{u}_k & - \end{pmatrix}$$

é chamada de matriz geradora de $\mathbf{C}$ associada à base

$$B = \{\mathrm{u}_1, \mathbf{u}_2, ..., \mathbf{u}_k\}$$

.

**Exemplo 5.3.** *Do exemplo anterior* $B = \{(0, 1, 0, 1, 1)\,, (1, 0, 1, 1, 0)\}$ *é uma base de* $\mathbf{C}$ *e*

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

*é uma matriz geradora do código linear* $\mathbf{C}$. *De fato,*

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

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

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

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

De maneira geral, consideramos a transformação linear definida por

$$\begin{array}{rccc} T & : & (\mathbb{F}_q)^k & \longrightarrow & (\mathbb{F}_q)^n \\ & & \mathbf{x} & \longmapsto & \mathbf{xG} \end{array}$$

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

Além disso, ressaltamos que a matriz geradora $\mathbf{G}$ não é única, pois ela depende da base $B$. Portanto, mudando para uma base $\overline{B}$, teremos uma outra matriz geradora $\overline{\mathbf{G}}$ para o mesmo código $\mathbf{C}$. Da Álgebra Linear, sabemos que $\overline{\mathbf{G}}$ pode ser obtida de $\mathbf{G}$ através de operações elementares com as linhas de $\mathbf{G}$ e vice versa.

Os códigos podem ser construídos a partir de matrizes geradoras $\mathbf{G}$. Basta tomar uma matriz cujas linhas sejam linearmente independentes e definir um código como sendo a transformação linear

$$\begin{array}{rccc} T & : & (\mathbb{F}_q)^k & \longrightarrow & (\mathbb{F}_q)^n \\ & & \mathbf{x} & \longmapsto & \mathbf{xG} \end{array}$$

.

**Códigos equivalentes.**

**Definição 5.4.** *Seja* $\mathbb{F}_q$ *um alfabeto e* $n$ *um número natural. Diremos que uma função* $T : (\mathbb{F}_q)^n \longrightarrow (\mathbb{F}_q)^n$ *é uma isometria de* $(\mathbb{F}_q)^n$ *se ela preserva distâncias de Hamming, isto é:*

$$d\left(T(u), T(v)\right) = d(u, v); u, v \in (\mathbb{F}_q)^n\,.$$

**Definição 5.5.** *Dados dois códigos* $\mathbf{C}$ *e* $\mathbf{C}'$ *em* $(\mathbb{F}_q)^n$ , *diremos que* $\mathbf{C}'$ *é equivalente a* $\mathbf{C}$ *se existir uma isometria* $T$ *de* $(\mathbb{F}_q)^n$ *tal que* $T(\mathbf{C}) = \mathbf{C}'$.

Observamos que dessa definição decorre que dois códigos equivalentes têm os mesmos parâmetros $n, k, d$,

$$pois \begin{cases} T \;\; é \;\; injetora \Longrightarrow leva\ base\ em\ base\ (k) \\ T \;\; é \;\; isometria \Longrightarrow preserva\ distância\ (d) \\ T \;\; : \qquad\qquad (\mathbb{F}_q)^n \longrightarrow (\mathbb{F}_q)^n \end{cases}$$

A equivalência de códigos é uma relação de equivalência (reflexiva, simétrica e transitiva).

Uma forma mais simples de se obter a partir de um código linear $\mathbf{C}$ um código $\mathbf{C}'$ equivalente é efetuando-se sequências de operações sobre a matriz geradora $\mathbf{G}$ do código linear $\mathbf{C}$ , do tipo:

- Permutação de duas colunas
- Multiplicação de uma coluna por um escalar não nulo.

Dessa forma, obtém-se uma matriza geradora $\mathbf{G}'$ de um código linear $\mathbf{C}'$ equivalente a $\mathbf{C}$, observando que realizar operações deste tipo em $\mathbf{G}$, implica realizá-las em todas as palavras de $\mathbf{C}$, o que caracteriza a isometria $T$.

A matriz $\mathbf{G}$ pode ser colocada na forma padrão efetuando-se as operarações elementares sobre as linhas ou colunas de $\mathbf{G}$. Denominaremos $\mathbf{G}^*$ a matriz de $\mathbf{G}$ na forma padrão.

$$\mathbf{G}^* = [I_k \,|A]$$

Assim, dado um código $\mathbf{C}$, existe um código $\mathbf{C}'$ com matriz geradora $\mathbf{G}^*$ na forma padrão.

**Exemplo 5.6.** *Dado o código* $\mathbf{C}$ *definido sobre* $\mathbb{F}_2$ *pela matriz* $\mathbf{G}$ *abaixo, encontre um código* $\mathbf{C}'$ *equivalente a* $\mathbf{C}$, *com matriz geradora na forama padrão.* $T : (\mathbb{F}_2)^4 \longrightarrow (\mathbb{F}_2)^6$

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

De $\mathbf{G}$, temos que $k = 4$, $n = 6$ e $|\mathbf{C}| = 2^4 = 16$

$$\begin{matrix} L_1 \\ L_2 \\ L_3 \\ L_4 \end{matrix} \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} L_1 + L_3 \quad \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} L3 + L_4$$

$$\begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} c_1 & c_2 & c_3 & c_4 & c_5 & c_6 \end{matrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} L_2 + L_1 \quad \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} L_4 + L_1$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \approx \quad \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \approx$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} L_2 + L_3 \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} c_3 \leftrightarrow c_4$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \approx \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \approx$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} = [I_4 \,|A] \text{ em que}$$

$$I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ e } A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}_{k\times(n-k)=4\times 2} .$$

## 6. CÓDIGOS DUAIS

Dados $u = (u_1, u_2, \ldots, u_n)$, $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_q)^n$, o produto interno de $u$ e $v$ é definido como sendo

$$\langle u, v\rangle = u_1v_1 + u_2v_2 + \cdots + u_nv_n.$$

**Propriedade 6.1.** $\langle u, v\rangle = \langle v, u\rangle$

**Propriedade 6.2.** $\langle u + \lambda w, v\rangle = \langle u, v\rangle + \lambda \langle w, v\rangle$ *para todo* $\lambda \in \mathbb{F}_q$.

**Definição 6.1.** *Seja* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *um código linear, o código*

$$\mathbf{C}^{\perp} = \{v \in (\mathbb{F}_q)^n : \langle u, v\rangle = 0, \forall u \in \mathbf{C}\}$$

*é chamado de código dual de* $\mathbf{C}$.

**Lema 6.2.** *Se* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *é um código linear, com matriz geradora* $\mathbf{G}$*, então*

$(i)$ $\mathbf{C}^{\perp}$ *é um sub-espaço vetorial de* $(\mathbb{F}_q)^n$
$(ii)$ $x \in \mathbf{C}^{\perp} \Leftrightarrow \mathbf{G}x^t = 0$

*Demonstração.* $(i)$ Dados $u, v \in \mathbf{C}^{\perp}$ e $\lambda \in K$, temos para todo $x \in \mathbf{C}$, que $\langle u + \lambda v, x\rangle = \langle u, x\rangle + \lambda \langle v, x\rangle = 0$ e portanto, $u + \lambda v \in \mathbf{C}^{\perp}$, provando que $\mathbf{C}^{\perp}$ é um sub-sepaço vetorial de $(\mathbb{F}_q)^n$.

$(ii)$ $x \in \mathbf{C}^{\perp} \Leftrightarrow x$ é ortogonal a todos elementos de $\mathbf{C} \Leftrightarrow \mathbf{G}\mathrm{x}^t = 0$ pois linhas de $\mathbf{G}$ formam uma base de $\mathbf{C}$. □

**Proposição 6.3.** *Seja* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *é um código linear de dimensão* $k$ *com matriz geradora* $\mathbf{G}$=$[I_k \,|A]$, *na forama padrão. Então*

$(i)$ $dim\mathbf{C}^{\perp} = n - k$
$(ii)$ $\boldsymbol{H}$=$[-A^t \,|I_{n-k}]$ *é uma matriz geradora de* $\mathbf{C}^{\perp}$.

*Demonstração.* (i) Temos que $v \in \mathbf{C}^{\perp} \Leftrightarrow \mathbf{G}v^t = 0$. Se $v = (v_1, v_2, \ldots, v_n)$ temos o sistema a seguir:

$$\left[\begin{array}{ccccc|ccc} 1 & 0 & 0 & 0 & 0 & a_{1,k+1} & \cdots & a_{1,n} \\ 0 & 1 & 0 & 0 & 0 & a_{2,k+1} & \cdots & a_{2,n} \\ 0 & 0 & \ddots & \vdots & \vdots & \vdots & \cdots & \\ \vdots & \vdots & \vdots & 1 & 0 & \vdots & \cdots & \\ 0 & 0 & \ldots & 0 & 1 & a_{k,k+1} & \cdots & a_{k,n} \end{array}\right]_{k\times n} \cdot \begin{bmatrix} v_1 \\ \vdots \\ \vdots \\ \vdots \\ v_n \end{bmatrix}_{n\times 1} = \begin{bmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{bmatrix}_{k\times 1}.$$

Assim:

$$\left\{\begin{array}{ccccccccccc} v_1 & & & & +a_{1,k+1}.v_{k+1} & + & \cdots & + & a_{1,n}.v_n & = & 0 \\ & v_2 & & & +a_{2,k+1}.v_{k+1} & + & \cdots & + & a_{2,n}.v_n & = & 0 \\ & & \ddots & & \vdots & & & & & \vdots & \Longrightarrow \\ & & & \ddots & \vdots & & & & & \vdots & \\ & & & v_k & +a_{k,k+1}.v_{k+1} & + & \cdots & + & a_{k,n}.v_n & = & 0 \end{array}\right.$$

$$\left\{\begin{array}{ccccccccc} v_1 & = & -(a_{1,k+1}.v_{k+1} & + & \cdots & + & a_{1,n}.v_n) \\ v_2 & = & -(a_{2,k+1}.v_{k+1} & + & \cdots & + & a_{2,n}.v_n) \\ \vdots & & & & & & \\ v_k & = & -(a_{k,k+1}.v_{k+1} & + & \cdots & + & a_{k,n}.v_n) \end{array}\right. \Rightarrow \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ \vdots \\ v_k \end{bmatrix} = -A \begin{bmatrix} v_{k+1} \\ v_{k+2} \\ \vdots \\ \vdots \\ v_n \end{bmatrix}$$

Logo:

$$v = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ \vdots \\ v_k \end{bmatrix}$$

$$v = \begin{bmatrix} -(a_{1,k+1}.v_{k+1} + \cdots + a_{1,n}.v_n) \\ -(a_{2,k+1}.v_{k+1} + \cdots + a_{2,n}.v_n) \\ \vdots \\ -(a_{k,k+1}.v_{k+1} + \cdots + a_{k,n}.v_n) \\ v_{k+1} \\ v_{k+2} \\ \vdots \\ v_n \end{bmatrix}$$

$$v = v_{k+1} \begin{bmatrix} -a_{1,k+1} \\ -a_{2,k+1} \\ \vdots \\ -a_{k,k+1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \cdots + v_n \begin{bmatrix} -a_{1,n} \\ -a_{2,n} \\ \vdots \\ -a_{k,n} \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

em que $v_{k+1\in}, v_{k+2}, \ldots, v_n \in \mathbb{F}_q$. Como $\mathbb{F}_q$ possui $q$ elementos, existem $q^{n-(k+1)+1} = q^{n-k}$ possibilidades para $v$, ou seja, $\mathbf{C}^{\perp}$ possui $q^{n-k}$ elementos, o que significa que sua dimensão é $n-k$.

(ii) As linhas de $\mathbf{H}$ são linearmente independentes, devido ao bloco $\mathrm{I}_{n-k}$. Portanto geram um sub-espaço vetorial de dimensão $n-k$. Desse modo, a $i-ésima$ linha de $\mathbf{H}$, denotada por $\mathbf{H}_i; 1 \leq i \leq n-k$, é dado por:

$$\mathbf{H}_i = \big(-a_{1i},\ -a_{2i},\ \ldots,\ -a_{ki},\ 0,\ 0,\ \ldots\ 1,\ 0,\ \ldots,\ 0\big)$$

$$\nearrow$$

Posição $i$

e a $j-ésima$ linha de $\mathbf{G}$, denotada por $\mathbf{G}_j; 1 \leq i \leq k$ é dada por

$$\mathbf{G}_j = \big(0,\ 0,\ \ldots\ 1,\ 0,\ \ldots,\ 0,\ a_{j1},\ a_{j2},\ \ldots,\ a_{jn-k}\big)$$

$$\uparrow$$

Posição $j$

Daí, $\langle \mathbf{H}_i, \mathbf{G}_j \rangle = -a_{ji} + a_{ji} = 0$, ou seja, todas as linhas de $\mathbf{H}$ são ortogonais às linhas de $\mathbf{G}$. Logo, o espaço gerado pelas linhas de $\mathbf{H}$ está contido em $\mathbf{C}^{\perp}$, e como esses dois espaços têm a mesma dimensão, eles coincidem, mostrando assim que $\mathbf{H}$ é uma matriz geradora de $\mathbf{C}^{\perp}$. □

**Proposição 6.4.** *Seja* $\mathbf{C}$ *um código com dimensão* $k$ *em* $(\mathbb{F}_q)^n$ *com matriz geradora* $\mathbf{G}$. *Uma matriz* $\mathbf{H}$ *de ordem* $(n-k)\times n$, *com coeficientes em* $\mathbb{F}_q$ *e com linhas linearmente independentes, é uma matriz geradora de* $\mathbf{C}^{\perp}$ *se, e somente, se* $\mathbf{G}\mathbf{H}^t = 0$.

*Demonstração.* Exercício. □

**Corolário 6.5.** $\left(\mathbf{C}^{\perp}\right)^{\perp} = \mathbf{C}$

*Demonstração.* Exercício. □

Como consequência temos a seguinte

**Proposição 6.6.** *Seja* $\mathbf{C}$ *um código linear e consideremos* $\mathbf{H}$ *uma matriz geradora de* $\mathbf{C}^{\perp}$. *Temos então que:* $v \in \mathbf{C} \Leftrightarrow \mathbf{H}v^t = o$.

*Demonstração.* $v \in \mathbf{C} \Leftrightarrow v \in \left(\mathbf{C}^{\perp}\right)^{\perp} \Leftrightarrow \mathbf{H}\mathrm{v}^t = o$. □

Esta proposição fornece uma maneira de caracterizar os elementos de um código $\mathbf{C}$ por uma condição de anulamento. A matriz $\mathbf{H}$, geradora de $\mathbf{C}^{\perp}$, é chamada *matriz verificação de paridade* de $\mathbf{C}$.

**Exemplo 6.7.** *Seja dado o código* $\mathbf{C}$ *sobre* $\mathbb{F}_2$ *com matriz geradora* $\mathbf{G} = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{array}\right)$.
*Verifique se o vetor* $v = \left(0,\ 1,\ 1,\ 1\right) \in (\mathbb{F}_2)^4$ *pertence a* $\mathbf{C}$.

**Solução 6.8.** *Nesse caso, temos* $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *e* $-A^t = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ *e daí*

$$\mathbf{H} = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right).$$

*Além disso,*

$$\mathbf{H}v^t = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}_{3\times 4} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$\therefore v \notin \mathbf{C}$.

**Definição 6.9.** *Dados um código* $\mathbf{C}$ *,com matriz de verificação de paridade* $\mathbf{H}$, *e um vetor* $v \in (\mathbb{F}_q)^n$, *chamamos o vetor* $\mathbf{H}v^t$ *de sídrome de* $v$.

A matriz de verificação de paridade de um código $\mathbf{C}$ determina ,de maneira simples, se um vetor $v \in (\mathbb{F}_q)^n$ pertence ou não a ele. Além disso, contém, de forma muito simples, informações sobre o valor do peso $W$ do código $\mathbf{C}$.

**Proposição 6.10.** *Seja* $\mathbf{H}$ *a matriz de verificação de paridade de um código* $\mathbf{C}$. *Temos que o peso de* $\mathbf{C}$ *é maior do que ou igual a* $s$ *se, e somente se, quaisquer* $s-1$ *colunas de* $\mathbf{H}$ *são linearmente independentes.*

*Demonstração.* ($\Leftarrow$)Admitamos que cada conjunto de $s-1$ colunas de $\mathbf{H}$ é linearmente independente.

Seja $v \in \mathbf{C} - \{o\}$, $v = (v_1, v_2, \ldots, v_n)$ e sejam $\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_n$ as colunas de $\mathbf{H}$. Como $\mathbf{H}v^t = o$, temos que $v_1\mathbf{H}_1 + v_2\mathbf{H}_2 + \cdots + v_n\mathbf{H}_n = 0$. Além disso, sabemos que

$W(\mathbf{C})$ é o número de $v_i \neq 0$; $i = 1, \ldots, n$. Logo se $W(\mathbf{C}) \leq s-1$ teríamos uma combinação de $s-1$ ou menos colunas de $\mathbf{H}$ igual ao vetor nulo, com coeficientes $v_i$ não todos nulos. Mas contraria a nossa hipótese. Logo, $W(\mathbf{v}) \geq s \ \forall \ v \in \mathbf{C}$ e, portanto $W(\mathbf{C}) \geq s$.

($\Rightarrow$) Admitamos que $W(\mathbf{C}) \geq s$.

Suponhamos por absurdo que $\mathbf{H}$ tenha pelo menos um conjunto com $s-1$ colunas linearmente dependentes, digamos, $\mathbf{H}_{i,1}, \mathbf{H}_{i,2}, \ldots, \mathbf{H}_{i,s-1}$. Logo, existiria $v_{i,1}, v_{i,2}, \ldots, v_{i,s-1} \in \mathbb{F}_q$, nem todos nulos, tais que

$$v_{i,1}\mathbf{H}_{i,1} + v_{i,2}\mathbf{H}_{i,2} + \cdots + v_{i,s-1}\mathbf{H}_{i,s-1} = 0$$

o que é equivalente a $\mathbf{H}v^t = o$, com

$$v = (0, \ldots v_{i,1}, 0, \ldots, v_{i,s-1}, 0, \ldots, 0) \in (\mathbb{F}_q)^n .$$

Nesse caso, $v \in \mathbf{C}$ e $W(\mathbf{C}) = s-1$, o que contraria a nossa hipótese. □

**Teorema 6.11.** *Seja* $\mathbf{H}$ *a matriz de verificação de paridade de um código* $\mathbf{C}$. *O peso de* $\mathbf{C}$ *é igual a* $s$, *se e somente se, quaisquer* $s-1$ *colunas de* $\mathbf{H}$ *são linearmente independentes e existem* $s$ *colunas de* $\mathbf{H}$ *linearmente dependentes.*

*Demonstração.* ($\Rightarrow$) Admitamos $W(\mathbf{C}) = s$.

Pela **Proposição 6.10** todo conjunto de $s-1$ colunas de $\mathbf{H}$ é linearmente independente. Se não existir pelo menos um conjunto com $s$ colunas de $\mathbf{H}$ linearmente dependentes, ter-se-ia pela proposição anterior que $W(\mathbf{C}) \geq s+1$, o que é absurdo.

Portanto, existe pelo menos um conjunto com $s$ colunas de $\mathbf{H}$ que é linearmente dependentes.

($\Leftarrow$) Todo conjunto com $s-1$ colunas de $\mathbf{H}$ é L.I. e existe um conjunto com $s$ colunas de $\mathbf{H}$ que é $L.D$.

Pela proposição anterior tem-se que $W(\mathbf{C}) \geq s$. Mas $W(\mathbf{C})$ não pode ser estritamente maior do que $s$, pois pela proposição anterior, todo conjunto com $s$ colunas de $\mathbf{H}$ seria linearmente independente, o que é absurdo. Portanto, $W(\mathbf{C}) = s$. □

**Corolário 6.12.** *Limitante de Singleton: Os parâmetros (n,k,d) de um código linear satisfazem à desigualdade* $d \leq n-k+1$.

*Demonstração.* Seja $\mathbf{H}$ uma matriz de verificação de paridade de um código linear $\mathbf{C}$, com parâmetros $(n, k, d)$. Então o posto de $\mathbf{H}$ é $n-k$, pois a mesma é uma matriz de ordem $(n-k) \times n$, isto é, $n-k$ linhas linearmente independentes. Logo, cada coluna de $\mathbf{H}$ tem $n-k$ entradas, ou seja, comprimento $n-k$, ou ainda estão em $(\mathbb{F}_q)^{n-k}$. Pelo teorema anterior, quaisquer $d-1$ colunas de $\mathbf{H}$ são linearmente independentes.

Como um conjunto de vetores de $(\mathbb{F}_q)^{n-k}$ que é $L.I.$ tem no máximo $n-k$ vetores, então $d-1 \leq n-k$. Daí $d \leq n-k+1$. □

## 7. DECODIFICAÇÃO

Decodificação é o procedimento de detecção e correção de erros num determinado código.

Inicialmente, define-se o vetor **e** como sendo a diferença entre o vetor recebido **r** e o vetor transmitido **v.**

$$\mathbf{e} = \mathbf{r} - \mathbf{v}$$

Se **H** é a matriz de verificação de paridade do código, temos que:

$$\mathbf{He}^t = \mathbf{H}\left(\mathbf{r} - \mathbf{v}\right)^t = \mathbf{Hr}^t - \mathbf{Hv}^t = \mathbf{Hr}^t, \text{pois } \mathbf{Hv}^t = o$$

Portanto, a palavra recebida **r** tem a mesma síndrome do vetor erro **e**.

Seja $\mathbf{H}_i$ a $i-$*ésima* coluna de **H**. Se $\mathbf{e} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ então

$$\sum_{i=1}^{n} \alpha_i \mathbf{H}_i = \mathbf{He}^t = \mathbf{Hr}^t.$$

**Lema 7.1.** *Seja* **C** *um código linear em* $(\mathbb{F}_q)^n$ *com capacidade de correção de erros igual a k. Se* $\boldsymbol{r} \in (\mathbb{F}_q)^n$ *e* $\mathbf{v} \in \mathbf{C}$ *são tais que* $d(\boldsymbol{v},\boldsymbol{r}) \leq k$, *então existe um único vetor* **e** *com* $W(\mathbf{e}) \leq k$ *cuja sídrome é igual à síndrome de* $\boldsymbol{r}$ *e tal que* $\boldsymbol{v}=\boldsymbol{r}$-**e**.

*Demonstração.* De fato, **v=r-e** tem a propriedade do Lema, já que

$$W(\mathbf{e}) = d(\mathbf{v}, \mathbf{r}) \leq k.$$

Para provar a unicidade, suponhamos que $\mathbf{e} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ e $\mathbf{e}' = (\alpha_1', \alpha_2', \ldots, \alpha_n')$ sejam tais que $W(\mathbf{e}) \leq k$ e $W(\mathbf{e}') \leq k$ e tenham a mesma síndrome que **r**. Então, se **H** é uma matriz de verificação de paridade de **C**, temos

$$\mathbf{He}^t = \mathbf{He}'^t \Longrightarrow \sum_{i=1}^{n} \alpha_i \mathbf{H}_i = \sum_{i=1}^{n} \alpha_i' \mathbf{H}_i,$$

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 $\alpha_i = \alpha_i'$ para todo $i$, logo $\mathbf{e} = \mathbf{e}'$. □

**Exemplo 7.2.** *Determine* **e** *quando* $W(\mathbf{e}) \leq 1$. *Admitamos que o código* **C** *tenha distância mínima* $d \geq 3$ *e que o vetor erro* **e**, *introduzido entre a palavra transmitida* $\boldsymbol{v}$ *e a palavra recebida* $\boldsymbol{r}$, *seja tal que* $W(\mathbf{e}) \leq 1$. *Isto é, o canal introduziu no máximo um erro. Se* $\mathbf{He}^t = o$, *então* $\boldsymbol{r} \in \mathbf{C}$ *e se toma* $\boldsymbol{v} = \boldsymbol{r}$. *Suponhamos* $\mathbf{He}^t \neq o$, *então* $W(\mathbf{e}) = 1$ *e, portanto,* **e** *tem apenas uma coordenada não nula. Nesse caso, consideremos que* $\mathbf{e} = (0, \ldots, \alpha, \ldots, 0)$ *com* $\alpha \neq 0$ *na* $i-$*ésima posição. Logo,*

$$\mathbf{He}^t = \alpha \mathbf{H}_i.$$

*Portanto, não conhecendo*

$$\mathbf{He}^t = \mathbf{Hr}^t = \alpha \mathbf{H}_i,$$

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

**Ilustração 7.3.** *Seja* **C** *o código do* ***Exemplo 5.3****. Esse código tem matriz teste de paridade*

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

*Seja* $\boldsymbol{r}$=$(1,0,1,0,0)$ *uma palavra recebida, logo,*

$$\mathbf{H}\mathbf{e}^t = \mathbf{H}\mathbf{r}^t = \begin{pmatrix}0\\1\\0\end{pmatrix} = 1.\mathbf{H}_4$$

*Portanto,* $\mathbf{e}$=$(0,0,0,1,0)$ *e, consequentemente,*

$$\mathbf{v} = \mathbf{r} - \mathbf{e} = (1,0,1,1,0.$$

Com base no exemplo anterior, será estabelecido um algoritmo de decodificação para códigos corretores de um erro.

Considere $\mathbf{H}$ a matriz de verificação de paridade do código $\mathbf{C}$ e seja $\mathbf{r}$ o vetor recebido.(Admitamos $d \geq 3$)

**(a):** Calcule $\mathbf{H}\mathbf{r}^t$.
**(b):** Se $\mathbf{H}\mathbf{r}^t = o$, aceite $\mathbf{r}$ como a palavra transmitida.
**(c):** Se $\mathbf{H}\mathbf{r}^t = \mathbf{s} \neq o$ compare $\mathbf{s}$ com colunas de $\mathbf{H}$.
**(d):** Se existirem $i$ e $\alpha$ tais que $\mathbf{s}^t = \alpha\mathbf{H}_i$, para $\alpha \in \mathbb{F}_q$, então $\mathbf{e}$ é a $n = upla$ com $\alpha$ na posição $i$ e zeros nas outras posições. Corrija $\mathbf{r}$ pondo $\mathbf{v} = \mathbf{r} - \mathbf{e}$.
**(e):** Se o contrário de **(d)** ocorrer, então mais de um erro foi cometido.

Considere $\mathbf{C}$ um código corretor de erros em $(\mathbb{F}_q)^n$ cuja matriz de verificação de paridade é $\mathbf{H}$. Sejam $d$ a distância mínima de $\mathbf{C}$ e $k = \left[\frac{d-1}{2}\right]$. Recorde que $\mathbf{e}$ e $\mathbf{r}$ têm a mesma síndrome e se

$$W(\mathbf{e}) = d(\mathbf{r},\mathbf{v}) < k,$$

então $\mathbf{e}$ é univocamente determinado por $\mathbf{r}$.

Seja $u \in (\mathbb{F}_q)^n$. Defina

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

**Lema 7.4.** *Os vetores* $u$ *e* $v$ *de* $(\mathbb{F}_q)^n$ *têm a mesma síndrome se, e somente se,* $u \in v + \mathbf{C}$.

*Demonstração.* $\mathbf{H}u^t = \mathbf{H}v^t \iff \mathbf{H}\left(u-v\right)^t = o \iff u - v \in \mathbf{C} \iff u \in v + \mathbf{C}$. □

**Exemplo 7.5.** *Seja* $\mathbf{C}$ *o (4,2)-código gerado sobre* $\mathbb{F}_2$ *pela matriz*

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

*Logo,*

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

*e as classes laterais segundo* $\mathbf{C}$ *são:*

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

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

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

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

Uma correspondência 1-1 entre classes laterais e síndromes é estabelecida pelo Lema acima. Todos os elementos de uma classe lateral têm a mesma síndrome.

**Definição 7.6.** *Um vetor de peso mínimo numa classe lateral é chamado de elemento líder dessa classe.*

**Proposição 7.7.** *Seja* $\mathbf{C}$ *um código linear em* $(\mathbb{F}_q)^n$ *com distância mínima d. Se* $u \in (\mathbb{F}_q)^n$ *é tal que*

$$W(u) \leq \left[\frac{d-1}{2}\right] = k,$$

*então u é o único elemento líder de sua classe.*

*Demonstração.* Suponhamos que $u$ e $v \in (\mathbb{F}_q)^n$ com $W(u) \leq \left[\frac{d-1}{2}\right]$ e $W(v) \leq \left[\frac{d-1}{2}\right]$. Se $u - v \in \mathbf{C}$, então

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

Logo, $u - v = o$ e, portanto, $u = v$. □

**Observação 7.8.** *:Para achar líderes de classes, tomamos os elementos u tais que* $W(u) \leq \left[\frac{d-1}{2}\right]$. *Cada um desses elementos é líder de uma e somente uma classe. Esses líderes são todos aqueles de peso menor ou igual a* $\left[\frac{d-1}{2}\right]$, *os outros líderes não serão considerados. Agora discutiremos um algoritmo de correção de mensagens que tenham sofrido um número de erros menor ou igual à capacidade de correção do código, que é* $k = \left[\frac{d-1}{2}\right]$.

Determine todos os elementos de $u \in (\mathbb{F}_q)^n$, tal que $W(u) \leq k$. Em seguida, calcule as síndromes desses elementos e coloque esses dados numa tabela. Seja $\mathbf{r}$ uma palavra recebida.

**O Algoritmo de Decodificação**

**(1):** Calcule a síndrome $\mathbf{s}^t = \mathbf{H}\mathbf{r}^t$.
**(2):** Se $\mathbf{s}$ está na tabela, seja $l$ o elemento líder da classe determinada por $\mathbf{s}$; troque por $\mathbf{r} - l$.
**(3):** Se $\mathbf{s}$ não está na tabela, então na mensagem recebida foram cometidos mais do que $k$ erros.

Justificativa: Dado $\mathbf{r}$, sejam $\mathbf{v}$ e $\mathbf{e}$, respectivamente, a mensagem transmitida e o vetor erro. Como $\mathbf{H}\mathbf{e}^t = \mathbf{H}\mathbf{r}^t$, temos que a classe lateral onde $\mathbf{e}$ se encontra está determinada pela síndrome de $\mathbf{r}$. Se

$W(\mathbf{e}) \leq k$, temos que $\mathbf{e}$ é o único elemento líder $l$ de sua classe e, portanto, é conhecido e se encontra na tabela. Consequentemente,$\mathbf{v} = \mathbf{r} - \mathbf{e} = \mathbf{r} - l$ é determinado.

**Exemplo 7.9.** *Considere o código linear definido sobre* $\mathbb{F}_2$ *com matriz de verificação de paridade* $\mathbf{H} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$. *Observe que n-k=3, como n=6, então k=3. Alé disso, duas a duas, as colunas de* $\mathbf{H}$ *são L.I. e existem três colunas* $1^a, 2^a$ *e* $4^a$ *L.D. Logo,* $d = 3$, *pois* $s - 1 = 2$ *e portanto, t=1. Os vetores de* $(\mathbb{F}_2)^6$ *com* $W(u) \leq 1$ *e suas respectivas síndromes estão relacionados*

*na tabela abaixo:*

| *Líder* | *Síndrome* |
|---|---|
| *(0,0,0,0,0,0)* | *(0,0,0)* |
| *(0,0,0,0,0,1)* | *(1,0,1)* |
| *(0,0,0,0,1,0)* | *(0,1,1)* |
| *(0,0,0,1,0,0)* | *(1,1,0)* |
| *(0,0,1,0,0,0)* | *(0,0,1)* |
| *(0,1,0,0,0,0)* | *(0,1,0)* |
| *(1,0,0,0,0,0)* | *(1,0,0)* |

*Suponhamos que a palavra recebida seja:*

**(a):** $\mathbf{r} =$ *(1,0,0,0,1,1). Logo,* $\mathbf{Hr}^t =$*(0,1,0)*$^t$ *e, portanto*

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

*Consequentemente,*

$$\mathbf{v} = \mathbf{r} - \mathbf{e} =(1, 0, 0, 0, 1, 1) - (0, 1, 0, 0, 0, 0) = (1, 1, 0, 0, 1, 1).$$

**(b):** $\mathbf{r} =$ *(1,1,1,1,1,1). Logo,* $\mathbf{Hr}^t =$*(1,1,1)*$^t$ *que não se encontra na tabela. Sendo assim, foi cometido mais do que 1 erro na mensagem* $\mathbf{r}$.

## 8. Conclusão

O mini-curso apresenta e desenvolve os fudamentos matemáticos da Teoria dos Códigos. E por se tratar de um vasto campo tendo várias ramificações em diversas áreas da matemática, concentra-se nos aspectos de natureza algébrica.

## Referências

[1] CAIN, J. B.,CLARK, G. C., e GEIST, J.M. *Punctured convolutional codes of rate (n- 1)/n and simplified maximum likelihood decoding*, IEEE Transactions on Information Theory, vol. IT-25, pp. 97-100, janeiro,1979.

[2] CLARK,G.C., e CAIN,J.B., *Error-Correction Coding for Digital Communication,* John Wiley, 1985.

[3] ELIAS P., e CAIN,J.B., *Coding for noisy channels,* IRE Conv. Rec., 4ª Parte, pp. 37-47,1955.

[4] HEFEZ, A. e VILELA, M.L.T., *Códigos Corretores de Erros,* IMPA, Série dee Computação e Matemática, Rio de Janeiro, 2002.

[5] LIN, S. e COSTELLO, Jr. D. J., *Error Control Coding: Fundamentals and Applications,* Prentice-Hall, 1983.

[6] MACWILLIAMS, F.J., E SLOANE, N.J.A., *The Theory of Error-Correcting Codes,* North-Holland, Amsterdã, 1992.

[7] MASSEY, J. L., *Shift Register Synthesis an BCH Decoding,* IEEE Trans. Inform. Theory, VOL. IT-15 pp. 122-127, January 1969.

[8] NIEDERRETER, H., e LIDL, R., *Introduction to Finite Fields and Their Applications,* Cambridge University Press.

[9] SINGH,S.,*O Livro dos Códigos,* Editora Record, Rio de Janeiro - São Paulo, 2003.

[10] VITERBI, A. J., *Error bounds for convolutional codes and an asymptotically optimum decoding algorithm*, IEEE Transactions on Information Theory IT-13 pp. 260- 269, abril,1967.

[11] WOZENCRAFT,J.M., e REIFEN, B., *Sequential decoding,* MIT Press, Cambridge, Massachussets,1961.

Mário José de Souza
UFG - Instituto de Matemática e Estatística
email: mjsouza@mat.ufg.br