CAPÍTULO 9

Códigos Reed-Solomon

Um dos problemas na Teoria de Códigos é determinar a distância mínima de um dado código. Tratando-se de códigos cíclicos, por vezes conseguimos controlar a distância mínima com uma "boa escolha" do polinómio gerador. É este o caso dos códigos Reed-Solomon. Estes códigos são MDS, ou seja, para o comprimento e a dimensão fixos, têm a maior distância mínima possível, e são ainda muito importantes na correcção de erros acumulados.

Definição 9.1. Um código Reed-Solomon q-ário é um código cíclico, de comprimento $q-1$, com polinómio gerador

$$g(t) = (t - \alpha^{a+1})(t - \alpha^{a+2}) \cdots (t - \alpha^{a+\delta-1}) \ ,$$

com $a \geq 0$ e $2 \leq \delta \leq q-1$, onde α é um elemento primitivo de $\mathbb{F}_q$.

Observação 9.2. (i) Pela Proposição 3.15, sabemos que $x^{q-1} = 1$ para qualquer $x \in \mathbb{F}_q \setminus \{0\}$, logo, se α é um elemento primitivo de $\mathbb{F}_q$, o polinómio $t^{q-1} - 1 \in \mathbb{F}_q[t]$ tem a seguinte factorização

$$t^{q-1} - 1 = (t-1)(t-\alpha)(t-\alpha^2) \cdots (t-\alpha^{q-2}) \ . \tag{9.1}$$

Portanto o polinómio $g(t)$ na Definição 9.1 é um divisor de $t^{q-1}-1$ e $g(t)$ é de facto o polinómio gerador de um código cíclico. Além disso, as raízes de $g(t)$ são todas distintas.

(ii) Como $\deg(g(t)) = \delta - 1$, a dimensão de C é $\dim(C) = n - (\delta - 1) = q - \delta$. Em particular $1 \leq \dim(C) \leq q-2$, logo os códigos triviais $\mathbb{F}_q^{q-1}$ e $\{\vec{0}\}$ não são códigos Reed-Solomon.

(iii) Não há códigos Reed-Solomon binários, pois $2 \leq \delta \leq q-1 \Rightarrow q \geq 3$.

Exemplo 9.3. Como 3 é um elemento primitivo de $\mathbb{F}_7$,

$$g(t) = (t-3^2)(t-3^3)(t-3^4) = 1 + 2t + 2t^2 + t^3$$

é o polinómio gerador de um código Reed-Solomon de parâmetros $[6, 3]$.

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

é uma matriz geradora, $h(t) = \frac{t^6-1}{g(t)} = 6 + 2t + 5t^2 + t^3$ é o polinómio de paridade e

$$H = \begin{bmatrix} 1 & 5 & 2 & 6 & 0 & 0 \\ 0 & 1 & 5 & 2 & 6 & 0 \\ 0 & 0 & 1 & 5 & 2 & 6 \end{bmatrix}$$

é uma matriz de paridade. A partir de H, aplicando o Teorema 4.16, podemos concluir que $\mathrm{d}(C) = 4$ e, portanto, trata-se de um código MDS.

1. Distância mínima

Nesta secção iremos ver que os códigos Reed-Solomon são MDS.

Proposição 9.4. *Seja C um código Reed-Solomon q-ário, com polinómio gerador $g(t) = (t - \alpha^{a+1})(t - \alpha^{a+2}) \cdots (t - \alpha^{a+\delta-1})$. Então*

$$C = \{c(t) \in R_{q-1} \,:\, c(\alpha^i) = 0\,, \forall\, i = a+1, \ldots, a+\delta-1\}\ .$$

Dem. (i) Pelo Lema 8.16, $c(t) \in C$ se e só se $c(t) = a(t)g(t)$ para algum $a(t) \in \mathbb{F}_q[t]$, portanto as raízes de g(t) são também raízes de qualquer palavra de código $c(t)$.
(ii) Seja agora $c(t) \in R_{q-1}$ tal que $c(\alpha^i) = 0$ para $i = a+1, \ldots, a+\delta-1$. Portanto $t - \alpha^i$ divide $c(t)$ (no anel $\mathbb{F}_q[t]$), para $i = a+1, \ldots, a+\delta-1$, e como estes α^i são todos distintos, podemos concluir que $g(t)$ divide $c(t)$, logo $c(t) \in C$. □

Note que a parte (i) da demonstração anterior é válida para qualquer código cíclico, e na parte (ii) apenas se usou o facto das raízes do polinómio gerador serem todas distintas. Podemos portanto generalizar a Proposição 9.4, com a mesma demonstração, para o seguinte resultado:

Teorema 9.5. *Se C é um código q-ário de comprimento n tal que o seu polinómio gerador $g(t)$, de grau r, tem raízes distintas $\alpha_1, \ldots, \alpha_r$ (não necessarimante em $\mathbb{F}_q$), então*

$$C = \{c(t) \in R_n \,:\, c(\alpha_i) = 0\,, \forall\, i = 1, \ldots, r\}\ .$$

Exemplo 9.6. Seja $C = \mathrm{Ham}(3, 2)$ com polinómio gerador $g(t) = 1 + t + t^3$. O comprimento de C é $n = 7$. No anel $\mathbb{F}_8$, o polinómio $t^7 - 1$ factoriza-se no produto de termos lineares distintos (ver ponto (i) na Obervação 9.2), portanto as raízes de $g(t)$ são distintas, porque $g(t) | t^7 - 1$. Pelo Teorema 9.5,

$$C = \{c(t) \in R_7 \,:\, c(\beta) = 0\,, \forall\ \beta \text{ raiz de } g(t)\}\ .$$

Como todos os elementos de $\mathbb{F}_8 \setminus \{0, 1\}$ são raízes de $c(t) = 1 + t + t^2 + t^3 + t^4 + t^5 + t^6 = \dfrac{t^7 - 1}{t - 1}$, então as raízes de $g(t)$ são também raízes de $c(t)$, donde $c(t) \in C \subset R_7$, ou seja $\vec{1} \in C \subset \mathbb{F}_2^7$.

Teorema 9.7. *Seja C um código Reed-Solomon de parâmetros $[q-1, q-\delta]_q$. Então* $\mathrm{d}(C) \geq \delta$.

Dem. Seja $g(t) = (t - \alpha^{a+1})(t - \alpha^{a+2}) \cdots (t - \alpha^{a+\delta-1})$ o polinómio gerador de C. Suponhamos, por absurdo, que $\mathrm{d}(C) = d < \delta$ e seja $c(t) = c_0 + c_1 t + \cdots + c_{n-1} t^{n-1} \in C$ com peso $\mathrm{w}(c(t)) = d$. Seja $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ o vector correspondente a $c(t)$.

Pela Proposição 9.4, $c(\alpha^i) = 0$ para qualquer $i = a+1, \ldots, a+\delta-1$. Por outro lado,

$$c(\alpha^i) = c_0 + c_1\alpha^i + \cdots + c_{n-1}(\alpha^i)^{n-1} = (1, \alpha^i, (\alpha^i)^2, \ldots, (\alpha^i)^{n-1}) \cdot c \ .$$

Portanto $Ac = 0$, onde

$$A = \begin{bmatrix} 1 & \alpha^{a+1} & (\alpha^{a+1})^2 & \cdots & (\alpha^{a+1})^{n-1} \\ 1 & \alpha^{a+2} & (\alpha^{a+2})^2 & \cdots & (\alpha^{a+2})^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{a+\delta-1} & (\alpha^{a+\delta-1})^2 & \cdots & (\alpha^{a+\delta-1})^{n-1} \end{bmatrix}$$

é uma matriz com $\delta - 1$ linhas e n colunas. Sejam $i_1, \ldots, i_d$ os índices tais que $c_{i_j} \neq 0$. Seja A' a matriz formada pelas colunas $i_1+1, i_2+1, \ldots, i_d+1$ de A. Então A' tem $\delta - 1$ linhas e d colunas. Como $d \leq \delta - 1$, a matriz A'' formada pelas d primeiras linhas de A' é uma matriz quadrada $d \times d$ e

$$A'' \begin{bmatrix} c_{i_1} \\ \vdots \\ c_{i_d} \end{bmatrix} = 0 \ ,$$

portanto $\det(A'') = 0$ porque $(c_{i_1}, \ldots, c_{i_d})$ é uma solução não nula do sistema linear homogénio $A''x = 0$. Por outro lado, como

$$A'' = \begin{bmatrix} (\alpha^{a+1})^{i_1} & (\alpha^{a+1})^{i_2} & \cdots & (\alpha^{a+1})^{i_d} \\ (\alpha^{a+2})^{i_1} & (\alpha^{a+2})^{i_2} & \cdots & (\alpha^{a+2})^{i_d} \\ \vdots & \vdots & & \vdots \\ (\alpha^{a+\delta-1})^{i_1} & (\alpha^{a+\delta-1})^{i_2} & \cdots & (\alpha^{a+\delta-1})^{i_d} \end{bmatrix} \ ,$$

usando as propriedade de multilinearidade do determinante nas colunas obtém-se

$$\begin{aligned} \det(A'') &= \prod_{j=1}^{d} (\alpha^{a+1})^{i_j} \det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_d} \\ \vdots & \vdots & & \vdots \\ (\alpha^{d-1})^{i_1} & (\alpha^{d-1})^{i_2} & \cdots & (\alpha^{d-1})^{i_d} \end{bmatrix} \\ &= \prod_{j=1}^{d} (\alpha^{a+1})^{i_j} \prod_{1 \leq k < l \leq d} (\alpha^{i_l} - \alpha^{i_k}) \ . \end{aligned}$$

Logo, $\det(A'') \neq 0$ pois $\alpha^{i_l} \neq \alpha^{i_k}$, porque α é um elemento primitivo e $d \leq \delta - 1 \leq q - 2$. Como não podemos ter simultaneamente $\det(A'') = 0$ e $\det(A'') \neq 0$, concluimos que $d \geq \delta$. □

Observação 9.8. Na demonstração do teorema anterior apenas se usou o facto de C ser o conjunto dos elementos $c(t) \in R_n$ que se anulam em todas as raízes do polinómio gerador $g(t)$ (o qual foi provado para qualquer código cíclico tal que as raízes de $g(t)$ são todas distintas) e o facto de $\delta - 1$ potências consecutivas de um elemento primitivo $\alpha \in \mathbb{F}_q$ serem raízes de $g(t)$ (para se obter uma matriz de Vandermonde no segundo cálculo de $\det(A'')$). Os códigos cíclicos que satisfazem estas condições dizem-se *códigos BCH*[1]. Os códigos Reed-Solomon são uma subfamília dos códigos BCH.

[1]Estes códigos foram descobertos por A. Hocquenghem em 1959 e, de forma independente, por R. C. Bose e D. K. Ray-Chaudhuri em 1960

Exemplo 9.9. Seja C o código de comprimento 7, binário, com polinómio gerador $g(t) = 1+t+t^3 \in \mathbb{F}_2[t]$. Como $g(t)$ é irredutível em $\mathbb{F}_2[t]$, podemos considerar $\mathbb{F}_8 = \mathbb{F}_2[t]/\langle g(t)\rangle$. Seja $\alpha \in \mathbb{F}_8$ uma raiz de $g(t)$. Então

$$g(t) = (t-\alpha)(t-\alpha^2)(t-\alpha^4) \ .$$

C não é um código Reed-Solomon, mas satisfaz as condições na Obeservação 9.8 com $\delta - 1 = 2$. Portanto podemos concluir que $\mathrm{d}(C) \geq \delta = 3$. Como $\mathrm{w}(g(t)) = 3$ (e $g(t) \in C$, claro!), então $\mathrm{d}(C) = 3$, resultado já conhecido pois $C = \mathrm{Ham}(3, 2)$.

Corolário 9.10. *Os códigos Reed-Solomon são códigos MDS.*

Dem. Seja C um código Reed-Solomon de parâmetros $[q-1, q-\delta]_q$. O polinómio gerador tem grau $r = \delta - 1$. Então $\mathrm{d}(C) \geq \delta$, pelo Teorema 9.7, e $\mathrm{d}(C) \leq \delta$, pela desigualdade de Singleton. □

Exemplo 9.11. Considere o código Reed-Solomon C sobre $\mathbb{F}_{16}$ com polinómio gerador $g(t) = \prod_{i=1}^{6}(t-\alpha^i)$, onde α é um elemento primitivo de $\mathbb{F}_{16}$. O código C tem comprimento $n = q-1 = 15$, dimensão $n - \deg(g(t)) = 9$ e, pelo teorema anterior, distância mínima $\mathrm{d}(C) = 7$. Para determinarmos $\mathrm{d}(C)$ usando o Teorema 4.16, como uma matriz de paridade H tem 6 linhas e 15 colunas, teriamos que verificar que

$$\binom{15}{6} = 5005$$

conjuntos de 6 colunas de H são linearmente independentes.

2. Extensão de códigos Reed-Solomon

Recorde que, para um código C qualquer com alfabeto $\mathbb{F}_q$, a extensão por paridade é definida por

$$\widehat{C} = \left\{(x, x_{n+1}) \in \mathbb{F}_q^{n+1} \ : \ x \in C,\, x_{n+1} = -\sum_{i=1}^{n} x_i\right\}$$

e, se C é linear de parâmetros $[n, k, d]$, a sua extensão $\widehat{C}$ também é linear e os seus parâmetros são $[n+1, k, \widehat{d}]$, com $d \leq \widehat{d} \leq d+1$.

Teorema 9.12. *Seja C um código Reed-Solomon com polinómio gerador*

$$g(t) = (t-\alpha)(t-\alpha^2)\cdots(t-\alpha^{\delta-1})$$

com $2 \leq \delta \leq q-1$ e α um elemento primitivo de $\mathbb{F}_q$. Então o código estendido $\widehat{C}$ é MDS.

Dem. Como o código C tem parâmetros $[q-1, q-\delta, \delta]_q$, porque é MDS, queremos mostrar que $\mathrm{d}(\widehat{C}) = \delta + 1$. Pela observação anterior ao teorema, ou pela desigualdade de Singleton, já sabemos que $\mathrm{d}(\widehat{C}) \leq \delta + 1$. Vamos então mostrar a desigualdade contrária. Seja

$$c(t) = \sum_{i=0}^{q-2} c_i t^i \in C \setminus \{0\} \qquad \text{e} \qquad \widehat{c} = (c_0, c_1, \ldots, c_{q-2}, -\sum_{i=0}^{q-2} c_i) \in \widehat{C} \ .$$

Então $\widehat{c} \neq 0$, porque $c(t) \neq 0$, e $\widehat{c} = (c_0, c_1, \ldots, c_{q-2}, -c(1))$, porque $c(1) = \sum_{i=0}^{q-1} c_i$. Como $c(t) \in C = \langle g(t)\rangle$, então $c(t) = f(t)g(t)$, para algum $f(t) \in \mathbb{F}_q[t]$ e, portanto, $c(1) = f(1)g(1)$.

Também temos que $g(1) \neq 0$ porque as raízes de $g(t)$ são $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$ com $\delta - 1 \leq q-2$, ou seja, nenhuma das raízes é 1 porque α tem ordem $q-1$. Há dois casos a considerar.

Caso 1: Se $f(1) \neq 0$, então $-c(1) \neq 0$, logo $\mathrm{w}(\widehat{c}) = \mathrm{w}(c) + 1 \geq \delta + 1$, pois $c \in C \setminus \{0\}$.

Caso 2: Se $f(1) = 0$, então $f(t) = u(t)(t-1)$ para algum $u(t) \in \mathbb{F}_q[t]$, donde $c(t) = u(t)(t-1)g(t)$ e, como $(t-1)g(t)$ divide $t^n - 1$ pois $g(1) \neq 0$, $(t-1)g(t)$ é o polinómio gerador de um código C' e $c(t) \in \langle (t-1)g(t) \rangle = C'$. Facilmente se vê que

$$(t-1)g(t) = (t - \alpha^{a+1})(t - \alpha^{a+2}) \cdots (t - \alpha^{a+\delta}) \ ,$$

com $a = q - 2 \geq 0$, e ainda $\deg(g(t)) \leq q-2$, pois caso contrário teriamos $(t-1)g(t) = t^{q-1} - 1$ e $C' = \langle t^{q-1} - 1 \rangle = \{0\}$, o que é impossível porque $c \in C'$ e $c \neq 0$. Como consequência, $(t-1)g(t)$ é o polinómio gerador de um código Reed-Solomon de parâmetros $[q-1, q-\delta']$, onde $\delta' = \delta + 1 \leq q-2$, logo $\mathrm{d}(C') = \delta'$ e, portanto, $\mathrm{w}(\widehat{c}) = \mathrm{w}(c) \geq \delta' = \delta + 1$.

Em ambos os casos, provámos que $\mathrm{w}(\widehat{c}) \geq \delta + 1$ para qualquer palavra de código $\widehat{c} \in \widehat{C}$ não nula, ou seja, $\mathrm{d}(\widehat{C}) = \mathrm{w}(\widehat{C}) \geq \delta + 1$. □

Exemplo 9.13. Considere o código Reed-Solomon, sobre $\mathbb{F}_7$, com o polinómio gerador $g(t) = (t - 3^2)(t - 3^3)(t - 3^4)$ do Exemplo 9.3. Como C tem parâmetros $[6, 3, 4]$, o código estendido $\widehat{C}$ tem parâmetros $[7, 3, 5]$, pelo teorema anterior. C corrige qualquer erro simples porque $\lfloor \frac{\mathrm{d}(C)-1}{2} \rfloor = 1$, mas $\widehat{C}$ corrige qualquer erro de peso ≤ 2 porque $\lfloor \frac{\mathrm{d}(\widehat{C})-1}{2} \rfloor = 2$.

Exemplo 9.14. Considere o código Reed-Solomon C, sobre $\mathbb{F}_7$, com o polinómio gerador $g(t) = (t - 3^0)(t - 3^1) = (t-1)(t-3)$. Portanto, C é um código $[6, 4, 3]$, $h(t) = (t^6 - 1)/g(t) = 2 + 5t + 6t^2 + 4t^3 + t^4$ é o polinómio de paridade,

$$H = \begin{bmatrix} 1 & 4 & 6 & 5 & 2 & 0 \\ 0 & 1 & 4 & 6 & 5 & 2 \end{bmatrix}$$

é uma matriz de paridade para C, e

$$\widehat{H} = \begin{bmatrix} 1 & 4 & 6 & 5 & 2 & 0 & 0 \\ 0 & 1 & 4 & 6 & 5 & 2 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

é uma matriz de paridade para $\widehat{C}$. Por definição de extensão de paridade, os parâmetros de $\widehat{C}$ são $[7, 4, \widehat{d}]$, com $3 \leq \widehat{d} \leq 4$. Além disso, se c_i denota a i-ésima coluna de $\widehat{H}$, como $c_1 + c_3 + 5c_6 = 0$ então $\widehat{d} \leq 3$, pelo Teorema 4.16, donde se conclui que $\widehat{d} = 3$ e, portanto, $\widehat{C}$ não é um código MDS. Porque é que este exemplo não contradiz o Teorema 9.12?

3. Concatenação de códigos Reed-Solomon

Como já se observou anteriormente, não existem códigos Reed-Solomon binários. No entanto, códigos binário são importantes do ponto de vista das aplicações. Nesta secção vamos estudar alguns códigos binários obtidos à custa de códigos Reed-Solomon. Seja então C um código Reed-Solomon de parâmetros $[2^m - 1, 2^m - \delta, \delta]$ sobre $\mathbb{F}_{2^m}$.

Caso 1: A concatenação de C com o código trivial $\mathbb{F}_2^m$ é um código binário C^* de parâmetros $[m(2^m - 1), m(2^m - \delta), d^*]$, com $d^* = \mathrm{d}(C^*) \geq \delta$, porque $\mathbb{F}_2^m$ é um código $[m, m, 1]_2$.

Caso 2: A concatenação de C com o código dos pesos pares $E_{m+1} = \{x \in \mathbb{F}_2^{m+1} : \mathrm{w}(x) \text{ é par}\}$ é um código binário C' de parâmetros $[(m+1)(2^m-1), m(2^m-\delta), d']$, com $d' = \mathrm{d}(C') \geq 2\delta$, porque E_{m+1} é um código $[m+1, m, 2]_2$.

Em ambos os casos aplicámos a Propoposição 5.15 sobre concatenação de códigos lineares.

Note que C^* e C' têm a mesma dimensão, mas $\mathrm{d}(C')$ pode ser cerca do dobro de $\mathrm{d}(C^*)$. Por isso, o código C' é mais útil para correcção de erros aleatórios, mas C^* é mais útil para correcção de erros acumulados — ver Teorema 9.16.

Recordando, do Capítulo 5, a definição de concatenação: Seja $\phi : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_2^m$ um isomorfismo linear sobre $\mathbb{F}_2$, então

$$C^* = \phi^*(C) = \{(\phi(c_1), \ldots, \phi(c_n)) : (c_1, \ldots, c_n) \in C\} .$$

Seja $\widehat{\phi} : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_2^{m+1}$ definido por $\widehat{\phi}(x) = (\phi(x), y_{m+1})$, onde $\phi(x) = (y_1, \ldots, y_m)$ e $y_{m+1} = \sum_{i=1}^m y_i$, ou seja, $y_{m+1} \in \mathbb{F}_2$ é escolhido de modo ao peso $\mathrm{w}(\widehat{\phi}(x))$ ser par. Portanto

$$\widehat{\phi} : \mathbb{F}_{2^m} \longrightarrow E_{m+1}$$

é um isomorfismo vectorial sobre $\mathbb{F}_2$, donde concluimos que o código $C' = \widehat{\phi}^*(C)$ tem distância mínima par.

Exemplo 9.15. Seja $\mathbb{F}_8 = \mathbb{F}[t]/\langle 1 + t + t^3 \rangle$ e $\alpha \in \mathbb{F}_8$ uma raiz de $1 + t + t^3$. Seja $\phi : \mathbb{F}_8 \longrightarrow \mathbb{F}_2^3$ definido por $\phi(a_0 + a_1\alpha + a_2\alpha^2) = (a_0, a_1, a_2)$. Considere o código Reed-Solomon C com polinómio gerador

$$g(t) = (t-\alpha)(t-\alpha^2)\cdots(t-\alpha^6) = 1 + t + t^2 + \cdots + t^6 .$$

Uma base de C como espaço vectorial sobre $\mathbb{F}_2$ é

$$\{(1,1,1,1,1,1,1), (\alpha,\alpha,\alpha,\alpha,\alpha,\alpha,\alpha), (\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2)\} .$$

Logo, $C^* = \phi^*(C)$ é o espaço vectorial sobre $\mathbb{F}_2$ gerado por

$$\begin{aligned} \phi^*(1,1,1,1,1,1,1) &= (100, 100, \ldots, 100) , \\ \phi^*(\alpha,\alpha,\alpha,\alpha,\alpha,\alpha,\alpha) &= (010, 010, \ldots, 010) \text{ e} \\ \phi^*(\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2) &= (001, 001, \ldots, 001) . \end{aligned} \tag{9.2}$$

Como C é um código $[7,1,7]$ sobre $\mathbb{F}_8$, os parâmetros de C^* são $[21, 3, d^*]$ com $d^* \geq 7$. Neste caso temos mesmo $d^* = 7$ — justifique! A partir de ϕ, definimos $\widehat{\phi} : \mathbb{F}_8 \longrightarrow \mathbb{F}_2^4$ por

$$\widehat{\phi}(a_0 + a_1\alpha + a_2\alpha^2) = (a_0, a_1, a_2, a_0 + a_1 + a_2) .$$

Portanto $C' = \widehat{\phi}^*(C)$ é gerado por

$$\begin{aligned} \widehat{\phi}^*(1,1,1,1,1,1,1) &= (1001, 1001, \ldots, 1001) , \\ \widehat{\phi}^*(\alpha,\alpha,\alpha,\alpha,\alpha,\alpha,\alpha) &= (0101, 0101, \ldots, 0101) \text{ e} \\ \widehat{\phi}^*(\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2) &= (0011, 0011, \ldots, 0011) , \end{aligned} \tag{9.3}$$

ou seja, a cada bloco de comprimeto 3 dos vectores (9.2) da base de C^* acrescentou-se um dígito de paridade, para obter os blocos de comprimento 4 dos vectores (9.3) da base de C'.

Teorema 9.16. *Seja C um código linear sobre $\mathbb{F}_{2^m}$. Então a concatenação $C^* = \phi^*(C)$, de C com o código trivial $\mathbb{F}_2^m$, corrige os erros acumulados de comprimento até $m(T-1)+1$, onde $T = \lfloor \frac{\mathrm{d}(C)-1}{2} \rfloor$.*

Dem. Seja n o comprimento do código C e seja $l = m(T-1)+1$. Vamos ver que todos os erros acumulado de comprimento menor ou igual a l pertencem a classes $y + C$ distintas.

Sejam $\vec{e}$ e $\vec{f}$ dois erros acumulados, distintos, de comprimento $\leq l$. Se $\phi : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_2^m$ é um isomorfismo linear sobre $\mathbb{F}_2$, $\phi^* : (\mathbb{F}_{2^m})^n \longrightarrow \mathbb{F}_2^{mn}$ também é. Sejam $\vec{x} = (\phi^*)^{-1}(\vec{e})$ e $\vec{y} = (\phi^*)^{-1}(\vec{f})$. Pondo $\vec{x} = (x_1, \ldots, x_n)$, com $x_i \in \mathbb{F}_{2^m}$, fica

$$\vec{e} = (\phi(x_1), \ldots, \phi(x_n)) = (0, 0, \ldots, 0, \underbrace{1, *, \ldots, *, 1}_{\leq l \text{ coordenadas}}, 0, \ldots, 0) \ ,$$

onde cada $\phi(x_i) \in \mathbb{F}_2^m$. Identificar $\phi(x_1), \ldots, \phi(x_n)$ no vector dado $\vec{e}$ corresponde a separar as mn coordenadas de $\vec{e}$ em blocos de comprimento m. O caso com mais $\phi(x_i)$ não nulos acontece quando a primeira coordenada não nula de $\vec{e}$ é a última coordenada de um bloco $\phi(x_j)$. Neste caso, há no máximo $1 + \lceil \frac{l-1}{m} \rceil$ blocos $\phi(x_i)$ que podem conter coordenadas não nulas de $\vec{e}$. Como ϕ é injectiva, $\phi(x_i) = 0$ se e só se $x_i = 0$, portanto

$$\mathrm{w}(\vec{x}) \leq 1 + \left\lceil \frac{l-1}{m} \right\rceil = T \ .$$

E analogamente se tem $\mathrm{w}(\vec{y}) \leq T$. Como $\vec{x} \neq \vec{y}$, porque $\vec{e} \neq \vec{f}$, e como ambos têm peso $\leq T$, então $\vec{x}$ e $\vec{y}$ são chefes de classes distintas. □

Exemplo 9.17. O código C^* do Exemplo 9.15 corrige apenas erros aleatórios de peso $\leq 3 = T$, mas corrige todos os erros acumulados de comprimento $\leq 7 = m(T-1)+1$.

Exercícios

9.1. Escreva uma matriz geradora e uma matriz de paridade para um código Reed-Solomon $[6, 4]$, e determine a distância mínima desse código.

9.2. Determine o polinómio gerador de um código Reed-Solomon, sobre $\mathbb{F}_{16}$, de dimensão 11. Escreva uma matriz de paridade para este código.

9.3. Mostre que o dual de um código Reed-Solomon é também um código Reed-Solomon.

9.4. Seja C o código Reed-Solomon sobre $\mathbb{F}_8$ com polinómio gerador $g(t) = (t-\alpha)(t-\alpha^2)(t-\alpha^3)$, onde $\alpha \in \mathbb{F}_8$ é uma raiz de $1 + t + t^3$.
   (a) Justifique que α é um elemento primitivo de $\mathbb{F}_8$.
   (b) Determine os parâmetros de C.
   (c) Determine os parâmetros do código dual $C^\perp$.
   (d) Determine os parâmetros da extensão $\widehat{C}$.
   (e) Determine os parâmetros da concatenação $C^* = \phi^*(C)$, onde $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ é a aplicação linear definida por $\phi(1) = 100$, $\phi(\alpha) = 010$ e $\phi(\alpha^2) = 101$.

9.5. (a) Escreva o polinómio gerador para um código Reed-Solomon C, de parâmetros $[7, 2]$.
(b) Seja α uma raiz do polinómio $1+t+t^3 \in \mathbb{F}_2[t]$ e considere a aplicação $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ definida por $\phi(a_0 + a_1\alpha + a_2\alpha^2) = (a_0, a_1, a_2)$. Determine os parâmetros de $C^* = \phi^*(C)$.
(c) Seja $\widehat{\phi} : \mathbb{F}_8 \to \mathbb{F}_2^4$ definida por $\widehat{\phi}(a_0 + a_1\alpha + a_2\alpha^2) = (a_0, a_1, a_2, a_0 + a_1 + a_2)$. Determine os parâmetros de $C' = \widehat{\phi}^*(C)$.
(d) O que pode concluir acerca da capacidade de correcção de erros aleatórios e/ou erros acumulados de C^* e de C'?

9.6. Considere o código Reed-Solomon C sobre $\mathbb{F}_8$ com o seguinte polinómio gerador:

$$g(t) = (t-\alpha)(t-\alpha^2)(t-\alpha^3)(t-\alpha^4) = \alpha^3 + \alpha t + t^2 + \alpha^3 t^3 + t^4 \ ,$$

onde identificamos $\mathbb{F}_8$ com o quociente $\mathbb{F}_2[t]/\langle 1+t+t^3\rangle$, e $\alpha \in \mathbb{F}_8$ é uma raiz de $1+t+t^3$.
(a) Indique, justificando, os parâmetros $[n, k, d]$ de C.
(b) Utilize o Algoritmo Caça ao Erro para descodificar os vectores recebidos

$$y = (0, 1, 0, \alpha^2, 0, 0, 0) \quad \text{e} \quad z = (0, \alpha^3, 0, 1, \alpha^3, 1, 1).$$

(c) Seja $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ um isomorfismo vectorial sobre $\mathbb{F}_2$. O que pode concluir sobre a capacidade de correcção de erros acumulados do código concatenação $C^* = \phi^*(C)$?

9.7. Um código linear C diz-se *auto-ortogonal* se $C \subseteq C^\perp$. Determine o polinómio gerador de todos os códigos Reed-Solomon, sobre $\mathbb{F}_{16}$, auto-ortogonais. Quais desses códigos são auto-duais?

9.8. Considere o códio sobre $\mathbb{F}_{11}$ com matriz geradora

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

Na Ficha 6, já se justificou que este código é equivalente a um código cíclico C. Determine o polinómio gerador e conclua que C é um código Reed-Solomon.

9.9. Generalize o exercício anterior para um código $[q-1, k]$ sobre $\mathbb{F}_q$ com matriz geradora

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{2(q-2)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \alpha^{3(k-1)} & \cdots & \alpha^{(q-2)(k-1)} \end{bmatrix} \ ,$$

onde α é um elemento primitivo de $\mathbb{F}_q$.