*CAPÍTULO 4*

# Códigos Lineares

## 1. Definição, pârametros e peso mínimo

Seja $\mathbb{F}_q$ o corpo de ordem $q$. Portanto, pelo Teorema 3.24, $q = p^m$ para algum primo $p$ e inteiro positivo $m$.

**Definição 4.1.**
- Um *código linear* $q$-ário, de comprimento $n$, é um subespaço vectorial de $\mathbb{F}_q^n$.
- Se $C$ é um código linear, $C^\perp$ diz-se o *código dual* de $C$.
- Se $C = C^\perp$, $C$ diz-se um *código auto-dual*.

**Exemplo 4.2.** O código de repetição $q$-ário de parâmetros $(n, q, n)_q$ é linear. É o subespaço de $\mathbb{F}_q^n$ gerado pelo vector $\vec{1} = (1, \ldots, 1)$, i.e., $C = \langle \vec{1} \rangle \subseteq \mathbb{F}_q^n$. O código dual de $C$ é

$$C^\perp = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \, : \, \sum_{i=1}^{n} x_i = 0\} \, .$$

Para $q = 2$, obtém-se o código dos pesos pares $C^\perp = \{x \in \mathbb{F}_2^n \, : \, \mathrm{w}(x) \text{ é par}\}$, também denotado por $E_n$ (de "even").

**Proposição 4.3.** *Seja $C$ um código linear de comprimento $n$ sobre $\mathbb{F}_q$. Então*

*(i)* $|C| = q^{\dim C}$, *i.e.,* $\dim C = \log_q |C|$

*(ii)* $\dim C + \dim C^\perp = n$

*(iii)* $(C^\perp)^\perp = C$

Esta proposição já foi demonstrada no capítulo anterior — ver fórmula (3.4) e Teoremas 3.40 e 3.44.

Como o número de palavras que $C$ contém está directamente relacionado com a sua dimenção, definimos que os parâmetros de um código linear são $[n, k, d]_q$ (ou simplesmente $[n, k, d]$, ou ainda apenas $[n, k]$), onde $k = \dim C$, e $n$ e $d$ são respectivamente o comprimento e a distância mínima, como anteriormente. Portanto, um código linear $[n, k, d]_q$ é também um código $(n, q^k, d)_q$.

Recorde que qualquer código, linear ou não, é equivalente a outro contendo a palavra (vector) $\vec{0} \in \mathbb{F}_q^n$, pelo Lema 2.5. No caso de um código linear, este contém necessariamente o vector nulo.

**Definição 4.4.** Seja $C$ um código qualquer, não necessarimanete linear. Definimos o *peso mínimo* de $C$ por

$$\mathrm{w}(C) = \min\{\mathrm{w}(x) \,:\, x \in C \setminus \{\vec{0}\}\} \ ,$$

se $C \neq \{\vec{0}\}$, e $\mathrm{w}(C) = 0$ se $C = \{\vec{0}\}$.

**Teorema 4.5.** *Seja $C \neq \{\vec{0}\}$ um código linear. Então $\mathrm{d}(C) = \mathrm{w}(C)$.*

**Dem.** Como $C \neq \{\vec{0}\}$, $C$ contém pelo menos duas palavras e, de acordo com a definição de distância mínima, $\mathrm{d}(C) = \min\{\mathrm{d}(x,y) \,:\, x,y \in C,\, x \neq y\}$. Sejam então $x, y \in C$ tais que $\mathrm{d}(x,y) = \mathrm{d}(C)$. Portanto

$$\mathrm{d}(C) = \mathrm{d}(x,y) = \mathrm{w}(x-y) \geq \mathrm{w}(C) \ .$$

Na desigualdade usou-se o facto de $x - y \in C$, por $C$ ser linear, e $x - y \neq \vec{0}$.

Seja agora $x \in C$ tal que $\mathrm{w}(x) = \mathrm{w}(C)$. Portanto

$$\mathrm{w}(C) = \mathrm{w}(x) = \mathrm{d}(x, \vec{0}) \geq \mathrm{d}(C) \ .$$

Na desigualdade usou-se o facto de $\vec{0} \in C$, por $C$ ser linear. □

Para calcular a distância mínima $\mathrm{d}(C)$ de um código $C$, contendo $M$ palavras, por definição, é preciso calcular a distância $\mathrm{d}(x,y)$ para $\binom{M}{2} = \frac{M(M-1)}{2}$ pares de palavras. Se $C$ é linear, o teorema anterior diz-nos que basta calcular o peso $\mathrm{w}(x)$ de $M-1$ palavras.

**Exemplo 4.6.** Continuação do Exemplo 4.2.

O código de repetição $C \subseteq \mathbb{F}_q^n$ tem dimensão 1. Como $\mathrm{w}(x) = n$ para qualquer palavra de código $x \in C \setminus \{\vec{0}\}$, então $\mathrm{d}(C) = n$. Portanto $C$ é um código $q$-ário $[n, 1, n]$.

Com $q = 2$ e $n \geq 2$, $E_n = C^\perp$, logo $\dim E_n = n - 1$. Também se tem que $\mathrm{w}(x)$ é par para qualquer $x \in E_n$. Por outro lado $(1, 1, 0, \ldots, 0) \in E_n$ e tem peso 2. Logo o peso mínimo é $\mathrm{w}(E_n) = 2$ e $E_n$ é um código binário de parâmetros $[n, n-1, 2]$.

# 2. Matriz geradora e matriz de paridade

**Definição 4.7.** Seja $C$ um código $q$-ário $[n, k]$.

- Se $\{v_1, \ldots, v_k\}$ é uma base de $C$, a matriz

$$G = \begin{bmatrix} \text{—} & v_1^T & \text{—} \\ & \vdots & \\ \text{—} & v_k^T & \text{—} \end{bmatrix}$$

  diz-se uma *matriz geradora* de $C$.
- $H$ diz-se uma *matriz de paridade* de $C$ se é uma matriz geradora do código dual $C^\perp$.

Em particular, $\dim C > 0$ para haver uma matriz geradora, e $\dim C < n$ para haver uma matriz de paridade.

Note-se que uma matriz geradora tem $k$ linhas e $n$ colunas, e uma matriz de paridade tem $n-k$ linhas e também $n$ colunas.

**Observação 4.8.** Da definição de matriz geradora $G$ e de paridade $H$, tem-se que $C$ é o espaço das linhas de $G$ e é também o núcleo de $H$. Analogamente, o código dual $C^\perp$ é o espaço das linhas de $H$ e o núcleo de $G$.

**Exemplo 4.9.** $G = \begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}$ é uma matriz geradora do código de repetição $C \subseteq \mathbb{F}_5^4$. Por definição de complemento ortogonal,

$$\begin{aligned} C^\perp &= \{x \in \mathbb{F}_5^4 \,:\, x \cdot \vec{1} = 0\} \\ &= \{(x_1, x_2, x_3, x_4) \,:\, x_1 + x_2 + x_3 + x_4 = 0\} \\ &= \{(-x_2 - x_3 - x_4, x_2, x_3, x_4) \,:\, x_2, x_3, x_4 \in \mathbb{F}_5\} \end{aligned}$$

logo $\{(4,1,0,0),(4,0,1,0),(4,0,0,1)\}$ é uma base de $C^\perp$ e

$$H = \begin{bmatrix}4 & 1 & 0 & 0\\ 4 & 0 & 1 & 0\\ 4 & 0 & 0 & 1\end{bmatrix}$$

é uma matriz de paridade para $C$.

**Exemplo 4.10.** Qualquer matriz $n \times n$, não singular[1], G é uma matriz geradora do código $\mathbb{F}_q^n$. Em particular, podemos escolher $G = I_n$, a matriz identidade.

**Definição 4.11.** Seja $C$ um código linear de dimensão $k$ e comprimento $n$.

- Uma matriz geradora $G_{k\times n}$ do código $C$ diz-se na *forma canónica* se $G = \begin{bmatrix}I_k & A\end{bmatrix}$, onde $A$ é uma matriz $k \times (n-k)$.
- Uma matriz de paridade $H_{(n-k)\times n}$ do código $C$ diz-se na *forma canónica* se $H = \begin{bmatrix}B & I_{n-k}\end{bmatrix}$, onde $B$ é uma matriz $(n-k) \times k$.

**Lema 4.12.** *Seja $C$ um código $[n,k]$ sobre $\mathbb{F}_q$ com matriz geradora $G$. Então $H$ é uma matriz de paridade para $C$ sse $HG^T = 0$ e as linhas de $H$ são linearmente independentes.*

**Dem.** Seja $\{v_1, \ldots, v_k\}$ a base de $C$ obtida à custa da matriz geradora $G$, mais precisamente, o vector $v_j$ é a linha $j$ de $G$. Sejam $w_1$, ...,$w_{n-k}$ as linhas da matriz $H$. Então, a entrada $(i,j)$ da matriz produto $HG^T$ é $w_i v_j$, que podemos ainda escrever como o produto interno $w_i \cdot v_j$ dos vectores $w_i, v_j \in \mathbb{F}_q^n$.

($\Longrightarrow$) Se $H$ é uma matriz de paridade de $C$, as suas linhas são linearmente independentes, por definição de matriz de paridade, e $w_i \cdot v_j = 0$ para todo o $i$ e $j$ porque $w_i \in C^\perp$ e $v_j \in C$. Donde sai que $HG^T = 0$.

($\Longleftarrow$) Seja $C'$ o espaço das linhas de $H$. Então $\dim C' = n-k$ porque as linhas de $H$ são linearmente independentes. Como $w_i \cdot v_j = 0$ para quaisquer $i, j$ (estamos a assumir que $HG^T = 0$) e o conjunto

[1] Recorde da Álgebra Linear que uma matriz quadrada é *não singular* se e só se tem determinante não nulo.

$\{v_1, \ldots, v_k\}$ é uma base de $C$, conclui-se que $C'$ é um subespaço de $C^\perp$. Mas como $C'$ e $C^\perp$ têm ambos dimensão $n-k$, temos necessariamente que $C' = C^\perp$ e, portanto, $H$ é uma matriz de paridade de $C$. □

No enunciado, a igualdade $HG^T = 0$ é equivalente a $GH^T = 0$, pois $(AB)^T = B^T A^T$, $(A^T)^T$ e a transposta de uma matriz nula é ainda uma matriz nula.

Se aplicarmos o lema anterior ao código dual $C^\perp$ obtém-se o resultado análogo para matrizes geradoras:

**Lema 4.13.** *Seja $C$ um código $[n,k]$ sobre $\mathbb{F}_q$ com matriz de paridade $H$. Então $G$ é uma matriz geradora de $C$ sse $HG^T = 0$ e as linhas de $G$ são linearmente independentes.*

**Teorema 4.14.** *Seja $C$ um código $[n,k]_q$ com uma matriz geradora $G = \begin{bmatrix} I_k & A \end{bmatrix}$ na forma canónica. Então $H = \begin{bmatrix} -A^T & I_{n-k} \end{bmatrix}$ é uma matriz de paridade para $C$ na forma canónica.*

**Dem.** Como as últimas $n-k$ colunas de $H$ formam a matriz identidade, tem-se imediatamente que as linhas de $H$ são linearmente independentes. Calculando o produto $HG^T$ fica

$$HG^T = \begin{bmatrix} -A^T & I_{n-k} \end{bmatrix} \begin{bmatrix} I_k \\ A^T \end{bmatrix} = -A^T I_k + I_{n-k} A^T = -A^T + A^T = 0 \ .$$

Aplicando o Lema 4.12, conclui-se que $H$ é de facto uma matriz de paridade para $C$. □

Como consequência, tendo uma matriz geradora $G$ na forma canónica, obtemos directamente uma base para o código dual, nomeadamente, as linhas da matriz de paridade associada a $G$.

**Exemplo 4.15.** Seja $C$ o código binário linear gerado pelo conjunto

$$S = \{11101, 10110, 01011, 11010\} \ .$$

Vamos determinar uma matriz geradora e uma de paridade para $C$. Seja $M$ a matriz cujas linhas são os vectores do conjunto $S$, e apliquemos o método de eliminação de Gauss a M:

$$M = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix} \overset{\substack{l_2 \mapsto l_2 + l_1 \\ l_4 \mapsto l_4 + l_1}}{\longrightarrow} \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \overset{l_3 \mapsto l_3 + l_2}{\longrightarrow} \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Daqui já podemos concluir que $\dim C = 3$, pois há apenas três linhas de $M$ linearmente independentes. Continuando a eliminação de Gauss a partir da última matriz obtida, mas agora "de baixo para cima", de modo a tentar obter a matriz identidade no lado esquerdo da matriz, fica

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \overset{l_1 \mapsto l_1 + l_2 + l_3}{\longrightarrow} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \overline{M}$$

Como a matriz $\overline{M}$ foi obtida de $M$ aplicando apenas operações nas linhas (i.e., não houve trocas de colunas), $M$ e $\overline{M}$ têm o mesmo espaço de linhas. Portanto

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

é uma matriz geradora do código $C$ e está na forma canónica, logo

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

é uma matriz de paridade para $C$ e está na forma canónica. Aplicou-se o Teorema 4.14 a $G$ para obter $H$.

**Teorema 4.16.** *Seja $C$ um código $[n,k]$ sobre $\mathbb{F}_q$, com matriz de paridade $H$. Então*

*(i)* $\mathrm{d}(C) \geq d$ *se e só se quaisquer $d-1$ colunas de $H$ são linearmente independentes,*

*(ii)* $\mathrm{d}(C) \leq d$ *se e só se existem $d$ colunas de $H$ linearmente dependentes.*

**Dem.** Pelo Teorema 4.5, sabemos que $\mathrm{d}(C) = \mathrm{w}(C)$. Designemos por $c_1, \ldots, c_n$ as colunas da matriz de paridade $H$. Seja $x = (x_1, \ldots, x_n)$ uma palavra do código $C \subseteq \mathbb{F}_q^n$ com peso $\mathrm{w}(x) = e > 0$ e suponhamos que as componentes de $x$ não nulas se encontram nas coordenadas $i_1, \ldots, i_e$. Como $C = \mathcal{N}(H)$, temos

$$\begin{aligned} x \in C \iff Hx = \vec{0} \quad &\iff \quad \sum_{i=1}^{n} x_i c_i = \vec{0} \\ &\iff x_{i_1} c_{i_1} + \cdots + x_{i_e} c_{i_e} = \vec{0} \qquad \text{com } x_{i_1}, \ldots, x_{i_e} \neq 0 \\ &\iff \text{existem } e = \mathrm{w}(x) \text{ colunas de } H \text{ linearmente dependentes.} \qquad (*) \end{aligned}$$

**(i)** Por definição de peso mínimo, $\mathrm{w}(C) \geq d$ se e só se $\mathrm{w}(x) \geq d$ para todas as palavras de código $x \in C \setminus \{\vec{0}\}$, ou seja, se e só se $C$ não contém nenhuma palavra $x$ não nula com peso $\mathrm{w}(x) \leq d-1$. Esta última afirmação é ainda equivalente a dizer que, por $(*)$, quaisquer $d-1$ colunas de $H$ são linearmente independentes.

**(ii)** Analogamente à alínea (i), $\mathrm{w}(C) \leq d$ se e só se existe uma palavra não nula $x$ do código $C$ com $0 < \mathrm{w}(x) \leq d$, o que é equivalente, por $(*)$, a existir um conjunto linearmente dependente de $d$ colunas de $H$. □

Juntando as duas afirmações deste teorema, podemos dizer que a distância mínima de um código linear $C$ com matriz de paridade $H$ é dada por

$$\boxed{\mathrm{d}(C) = \text{ número mínimo de colunas de } H \text{ linearmente dependentes}} .$$

**Exemplo 4.17.** Seja $C$ o código linear binário com a seguinte matriz de paridade

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

Qual a distância mínima de $C$? Designemos por $c_i$ a coluna $i$ de $H$. Como $H$ tem três linhas (ou seja, cada coluna é um vector em $\mathbb{F}_2^3$), quaisquer 4 colunas são linearmente dependentes, portanto, $\mathrm{d}(C) \leq 3$. Por outro lado

- como não há colunas nulas, qualquer coluna é linearmente independente,
- como não há colunas repetidas, i.e., como $c_i \neq c_j$ se $i \neq j$, então $c_i + c_j \neq \vec{0}$ para $i \neq j$, e quaisquer duas colunas são linearmente independentes,
- como $c_2 + c_4 + c_5 = \vec{0}$, há três colunas linearmente dependentes (também podiamos escolher $c_1 + c_2 + c_3 = \vec{0}$).

Donde se conclui, pelo Teorema 4.16, que $\mathrm{d}(C) = 2$.

# 3. Equivalência Linear

Considere os três seguintes códigos ternários, de comprimento 3:

$$C_1 = \{000, 121, 212\}\ , \qquad C_2 = \{000, 111, 222\} \qquad \text{e} \qquad C_3 = \{001, 122, 210\}\ .$$

De acordo com a definição de equivalência dada no Capítulo 2 (ver Definição 2.3), estes três códigos são equivalentes entre si pois:

- $C_2$ é obtido de $C_1$ aplicando a permutação de símbolos $\pi_2 = \left(\begin{smallmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{smallmatrix}\right)$ na segunda coordenada, e
- $C_3$ é obtido de $C_2$ aplicando a permutação de símbolos $\pi_3 = \left(\begin{smallmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{smallmatrix}\right)$ na terceira coordenada.

No entanto, os códigos $C_1$ e $C_2$ são lineares, mas $C_3$ não é. Ou seja, a operação (ii) na Definição 2.3 nem sempre preserva a linearidade de um código. Interessa, portanto, restringir as operações permitidas na noção de equivalência já dada, de modo a se obter ainda códigos lineares.

**Definição 4.18.** Seja $C$ um código linear $q$-ário $[n, k, d]$. $C'$ diz-se um *código linearmente equivalente* a $C$ se é obtido de $C$ através da aplicação sucessiva das seguintes operações:

(i) permutar a ordem das coordenadas de todas as palavros do código, i.e., substituir todo o $c = c_1 c_2 \cdots c_n \in C$ por $c_{\sigma(1)} c_{\sigma(2)} \cdots c_{\sigma(n)}$, onde $\sigma$ é uma permutação dos índices $\{1, 2, \ldots, n\}$

(ii) multiplicar a coordenada $i$ (fixa) de todas as palavras do código por um escalar não nulo $\lambda_i \in \mathbb{F}_q \setminus \{0\}$, mais precisamente, substituir todo o $c = c_1 c_2 \cdots c_n \in C$ por $(\lambda_1 c_1, \lambda_2 c_2, \cdots, \lambda_n c_n)$.

No exemplo do início desta secção, aplicar a permutação $\pi_2 = \left(\begin{smallmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{smallmatrix}\right)$ corresponde a multiplicar por $\lambda_2 = 2$. A permutação $\pi_3$ não corresponde à multiplicação por nenhum escalar, porque $\pi_3(0) \neq 0$.

**Proposição 4.19.** *Seja $C$ um código linear e seja $C'$ um código linearmente equivalente a $C$. Então, $C'$ é também linear.*

Deixamos a demonstração desta proposição como exercício.

**Teorema 4.20.** *Qualquer código linear $C \neq \{\vec{0}\}$ é linearmente equivalente a outro com uma matriz geradora na forma canónica.*

**Dem.** Apenas fazemos um esboço da demonstração e deixamos como exercício justificar com detalhe todos os passos do argumento apresentado. Seja $G$ uma matriz geradora de $C$. Se $G$ não está na forma canónica, aplicamos o método de eleminação de Gauss, usando apenas operações nas linhas, e obtemos uma matriz $\bar{G}$ na forma

$$\bar{G} = \begin{bmatrix} 0 & \cdots & 0 & 1 & * & 0 & * & 0 & * & 0 & * \\ 0 & \cdots & 0 & 0 & 0 & 1 & * & 0 & * & 0 & * \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 1 & * & 0 & * \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \ddots & 0 & * \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * \end{bmatrix},$$

que ainda gera o mesmo código $C$, porque $G$ e $\bar{G}$ têm exactamente o mesmo espaço de linhas. Permutando agora as colunas de $\bar{G}$ de modo a colocar os pivots nas primeiras colunas, obtém-se uma matriz geradora $G'$ na forma canónica. O código $C'$ gerado pelas linhas da matriz $G'$ pode não ser igual a $C$, mas é certamente equivalente a este, pois permutar colunas numa matriz geradora corresponde a aplicar a operação (i) da definição de equivalência linear. □

**Exemplo 4.21.** Considere os códigos binários lineares $C = \langle 1100, 0011 \rangle$ e $C' = \langle 1010, 0101 \rangle$. As matrizes

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

são matrizes geradoras de $C$ e de $C'$, respectivanemte. $G'$ está na forma canónica. $G$ não está, nem nenhuma outra matriz geradora de $C$ está na forma canónica. Porquê? Mas estes dois códigos são equivalentes: se aplicarmos a operacão (i) da Definição 4.18 a $C$ com $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$ obtemos $C'$.

**Exemplo 4.22.** A forma canónica de uma matriz geradora pode não ser única: seja $C$ o código binário com matriz geradora

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

Se aplicarmos a operação (i) da Definição 4.18 com $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{smallmatrix}\right)$, obtemos um código $C_1$ com a seguinte matriz geradora

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

que está na forma caónica. Se usarmos a permutação $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{smallmatrix}\right)$, obtemos um código $C_2$ com a seguinte matriz geradora

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

que também está na forma canónica, mas $G_1 \neq G_2$.

# 4. Codificação e descodificação

## 4.1. Codificação sistemática

Seja $C$ um código $[n,k]$ sobre $\mathbb{F}_q$. Como $C$ contém $M = q^k$ palavras distintas, qualquer vector $m \in \mathbb{F}_q^k$ poder ser codificado por $C$.

Seja $\mathcal{B} = \{v_1 \ldots, v_k\} \subseteq \mathbb{F}_q^n$ uma base de $C$ e considere-se o vector mensagem $m = (m_1, \ldots, m_k) \in \mathbb{F}_q^k$. Seja $x = \sum_{i=1}^k m_i v_i$, ou seja, $x$ é a combinação linear dos vectores da base $\mathcal{B}$ tendo por coeficientes as corrdenadas do vector mensagem $m$, logo $x \in C$. O vector $x$ também se pode escrever $x = G^T m$, onde $G$ é a matriz cujas linhas são os vectores de $\mathcal{B}$. Fica então definida uma aplicação

$$\begin{aligned} f : \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ m &\longmapsto x = G^T m \ . \end{aligned}$$

Esta aplicação $f$ é injectiva e a sua imagem é $C$, pois as colunas de $G^T$ formam a base $\mathcal{B}$ de $C$. Portanto, depois de restringirmos o conjunto de chegada para $C$, obtemos uma função de codificação $f : \mathbb{F}_q^k \longrightarrow C$ (ver a Definição 1.8).

Suponhamos agora que a matriz geradora $G$ está na forma canónica: $G = \begin{bmatrix} I_k & A \end{bmatrix}$, com $A$ uma matriz $(n-k) \times k$. Então o vector codificado $x$ toma a forma

$$x = G^T m = \begin{bmatrix} I_k \\ A^T \end{bmatrix} m = (m, A^T m) \ . \tag{4.1}$$

Como as $k$ componentes do vector mensagem $m$ são também componentes do vector codificado $x$, dizemos que se trata de uma *codificação sistemática*. A essas compomentes de $x$ chamamamos *dígitos de mensagem*. Às restantes componentes de $x$ chamamos *dígitos de verificação ou redundância*. Escrevendo explicitamente as coordenadas em (4.1):

$$x = (\underbrace{m_1, \ldots, m_k}_{\text{dígitos de mensagem}}, \overbrace{x_{k+1}, \ldots, x_n}^{\text{dígitos de verificação ou redundância}}) \ , \tag{4.2}$$

onde $(x_{k+1}, \ldots, x_n) = A^T m$. Dado um vector codificado $x \in C$, a mensagem original $m$ é obtida simplesmente apagando os dígitos de verificação.

**Exemplo 4.23.** O código ISBN não é linear, mas pode ser obtido a partir do seguinte código linear

$$C = \{(x_1, \ldots, x_{10}) \in \mathbb{F}_{11}^{10} \ : \ x_{10} = \sum_{i=1}^{10} i x_i\} \ .$$

Como a condição $x_{10} = \sum_{i=1}^{10} i x_i$ é equivalente a $\sum_{i=1}^{10} (-i) x_i + x_{10} = 0$, a seguinte matriz

$$H = \begin{bmatrix} -1 & -2 & \cdots & -9 & 1 \end{bmatrix} = \begin{bmatrix} X & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$$

é uma matriz de paridade para $C$ e está na forma canónica $\begin{bmatrix} B & I_1 \end{bmatrix}$ com

$$B = \begin{bmatrix} X & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \end{bmatrix} \ .$$

Pelo Teorema 4.14, $G = \begin{bmatrix} I_9 & -B^T \end{bmatrix}$ é uma matriz geradora de $C$.

Usando esta matriz $G$ para codificar os vectores $m \in \mathbb{F}_{11}^9$, fica

$$x = G^T m = (m_1, \ldots, m_9, x_{10})$$

onde a última componente é dada por

$$x_{10} = -Bm = \sum_{i=1}^{9} i m_i = \sum_{i=1}^{9} i x_i$$

e esta é precisamente a condição imposta na definição do código $C$ (e também na do código ISBN). Recupera-se a mensagem original $m$ a partir da mensagem codificada $x$ apagando o dígito de verificação $x_{10}$. Em particular obtém-se

$$\text{ISBN} = \{G^T m \,:\, m \in (\mathbb{F}_{11} \setminus \{X\})^9\} \,.$$

## 4.2. Descodificação por Tabelas de Slepian

Seja $C$ um código linear $[n, k]$ sobre $\mathbb{F}_q$. Para cada vector $a \in \mathbb{F}_q^n$, definimos a *classe* ou *coconjunto* de $a$ por

$$a + C := \{a + x \,:\, x \in C\} \,. \tag{4.3}$$

**Observação 4.24.** A operação soma de vectores num espaço vectorial $V$ satisfaz todos os axiomas de um grupo abeliano. Assim, quando ignoramos a operação produto por um escalar, o que sobra é o grupo abeliano $(V, +)$. Em particular, $(\mathbb{F}_q^n, +)$ é um grupo abeliano e um código $C$ é um subgrupo $(C, +)$, necessariamente normal. Assim, fica definida uma relação de equivalência em $\mathbb{F}_q^n$ do seguinte modo: $a$ e $b$ são equivalentes se e só se $a - b \in C$, cujas classes de equivalência são precisamente os conjuntos em (4.3). Além disso, por $C$ ser um subgrupo normal de $\mathbb{F}_q^n$, as classes de equivalência formam ainda um grupo.

Em vez de usarmos a maquinaria de Teoria de Grupos, podemos simplesmente definir primeiro as classes (4.3) e provar de seguida o seguinte resultado, cuja demonstração elementar pode ser consultada em [**2**] ou em [**1**].

**Teorema 4.25.** *Sejam $a, b \in \mathbb{F}_q^n$ vectores arbitrários. Então:*

*(i) Qualquer vector $a \in \mathbb{F}_q^n$ pertence a uma classe.*

*(ii) Todas as classes contêm o mesmo número de elementos, i.e., $|a + C| = |C| = q^k$.*

*(iii) $b \in a + C$ se e só se $a + C = b + C$*

*(iv) Ou $a + C = b + C$ ou $(a + C) \cap (b + C) = \varnothing$.*

*(v) Existem precisamente $q^{n-k}$ classes distintas.*

*(vi) $a - b \in C$ se e só se $a$ e $b$ pertencem à mesma classe.*

Uma consequência directa deste teorema é o *espaço quociente*

$$\mathbb{F}_q^n / C := \{a + C \,:\, a \in \mathbb{F}_q^n\}$$

estar bem definido e conter exactamente $q^{n-k}$ classes.

A um representante da classe $a + C$ com o menor peso possível chamamos *chefe de classe*, mais precisamente,

$$c_a \in a + C \quad \text{é um chefe de classe se e só se} \quad \mathrm{w}(x) \geq \mathrm{w}(c_a) \quad \forall\, x \in a + C \ .$$

Uma classe pode conter mais do que um chefe de classe. No entanto, a classe do vector nulo $\vec{0} + C = C$ contém um único chefe de classe, nomeadamente, o próprio vector nulo.

**Exemplo 4.26.** Considere o código linear binário $C = \langle 1011, 0101 \rangle = \{0000, 1011, 0101, 1110\}$. A classe de 0001 é o conjunto

$$0001 + C = \{0001, 1010, 0100, 1110\} \ .$$

Como $\mathrm{w}(0001) = \mathrm{w}(0100) = 1$, $\mathrm{w}(1010) = 2$ e $\mathrm{w}(1110) = 3$, os vectores 0001 e 0100 são ambos chefes da classe $0001 + C$.

Considere o seguinte algoritmo de descodificação:

Recebido $y \in \mathbb{F}_q^n$, procuramos o chefe de classe $c_y \in y + C$ e descodificamos $y$ por $y - c_y$. (Caso não haja unicidade de chefes de classe, devemos indicar a priori qual o que vamos usar para o algoritmo, ou então optar por uma descodificação incompleta.)

Para aplicar este algoritmo sistematicamente, construimos uma *Tabela (Padrão) de Slepian*:

- enumeramos as plavaras de código $C = \{x^1, x^2 \ldots, x^{q^k}\}$;
- escolhemos chefes de classes $a^0 = \vec{0}$, $a^1$, $a^2$, ..., $a^{s-1}$, onde $s = q^{n-k}$ é o número de classes distintas
- escrevemos uma tabela

$$\begin{array}{rcccccc}
a^0 + C = C: & x^1 & x^2 & \cdots & x^j & \cdots & x^{q^k} \\
a^1 + C: & a^1 + x^1 & a^1 + x^2 & \cdots & a^1 + x^j & \cdots & a^1 + x^{q^k} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
a^i + C: & a^i + x^1 & a^i + x^2 & \cdots & a^i + x^j & \cdots & a^i + x^{q^k} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
a^{s-1} + C: & a^{s-1} + x^1 & a^{s-1} + x^2 & \cdots & a^{s-1} + x^j & \cdots & a^{s-1} + x^{q^k}
\end{array}$$

$\left.\rule{0pt}{3em}\right\} s = q^{n-k}$ linhas

$\underbrace{\rule{12em}{0pt}}_{q^k \text{ colunas}}$

Note que nesta tabela encontram-se todos os vectores de $\mathbb{F}_q^n$, sem repetições, e na primeira linha encontram-se as palavras do código $C$. Assim, o algoritmo de descodificação também pode ser descrito da seguinte maneira:

| Recebido um vector $y \in \mathbb{F}_q^n$, encontrar a sua posição na Tabela de Slepian, i.e., encontrar a entrada $(i, j)$ tal que $y = a^i + x^j$, assumir o erro $a^i$ e descodificar $y$ por $y - a^i = x^j \in C$. |
|---|

Estamos a assumir que o erro ocorrido é o chefe de classe $a^i$ que, por definição, tem peso mínimo entre os elementos da sua classe. Portanto, ao usarmos este algoritmo, estamos a descodificar por distância mínima. Conclui-se também que os vectores erro que este algoritmo permite corrigir são precisamente os chefes de classe escolhidos $a^1$, $a^2$, ..., $a^{s-2}$ e $a^{s-1}$.

**Exemplo 4.27.** Continuando com o Exemplo 4.26, sejam $x^0 = 0000$, $x^1 = 1011$, $x^2 = 0101$ e $x^3 = 1110$ as quatro palavras do códiogo $C$, que formam a primeira linha duma Tabela de Slepian. Para escrevermos a segunda linha, temos de esolher uma palavra de peso mínimo em $\mathbb{F}_2^4 \backslash C$. Qualquer palavra de peso 1 serve. Por exemplo, pondo $a^1 = 0001$, a segunda linha da tabela fica

$$0001 + C: \quad 0001 \quad 1010 \quad 0100 \quad 1111$$

Para a próxima linha, escolhemos para $a^2$ uma palavra de peso mínimo entre os vectores de $\mathbb{F}_q^n$ que ainda não aparecem em nenhuma das linhas anteriores já escritas. Continuando este procedimento, obtemos a seguinte Tabela de Slepian:

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

(Outra possível Tabela de Slepian, seria escolhermos 0100 para chefe da classe $0001 + C$. Nas outras três classes, há apenas uma escolha possível.)

Para descodificar a palavra recebida $y = 1101$, localizamos $y = 1000 + 0101 = a^3 + x^2$ na tabela e descodificamo-la pela palavra no topo da coluna correspondente, neste caso por $x^2 = 0101$.

Como se pode imaginar, construir uma Tabela de Slepian é um procedimento moroso e não muito prático se $\mathbb{F}_q^n$ contiver um número elevado de palavras. No entanto, sabermos quais são os chefes de classe (que corresponde a ter a primeira coluna da tabela, se escolhermos $x^0 = \vec{0}$) já nos dá alguma informação sobre a distância mínima do código. No exemplo acima, sabendo apenas que os chefes de classe não nulos são $a^1 = 0001$, $a^2 = 0010$ e $a^3 = 1000$ e têm todos peso 1, mas não incluem todos os vectores de $\mathbb{F}_2^4$ com este peso, já nos permite concluir que a distância mínima do código é $\mathrm{d}(C) < 3$, pois o código não corrige todos os erros de peso 1.

**Proposição 4.28.** *Se* $\mathrm{d}(C) = d$*, então todas as palavras de peso menor ou igual a* $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ *são chefes de classes distintas.*

Deixamos a demostração desta proposição como exercício. Resolva também o Exercício 4.5.

### 4.2.1. Probabilidade de descodificação correcta e de detecção de erros

Seja $C$ um código linear binário e considere um canal de transmissão binário simétrico, com probabilidade de troca de símbolos $p < \frac{1}{2}$. A probabilidade de ocorrer um vector erro $\vec{e}$ de peso $\mathrm{w}(\vec{e}) = i$ é $p^i(1-p)^{n-i}$, pois ocorreram precisamente $i$ trocas de símbolos. Seja

$$\alpha_i = \#\{\text{chefes de classe } a^j \text{ com peso } \mathrm{w}(a^j) = i\} \ . \tag{4.4}$$

Portanto, a probabilidade de descodificar correctamente (ver (1.9)) a palavra recebida $y$ pela palavra de código de facto enviada é

$$P_{corr}(C) = \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i} \ ,$$

pois corresponde à probabilidade do vector erro ser um chefe de classe. Note que $P_{corr}(C)$ apenas depende dos chefes de classe. Em relação ao número destes, temos o seguinte resultado.

**Proposição 4.29.** *Seja* $t = \lfloor \frac{\mathrm{d}(C)-1}{2} \rfloor$. *Então* $\alpha_i = \binom{n}{i}$, *para qualquer* $0 \leq i \leq t$.

Suponhamos agora que o código $C$ é usado apenas para detecção de erros. Se $x \in C$ é a palavra enviada e $y$ é a palavra recebida, o vector erro $\vec{e} = y - x$ não é detectado se e só se $y \in C \setminus \{x\}$, o que é ainda equivalente a $\vec{e} \in C \setminus \{\vec{0}\}$. Portanto a probabilidade de não se detectar um erro não depende da palavra enviada $x$ e é dada por

$$P_{undetec}(C) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i} \ ,$$

onde

$$A_i = \#\{x \in C \ : \ \mathrm{w}(x) = i\} \ . \tag{4.5}$$

A *probabilidade de detecção de erros* é então dada por $P_{detec}(C) = 1 - P_{undetec}(C)$.

## 4.3. Descodificação por síndrome

A descodificação por síndrome é também um método de descodificação por distância mínima, é equivalente ao algoritmo usando um Tabela de Slepian, mas muitíssimo mais eficiente.

Fixemos um código linear $C$, de parâmetros $[n,k]_q$, com matriz de paridade $H$.

**Definição 4.30.** O *sintoma* de $x \in \mathbb{F}_q^n$ é o vector $S(x) = Hx$.

Como habitualmente, identificamos um vector $x$ com a matriz coluna cujas entradas são as coordenadas de $x$.

**Lema 4.31.** *Dois vectores* $x, y \in \mathbb{F}_q^n$ *têm o mesmo sintoma se e só se pertencem à mesma classe de* $C$, *i.e.,* $S(x) = S(y)$ *sse* $x + C = y + C$.

**Dem.** $S(x) = S(y) \Leftrightarrow Hx = Hy \Leftrightarrow H(x-y) = \vec{0} \Leftrightarrow x - y \in \mathcal{N}(H) = C \Leftrightarrow x + C = y + C$. □

Por definição, a aplicação

$$\begin{aligned} S : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^{n-k} \\ x &\longmapsto S(x) = Hx \end{aligned}$$

é uma aplicação linear. O lema anterior garante que esta aplicação $S$ induz uma aplicação $\tilde{S}$ (necessariamente linear) no espaço quociente $\mathbb{F}_q^n/C$

$$\begin{aligned} \tilde{S} : \mathbb{F}_q^n/C &\longrightarrow \mathbb{F}_q^{n-k} \\ x + C &\longmapsto S(x) = Hx \end{aligned}$$

e que $\tilde{S}$ é injectiva. Como $\mathbb{F}_q^n/C$ contém precisamente $q^{n-k}$ classes distintas, então $\tilde{S}$ também é sobrejectiva, logo é bijectiva, i.e., $\tilde{S}$ é um isomorfismo de espaços lineares.

Portanto, para definir um algoritmo de descodificação é preciso determinar a aplicação inversa de $\tilde{S}$ e escolher um representante de cada classe $x + C$ (estes representantes vão ser os erros corrigidos

pelo algoritmo), por exemplo, os chefes de classe $a^i$ também usados nas Tabelas de Slepian. Para facilitar a desodificação, começamos por escrever uma *tabela de síndrome*:

| $a^i$ | $S(a^i)$ |
|---|---|
| $a^0 = \vec{0}$ | $S(a^0) = \vec{0}$ |
| $a^1$ | $S(a^1)$ |
| $\vdots$ | $\vdots$ |
| $a^{s-1}$ | $S(a^{s-1})$ |

onde $s = q^{n-k}$ é o número de classes distintas e $a^0 = \vec{0}, a^1, \ldots, a^{s-1}$ são chefes de classe. O algoritmo de *descodificação por síndrome* é o seguinte

> Recebido um vector $y \in \mathbb{F}_q^n$, calcular o sintoma $S(y)$, determinar o chefe de classe $a^i$ tal que $S(y) = S(a^i)$, assumir o erro $a^i$ e descodificar $y$ por $y - a^i = x^j \in C$.

**Exemplo 4.32.** Considere novamente o código linear $C = \langle 1011, 0101 \rangle$ do Exemplo 4.27. Já determinámos chefes de classe $a^0 = 0000$, $a^1 = 0001$, $a^2 = 0010$ e $a^3 = 1000$. Agora precisamos de uma matriz de paridade para calcularmos os sintomas. Como a matriz geradora

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

está na forma canónica, conclui-se imediatamente que

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

é uma matriz de paridade para $C$. A tabela de síndrome fica então

| $a^i$ | $S(a^i)$ |
|---|---|
| 0000 | 00 |
| 0001 | 01 |
| 0010 | 10 |
| 0100 | 11 |

(Note que na coluna dos sintomas $S(a^i)$ aparecem exactamente os quatro vectores em $\mathbb{F}_2^4$.) Seja $y = 0110$ a palavra recebida. Como $S(0110) = 11 = S(1000)$, descodificamos $y$ por $y - 1000 = 1110 \in C$.

Por vezes não é necessário escrevermos a tabela de síndrome para aplicarmos o algoritmo.

**Exemplo 4.33.** Seja $C$ o código linear sobre $\mathbb{F}_{11} = \{0, 1, 2, \ldots, 9, X\}$ com a seguinte matriz de paridade

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & X \end{bmatrix}$$

A coluna $i$ de $H$ é $c_i = \begin{bmatrix} 1 & i \end{bmatrix}^T$, portanto

$$\det \begin{bmatrix} | & | \\ c_i & c_j \\ | & | \end{bmatrix} = \det \begin{bmatrix} 1 & 1 \\ i & j \end{bmatrix} = j - i \neq 0 \quad \forall i \neq j$$

donde concluimos que quaisquer duas colunas distintas são linearmente independentes. Como as colunas de $H$ são vectores em $\mathbb{F}_{11}^2$, quaisquer três colunas são linearmente dependentes (bastava haver três colunas linearmente dependentes). Aplicando o Teorema 4.16, obtêm-se que $\mathrm{d}(C) = 3$ e, portanto, o código $C$ pode ser usado para corrigir qualquer erro simples de troca de símbolos.

Vamos ver que, usando uma descodificação incompleta, para além de corrigir os erros simples, $C$ também permiter detectar os erros duplos de transposição.

Seja $x = (x_1, \ldots, x_{10}) \in C$ a palavras transmitida, e seja $y = (y_1, \ldots, y_{10}) \in \mathbb{F}_{11}^{10}$ a palavra recebida. No caso de ocorrer um erro simples, então $y = x + (0, \ldots, 0, k, 0, \ldots, 0)$ com $k \in \mathbb{F}_{11} \setminus \{0\}$ na coordenada $j$. Pondo

$$A = \sum_{i=1}^{10} y_i \qquad \text{e} \qquad B = \sum_{i=1}^{10} i y_i$$

fica $S(y) = (A, B)$. No caso particular do vector recebido, ainda fica

$$A = \sum_{i=1}^{10} x_i + k = k \qquad \text{e} \qquad B = \sum_{i=1}^{10} i x_i + jk = jk$$

porque $S(x) = 0$. Portanto ambas as compomentes do sintoma $S(y)$ são não nulas e podemos ainda concluir que que ocorreu um erro de amplitude $k = A$ na coordenada $j = BA^{-1}$.

No caso de ocorrer um erro de transposição, o vector recebido é

$$y = (x_1, \ldots, x_{j-1}, x_k, x_{j+1}, \ldots, x_{k-1}, x_j, x_{k+1}, \ldots, x_{10})$$

para algum par de coordenadas $1 \leq j < k \leq 10$, com $x_j \neq x_k$ na palavra enviada (se $x_k = x_j$ e se permutarmos as coordenadas $j$ e $k$, não alteramos o vector $x$). Portanto, as coordenadas do sintoma $S(y)$ são agora dadas por

$$A = \sum_{i=1}^{10} y_i = \sum_{i=1}^{10} x_i = 0 \qquad \text{e}$$
$$B = \sum_{i=1}^{10} i y_i = \sum_{i=1}^{10} i x_i + (j x_k + k x_j) - (j x_j + k x_k) = (k - j)(x_j - x_k) \neq 0$$

Portanto, $S(y) = (0, B)$ com $B \neq 0$, mas não conseguimos determinar o tipo de erro ocorrido apenas conhecendo o valor de $B$.

Acabámos de provar que o seguinte algoritmo de descodificação incompleta corrige erros simples e detecta erros duplos de transposição:

1. Recebido $y \in \mathbb{F}_{11}^{10}$, calcular o sintoma $S(y) = (A, B) \in \mathbb{F}_{11}^2$.
2. Se $(A, B) = (0, 0)$, então assumir que não ocorreram erros de tansmissão e descodificar a palavra $y$ por ela própria, uma vez que $y \in C$.
3. Se $A \neq 0$ e $B \neq 0$, assumir que ocorreu um erro simples na posição $j = BA^{-1}$ de amplitude $A$, e descodificar $y$ por $y - (0, \ldots, 0, A, 0, \ldots, 0)$ ($A$ na coordenada $j$).
4. Se $A \neq 0$ ou $B \neq 0$ (mas não $A \neq 0$ e $B \neq 0$), assumir pelo menos dois erros e pedir retransmissão.

## Exercícios

4.1. Resolver a Ficha 4.

4.2. Seja $C$ um código linear $[n, k]$ sobre $\mathbb{F}_q$. Para cada $i \in \{1, \ldots, n\}$ fixo, mostre que, ou $x_i = 0$ para todo o $x = (x_1, \ldots, x_n) \in C$, ou o número de palavras em $C$ com $x_i = a$, para $a \in \mathbb{F}_q$ fixo, é $\frac{|C|}{q} = q^{k-1}$.

4.3. Seja $C$ um código linear binário de comprimento $n \geq 4$. Seja $H$ uma matriz de paridade para $C$ tais que as colunas de $H$ são todas distintas e têm todas peso ímpar. Prove que $\mathrm{d}(C) \geq 4$.

4.4. Demostre a Proposição 4.28.

4.5. Seja $C$ um código linear perfeito de distância mínima $\mathrm{d}(C) = 2t + 1$. Numa Tabela de Slepian para o código $C$, quais são os chefes de classe?

4.6. Demonstre a Proposição 4.29. Mostre ainda que, no caso de um código perfeito, também se tem que $\alpha_i = 0$ para qualquer $i > t$.

4.7. (a) Quantas palavras do código ISBN terminam no símbolo $X \in \mathbb{F}_{11}$?
(b) Quantas palavras do código ISBN terminam no símbolo $a \in \{0, 1, \ldots, 9\} \subset \mathbb{F}_{11}$?
(c) Seja $C$ o código linear sobre $\mathbb{F}_{11}$ definido no Exemplo 4.33 e seja $C' \subset C$ o subcódigo definido por

$$C' = \{x \in C : x_i \neq X \quad \forall\, i = 1, \ldots, 10\} .$$

Mostre que $|C'| = 82644629$.

[Sugestão: use o princípio de inclusão-exclusão e o resultado do Exerício 4.2.]