CAPÍTULO 5

Construção de Códigos

Alguns casos particulares das contruções apresentadas neste capítulo já têm sido usadas, quer em demonstrações, quer em exemplos. Começamos por apresentar construções envolvendo um código apenas (Secções 1 a 5), as restantes envolvem dois códigos ou mais.

1. Extensão

Dado um código C de parâmetros $(n, M, d)_q$, linear ou não, constrói-se um novo código $\widehat{C}$ de parâmetros $(n+s, M, \widehat{d})_q$ acrescentando s componentes a cada uma das palavras de C, podendo estas s componentes ser definidas à custa das n primeiras. $\widehat{C}$ diz-se uma *extensão* de C.

Um caso particular importante é a *extensão por paridade* de C, usada na demonstração do Teorema 2.9 para códigos binários. Para códigos q-ários a definição é a seguinte

$$\widehat{C} = \{(x_1, \ldots, x_n, x_{n+1}) : (x_1, \ldots, x_n) \in C, \quad \sum_{i=1}^{n+1} x_i \equiv 0 \pmod{q}\} ,$$

onde a ditância mínima de $\widehat{C}$ satisfaz $d \leq \widehat{d} \leq d+1$.

No caso de C ser um código binário linear $[n, k, d]$, a extensão por paridade $\widehat{C}$ tem parâmetros $[n+1, k, \widehat{d}]$, com $\widehat{d}$ par e matriz de paridade

$$\widehat{H} = \left[\begin{array}{ccc|c} & & & 0 \\ & H & & \vdots \\ & & & 0 \\ \hline 1 & \cdots & 1 & 1 \end{array}\right] , \tag{5.1}$$

onde H é uma matriz de paridade para C.

Exemplo 5.1. A extensão por paridade do código binário $\mathbb{F}_2^n$ é o código dos pesos pares

$$E_{n+1} = \{x \in \mathbb{F}_2^{n+1} : \mathrm{w}(x) \text{ é par}\} \subseteq \mathbb{F}_2^{n+1} .$$

Como consequência, temos o seguinte lema.

Lema 5.2. *Seja C código binário, de comprimento n, com $\mathrm{d}(C) = d$ ímpar. Então a extensão por paridade $\widehat{C} \subseteq E_{n+1}$ tem distância mínima $\mathrm{d}(\widehat{C}) = d + 1$.*

Dem. Basta observar que $C \subseteq \mathbb{F}_2^n$ e que a extensão $\widehat{C}$ tem distância par, pois $\widehat{C} \subseteq E_{n+1}$. □

Como exemplos, iremos ver no Capítulo 6 a extensão por paridade dos códigos de Hamming binários.

2. Pontuação

Dado um código C de parâmetros $(n, M, d)_q$, contrói-se outro código $\mathring{C}$ com parâmetros $(n-s, M, \mathring{d})_q$ eliminando $s < d$ componentes a cada uma das palavras de C, portanto $\mathring{d} \leq d$. Ao código $\mathring{C}$ assim obtido chamados o *pontuado* de C.

Esta construção já foi usada na demonstração do Teorema 2.9, com $s = 1$, e também para provar a desigualdade de Singleton, Proposição 2.11, com $s = d - 1$.

No caso de C ser um código linear $[n, k, d]_q$ com matriz geradora G, o pontuado $\mathring{C}$ é ainda linear e obtem-se uma matriz geradora $\mathring{G}$ para $\mathring{C}$ apagando as s colunas correspondentes às s componentes eliminadas.

No Capítulo 6, iremos definir os códigos de Golay G_{23} e G_{11} como os pontuados na última componente de G_{24} e G_{12}, respectivamente.

3. Expansão

Dado o código C de parâmetros $(n, M, d)_q$, obtém-se um novo código $\overline{C}$ com parâmetros $(n, \overline{M}, \bar{d})_q$, acrescentando palavras a C. Portanto $\overline{M} \geq M$ e $\bar{d} \leq d$.

Exemplo 5.3. Seja C um código binário (n, M, d) e defina-se o código complementar

$$C^c = \{x^c \stackrel{\text{def}}{=} \vec{1} - x \,:\, x \in C\} \,,$$

onde $\vec{1}$ denota o vector com todas as componentes iguais a 1. Por exemplo, com $x = 01011$, o vector "complementar" é $x^c = 10100$. Ou seja, obtém-se C^c trocando os 0 e os 1 em todas as palavras de C. Seja $\overline{C} = C \cup C^c$. Este código $\overline{C}$ tem parâmetros $(n, \overline{M}, \bar{d})$ com $\overline{M} \leq 2M$, mais precisamente

$$\overline{M} = 2M - |C \cap C^c| \qquad \text{e} \qquad \bar{d} = \min\{d, n - \max\{d(x, y) \,:\, x, y \in C,\, x \neq y^c\}\} \,. \tag{5.2}$$

No caso de C ser um código linear $[n, k, d]_q$, uma extensão de C é um subespaço $\overline{C} \subseteq \mathbb{F}_q^n$ que contenha C. Se G é uma matriz geradora de C, obtém-se uma uma matriz gerador $\overline{G}$ de $\overline{C}$ acrescentado linhas a G, mais precisamente, dada uma base $\mathcal{B} = \{v_1, \ldots, v_k\}$ de C, completa-se $\mathcal{B}$ para obter uma base $\bar{\mathcal{B}} = \{v_1, \ldots, v_k, w_1, \ldots, w_l\}$ para $\overline{C}$.

Exemplo 5.4. Considere o código binário $C = \{000000, 010010, 001100, 011110\}$. Este código é linear e uma base pode ser, por exemplo, $\{010010, 001100\}$. O código complementar de C é $C^c = \{111111, 101101, 110011, 100001\}$, que não é linear pois não contém o vector nulo. A reunião deste dois códigos é

$$C \cup C^c = \{000000, 010010, 001100, 011110, 111111, 101101, 110011, 100001\}$$

e tem parâmetros $(8, 8, 2)$, pois $\mathrm{d}(C) = 2$. Note que, neste caso, $C \cup C^c$ é um código linear e

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

é uma matriz geradora — justifique.

4. Eliminação ou Subcódigos

Dado um código C de parâmetros $(n, M, d)_q$, eliminando palavras em C obtém-se um novo código $\underline{C}$ de parâmetros $(n, \underline{M}, \underline{d})_q$. Portanto $\underline{M} \leq M$ e $\underline{d} \geq d$. $\underline{C}$ diz-se um subcódigo de C.

Exemplo 5.5. (i) As *secções* de C

$$C_{i,a} = \{x = (x_1, \ldots, x_n) \in C \,:\, x_i = a\}\,, \tag{5.3}$$

com $i \in \{1, \ldots, n\}$ e $a \in \mathcal{A}_q$ fixos, são subcódigos de C.

(ii) O código ISBN é obtido do código linear C, sobre $\mathbb{F}_{11}$, com matriz de paridade

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

usando eliminação — ver Exemplo 4.23. No entanto, o código ISBN não é uma secção de C.

No caso linear, a eliminação corresponde a tomar um subespaço $\underline{C}$ de C.

Atenção! Uma matriz geradora de $\underline{C}$ não é necessariamente obtida de uma matriz geradora de C apagando linhas.

Exemplo 5.6. Seja C um código linear. Então $C_{i,0} = \{x \in C \,:\, x_i = 0\}$ são as únicas secções de C que ainda são códigos lineares (as outras secções não contêm o vector nulo), e

$$\dim C - 1 \leq \dim C_{i,0} \leq \dim C \qquad \forall\, i.$$

Exemplo 5.7. Seja C o código binário com matriz geradora

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

Vamos determinar uma matriz geradora $\underline{G}$ para a secção $C_{6,0} = \{x \in C \,:\, x_6 = 0\}$. Note que, se apagarmos as linhas de G que não estão em $C_{6,0}$, obteriamos uma matriz linha geradora de um código de dimensão 1, que não é $C_{6,0}$, pois esta secção é um espaço vectorial de dimensão 2 (justifique).

Como G está na forma canónica $\begin{bmatrix} I & A \end{bmatrix}$, então

$$H = \begin{bmatrix} -A^T & I \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

é uma matriz de paridade para C. A condição $x_6 = 0$ traduz-se numa linha $\begin{bmatrix} 0 & \cdots & 0 & 1 \end{bmatrix}$, donde

$$\underline{H} = \left[\begin{array}{c} H \\ \hline 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \end{array}\right] = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

é uma matriz de paridade para $C_{6,0}$, se as suas linhas forem linearmente independentes. Aplicando o método de eleminação de Gauss a $\underline{H}$ para tentar obter uma forma canónica:

$$\underline{H} \xrightarrow{l_3 \mapsto l_3 + l_4} \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{\substack{\text{permutar} \\ \text{linhas}}} \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{l_3 \mapsto l_3 + l_1} \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

logo podemos concluir que as 4 linhas de $\underline{H}$ são linearmente independentes e que

$$\underline{G} = \begin{bmatrix} I_2 & -B^T \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

é uma matriz geradora de $C_{6,0}$.

5. Contracção

Uma contração de um código C é obtida aplicando as construções de eliminação e pontuação. Um exemplo importante é a pontuação de uma secção, que passamos a descrever.

Dado um código C de parâmetros $(n, M, d)_q$, pontuando na componente i da secção $C_{i,a}$ de C (definida em (5.3)), obtém-se um *código contraído* C' de parâmetros $(n-1, M', d')_q$ com $M' \leq M$ e $d' \geq d$.

No caso de um código linear $[n, k, d]_q$, a secção $C_{i,a}$ (com $i \in \{1, \ldots, n\}$ e $a \in \mathbb{F}_q$ fixos) não é necessariamente um subespaço vectorial de C, mas contém q^{k-1} palavras se $C \neq C_{i,0}$ (consequência do Exercício 4.2). Supondo então que $C_{i,0} \neq C$, $C_{i,a}$ é um código de parâmetros $(n, q^{k-1}, d')_q$ com $d' \geq d$. Pontuando $C_{i,a}$ na componente i, obtemos um código linear C' de parâmetros $[n-1, k-1, d']_q$ e uma matriz de paridade para C' pode ser obtida apagando a coluna i de uma matriz de paridade para C — justifique!

Usando várias das contruções que definimos até agora, podemos provar o seguinte teorema.

Teorema 5.8. *Se existe um código linear de parâmetros $[n, k, d]_q$, então também existe um código linear de parâmetros $[n + r, k - s, d - t]_q$, para quaisquer $r \geq 0$, $0 \leq s \leq k - 1$ e $0 \leq t \leq d$.*

Dem. Seja C um código $[n,k,d]_q$.
(i) Fixemos $r \geq r$. Usando extensão por zeros, ou seja, acrescentando r componentes todas nulas a cada palavra do código C, obtemos um novo código de parâmetros $[n+r,k,d+r]_q$.
(ii) Fixemos $0 \leq s \leq k-1$. Seja $x \in C$ uma palavra com peso $\mathrm{w}(x) = d = \mathrm{d}(C)$. Seja $\{v_1, v_2, \ldots, v_k\}$ uma base de C com $v_1 = x$. Então o subespaço $C' = \langle v_1, \ldots, v_{k-s} \rangle \subseteq C$ é um código $[n, k-s, d]_q$. Para justificar que $\mathrm{d}(C') = d$, basta observar que $x \in C'$ pois $k - s \geq 1$.
(iii) Fixemos $0 \leq t \leq d-1$. Seja $x \in C$ com peso $\mathrm{w}(x) = d = \mathrm{d}(C)$. Pontuando em t componentes $1 \leq i_1 < i_2 < \cdots < i_t \leq n$ tais que $x_{i_k} \neq 0$ para $k = 1, \ldots, t$ (que existem porque $t \leq d-1 < \mathrm{w}(x)$), obtemos um código $\overset{\circ}{C}$ de parâmetros $[n-t, k, d-t]_q$. Aplicando agora a alínea (i) desta demonstração ao código $\overset{\circ}{C}$ com $r = t$, obtemos um código de parâmetros $[n,k,d-t]_q$. □

6. Soma directa

Dados dois códigos q-ários C_1 e C_2 de parâmetros (n_1, M_1, d_1) e (n_2, M_2, d_2), respectivamente, define-se o *código soma* por

$$C_{1\oplus 2} = C_1 \oplus C_2 = \{(x_1, x_2) \,:\, x_1 \in C_1,\, x_2 \in C_2\} \ .$$

Portanto, o código soma contém $M_1 M_2$ palavras de comprimento $n_1 + n_2$.

Lema 5.9. *A distância mínima de $C_1 \oplus C_2$ é $d = \min\{d_1, d_2\}$.*

Dem. Sem perda de generalidade, suponhamos que $d_1 \leq d_2$. Sejam $x_1, y_1 \in C_1$ tal que $\mathrm{d}(x_1, y_1) = d_1 = \mathrm{d}(C_1)$ e seja $x_2 \in C_2$. Como $(x_1, x_2), (y_1, x_2) \in C_{1\oplus 2}$, então

$$\mathrm{d}(C_{1\oplus 2}) \leq \mathrm{d}((x_1, x_2), (y_1, x_2)) = \mathrm{d}(x_1, y_1) \leq d_1 \ .$$

Por outro lado, para quaisquer palavras $(x_1, x_2), (y_1, y_2) \in C_{1\oplus 2}$ distintas , tem-se

$$\begin{aligned} \mathrm{d}((x_1, x_2), (y_1, y_2)) &\geq \mathrm{d}(x_1, y_1) \geq d_1 && \text{se } x_1 \neq y_1 \ , \\ \mathrm{d}((x_1, x_2), (y_1, y_2)) &\geq \mathrm{d}(x_2, y_2) \geq d_2 \geq d_1 && \text{se } x_2 \neq y_2 \ , \end{aligned}$$

portanto, tomando o mínimo entre pares de palavras distintas, $\mathrm{d}(C_{1\oplus 2}) \geq d_1$. □

No caso de C_1 e C_2 serem códigos lineares de parâmetros $[n_1, k_1, d_1]_q$ e $[n_2, k_2, d_2]_q$, respectivamente, $C_1 \oplus C_2$ é a soma directa de espaços vectoriais, portanto é ainda um espaço vectorial. Como $|C_1 \oplus C_2| = M_1 M_2 = q^{k_1+k_2}$, conclui-se que $\dim(C_1 \oplus C_2) = k_1 + k_2$. Resolva o Exercício 5.4 para obter uma matriz geradora de $C_1 \oplus C_2$ à custa de matrizes geradoras de C_1 e C_2.

7. Construção de Plotkin

Dados dois códigos q-ários C_1 e C_2 de parâmetros (n, M_1, d_1) e (n, M_2, d_2), respectivamente, define-se um novo código por[1]

$$C_{1*2} = C_1 * C_2 = \{(x, x+y) \,:\, x \in C_1,\, y \in C_2\} \ .$$

[1]Embora não se exija que C_1 e C_2 sejam lineares, a definição da construção de Plotkin assume que esteja definida uma operação soma no alfabeto dos códigos.

Os parâmteros de $C_1 * C_2$ são $(2n, M_1M_2, d)$, onde $d = \min\{2d_1, d_2\}$ — a distância mínima foi calculada na Ficha 2.

No caso de C_1 e C_2 serem códigos lineares, então a construção de Plotkin C_{1*2} também é um código linear: basta verificar o fecho da soma de vectores e do produto de um vector por um escalar, pois C_{1*2} é um subconjunto do espaço vectorial $\mathbb{F}_q^{2n}$. Para matrizes geradora e de paridade, resolva o Exercício 5.5.

Exemplo 5.10. Seja $C_1 = E_2 = \{x \in \mathbb{F}_2^3 : \mathrm{w}(x) \text{ é par}\}$ e seja C_2 o código de repetição binário de comprimento 3. Então $C_1 = \langle 110, 101\rangle$ e $C_2 = \langle 111\rangle$ têm parâmetros $[3, 2, 2]$ e $[3, 1, 3]$, respectivamente. Portanto, $\{110110, 101101, 000111\}$ é uma base de $C_1 * C_2$ — justifique — e os parâmetros deste código são $[6, 3, 3]$.

8. Concatenação

Definimos concatenação apenas no caso linear.

Recorde que o corpo $\mathbb{F}_{q^m}$ é um espaço vectorial de dimensão m sobre $\mathbb{F}_q$. Se $f(t) \in \mathbb{F}_q[t]$ é um polinómio irredutível de grau m, então $\mathbb{F}_{q^m} = \mathbb{F}_q[t]/\langle f(t)\rangle$. Se $\alpha \in \mathbb{F}_{q^m}$ é uma raiz de $f(t)$ então ainda podemos escrever

$$\mathbb{F}_{q^m} = \mathbb{F}_q[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} : a_i \in \mathbb{F}_q\} .$$

Portanto, a aplicação

$$\begin{aligned} \phi : \mathbb{F}_{q^m} &\longrightarrow (\mathbb{F}_q)^m \\ a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} &\longmapsto (a_0, a_1, \ldots, a_{m-1}) \end{aligned} \tag{5.4}$$

é um isomorfismo linear sobre $\mathbb{F}_q$, i.e., ϕ é uma aplicação linear bijectiva. Recorde ainda que $\{1, \alpha, \ldots, \alpha^{m-1}\}$ é uma base de $\mathbb{F}_{q^m}$ como espaço vectorial sobre $\mathbb{F}_q$, por isso, para definir ϕ, basta dar $\phi(\alpha^i) = \vec{e}_{i+1}$, com $i \in \{0, 1, \ldots, m-1\}$, onde $\vec{e}_j \in \mathbb{F}_q^m$ é o vector com 1 na componente j e 0 nas restantes. Seja ϕ^* a aplicação definida por

$$\begin{aligned} \phi^* : \overbrace{\mathbb{F}_{q^m} \times \cdots \mathbb{F}_{q^m}}^{N \text{ vezes}} = \mathbb{F}_{q^m}^N &\longrightarrow (\mathbb{F}_q^m)^N = \mathbb{F}_q^{mN} \\ x = (x_1, \ldots, x_N) &\longmapsto (\phi(x_1), \ldots, \phi(x_N)) \end{aligned} \tag{5.5}$$

Então ϕ^* também é uma aplicação linear sobre $\mathbb{F}_q$. Além disso, usando apenas a injectividade de ϕ, tem-se

$$\phi^*(x_1, \ldots, x_n) = 0 \iff \phi(x_i) = 0 \ \forall i \iff x_i = 0 \ \forall i \iff (x_1, \ldots, x_n) = 0 ,$$

portanto ϕ^* é injectiva.

1º caso: concatenação com um código trivial

Seja A um código linear $[N, K, D]$ sobre $\mathbb{F}_{q^m}$. Em particular A é um subespaço vectorial de $\mathbb{F}_{q^m}^N$ e podemos aplicar ϕ^* às palavras de A. Seja

$$A^* := \phi^*(A) = \{(\phi(c_1), \phi(c_2), \ldots, \phi(c_N)) : (c_1, \ldots, c_N) \in A\} .$$

A^* diz-se a *concatenação* de A com o código trivial $\mathbb{F}_q^m$. Como A é um código linear e ϕ^* é uma aplicação linear sobre $\mathbb{F}_q$, a concatenação $A^* = \phi^*(A)$ é ainda um código linear (a imagem de um subespaço vectorial por uma aplicação linear é um espaço vectorial).

Exemplo 5.11. Com a notação já habitual que temos vindo a usar, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ onde α é uma raiz do polinómio $1 + t + t^2 \in \mathbb{F}_2[t] \subset \mathbb{F}_4[t]$, ou seja, $\alpha^2 = 1 + \alpha$. A aplicação $\phi : \mathbb{F}_4 \longrightarrow \mathbb{F}_2^2$ é definida por

$$\phi(0) = 00\ , \qquad \phi(1) = 10\ , \qquad \phi(\alpha) = 01 \qquad \text{e} \qquad \phi(\alpha^2) = \phi(1 + \alpha) = 11\ .$$

Atendendo a que $\{1, \alpha\}$ é uma base de $\mathbb{F}_4$ como espaço vectorial sobre $\mathbb{F}_2$, bastava indicar $\phi(1)$ e $\phi(\alpha)$ para definir a aplicação linear ϕ.

Seja A o código de repetição binário de comprimento 3 sobre $\mathbb{F}_4$. A concatenação de A com $\mathbb{F}_2^2$ é o código binário

$$A^* = \phi^*(A) = \{000000, 010101, 101010, 111111\} = \langle 010101, 101010\rangle\ . \tag{5.6}$$

Exemplo 5.12. Ainda sobre $\mathbb{F}_4$ como no exemplo anterior, considere o código

$$A = \langle (1, \alpha, \alpha^2)\rangle = \{(0, 0, 0), (1, \alpha, \alpha^2), (\alpha, \alpha^2, 1), (\alpha^2, 1, \alpha)\}\ .$$

A concatenação de A é o código binário

$$A^* = \phi^*(A) = \{000000, 100111, 011110, 111001\} = \langle 100111, 011110\rangle\ . \tag{5.7}$$

2º caso: concatenação de dois códigos

Consideremos dois códigos lineares: um código A de parâmetros $[N, K, D]$ sobre $\mathbb{F}_{q^m}$ e um código B de parâmetros $[n, m, d]$ sobre $\mathbb{F}_q$. Como $\dim B = m = \dim \mathbb{F}_{q^m}$, então B e $\mathbb{F}_{q^m}$ são isomorfos como espaços vectoriais sobre $\mathbb{F}_q$. Fixemos, então um isomorfismo linear

$$\phi : \mathbb{F}_{q^m} \longrightarrow B$$

e seja ϕ^* a aplicação definida como em (5.5) à custa deste ϕ. Portanto ϕ^* é $\mathbb{F}_q$-linear, injectiva, e, como $\phi(x_i) \in B$ para qualquer $x_i \in \mathbb{F}_{q^m}$, a sua imagem é um subespaço de B^N.

Como o código A é um subespaço vectorial de $\mathbb{F}_{q^m}^N$ sobre $\mathbb{F}_{q^m}$ e como este corpo é um espaço vectorial sobre $\mathbb{F}_q$, então A é também um subespaço vectorial sobre $\mathbb{F}_q$ (trata-se de um caso particular do Exercício 5.7) e, portanto, $\phi^*(A)$ é um subespaço de $\mathbb{F}_q^{mN}$ sobre $\mathbb{F}_q$ porque ϕ^* é uma aplicaçao $\mathbb{F}_q$-linear.

Definição 5.13. Dado o *código exterior* A de parâmetros $[N, K, D]$ sobre $\mathbb{F}_{q^m}$ e o *código interior* B de parâmetros $[n, m, d]$ sobre $\mathbb{F}_q$, e um isomorphismo vectorial $\phi : \mathbb{F}_{q^m} \longrightarrow B$, o código linear $C = \phi^*(A)$ diz-se a *concatenação* de A e B.

Exemplo 5.14. Seja $\mathbb{F}_8 = \mathbb{F}_2[t]/\langle 1 + t + t^3\rangle = \mathbb{F}[\alpha]$, onde α é uma raiz do polinómio $1 + t + t^3$. Seja A o código linear sobre $\mathbb{F}_8$ gerado pelo vector $(1, \alpha) \in \mathbb{F}_8^2$, e seja $B = \mathbb{F}_2^3$. Considere as aplicações lineares $\phi_1, \phi_2 : \mathbb{F}_8 \longrightarrow \mathbb{F}_2^3 = B$ definidas por

$$\phi_1(1) = 001,\ \phi_1(\alpha) = 010,\ \phi_1(\alpha^2) = 100 \qquad \text{e} \qquad \phi_2(1) = 111,\ \phi_2(\alpha) = 100,\ \phi_2(\alpha^2) = 110\ .$$

ϕ_1 e ϕ_2 são isomorfismos, por isso podemos formar as concatenações $C_1 = \phi_1^*(A)$ e $C_2 = \phi_2(A)$, que são códigos binários de parâmetros $[6, 3, 2]$ e $[6, 3, 3]$, respectivamente — justifique! Logo C_1 e C_2 não são códigos equivalentes, apesar dos códigos exterior A e interior B serem os mesmos.

Proposição 5.15. *Se A e B são códigos $[N, K, D]_{q^m}$ e $[n, m, d]_q$, repectivamente, então a concatenação C é um código $[nN, mK, d']_q$, onde $d' \geq dD$.*

Dem. Por construção, o comprimento do código concatenação é nN, uma vez que $C \subseteq \mathbb{F}_q^{nN}$.

Como ϕ^* é uma aplicação injectiva e $C = \phi^*(A)$, então $|C| = |A| = (q^m)^{\dim A} = q^{mK}$, logo $\dim C = \log_q |C| = mK$.

Quanto à distância mínima, pelo Teorema 4.5, basta ver que $\mathrm{w}(y) \geq dD$ para qualquer $y \in C \setminus \{\vec{0}\}$. Seja $(x_1, \ldots, x_N) \in A \setminus \{\vec{0}\}$ com $x_i \in \mathbb{F}_{q^m}$. Para cada j tal que $x_j \neq 0$, tem-se $\phi(x_j) \neq \vec{0}$, porque ϕ é injectiva e linear. Portanto $\mathrm{w}(\phi(x_i)) \geq d = \mathrm{d}(B)$ porque $\phi(x_i) \in B \setminus \{\vec{0}\}$. Por outro lado, $\mathrm{w}(x_1, \ldots, x_N) \geq D = \mathrm{d}(A)$, donde

$$\mathrm{w}(y) = \mathrm{w}(\phi^*(x_1, \ldots, x_n)) = \mathrm{w}(\phi(x_1), \ldots, \phi(x_N)) \geq dD \ ,$$

porque há pelo menos D coordenadas x_j não nulas. Como $y = \phi^*(x_1, \ldots, x_N)$ é uma palavra arbitrária de C, conclui-se que $\mathrm{d}(C) \geq dD$. □

Corolário 5.16. *Se existe um código $[N, K, D]_{q^m}$, então também existe um código $[mN, mK, D]_q$.*

Dem. Seja A um código $[N, K, D]$ sobre $\mathbb{F}_{q^m}$ e seja $B = \mathbb{F}_q^m$ sobre $\mathbb{F}_q$. Como os parâmetros de B são $[m, m, 1]_q$, pela Proposição 5.15, a concatenação C de A e B é um código $[mN, mK, d']_q$ com $d' \geq D$. Pelo Teorema 5.8 aplicado a C com $t = d' - D \geq 0$ e $s = r = 0$, obtemos um código $[mN, mK, D]_q$ como pretendiamos. □

Exemplo 5.17. No Exemplo 5.11, o código exterior A e o código interior $B = \mathbb{F}_2^2$ tem parâmetros $[3, 1, 3]_4$ e $[2, 2, 1]_2$, respectivamente. Os parâmetros da concatenação podem ser determinados directamente da lista das palavras em (5.6) e são $[6, 2, 3]_2$. Neste caso $d' = 3 = dD$. No Exemplo 5.12, o código interior é o mesmo B, o código exterior A é diferente, mas tem também parâmetros $[3, 1, 3]_4$ (na realidade, este A é equivalente ao código de repetição). A concatenação A^* tem parâmetros $[6, 2, 4]_2$ — ver a lista das palavras em (5.7). Neste caso $d' = 4 > 3 = dD$.

Exercícios

5.1. Verifique as igualdades (5.2) no Exemplo 5.3.

5.2. Mostre que se existir um código $[n, k, d]_q$ então também existe um código $[n - r, k - r, d]$ para qualquer $0 \leq r \leq k - 1$.

5.3. Dado um código C $[n, k, d]_q$,
   (a) será que existe sempre um código $[n + 1, k, d + 1]$?
   (b) será que existe sempre um código $[n + 1, k + 1, d]$?

5.4. (a) Sejam G_1 e G_2 matrizes geradoras dos códigos lineares q-ários C_1 e C_2, respectivamente. Mostre que

$$G = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}$$

é uma matriz geradora do código soma $C_1 \oplus C_2$.

(b) Escreva uma matriz se paridade para $C_1 \oplus C_2$ em termos de matrizes de paridade H_1 e H_2 de C_1 e C_2, respectivamente.

5.5. Repita o exercício anterior para a Construção de Plotkin:

(a) Sejam G_1 e G_2 matrizes geradoras dos códigos lineares q-ários C_1 e C_2, respectivamente, ambos de comprimento n. Mostre que

$$G = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}$$

é uma matriz geradora do código $C_1 * C_2$.

(b) Escreva uma matriz se paridade para $C_1 * C_2$ em termos de matrizes de paridade H_1 e H_2 de C_1 e C_2, respectivamente.

5.6. Considere dois códigos lineares C_1 e C_2 sobre $\mathbb{F}_q$, de comprimento n e dimensões $\dim(C_i) = k_i$, $i = 1, 2$, e defina

$$C = \{(a + x, b + x, a + b + x) \,:\, a, b \in C_1, x \in C_2\} \,.$$

(a) Mostre que C é um código linear de parâmetros $[3n, 2k_1 + k_2]$.

(b) Escreva uma matriz geradora de C em termos de matrizes geradoras G_1 e G_2 de C_1 e C_2, respectivamente.

(c) Escreva uma matriz de paridade de C em termos de matrizes de paridade H_1 e H_2 de C_1 e C_2, respectivamente.

5.7. Seja V um espaço vectorial de dimensão finita sobre $\mathbb{F}_{q^m}$. Mostre que V é também um espaço vectorial sobre $\mathbb{F}_q$ e

$$\dim_{\mathbb{F}_{q^m}}(V) = m \dim_{\mathbb{F}_q}(V) \,,$$

onde $\dim_{\mathbb{F}}(V)$ designa a dimensão de V como espaço vectorial sobre o corpo $\mathbb{F}$.

5.8. Seja α uma raíz do polinómio $1 + t^2 + t^3 \in \mathbb{F}_2[t]$ e considere a aplicação $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ definida por $\phi(a_1 + a_2\alpha + a_3\alpha^2) = (a_1, a_2, a_3)$, onde $a_1, a_2, a_3 \in \mathbb{F}_2$. Considere o código linear

$$A = \langle(\alpha + 1, \alpha^2 + 1, 1)\rangle$$

sobre $\mathbb{F}_8$. Quais os parâmetros de $\phi^*(A)$?

5.9. Seja α uma raíz do polinómio $1 + t + t^2 \in \mathbb{F}_2[t]$. Considere o código linear

$$A = \langle(1, 1), (\alpha, 1 + \alpha)\rangle$$

sobre $\mathbb{F}_4$ e o código binário

$$B = \{0000, 1100, 1010, 0110\} \,.$$

Seja $\phi : \mathbb{F}_4 \to B$ a aplicação linear definida por $\phi(1) = 1100$ e $\phi(\alpha) = 1010$. Quais os parâmetros de $C = \phi^*(A)$?

CAPÍTULO 6

Exemplos de Códigos Lineares

1. Códigos de Hamming

A *redundância* de um código linear $[n, k, d]_q$ é $r = n - k$, ou seja, é o número de linhas de uma matriz de paridade.

Seja H uma matriz cujas colunas são todos os vectores não nulos do espaço vectorial $\mathbb{F}_2^r$. Portanto H tem r linhas e $2^r - 1$ colunas. Além disso, como os vectores da base canónia $\vec{e_1}, \ldots, \vec{e_r}$ são colunas de H, a matriz identidade I_r é uma submatriz de H com deteminante $\det(I_r) = 1 \neq 0$, portanto as r linhas de H são linearmente independentes, logo este H é uma matriz de paridade de um código binário.

Definição 6.1. Seja H uma matriz $r \times (2^r - 1)$ cujas colunas são todos os vectores em $\mathbb{F}_2^r \setminus \{\vec{0}\}$. O código binário $\mathrm{Ham}(r, 2)$ com esta matriz de paridade H diz-se um *código de Hamming binário de redundância* r.

Exemplo 6.2. (a) O código de Hamming binário de redundância 2, $\mathrm{Ham}(2, 2)$, tem matriz de paridade

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

Como H está na forma canónica, $G = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$ é uma matriz geradora e, portanto, $\mathrm{Ham}(2, 2)$ é o código de repetição binário de comprimento 3, de parâmetros $[3, 1, 3]$.

(b) A matriz

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

é uma matriz de paridade de um código $\mathrm{Ham}(3,2)$. Este código tem parâmetros $[7,4,3]$ — podemos determinar a distância mínima aplicando o Teorema 4.16.

Teorema 6.3. *Seja $r \geq 2$. Então*

(i) $\mathrm{Ham}(r,2)$ *tem parâmetros* $[2^r-1, 2^r-r-1, 3]$*;*

(ii) $\mathrm{Ham}(r,2)$ *é um código perfeito.*

Dem. (i) Por construção, $\mathrm{Ham}(r,2)$ tem comprimento $|\mathbb{F}_2^r \setminus \{\vec{0}\}| = 2^r-1$ e dimensão $k = n-r = 2^r-r-1$. Só falta ver que a distância mínima é $d=3$. Sejam c_i, com $i = 1, \ldots, 2^r-1$, as colunas de uma matriz de paridade H para $\mathrm{Ham}(r,2)$. Por construção, $c_i \neq c_j$ para quaisquer $i \neq j$, e nenhuma coluna é o vector nulo, logo quaisquer duas colunas de H são linearmente independentes. Por outro lado $c_i = (0,\ldots,0,0,1)$, $c_j = (0,\ldots,0,1,0)$ e $c_k = (0,\ldots,0,1,1)$ são colunas de H, se $r \geq 2$. Como $c_k = c_i + c_j$, estas três colunas são linearmente dependentes. Logo, pelo Teorema 4.16, $\mathrm{d}(\mathrm{Ham}(r,2)) = 3$.

(ii) Basta ver que os parâmetros determinados em (i) satisfazem a igualdade no majorante de empacotamento de esferas de Hamming. Como $n = 2^r-1$, $M = 2^{n-r}$ e $d=3$, então $t = \lfloor \frac{d-1}{2} \rfloor = 1$ e

$$M \,\mathrm{vol}(B_t(x))) = 2^{n-r}\left(\binom{n}{0} + \binom{n}{1}\right) = 2^{n-r}(1+n) = 2^{n-r}2^r = 2^n \ . \qquad \square$$

Observação 6.4.
- Para r fixo, os códigos $\mathrm{Ham}(r,2)$ são todos equivalentes (basta permutar as colunas numa matriz de paridade) e qualquer código linear com os mesmos parâmetros é equivalente a um $\mathrm{Ham}(r,2)$.
- Existem códigos binários não lineares com parâmetros $(n, 2^{n-r}, 3)$ com $n = 2^r-1$ (ver [**4**], por exemplo).

Algoritmo de descodificação para os códigos de Hamming binários

Como $\mathrm{Ham}(r,2)$ é um código perfeito de distância mínima 3, os chefes de classe são precisamente os vectores $x \in \mathbb{F}_2^n$ de peso $\mathrm{w}(x) = 1 = \lfloor \frac{d-1}{2} \rfloor$ (pela Proposição 4.28 e pelo Exercício 4.5). Supondo que as colunas de H estão ordenadas por ordem crescente, i.e., a i-ésima coluna é o número $i \in \{1,\ldots,n=2^r-1\}$ escrito na base 2 (como foi feito no exemplo anterior), se $e_i = (0,\ldots,0,1,0\ldots,0)$, com 1 na coordenada i, então o sintoma $S(e_i)$ é a representação binária de i. Assim, temos o seguinte algoritmo de descodificação para $\mathrm{Ham}(r,2)$:

1. Recebido $y \in \mathbb{F}_2^n$, calcular o sintoma $S(y) = Hy$.
2. Se $S(y) = 0$, assumir que não ocorreram erros de transmissão e descodificar y por y.
3. Se $S(y) \neq 0$, então $S(y)$ é uma coluna de H e, se estas estão por ordem crescente, assumir que ocorreu um erro na coordenada i correspondente ao número $S(y)$ na base 2, e descodificar y por $y - e_i$.

Exemplo 6.5. Seja $C = \mathrm{Ham}(4,2)$, portanto $n = 15$. Seja $y = 001100000100000 \in \mathbb{F}_2^{15}$ o vector recebido. As coordenadas 1 de y estão nas posições 3, 4 e 10. Como $3_{(10)} = 0011_{(2)}$, $4_{(10)} = 0100_{(2)}$

e $10_{(10)} = 1010_{(2)}$, fica

$$S(y) = c_3 + c_4 + c_{10} = \begin{bmatrix}0\\0\\1\\1\end{bmatrix} + \begin{bmatrix}0\\1\\0\\0\end{bmatrix} + \begin{bmatrix}1\\0\\1\\0\end{bmatrix} = \begin{bmatrix}1\\1\\0\\1\end{bmatrix} = c_{13}$$

pois $13_{(10)} = 1101_{(2)}$. Descodificamos y por $y - e_{13} = 001100000100100 \in C$.

Como se pode ver neste exemplo, a vantagem de assumir que as colunas de H estão escritas por ordem crescente é não ser necessário escrever a matriz H para se calcular os sintomas.

Códigos de Hamming binários estendidos

Consideremos a extensão por paridade $\widehat{\text{Ham}}(r,2)$ do código de Hamming binário $\text{Ham}(r,2)$ definida na Secção 1 do Capítulo 5. Portanto o código estendido $\widehat{\text{Ham}}(r,2)$ é linear e, pelo Lema 5.2, tem parâmetros $[2^r, 2^r - r - 1, 4]$.

Como $\text{d}(\widehat{\text{Ham}}(r,2)) = 4$, este código apenas corrige um erro, tal como $\text{Ham}(r,2)$, mas o código estendido pode ser usado para simultaneamente corrigir qualquer erro simples e detectar qualquer erro duplo. Deixamos como exercício descrever um tal algoritmo.

Códigos de Hamming q-ários

Um código de Hamming q-ário de redundância r, $\text{Ham}(r,q)$, é um código de parâmetros

$$\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3\right] .$$

Para mostrar que existem, vamos determinar uma matriz de paridade H para $\text{Ham}(r,q)$. Para termos $\text{d}(\text{Ham}(r,q)) = 3$, quaisquer duas colunas de H têm de ser linearmente independentes e têm de existir três colunas linearmente dependentes. Seja

$$M_v = \{\lambda v \,:\, \lambda \in \mathbb{F}_q \setminus \{0\}\} ,$$

com $v \in \mathbb{F}_q^r \setminus \{\vec{0}\}$. Ou seja, M_v é o conjunto dos múltiplos escalares não nulos do vector $v \neq \vec{0}$. Portanto $|M_v| = q-1$ e dois vectores v_1 e v_2 são linearmente independentes se e só se $M_{v_1} \cap M_{v_2} = \varnothing$, donde se conclui que há precisamente

$$\frac{|\mathbb{F}_q^r \setminus \{\vec{0}\}|}{|M_v|} = \frac{q^r-1}{q-1}$$

classes de vectores linearmente independentes dois a dois em $\mathbb{F}_q^r$. As colunas de H são obtidas escolhendo um vector em cada classe M_v. Por outro lado, os vectores $(0,\ldots,0,0,a)$, $(0,\ldots,0,b,0)$ e $(0,\ldots,0,c,c)$ são colunas de H, para alguma escolha $a,b,c \in \mathbb{F}_q \setminus \{0\}$, e são linearmente dependentes. Pelo Teorema 4.16, um código com esta matriz de paridade tem distância mínima 3.

Agora só falta ver que as linhas de H são linearmente independentes, para H ser de facto uma matriz de paridade. Deixamos essa verificação como exercício.

Observação 6.6. Tal como no caso binário, os códigos $\mathrm{Ham}(r,q)$, com r e q fixos, são todos linearmente equivalentes por construção: qualquer matriz de paridade é obtida a partir de outra permutando colunas (escolher vectores em classes distintas M_v por ordens diferentes) e/ou multiplicando colunas por escalares não nulos (escolher dois vectores diferentes na mesma classe M_v, para matrizes H diferentes).

Exemplo 6.7. $\mathrm{Ham}(2,3)$ é um código ternário (ou é uma classe de códigos) com parâmetros $[4,2,3]$. Como as classes de vectores linearmente independentes são

$$M_{(0,1)} = \{(0,1),(0,2)\},\ M_{(1,0)} = \{(1,0),(2,0)\},\ M_{(1,1)} = \{(1,1),(2,2)\} \text{ e } M_{(1,2)} = \{(1,2),(2,1)\}.$$

as matrizes

$$H_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{bmatrix},\ H_2 = \begin{bmatrix} 0 & 1 & 2 & 1 \\ 2 & 0 & 2 & 2 \end{bmatrix},\ H_3 = \begin{bmatrix} 2 & 0 & 1 & 2 \\ 0 & 2 & 1 & 1 \end{bmatrix} \text{ e } H_4 = \begin{bmatrix} 0 & 1 & 1 & 2 \\ 1 & 0 & 2 & 2 \end{bmatrix}$$

são matrizes de paridade destes códigos equivalentes, estando H_1 e H_4 na forma canónica.

Exemplo 6.8. $\mathrm{Ham}(3,3)$ tem parâmetros $n = \frac{3^3-1}{3-1} = 13$, $k = n - r = 10$ e $d = 3$, e

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$$

é uma matriz de paridade para este código.

Teorema 6.9. *Os códigos de Hamming* $\mathrm{Ham}(r,q)$ *são perfeitos.*

A demosntração é análoga ao caso binário. como consequência, tem-se que, para $n = \dfrac{q^r-1}{q-1}$,

$$A_q(n,3) = q^{n-r} \quad \forall r \geq 2\ .$$

Algoritmo de descodificação para os códigos de Hamming q-ários

Vamos assumir que a matriz de paridade H tem as colunas escritas por ordem lexicográfica e que a primeira entrada não nula de cada coluna é 1. No Exemplo 6.7 escolheriamos a matriz H_1, no Exemplo 6.8 a matriz H está na forma pretendida.

Como $\mathrm{Ham}(q,r)$ é um código perfeito de distância mínima 3, o sintoma de qualquer vector y é $S(y) = \vec{0}$ ou $S(y) = S(\lambda e_i)$ para algum $\lambda \in \mathbb{F}_q$ e $e_i = (0,\ldots,0,1,0,\ldots,0)$ com 1 na coordenada $i \in \{1,\ldots,n\}$. Portanto:

1. Recebido $y \in \mathbb{F}_q^n$, calcular o sintoma $S(y)$.
2. Se $S(y) = 0$, então assumir que não houve erros de transmissão.
3. Caso contrário, $S(y) = \lambda c_i \neq 0$ para alguma coluna c_i de H e escalar não nulo λ. Assumir que o vector de erro é λe_i e descodificar y por $y - \lambda e_i$.

O algoritmo descrito para os códigos de Hamming binários é um caso particular deste, onde se tem necessarimante $\lambda = 1$.

Exemplo 6.10. Seja $C = \mathrm{Ham}(3,3)$ com a matriz de paridade do Exemplo 6.8. Supondo que recebemos o vector $y = 1101112211201 \in \mathbb{F}_3^{13}$, como

$$S(y) = Hy = \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix} = 2 \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix} ,$$

assumimos que ocorreu um erro na coordenada 7 descodificamos y por $y - 2e_7 = 1101110211201$.

Se aplicarmos a construção contracção definida na Secção 5 do Capítulo 5 a um código de Hamming $\mathrm{Ham}(r,q)$ obtêm-se códigos $[n-s, n-r-s, d]$ com $d \geq 3$. Se a redundância r for pequena, em muitos casos ainda ficamos com códigos de distância mínima $d = 3$ mas, em geral, com maior capacidade de detecção de erros.

Exemplo 6.11. Consideremos o código $C = \mathrm{Ham}(2,11)$, sobre $\mathbb{F}_{11}$, com matriz de paridade

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & X \end{bmatrix} .$$

Contraíndo nas duas primeiras coordenadas, obtemos o código C' com matriz de paridade

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

ou seja, o código contraído é o código já estudado no Exemplo 4.33. Como foi visto, $\mathrm{d}(C') = 3$ mas C' pode ser usado para corrigir erros simples e, simultâneamente, detectar erros duplos de transposição.

Códigos simplex

Por definição, um código *simplex* é o dual de um código de Hamming

$$S(r,q) \stackrel{\mathrm{def}}{=} \mathrm{Ham}(r,q)^{\perp} ,$$

portanto, $S(r,q)$ é um código de comprimento $n = \frac{q^r-1}{q-1}$ e dimensão r.

Proposição 6.12. *Se $x \in S(r,q) \setminus \{\vec{0}\}$, então $\mathrm{w}(x) = q^{r-1}$. Em particular, $\mathrm{d}(S(r,q)) = q^{r-1}$.*

Dem. Seja G uma matriz geradora de $S(r,q)$, portanto G é uma matriz de paridade de $\mathrm{Ham}(r,q)$ e, por construção dos códigos de Hamming, cada uma das coluna de G pertence a uma classe $M_x = \{\lambda x : \lambda \in \mathbb{F}_q \setminus \{0\}\}$, com $x \in \mathbb{F}_q^r \setminus \{\vec{0}\}$. Como já se observou anteriormente, cada uma das $n = \frac{q^r-1}{q-1}$ classes M_x contém $q-1$ vectores. Logo, se $v \in \mathbb{F}_q^r$ é um vector não nulo, então $\langle v \rangle^{\perp} \setminus \{\vec{0}\}$ é a união disjunta de $\frac{q^{r-1}-1}{q-1}$ classes M_x (porque o código dual $\langle v \rangle^{\perp}$ tem dimensão $r-1$), o que implica que $c \cdot v = 0$ para as $\frac{q^{r-1}-1}{q-1}$ colunas de G pertencentes às classes M_x contidas em $\langle v \rangle^{\perp}$.

Por outro lado, sendo c_i, com $i = 1, \ldots, n$ as colunas de G, como $S(r, q)$ é o espaço das linhas de G, os vectores em $S(r, q)$ são da forma

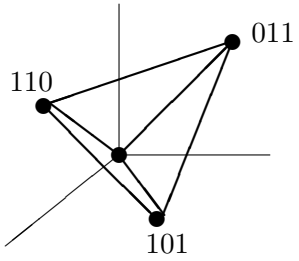
$$G^T v = \begin{bmatrix} c_1 \cdot v \\ \vdots \\ c_n \cdot v \end{bmatrix}$$

onde $v \in \mathbb{F}_q^r$. Donde se conclui que as palavras não nulas em $S(r, q)$ têm peso

$$\mathrm{w}(G^T v) = n - \frac{q^{r-1} - 1}{q - 1} = \frac{q^r - 1}{q - 1} - \frac{q^{r-1} - 1}{q - 1} = q^{r-1} \ . \qquad \square$$

O nome simplex deste códigos é justificado pela proposição anterior, no caso binário: as palavras de $S(r, 2)$ são os vértices de um símplice-n regular (para a distância de Hamming) em $\mathbb{F}_2^n$, com $n = 2^r - 1$. Um símplice-2 é um triângulo e tem três vértices, um símplice-3 é um tetraedro e tem quatro vértices. Em geral, um símplice-n é um "sólido" em $\mathbb{F}_2^n$ (ou $\mathbb{R}^n$ ou $\mathbb{F}_q^n$ ou ...) com $n + 1$ vértices tal que o hiperplano definido por n dos vértices não contém o outro vértice.

Exemplo 6.13. Para $r = 2$, temos $n = 2^r - 1 = 3$ e $|S(r, 2)| = 2^r = 4 = n + 1$, portanto $S(2, 2) = \{000, 110, 101, 011\} \subset \mathbb{F}_2^3$ e podemos representar as palavras deste código na figura



2. Códigos de Reed-Muller

Na Ficha 2, já definimos a família dos códigos de Reed-Muller por:

$$\begin{aligned} \mathcal{RM}(0, m) &= \{\vec{0}, \vec{1}\} = \text{código binário de repetição de comprimento } 2^m \ ; \\ \mathcal{RM}(m, m) &= (\mathbb{F}_2)^{2^m} \ ; \\ \mathcal{RM}(r, m) &= \mathcal{RM}(r, m-1) * \mathcal{RM}(r-1, m-1) \ , \quad 0 < r < m \ . \end{aligned}$$

Uma vez que os códigos de repetição e que $(\mathbb{F}_2)^{2^m}$ são todos códigos lineares, qualquer $\mathcal{RM}(r, m)$ é também um código linear, pois a construção de Plotkin preserva a linearidade, e, como foi visto na Ficha 2, os seus parâmetros são $[2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}]$.

Proposição 6.14. *Seja $m \in \mathbb{N}$. Seja $x \in \mathcal{RM}(1, m)$. Então $x = \vec{0}$ ou $x = \vec{1}$ ou $\mathrm{w}(x) = 2^{m-1}$.*

Dem. Exercício da Ficha 5. $\square$

Em particular, $\mathcal{RM}(1, m)$ contém $2^{m-1} - 2$ vectores de peso 2^{m-1}.

Proposição 6.15. *Seja* $0 \leq r < m$. *Então* $\mathcal{RM}(r,m)^\perp = \mathcal{RM}(m-r-1,m)$.

Dem. Exercício da Ficha 5. □

Proposição 6.16. *Seja* $m \geq 1$. *Então* $\mathcal{RM}(1,m)^\perp$ *é equivalente ao código de Hamming binário estendido* $\widehat{Ham}(m,2)$.

Dem. Uma maneira de provar este resultado, que deixamos como exercício, é obtê-lo como corolário da Proposição 6.15. Aqui apresentamos uma demonstração que usa a Proposição 6.14 e matrizes geradoras dos códigos Reed-Muller e de paridade dos códigos de Hamming binários estendidos.

Uma matriz de paridade para $\mathcal{RM}(1,m)^\perp$ é uma matriz geradora G_m para $\mathcal{RM}(1,m)$. Como $\mathcal{RM}(1,1) = \mathbb{F}_2^2$, podemos escolher

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

como matriz geradora. Como $\vec{1} \in \mathcal{RM}(1,m)$, pela Proposição 6.14, podemos escolher uma matriz geradora de $\mathcal{RM}(1,m)$ na forma

$$G_m = \left[\begin{array}{c|ccc} 1 & 1 & \cdots & 1 \\ \hline 0 & & & \\ \vdots & & H_m & \\ 0 & & & \end{array}\right]$$

para alguma matriz H_m. Note que G_1 também está nesta forma. Seja

$$G'_m = \left[\begin{array}{ccc|c} & & & 0 \\ & H_m & & \vdots \\ & & & 0 \\ \hline 1 & \cdots & 1 & 1 \end{array}\right].$$

Então G'_m gera um código equivalente a $\mathcal{RM}(1,m)$ e é uma matriz de paridade de um código estendido $\widehat{C}$, onde $C = \mathcal{N}(H_m)$. Vamos agora provar, por indução matemática em m, que H_m é uma matriz de paridade para $\mathrm{Ham}(m,2)$, ou seja, vamos mostrar que as colunas de H_m são todos os vectores não nulos em $\mathbb{F}_2^m$.

<u>$m = 1$:</u> De G_1 vem que $H_1 = \begin{bmatrix} 1 \end{bmatrix}$ que é a matriz de paridade de $\mathrm{Ham}(1,2)$.

<u>$m \Rightarrow m+1$:</u> Suponhamos agora que H_m é uma matriz de paridade de $\mathrm{Ham}(m,2)$. Como

$$G_{m+1} = \left[\begin{array}{ccc|ccc} & G_m & & & G_m & \\ \hline 0 & \cdots & 0 & 1 & \cdots & 1 \end{array}\right] = \left[\begin{array}{c|ccc|c|ccc} 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ \hline 0 & & & & 0 & & & \\ \vdots & & H_m & & \vdots & & H_m & \\ 0 & & & & 0 & & & \\ \hline 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \end{array}\right]$$

então

$$H_{m+1} = \left[\begin{array}{ccc|c|ccc} & & & 0 & & & \\ & H_m & & \vdots & & H_m & \\ & & & 0 & & & \\ \hline 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \end{array}\right] .$$

Por hipótese de indução, as colunas de H_m são todos os vectores em $\mathbb{F}_2^m \setminus \{\vec{0}\}$, i.e., representam os números em $\{1, \ldots, 2^m - 1\}$ na base 2. As colunas de H_{m+1} são

$$\left[\begin{array}{c} | \\ c \\ | \\ \hline 0 \end{array}\right] , \qquad \left[\begin{array}{c} 0 \\ \vdots \\ 0 \\ \hline 1 \end{array}\right] \qquad \text{e} \qquad \left[\begin{array}{c} | \\ c \\ | \\ \hline 1 \end{array}\right] ,$$

onde c é uma coluna de H_m. Estes três tipos de coluna representam, respectivamente, qualquer número par $2i$ com $i \in \{1, \ldots, 2^m - 1\}$, o número 1 e os números $2i + 1$ com $i \in \{1, \ldots, 2^m - 1\}$, donde se conclui que H_{m+1} é de facto uma matriz de paridade para um código de Haming binário $\mathrm{Ham}(m, 2)$. □

3. Minorante de Gilbert-Varshamov Linear

O método usado para construir uma matriz de paridade para $\mathrm{Ham}(r, q)$ permite obter minorantes para $A_q(n, d)$, onde q é uma potência de um número primo.

Teorema 6.17 (Gilbert-Varshamov)**.** *Seja q uma potência de um número primo, $2 \leq d \leq n$ e $1 \leq k \leq n$. Se*

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k} \tag{6.1}$$

então existe um código linear $[n, k, d']$ sobre $\mathbb{F}_q$ com $d' \geq d$.

Dem. Assumindo a desigualdade (6.1), vamos provar que existe uma matriz $H_{n-k,n}$ tal que quaisquer $d - 1$ colunas são linearmente independentes. Seja $r = n - k$ e seja c_j a coluna j de H. Escolhemos

$$c_1 \in \mathbb{F}_q^r \setminus \{\vec{0}\} , \qquad c_2 \in \mathbb{F}_q^r \setminus \langle c_1 \rangle , \qquad c_3 \in \mathbb{F}_q^r \setminus \langle c_1, c_2 \rangle .$$

Para $2 \leq j \leq n$, c_j pode ser qualquer vector em $\mathbb{F}_q^r$ que não seja combinação linear de $d - 2$ (ou menos) colunas $c_1, \ldots, c_{j-1}$ já escolhidas. Portanto, sendo $N(j)$ o número de vectores em $\mathbb{F}_q^r$ que não podem ser escolhidos para c_j, tem-se

$$N(j) = 1 + \binom{j-1}{1}(q-1) + \binom{j-1}{2}(q-1)^2 + \cdots + \binom{j-1}{d-2}(q-1)^{d-2}$$

onde a primeira parcela conta o vector nulo, a segunda parcela conta os múltiplos não nulos das $j - 1$ colunas já escolhidas, etc, a i-ésima parcela conta o número de combinações lineares de $i - 1$

das colunas já escolhidas com todos os coeficientes não nulos. Ou seja

$$N(j) = \sum_{i=0}^{d-2} \binom{j-1}{i} (q-1)^i \ .$$

É possível escolher a j-ésima coluna c_j se e só se $N(j) < q^r = |\mathbb{F}_q^r|$. Por hipótese, $N(n) < q^r$, logo existe uma matriz $H_{n-k,n}$ tal que quaisquer $d-1$ colunas são linearmente independentes, como pretendiamos. No entanto não temos garantia de que as linhas de H sejam linearmente independentes para poder ser uma matriz de paridade de um código, mas podemos ainda tomar $C = \mathcal{N}(H)$. O núcleo de uma matriz é sempre um espaço vectorial, portanto C é um código linear de comprimento n, dimenão $\dim C \geq k$ (igualdade apenas se as linhas de H são linearmente independentes) e $\mathrm{d}(C) \geq d$ pelo Teorema 4.16. Aplicando agora o Teorema 5.8 sabemos que existe um código C' de parâmetros $[n, k, d']$ com $d' \geq \mathrm{d}(C) \geq d$. □

Corolário 6.18. *Seja q uma potência de um número primo e $2 \leq d \leq n$. Então*

$$A_q(n,d) \geq q^m \qquad \textit{onde} \qquad m = \max\left\{k \in \mathbb{N} \,:\, q^k \leq \frac{q^n}{\sum_{i=0}^{d-2} \binom{n-1}{i}(q-1)^i}\right\} \ .$$

Dem. Pelo teorema anterior, sabemos que existe um código C de parâmetros $[n, m, d']$ sobre $\mathbb{F}_q$, com $d' \geq d$. Aplicando o Teorema 5.8 a C com $r = s = 0$ e $t = d - d'$, obtemos um código $[n, m, d]$, que contém q^m palavras, logo $A_q(n,d) \geq q^m$. □

4. Códigos de Golay

Seja G_{24} o código binário com matriz geradora na forma canónica $G = \begin{bmatrix} I_{12} & A \end{bmatrix}$, onde

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

G_{24} diz-se o código de Golay binário estendido.

Lema 6.19. *(i) G_{24} é um código auto-dual, i.e., $G_{24}^{\perp} = G_{24}$;*
(ii) $\begin{bmatrix} A & I_{12} \end{bmatrix}$ é uma matriz geradora de G_{24};
(iii) $\forall\, x \in G_{24}, \mathrm{w}(x) \equiv 0 \mod 4$;
(iv) $\forall\, x \in G_{24}, \mathrm{w}(x) \neq 4$;

Para a demostração deste lema, consultar [**2**].

Teorema 6.20. *O código de Golay binário G_{24} tem parâmetros* $[24, 12, 8]$.

Dem. Por construção, tem-se directamente que G_{24} tem comprimento 24 e dimensão 12. Atendendo a que qualquer linha da matriz geradora $G = \begin{bmatrix} I_{12} & A \end{bmatrix}$, excepto a primeira, tem peso 8, as alíneas (iii) e (iv) do Lema 6.19 implicam que $\mathrm{d}(G_{24}) = 8$. □

O código de Golay G_{23} é o pontuado, na última coordenada, do código G_{24}, portanto os seus parâmetros são $[23, 12, d]$, ou $(23, 2^{12}, d)$, com $7 \leq d \leq 8$. Uma vez que a primeira linha de G é uma palavra de G_{24} com peso 8 e última coordenada igual a 1, o código G_{23} contém uma palavra de peso 7, donde se conclui que G_{23} tem distância mínima $d = 7$ e é um código perfeito. Note ainda que a extensão por paridade de G_{23} é $\widehat{G}_{23} = G_{24}$.

A definição dos códigos de Golay ternários é análoga à dos binários. Seja $G = \begin{bmatrix} I_6 & B \end{bmatrix}$, onde

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

Seja G_{12} o código ternário com matriz geradora G. Deixamos a demosntrção do seguinte teorema como exercício.

Teorema 6.21. *(i) G_{12} é um código auto-dual;*

(ii) O código de Golay ternário G_{12} tem parâmetros $[12, 6, 6]$.

Definimos G_{11} como o pontuado do código G_{12} na última coordenada, portanto os seus parâmetros são $[11, 6, 5]$, ou $(11, 3^6, 5)$, e é um código perfeito.

5. Códigos de distância máxima de separação ou MDS

A estimativa de Singleton 2.11 para códigos lineares $[n, k, d]_q$ pode ser provada de outra maneira usando o Teorema 4.16: como as colunas de uma matriz de paridade são vectores em $\mathbb{F}_q^{n-k}$ e quaisquer $d - 1$ colunas são linearmente dependentes, logo $d \leq n - k + 1$.

Definição 6.22. Um código linear de parâmetros $[n, k, d]$ tal que $d = n - k + 1$ diz-se um *código de distância máxima de separação*, ou MDS.

Exemplo 6.23. (i) $C = \mathbb{F}_q^n$ tem parâmetros $[n, n, 1]$, é MDS.

(ii) O código de repetição $\langle \vec{1} \rangle \subset \mathbb{F}_q^n$ tem parâmetros $[n, 1, n]$, e também é MDS.

(iii) O dual de um código de repetição tem parâmetros $[n, n-1, 2]$, e também é MDS.

Definição 6.24. Qualquer código equivalente a um dos do Exemplo 6.23 diz-se um *código MDS trivial*.

O código $[10, 8, 3]$ sobre $\mathbb{F}_{11}$ do Exemplo 4.33 e os dos problemas 1 e 2 da Ficha 4 são exemplos de códigos MDS não triviais.

Lema 6.25. *Seja C um código linear $[n, k]_q$ com matriz de paridade H. Então C é MDS se e só se quaisquer $n - k$ colunas de H são linearmente independentes.*

Dem. ($\Longrightarrow$) É consequência imediata do Teorema 4.16.

($\Longleftarrow$) $\mathrm{d}(C) \geq n - k + 1$, pelo Teorema 4.16, e $\mathrm{d}(C) \leq n - k + 1$, pela estimativa de Singleton. □

Teorema 6.26. *O dual de um código MDS é também um código MDS.*

Dem. Seja C um código linear $[n, k, d]_q$ com $d = n - k + 1$. Seja H uma matriz de paridade para C, portanto H é uma matriz geradora do código dual $C^\perp$, de parâmetros $[n, n - k, d']$. Queremos ver que $d' = k + 1$. Como $d' \leq k + 1$, pela estimativa de Singleton, basta ver que $d' \geq k + 1$. Como $\mathrm{d}(C^\perp) = \mathrm{w}(C^\perp)$, basta ver que $\mathrm{w}(x) \geq k + 1$ para todo o $x \in C^\perp \setminus \{\vec{0}\}$.

Seja $x \in C^\perp$ tal que $\mathrm{w}(x) \leq k$. Sem perda de generalidade, como x tem no máximo $n-k$ coordenadas nulas, podemos assumir que $x = (x', \vec{0})$ com $x' \in \mathbb{F}_q^k$ e $\vec{0} \in \mathbb{F}_q^{n-k}$. Seja H' a submatriz de H formada pelas últimas $n - k$ colunas desta, ou seja

$$H = \begin{bmatrix} A & H' \end{bmatrix}$$

com A uma matriz $(n - k) \times k$ e H' uma matriz quadrada. Pelo Lema 6.25, porque C é um código MDS, as colunas de H' são linearmente independentes, logo as linhas de H' também são linearmente independentes, porque o espaço das linhas e o espaço das colunas duma matriz têm a mesma dimensão.

Por outro lado, o vector $x = (x', \vec{0})$ é combinação linear das linhas de H, i.e., se $l_1, \ldots, l_{n-k}$ são as linhas de H, então

$$x = \sum_{i=1}^{n-k} \alpha_i l_i \ ,$$

onde os coeficientes $\alpha_i \in \mathbb{F}_q$ são unicamente determinados por x, donde

$$\vec{0} = \sum_{i=1}^{n-k} \alpha_i l'_i \ ,$$

onde l'_i é a i-ésima linha de H' (portanto as entradas de l'_i são as últimas $n - k$ entradas de l_i), logo $\alpha_i = 0$ para todo o i, porque $\{l'_1, \ldots, l'_{n-k}\}$ é um conjunto linearmente independente. Donde se conclui que $x = \vec{0}$ e, portanto, as palavras não nulas de $C^\perp$ têm peso pelo menos $k + 1$. □

A alínea (iii) do Exemplo 6.23 é um caso particular deste teorema.

Exercícios

6.1. Resolva a Ficha 5.

6.2. Descreva um algoritmo de descodificação para o código de Hamming binário estendido $\widehat{\mathrm{Ham}}(r, 2)$ que permita corrigir qualquer erro simples e detectar erros duplos simultameamente.

6.3. Justifique que os códigos de Hamming $\mathrm{Ham}(2, q)$, de redundância 2, são códigos MDS.

6.4. Seja $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, onde α é uma raiz de $1 + t + t^2$. Seja C um código linear sobre $\mathbb{F}_4$ com matriz geradora

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \end{bmatrix} .$$

Escreva uma matriz geradora para o código dual $C^\perp$. Mostre que C e $C^\perp$ são códigos MDS.

6.5. Mostre que os únicos códigos MDS binários são os triviais.

6.6. Seja C um código q-ário MDS de parâmetros $[n, k]$ com $k < n$.

(a) Mostre que existe um código q-ário MDS de comprimento n e dimensão $n - k$.

(b) Mostre que existe um código q-ário MDS de comprimento $n - 1$ e dimensão k.