CAPÍTULO 8

Códigos Cíclicos

1. Introdução

Um código linear C tem várias vantagens em relação a um código arbitrário sem qualquer estrutura adicional: C fica completamente descrito por uma matriz geradora (apenas k palavras em vez da lista de todas as q^k palavras de código), é mais fácil testar se uma dada palavra pertence ao código através de uma matriz de paridade, há algoritmos de descodificão que requerem "pouca informação armazenada" (pelo menos em relação a um código qualquer). Os códigos cíclicos são uma subclasse dos códigos lineares que ainda requerem menos informação para se poder descrever todas as palavras de código, basta um polinómio de grau menor do que o comprimento das palavras, e com algoritmos de descodificação mais eficientes. Além disso, os códigos de Hamming binários, os códigos de Golay G_{11} e G_{23}, e outras famílias importantes (como, por exemplos, os códigos BCH, Reed-Solomom e Goppa) são códigos cíclicos.

Definição 8.1. Um código C diz-se *cíclico* se

(i) C é linear (portanto C é subespaço de algum $\mathbb{F}_q^n$) e

(ii) se $x = (x_1, x_2, \ldots, x_{n-1}, x_n) \in C$, então $(x_n, x_1, x_2, \ldots, x_{n-1}) \in C$.

O vector $(x_n, x_1, x_2, \ldots, x_{n-1}) \in \mathbb{F}_q^n$ diz-se um *desvio cíclico* de $x \in \mathbb{F}_q^n$, e iremos denotá-lo por $\sigma(x)$. Portanto, um código é cíclico se é linear e se contém os desvios cíclicos de todas as palavras de código. Mais geralmente, se C é um código cíclico, então $\sigma^i(c) \in C$ para todo o $c \in C$ e todo o $i \in \mathbb{Z}$ — ver Exercício 8.2.

Exemplo 8.2.
- Os códigos triviais $\{\vec{0}\}$ e $\mathbb{F}_q^n$ são cíclicos.
- O código binário $E_2 = \{000, 110, 101, 011\}$ é cíclico.
- O código simplex $S(3,2) = \{0000000, 1011100, 0101110, 0010111, 1001011, 1100101, 1110010, 0111001\}$ é cíclico.
- $C_1 = \{0000, 1010, 0101, 1111\}$ é um código cíclico.

- O código $C_2 = \{0000, 1001, 0110, 1111\}$ não é cíclico, embora seja linear, e é equivalente ao código C_1 do ponto anterior.
- O código $C_3 = \{0000, 1010, 0101\}$ não é cíclico porque não é linear, mas contém todos os desvios cíclicos.
- $\mathrm{Ham}(2, 3)$ não é cíclico nem equivalente a um código cíclico — a ver mais tarde.

Teorema 8.3. *O dual de um código cíclico é ainda um código cíclico.*

Dem. Seja C um código cíclico de comprimento n. Como o dual de um código linear é linear, só temos de verificar a condição (ii) na definição de código cíclico para $C^\perp$. Por definição de dual e porque C é cíclico,

$$x \in C^\perp \iff x \cdot \sigma^{-1}(c) = 0 \quad \forall\, c \in C \ ,$$

mas como

$$x \cdot \sigma^{-1}(c) = \sum_{i=1}^{n} x_i c_{i+1} = \sigma(x) \cdot c \ ,$$

onde os índices são tomados módulo n, fica

$$x \in C^\perp \iff \sigma(x) \in C^\perp \ . \qquad \square$$

Como consequência deste teorema e do terceiro ponto do Exemplo 8.2, o código de Hamming binário $\mathrm{Ham}(3, 2)$ é cíclico. Iremos ver que qualquer código de Hamming binário é equivalente a um código cíclico. Tal não se verifica, em geral, para os códigos de Hamming q-ários.

2. Polinómio gerador

Iniciamos esta secção apresentando algumas noções de álgebra de que iremos precisar já de seguida. Os anéis que iremos considerar no resto do capítulo são o anel dos polinómios $\mathbb{F}_q[t]$ e quocientes deste, por isso vamos sempre assumir que R é um anel comutativo com unidade.

Definição 8.4. O subconjunto não vazio $I \subseteq R$ diz-se um *ideal* de R se é fechado para a soma e para o produto por qualquer elemento de R, mais precisamente, se $a + b \in I$ e $ar \in I$ para todo o $a, b \in I$ e $r \in R$.

Dado $a \in R$, o conjunto $\langle a \rangle := \{ar : r \in R\}$ é um ideal (verifique) e diz-se o *ideal gerado por* r e o elemento a diz-se um *gerador* do ideal, e pode não ser único. Mais geralmente, o conjunto $\langle a_1, \ldots, a_N \rangle := \{\sum_i a_i r_i : r_i \in R\}$ é um ideal e $\{a_1, \ldots, a_N\}$ diz-se um conjunto gerador.

Definição 8.5. Um ideal $I \subset R$ diz-se um *ideal principal* se $I = \langle a \rangle$ para algum $a \in R$. Se todos os ideais são principais, R diz-se um *anel de ideais principais*[1].

Exemplo 8.6.
- O conjunto $\{0\}$ e o próprio anel $R = \langle 1 \rangle$ são ideais principais.
- Se R é um corpo, $\{0\}$ e R são os únicos ideais.
- No anel dos inteiros $\mathbb{Z}$, o conjunto dos números pares é um ideal e também é principal: $\langle 2 \rangle = \{2x : x \in \mathbb{Z}\}$. O inteiro -2 também é um gerador deste ideal.

[1] E se R for um domínio integral onde todos os ideias são principais, dizemos que R é um domínio de ideais principais ou, abreviadamente, um d.i.p.

- Em $\mathbb{Z}[t]$, o ideal $\langle 2, t\rangle$ não é principal.

Teorema 8.7. *$\mathbb{F}_q[t]$ é um anel de ideais principais[2]. Mais concretamente, se $I \neq \{0\}$ é um ideal, então $I = \langle g(t)\rangle$, onde $g(t)$ é um polinómio mónico de grau mínimo em I. Além disso, este $g(t)$ é único.*

Dem. Seja $I \neq \{0\}$ um ideal de $\mathbb{F}_q[t]$. Seja $g(t)$ um polinómio não nulo de grau mínimo em I. Sem perda de generalidade, podemos assumir que $g(t)$ é mónico (caso não seja, multiplicamos $g(t)$ pelo inverso do coeficiente de maior grau). Queremos ver que este $g(t)$ é um gerador do ideal I. Seja $a(t)$ um elemento em I qualquer. Pelo algoritmo da divisão em $\mathbb{F}_q[t]$, existem polinómios $q(t)$ e $r(t)$ tais que $a(t) = g(t)q(t) + r(t)$, com $\deg(r(t)) < \deg(g(t))$, portanto $r(t) = a(t) - g(t)q(t) \in I$. Como $g(t)$ tem grau mínimo entre os polinómios não nulos em I, então o resto $r(t)$ é nulo e $a(t) = g(t)q(t) \in \langle g(t)\rangle$. Como $a(t) \in I$ é arbitário, conclui-se que $I \subseteq \langle g(t)\rangle$. E como $g(t) \in I$, também se verifica a inclusão inversa $I \supseteq \langle g(t)\rangle$, donde $I = \langle g(t)\rangle$.
Deixamos como exercício verificar que existe um único polinómio mónico gerador do ideal I. □

Com o mesmo tipo de demonstração, usando o algoritmo da divisão para os inteiros, também se prova que $\mathbb{Z}$ é um anel de ideais principais. O caso do anel $\mathbb{F}_q[t]$ vai ser útil no contexto dos códigos cíclicos.

Vamos agora traduzir a condição combinatórica dos desvios cíclicos na Definição 8.1 numa condição algébrica. Considere o anel quociente $R_n = \mathbb{F}_q[t]/\langle t^n - 1\rangle$. Este anel tem uma estrutura natural de espaço vectorial sobre $\mathbb{F}_q$. Considere a aplicação linear, sobre $\mathbb{F}_q$,

$$\begin{aligned} \varphi : \mathbb{F}_q^n &\longrightarrow R_n \\ a = (a_0, a_1, \ldots, a_{n-1}) &\longmapsto a(t) = a_0 + a_1 t + \cdots + a_{n-2}t^{n-2} + a_{n-1}t^{n-1} \end{aligned}$$

Como cada classe em R_n tem um único representate em $\mathbb{F}_q[t]$ de grau menor ou igual a $n-1$ (nomeadamente o resto da divisão por $t^n - 1$), a aplicação φ é um isomorfismo vectorial (verifique!), além disso

$$\begin{aligned} \varphi(\sigma(a)) &= \varphi(a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \\ &= a_{n-1} + a_0 t + \cdots + a_{n-2}t^{n-1} \\ &= ta(t) \ , \end{aligned}$$

onde se usou $t^n = 1$, em R_n, no último passo. Portanto

$$\boxed{\varphi(\sigma(a)) = t\varphi(a)} \tag{8.1}$$

ou seja, tomar o desvio cíclico $\sigma(a)$ em $\mathbb{F}_q^n$ corresponde à multiplicação por t em R_n.

Teorema 8.8. *Um subconjunto $C \subseteq \mathbb{F}_q^n$ não vazio é um código cíclico se e só se $I = \varphi(C)$ é um ideal de R_n.*

Dem. ($\Longleftarrow$) Como I é um ideal, então I é fechado para a soma e para o produto por escalares (que são identificados com os polinómio constantes em R_n), ou seja, I é um subespaço vectorial de

[2]Este resultado verifica-se para $K[t]$, onde K é um corpo qualquer, não necessarimente finito

R_n, portanto $C = \varphi^{-1}(I)$ é um subespaço vectorial de $\mathbb{F}_q^n$. Como I é fechado para o produto por t, porque é um ideal, então, por (8.1), C é fechado para desvios cíclicos.

($\Longrightarrow$) Como qualquer elemento de R_n é combinação linear de $1, t, \ldots, t^{n-1}$ e I é um subespaço vectorial de R_n, basta verificar que I é fechado para o produto por t^k, com $0 < k < n$.

Por indução em k:

$k = 1$: Seja $a(t) \in I$ e seja $a = \varphi^{-1}(a(t)) \in C \subseteq \mathbb{F}_q^n$. Como C é cíclico, então $\sigma(a) \in C$, logo $\varphi(\sigma(a)) = ta(t) \in I$, por (8.1).

$k \Rightarrow k+1$: Se $a(t) \in I$, então $t^k a(t) \in I$, por hipótese de indução, logo $t^{k+1}a(t) = t(t^k a(t)) \in I$, pela base de indução. □

Exemplo 8.9. (a) Ao código trivial $C = \{\vec{0}\} \subset \mathbb{F}_q^n$ corresponde o ideal trivial $I = \{0\} \subset R_n$.

(b) Ao código trivial $C = \mathbb{F}_q^n$ corresponde o ideal trivial $I = R_n$.

(c) Para o código dos pesos pares $E_3 = \{000, 110, 101, 011\} \subset \mathbb{F}_2^3$, tem-se

$$I = \varphi(E_3) = \{0, 1+t, 1+t^2, t+t^2\} \subset R_3 = \mathbb{F}_2[t]/\langle t^3 - 1\rangle \ .$$

Como $t + t^2 = t(1 + t)$ e $1 + t^2 \equiv t^2(1 + t) \pmod{t^3 - 1}$, então $I = \langle 1 + t\rangle$. Mas também é verdade que $I = \langle 1 + t^2\rangle = \langle t + t^2\rangle$, como ideal em R_3.

(d) Para o código binário $C_1 \subset \mathbb{F}_2^4$ do Exemplo 8.2, o ideal correspondente em R_4 é $I = \varphi(C) = \{0, 1 + t^2, t + t^3, 1 + t + t^2 + t^3\} = \langle 1 + t^2\rangle$, que também é gerado por $t + t^3$.

Tendo em conta o Teorema 8.8, interessa caracterizar os ideais de R_n. Considere a aplicação quociente, que é um homomorfismo de anéis,

$$\pi : \mathbb{F}_q[t] \longrightarrow R_n = \mathbb{F}_q[t]/\langle t^n - 1\rangle \ .$$

Lema 8.10. *Se J é um ideal em $\mathbb{F}_q[t]$ então $\pi(J)$ é um ideal em R_n. Se I é um ideal em R_n, então $\pi^{-1}(I)$ é um ideal em $\mathbb{F}_q[t]$ que contém $t^n - 1$.*

Dem. O resultado segue da definição de ideal, tendo em conta que a imagem e a pré-imagem de conjuntos são, respectivamente,

$$\pi(J) := \{\pi(j) \in R_n \ : \ j \in J\} \qquad \text{e} \qquad \pi^{-i}(I) := \{i \in \mathbb{F}_q[t] \ : \ \pi(i) = [i] \in I\} \ . \qquad \square$$

Como consequência deste lema, a aplicação π define uma correspondência biunívoca[3] entre os ideais no quociente R_n e os ideais contendo $t^n - 1$ no anel dos polinómios $\mathbb{F}_q[t]$.

Exemplo 8.11. Considere o ideal $I = \langle 1 + t\rangle \subset R_3$ associado ao código E_3 (ver Exemplo 8.9). De acordo com o Lema 8.10, $\pi^{-1}(I) = \langle 1 + t, 1 + t^2, t + t^2, t^3 - 1\rangle$, mas como

$$1 + t^2 = (1 + t)^2 \ , \qquad t + t^2 = (t + 1)t \qquad \text{e} \qquad t^3 - 1 = (t + 1)(1 + t + t^2) \ ,$$

ou seja, como os três polinómios $1+t^2$, $t+t^2$ e t^3-1 são múltiplos de $t+1$, então $\pi^{-1}(I) = \langle 1+t\rangle \subset \mathbb{F}_2[t]$.

[3]Esta caracterização dos ideais no anel quociente R/A é válida para qualquer anel comutativo R e qualquer ideal $A \subset R$, não necessariamente principal.

Observação 8.12. Nota à notação e terminologia: Recorde que os elementos de R_n são classes de equivalência de polinómios, geralmente identificados com um representante muito "especial", o resto da divisão por $t^n - 1$. Definimos, portanto, grau de um elemento de R_n como o grau deste representante. Rigorosamente, para qualquer $f(t) \in \mathbb{F}_q[t]$, definimos o grau da classe $[f(t)] \in R_n$ por

$$\deg([f(t)]) := \min\{\deg(k(t)) : k(t) \equiv f(t) \pmod{t^n - 1}\} .$$

Portanto, o grau dos elementos de R_n é sempre menor do que n. Note ainda que, em $\mathbb{F}_q[t]$ é sempre verdade que $\deg(a(t)b(t)) = \deg(a(t)) + \deg(b(t))$, mas em R_n apenas se verifica que

$$\deg(a(t)b(t)) \leq \deg(a(t)) + \deg(b(t)) \quad \forall\, a(t), b(t) \in R_n .$$

Por exemplo, em R_3, $t - 1$ e $1 + t + t^2$ têm graus 1 e 2 respectivamente, mas o seu produto $(t - 1)(1 + t + t^2) = t^3 - 1$ representa a classe nula em R_3, tendo portanto grau $-\infty$ e não grau 3.

Teorema 8.13. *R_n é um anel de ideais principais. Mais concretamente, se $I \neq \{0\}$ é um ideal em R_n, então $I = \langle g(t)\rangle$, onde $g(t)$ é um polinómio mónico de grau mínimo em I. Além disso, este $g(t)$ é único, $g(t)|t^n - 1$ e $g_0 = g(0) \neq 0$.*

Dem. Seja $I \neq \{0\}$ um ideal em R_n e seja $J = \pi^{-1}(I)$. Pelo Lema 8.10, J é um ideal em $\mathbb{F}_q[t]$ que contém $t^n - 1$. Pelo Teorema 8.7, existe um único polinómio mónico $g(t)$ de grau mínimo em J tal que $J = \langle g(t)\rangle \subseteq \mathbb{F}_q[t]$. Como $t^n - 1 \in J$, então $g(t)$ divide $t^n - 1$ e, como consequência, também se verifica que $g(0) \neq 0$ (caso contrário t seria um divisor de $t^n - 1$ en $\mathbb{F}_q[t]$). Aplicando o Lema 8.10 novamente, $I = \pi(J)$ é gerado pela classe $[g(t)]$ (note que $\pi(\pi^{-1}(A)) = A$, para qualquer $A \subseteq R_n$, porque π é uma aplicação sobrejectiva). □

Definição 8.14. O polinómio $g(t) \in \mathbb{F}_q[t]$ no Teorema 8.13 diz-se o *polinómio gerador* do código cíclico $C = \varphi(I)$.

Exemplo 8.15. Continuação do Exemplo 8.9:

(a) O polinómio gerador de E_3 é $1 + t$, os outros dois geradores de $I = \varphi(E_3)$ têm grau 2. Note que o polimónio gerador $1 + t$ é precisamente o gerador mónico de $\pi^{-1}(I)$, como se viu no Exemplo 8.11.

(b) O polinómio gerador do código cíclico $\langle 1010, 0101\rangle \subset \mathbb{F}_2^4$ é $1 + t^2$.

A partir de agora identificamos I e C sem fazer necessariamente referência ao isomorfismo vectorial $\varphi : \mathbb{F}_q^n \longrightarrow R_n$.

Lema 8.16. *Seja $g(t) \in \mathbb{F}_q[t]$ tal que $g(t)|t^n - 1$. Então $a(t) \equiv g(t)x(t) \pmod{t^n - 1}$ se e só se $g(t)$ divide $g(t)$ em $\mathbb{F}_q[t]$.*

Dem. Seja $h(t) \in \mathbb{F}_q[t]$ tal que $g(t)h(t) = t^n - 1$. Então

$$\begin{aligned} a(t) \equiv g(t)x(t) \pmod{t^n - 1} & \\ \iff \quad & a(t) = g(t)x(t) + (t^n - 1)y(t) , \quad \text{para algum } y(t) \in \mathbb{F}_q[t] \\ \iff \quad & a(t) = g(t)x(t) + g(t)h(t)y(t) = g(t)(x(t) + h(t)y(t)) \end{aligned}$$

ou seja, $g(t)$ divide $a(t)$. □

Teorema 8.17. *Seja $f(t) \in \mathbb{F}_q[t]$. Então $f(t)|t^n-1$ e $f(t)$ é mónico se e só se $f(t)$ é o polinómio gerador de algum código cíclico.*

Dem. ($\Longleftarrow$) Consequência imediata do Teorema 8.13
($\Longrightarrow$) Seja $a(t) \in \mathbb{F}_q[t]$ tal que $f(t)a(t) = t^n - 1$, seja $C = \langle f(t)\rangle$ e seja $g(t)$ o polinómio gerador do código C. Queremos ver que $f(t) = g(t)$. Como $g(t) \in \langle f(t)\rangle \subset R_n$, então existe $b(t) \in \mathbb{F}_q[t]$ tal que $g(t) \equiv f(t)b(t) \pmod{t^n-1}$, portanto, pelo Lema 8.16, $f(t)$ divide $g(t)$ em $\mathbb{F}_q[t]$. Como $g(t)$ é o polinómio mónico de grau mínimo em C e $f(t)$ é mónico, conclui-se que $f(t) = g(t)$. □

O teorema anterior permite-nos classificar todos os códigos cíclicos q-ários de comprimento n à custa da factorização de $t^n - 1$ em polinómios irredutíveis em $\mathbb{F}_q[t]$.

Exemplo 8.18. Como $t^3 - 1 = (1 + t)(1 + t + t^2)$ e $1 + t + t^2$ é irredutível em $\mathbb{F}_2[t]$ (porque tem grau 2 e não possui raízes em $\mathbb{F}_2$), então os únicos códigos cíclicos binários de comprimento 3 são

$$R_3 = \langle 1\rangle\ , \quad \langle 1+t\rangle\ , \quad \langle 1+t+t^2\rangle = \{0, 1+t+t^2\} \quad \text{e} \quad \langle t^3-1\rangle = \{0\}\ ,$$

ou, vistos como subespaços vectoriais de $\mathbb{F}_2^3$, os único códigos cíclicos de comprimento 3 são $\mathbb{F}_2^3$, o código dos pesos pares E_3, o código de repetição $\{000, 111\}$ e o código nulo $\{\vec{0}\}$.

3. Matriz geradora e matriz de paridade

Nesta secção recuperamos as características lineares de um código cíclico à custa do seu polinómio gerador.

Teorema 8.19. *Seja $g(t) = g_0 + g_1 t + \cdots + g_r t^r$ o polinómio gerador do código cíclico $C \subset R_n$. Então*

$$G_{(n-r)\times n} = \begin{bmatrix} g_0 & g_1 & \cdots & g_r & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_r & 0 \\ 0 & \cdots & \cdots & 0 & g_0 & g_1 & \cdots & g_r \end{bmatrix} = \begin{bmatrix} — & g(t) & — \\ — & tg(t) & — \\ & \vdots & \\ — & t^{n-r-1}g(t) & — \end{bmatrix}$$

é uma matriz geradora de C e $\dim C = n - r = n - \deg(g(t))$, ou seja, o grau de g(t) é a redundância do código C.

Dem. Como $g_0 \neq 0$, as linhas de G são linearmente independentes. Vamos ver que as linhas também formam um conjunto gerador, como espaço vectorial, do código C. Seja $a(t) \in C = \langle g(t)\rangle$. Então $\deg(a(t)) < n$ e, pelo Lema 8.16, $a(t) = g(t)q(t)$ para algum polinómio $q(t) \in \mathbb{F}_q[t]$. Como $\deg(a(t)) = \deg(g(t)q(t)) = \deg(g(t)) + \deg(q(t))$, então $\deg(q(t)) < n - r$, ou seja,

$$q(t) = q_0 + q_1 t + \cdots + q_{n-r-1}t^{n-r-1} \qquad \text{e}$$
$$a(t) = g(t)q(t) = q_0 g(t) + q_1 tg(t) + \cdots + q_{n-r-1}t^{n-r-1}g(t)\ ,$$

ou seja, $a(t)$ é combinação linear de $g(t), tg(t), \ldots, t^{n-r-1}g(t)$, que são precisamente as linhas da matriz G.
Uma vez que as $n - r$ linhas de G formam uma base de C, conclui-se C tem dimensão $n - r$. □

Exemplo 8.20. Já vimos que $g(t) = 1+t^2+t^3+t^4$ é o polinómio gerador do código simplex $S(3,2)$. Pelo teorema anterior,

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

é uma matriz geradora deste código. Note que as colunas de G são de facto os sete vectores não nulos de $\mathbb{F}_2^3$, como devia ser, pois $S(3,2)^\perp = \mathrm{Ham}(3,2)$.

Definição 8.21. Se C é um código cíclico, de comprimento n, com polinómio gerador $g(t)$, então $h(t) = \dfrac{t^n-1}{g(t)} \in \mathbb{F}_q[t]$ diz-se o *polinómio de paridade* de C.

Uma vez que $g(t)$ é mónico, então $h(t)$ também é, pois $h(t)g(t) = t^n - 1$.

Atenção! O polinómio de paridade de um código cíclico C não é, em geral, o polinómio gerador do código dual $C^\perp$, embora este seja cíclico, pelo Teorema 8.3.

Exemplo 8.22. Para o código simplex $S(3,2)$, com polinómio gerador $g(t) = 1 + t^2 + t^3 + t^4$, o polinómio de paridade é $h(t) = \dfrac{t^3-1}{1+t^2+t^3+t^4} = 1 + t^2 + t^3$. Pelos Teoremas 8.17 e 8.19, este $h(t)$ é o polinómio gerador de um código cíclico C com matriz geradora

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

Seja G a matriz geradora de $S(3,2)$ do exemplo anterior. Então, como $G_h G^T \neq 0$, a matriz G_h não é uma matriz de paridade para $S(3,2)$, logo $C \neq S(3,2)^\perp$. No entanto, C e $S(3,2)^\perp$ são códigos linearmente equivalentes — verifique!

Proposição 8.23. *$c(t) \in C$ se e só se $c(t)h(t) \equiv 0 \pmod{t^n-1}$.*

Dem. Seja $c(t) \in \mathbb{F}_q[t]$ um polinómio qualquer. Então

$$\begin{aligned} c(t)h(t) \equiv 0 \pmod{t^n-1} &\iff c(t)h(t) = b(t)(t^n-1)\ , \quad \text{para algum } b(t) \in \mathbb{F}_q[t], \\ &\iff c(t) = b(t)g(t) \\ &\iff c(t) \in \langle g(t) \rangle = C \end{aligned}$$

onde, na última equivalência, se usou o Lema 8.16. □

Teorema 8.24. *Seja C um código cíclico, de comprimento n e dimensão k, com polinómio de paridade $h(t) = h_0 + h_1 t + \cdots + h_k t^k$. Então*

(i) a matriz

$$H = \begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & \cdots & 0 \\ 0 & k_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 & 0 \\ 0 & \cdots & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \end{bmatrix}$$

é uma matriz de paridade para C;

(ii) $\bar{h}(t) := h_0^{-1} t^k h(t^{-1}) \in \mathbb{F}_q[t]$ *é o polinómio gerador de* $C^\perp$.

Dem. (i) Como $h_k = 1 \neq 0$ (lembre-se que $h(t)$ é um polinómio mónico), as linhas de H são linearmente independentes. Portanto, para mostrar que H é uma matriz de paridade para C, basta ver que $Hc = 0$ se e só se $c \in C$.

Pela Proposição 8.23, $c(t) = c_0 + c_1 t + \cdots + c_{n-1} t^{n-1} \in C$ se e só se $c(t)h(t) \equiv 0 \pmod{t^n - 1}$. Desenvolvendo o produto em $\mathbb{F}_q[t]$, fica

$$\begin{aligned} c(t)h(t) =& c_o h_o + (c_0 h_1 + c_1 h_0) + \cdots + \Big(\sum_{i+j=k} c_i h_j \Big) t^k + \cdots + \Big(\sum_{i+j=n-1} c_i h_j \Big) t^{n-1} \\ &+ \Big(\sum_{i+j=n} c_i h_j \Big) t^n + \cdots + c_{n-1} h_k t^{n+k-1} \ . \end{aligned} \tag{8.2}$$

Módulo $t^n - 1$, os termos de graus n a $n + k - 1$ tansformam-se em termos de graus 0 a $k - 1$, respectivamente, portanto, os termos de graus k a $n - 1$ em (8.2) já estão correctos módulo $t^n - 1$ e os seus coeficientes têm de ser zero. Logo, $c = (c_0, c_1 \ldots, c_{n-1}) \in C$ se e só se é solução do seguinte sistema de equações lineares

$$\begin{aligned} c_0 h_k + c_1 k_{k-1} + \cdots + c_k h_0 &= 0 \\ c_1 h_k + \cdots + c_k h_1 + c_{k+1} h_0 &= 0 \\ \ddots \quad &\vdots \\ c_{n-k-1} k_k + \cdots + c_{n-1} h_0 &= 0 \end{aligned}$$

que, em notação matricial, se escreve $Hc = 0$.

(ii) Só falta ver que $\bar{h}(t) | t^n - 1$, pois $\bar{h}(t)$ é mónico e $h_0 \neq 0$. Mas $h(t^{-1})g(t^{-1}) = t^{-n} - 1$, porque $h(t)g(t) = t^n - 1$, logo $t^k h(t^{-1}) t^{n-k} g(t^{-1}) = t^n(t^{-n} - 1) = 1 - t^n$, logo $h_0^{-1} t^k h(t^{-1}) = \bar{h}(t)$ divide $t^n - 1$. □

Observação 8.25. Ao polinómio $t^k a(t^{-1}) \in \mathbb{F}_q[t]$, onde $k = \deg a(t)$, costuma-se chamar *polinómio recíproco* de $a(t)$. Deixamos como exercício verificar que, se $a(t)$ divide $t^n - 1$, então $a(t)$ e o seu recíproco geram códigos equivalentes — ver Exercício 8.9.

Exemplo 8.26. Para o código simplex $S(3, 2)$, o polinómio de paridade é $h(t) = 1 + t^2 + t^3$. Portanto

$$\bar{h}(t) = t^3 h(t^{-1}) = t^3(1 + t^{-2} + t^{-3}) = t^3 + t + 1$$

é o polinómio recíproco de $h(t)$ e também o polinómio gerador do código dual $S(3, 2)^\perp = \mathrm{Ham}(3, 2)$.

Exemplo 8.27. Em $\mathbb{F}_2[t]$, temos a seguinte factorização $t^{23} - 1 = (t - 1)g_1(t)g_2(t)$, onde

$$g_1(t) = 1 + t^2 + t^4 + t^5 + t^6 + t^{10} + t^{11} \qquad \text{e} \qquad g_2(t) = 1 + t + t^5 + t^6 + t^7 + t^9 + t^{11} \ .$$

Seja $C_1 = \langle g_1(t) \rangle$ e $C_2 = \langle g_2(t) \rangle$. Como $\bar{g}_1(t) := t^{11} g_1(t^{-1}) = g_2(t)$, então, pelo Exercício 8.9, C_1 e C_2 são códigos equivalentes com parâmetros $[23, 12]$. Se mostrarmos que $\mathrm{d}(C_1) = 7$ (ver Problema 2 da Ficha 6), podemos concluir que C_1 é equivalente ao código de Golay binário G_{23}.

Exemplo 8.28. Em $\mathbb{F}_3[t]$, $t^{11} - 1 = (t - 1)g_1(t)g_2(t)$, onde

$$g_1(t) = -1 + t^2 - t^3 + t^4 + t^5 \qquad \text{e} \qquad g_2(t) = -1 - t + t^2 - t^3 + t^5 \ .$$

Como $\bar{g}_1(t) = -t^5 g_1(t^{-1}) = g_2(t)$, os códigos gerados pelos polinómios $g_1(t)$ e $g_2(t)$ são equivalentes com parâmetros $[11, 6]_3$. Se mostrarmos que a distância mínima deste(s) código(s) é 5 (ver [**2**]), podemos concluir que o código de Golay ternário G_{11} é equivalente a estes códigos cíclicos.

3.1. Códigos de Hamming revisitados

Terminamos esta secção mostrando que os códigos de Hamming binários $\mathrm{Ham}(r, 2)$ são cíclicos.

Seja $\alpha \in \mathbb{F}_{2^r}$ um elemento primitivo, e seja $p(t) \in \mathbb{F}_2[t]$ um polinómio irredutível[4] de grau r tal que $p(\alpha) = 0$. Portanto $\mathbb{F}_{2^r} = \mathbb{F}_2[t]/\langle p(t)\rangle$ e

$$\mathbb{F}_{2^r} = \{0, 1 = \alpha^0, \alpha, \alpha^2, \ldots, \alpha^{2^r-2}\} .$$

Como $\mathbb{F}_{2^r}$ é um espaço vectorial de dimensão r sobre $\mathbb{F}_2$ (ver Exercício 3.4) e

$$a(t) = a_0 + a_1 t + \cdots + a_{r-1} t^{r-1} \longmapsto (a_0, \ldots, a_{r-1})$$

define um isomorfismo vectorial, podemos identificar o elemento $a_0 + a_1 t + \cdots + a_{r-1} t^{r-1} \in \mathbb{F}_2[t]/\langle p(t)\rangle$ com o vector coluna

$$\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{r-1} \end{bmatrix} \in \mathbb{F}_2^r .$$

Com esta identificação, considere a matriz

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^r-2} \end{bmatrix}_{r \times (2^r-1)} ,$$

ou seja, as colunas de H são os elementos não nulos do corpo $\mathbb{F}_{2^r}$, donde H é uma matriz de paridade de um código de Hamming binário de redundância r e comprimento $n = 2^r - 1$. Só falta mostrar que este código C é cíclico. Como

$$\begin{aligned} C = \mathcal{N}(H) &= \{c \in \mathbb{F}_2^n \,:\, Hc = 0\} \\ &= \{(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_2^n \,:\, c_0 1 + c_1 \alpha + \cdots + c_{n-1}\alpha^{n-1} = 0 \text{ em } \mathbb{F}_{2^r}\} \\ &= \{c(t) \in R_n \,:\, c(\alpha) = 0 \pmod{p(t)}\} . \end{aligned}$$

Agora é fácil verificar, usando a definição de ideal, que C é um ideal em R_n, logo, pelo Teorema 8.8, concluimos que C é um código cíclico. Já agora vamos determinar o polinómio gerador $g(t)$ de C. Note que $p(t) \in C$, pois $p(\alpha) = 0$, logo, pelo Lema 8.16, $g(t)$ divide $p(t)$ no anel $\mathbb{F}_2[t]$ e, portanto, temos necessariamente que $g(t) = p(t)$, porque $p(t)$ é irredutível.

4. Codificação e descodificação

Como um código cíclico também é linear, já conhecemos algoritmos de codificação e descodificação. O objectivo desta secção é descrever esses algoritmos, e/ou deduzir outros, à custa do polinómio gerador.

[4] $p(t)$ diz-se o *polinómio mínimo* de α

Seja $C \subset R_n = \mathbb{F}_q[t]/\langle t^n - 1\rangle$ um código cíclico q-ário $[n,k]$, com polinómio gerador $g(t) = g_0 + g_1 t + \cdots + g_r t^r$. Portanto $r = n-k$, $g_r = 1$ e

$$G' = \begin{bmatrix} g_0 & g_1 & \cdots & g_r & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_r & 0 \\ 0 & \cdots & \cdots & 0 & g_0 & g_1 & \cdots & g_r \end{bmatrix}$$

é uma matriz geradora de C, pelo Teorema 8.19. Se apliacarmos o método de eliminação de Gauss para "matarmos" as entradas por baixo de cada $g_r = 1$, usando apenas operações nas linhas, obtemos uma matriz na forma

$$G_{k\times n} = \begin{bmatrix} R_{k\times r} & I_k \end{bmatrix} , \tag{8.3}$$

que é ainda uma matriz geradora do mesmo código C. Se designarmos por $-\rho_i(t)$ o polinómio correspondente à linha i da matriz R, à linha i de G corresponde o polinómio $-\rho_i(t) + t^{r+i}$, onde $\deg(\rho_i(t)) \leq r-1$, porque R é uma matriz de r colunas.

Por outro lado, cada linha de G é uma palavra do código C, logo um múltiplo de $g(t)$ pelo Lema 8.16, donde

$$-\rho_i(t) + t^{r+i} = g(t)q_i(t),$$

para algum polinómio $q_i(t)$. Ou seja,

$$t^{r+i} = g(t)q_i(t) + \rho_i(t) \qquad \forall\, i \in \{0,\ldots,k-1\} \tag{8.4}$$

com $\deg(\rho(t)) \leq r-1 < r = \deg(g(t))$, i.e., $\rho_i(t)$ é o resto da divisão de t^{r+i} por $g(t)$.

Um algoritmo de codificação sistemática:

Dada a mensagem $m(t) = m_0 + m_1 t + \cdots + m_{k-1}t^{k-1} \in \mathbb{F}_q[t]$ (ou, equivalentemente, dado o vector mensagem $(m_0,\ldots,m_{k-1}) \in \mathbb{F}_q^k \cong C$):

- determinar o resto $\rho(t)$ da divisão de $t^r m(t)$ por $g(t)$, i.e., determinar $\rho(t)$ tal que
$$t^r m(t) = g(t)q(t) + \rho(t) \quad \text{ e } \quad \deg(\rho(t)) \leq r-1 \ ;$$
- codificar $m(t)$ pelo polinómio de código
$$c(t) = -\rho(t) + t^r m(t) \in \langle g(t)\rangle = C$$

Trata-se de facto de uma codificação sistemática pois o polinómio de código obtido é da forma

$$c(t) = -\rho_0 - \rho_1 t - \cdots - \rho_{r-1}t^{r-1} + m_0 t^r + m_1 t^{r+1} + \cdots + m_{k-1}t^{n-1} \in R_n$$

porque $\deg(\rho(t)) \leq r-1$, ou, equivalentemente, o vector código é da forma

$$c = (\underbrace{-\rho_0, -\rho_1, \ldots, -\rho_{r-1}}_{\text{símbolos de verificação ou de redundância}}, \overbrace{m_0,\ldots,m_{k-1}}^{\text{símbolos de mensagem}}) \in C \ .$$

Os símbolos de mensagem aparecem agora nas últimas componentes do vector — comparar com a expressão (4.2). Note que, tal como em (4.1), o vector c também se escreve

$$c = G^T m = (R^T m, m) \ .$$

Note ainda que, para se codificar $m(t)$ (ou $m \in \mathbb{F}_q^k$), não foi necessário conhecermos uma matriz geradora, bastou calcular o resto da divisão pelo polinómio gerador $g(t)$ do código cíclico C.

Passemos agora à descodificação. Recorde que, na descodificação por síndrome para códigos lineares, o primeiro passo é sempre calcular o sintoma $S(y)$ do vector recebido $y \in \mathbb{F}_q^n$.

Teorema 8.29. *O sintoma $S(y(t))$ é o resto da divisão de $y(t)$ pelo polinómio gerador $g(t)$.*

Dem. Uma vez que $G = \begin{bmatrix} R & I_k \end{bmatrix}$ é uma matriz geradora, $H = \begin{bmatrix} I_r & -R^T \end{bmatrix}$ é uma matriz de paridade, pelo Lema 4.12, e as colunas de $-R^T$ são os vectores correspondentes aos polinómios $\rho_0(t)$, $\ldots$, $\rho_{k-1}(t)$ determinados anteriormente, i.e. $\rho_i(t)$ é o resto da divisão de t^{r+i} por $g(t)$.
Seja $y = (y_0, \ldots, y_{n-1}) \in \mathbb{F}_q^n$ e seja $y(t) = y_0 + y_1 t + \cdots y_{n-1} t^{n-1}$ o polinómio correspondente. O sintoma de y é $S(y) = Hy \in \mathbb{F}_q^r$. Portanto, em notacção polinomial, $S(y(t))$ é um polinómio de grau menor ou igual a $r-1$ e, usando a matriz de paridade $H = \begin{bmatrix} I_r & -R^T \end{bmatrix}$, fica

$$\begin{aligned} S(y(t)) &= y_0 + y_1 t + c \cdots + y_{r-1} t^{r-1} + y_r \rho_0(t) + \cdots + y_{n-1} \rho_{k-1}(t) \\ &= y(t) - \sum_{i=0}^{k-1} y_{r+i} (\rho_i(t) - t^{r+i}) \\ &= y(t) - \Big(\sum_{i=0}^{k-1} y_{r+i} q_i(t) \Big) g(t) \ , \end{aligned}$$

usando as igualdades (8.4). Pondo $q(t) = -\sum_{i=0}^{k-1} y_{r+i} q_i(t)$, obtem-se $S(y(t)) = y(t) - g(t)q(t)$, ou seja,

$$y(t) = g(t)q(t) + S(y(t)) \ .$$

Como $\deg(S(y(t))) \leq r-1$, da última igualdade conclui-se que $S(y(t))$ é o resto da divisão de $y(t)$ por $g(t)$. □

Define-se o peso $\mathrm{w}(x(t))$ de um elemento $x(t) \in R_n$ como o peso do vector correspondente $x \in \mathbb{F}_q^n$, ou equivalentemente, $\mathrm{w}(x(t))$ é o peso do único representante de grau menor ou igual a $n-1$.

Corolário 8.30. *Seja $s(t) = S(y(t))$. Se $\mathrm{w}(s(t)) \leq T := \left\lfloor \frac{\mathrm{d}(C)-1}{2} \right\rfloor$, então $s(t)$ é um chefe de classe de $y(t) + C$ e, portanto, descodificamos $y(t)$ por $x(t) = y(t) - s(t) \in C$.*

Exemplo 8.31. Seja C o código cíclico binário, de comprimento 7, com polinómio gerador $g(t) = 1 + t + t^3$. Como C é um código de Hamming binário $\mathrm{Ham}(3, 2)$ — ver Exemplo 8.26 — então C é um código perfeito de distância mínima $\mathrm{d}(C) = 3$, portanto $T = 1$ e os chefes de classe são precisamente os elementos de R_7 peso ≤ 1.

(i) Seja $y(t) = t + t^2 + t^3 + t^5 \in R_7$ o vector recebido. Como $y(t) = t + t^2(1 + t + t^3)$, então $s(t) := S(y(t)) = t$, pelo Teorema 8.29. Além disso, como $\mathrm{w}(s(t)) = 1$, $s(t)$ é um chefe de classe e podemos descodificar $y(t)$ por $y(t) - s(t) = t^2 + t^3 + t^5$, pelo Corolário 8.30.

(ii) Seja agora $z(t) = 1 + t^4$ o vector recebido. Como $y(t) = t(1 + t + t^3) + 1 + t + t^2$, então o sintoma de $z(t)$ é $S(z(t)) = 1 + t^2 + t^2$, que tem peso $3 > T = 1$. Não se pode aplicar Corolário 8.30. No entanto,

$$z(t) = 1 + t^4 \equiv t^7 + t^4 = t^4(t^3 + 1) = t^4(t^3 + t + 1) + t^5 \pmod{t^7 - 1}$$

ou seja, $z(t) = t^4 g(t) + t^5$. O resto da divisão de $z(t)$ pelo polinómio gerador não é t^5, pois $\deg(t^5) = 5 \geq 3 = \deg(g(t))$, mas, como $\mathrm{w}(t^5) = 1$, t^5 é o chefe da classe $z(t) + C$. Portanto descodificamos $z(t)$ por $z(t) - t^5 = 1 + t^4 + t^5 = t^4 g(t) \in C$.

Como se viu neste exemplo, determinar o chefe de classe pode não ser imediato usando apenas o sintoma, se este tem peso maior do que T.

Note que $t^i y(t) \in R_n$ contém a mesma informação que $y(t)$. Logo, se conseguirmos descodificar $t^i y(t)$ para algum i, então também descodificamos $y(t)$. Interessa, portanto, sabermos calcular os sintomas dos desvios cíclicos $t^i y(t)$ e também sabermos quando vai existir um destes sintomas de peso menor ou igual a T. É o que faremos de seguida.

Teorema 8.32. *Dado $y(t) \in R_n$, o sintoma do desvio cíclico de $y(t)$ é*

$$S(ty(t)) = tS(y(t)) - s_{r-1} g(t) \ ,$$

onde s_{r-1} é o coeficiente do termo de grau $r - 1$ de $S(y(t))$.

Dem. Seja $s(t) = S(y(t))$ o sintoma de $y(t)$. Portanto $y(t) = q(t)g(t) + s(t)$, com $\deg(s(t)) \leq r - 1$, para algum $q(t)$. Pondo $s(t) = s_{r-1} t^{r-1} + s'(t)$ e $g(t) = t^r + g'(t)$, onde $\deg(s'(t)) < r - 1$ e $\deg(g'(t) < r$ (recorde que $g(t)$ é mónico e tem grau r), fica

$$\begin{aligned} ty(t) &= tq(t)g(t) + ts(t) \\ &= t(q(t) + s_{r-1})g(t) + (ts(t) - s_{r-1} g(t)) \end{aligned}$$

e $ts(t) - s_{r-1} g(t) = ts'(t) - s_{r-1} g'(t)$ tem grau menor do que r. Logo, pelo Teorema 8.29, o sintoma de $ty(t)$ é $ts(t) - s_{r-1} g(t)$. □

Exemplo 8.33. Para o código do Exemplo 8.31, o sintoma de $z(t) = 1 + t^4$ é $S(z(t)) = 1 + t + t^2$, logo, pelo teorema anterior, os sintomas dos restantes desvios cíclicos de $z(t)$ são

$$\begin{aligned} S(tz(t)) &= 1 + t^2 \ , & S(t^2 z(t)) &= 1 \ , \\ S(t^3 z(t)) &= t \ , & S(t^4 z(t)) &= t^2 \ , \\ S(t^5 z(t)) &= 1 + t \ , & S(t^6 z(t)) &= t + t^2 \ . \end{aligned}$$

Definição 8.34. Diz-se que $x = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_q^n$ contém uma *sequência cíclica de k zeros*, se existe $j \leq n - 1$ tal que $x_j = x_{j+1} = \cdots = x_{j+k-1} = 0$, onde os índices são calculados módulo n.

Exemplo 8.35.

- $(1, 1, 0, 0, 0, 1, 0) \in \mathbb{F}_2^7$ contém uma sequência de três zeros.
- $x = (0, 0, 1, 0, 5, 0, 0, 0, 0) \in \mathbb{F}_7^9$ contém uma sequência cíclica de $k = 6$ zeros. Tomando dois desvios cíclicos para a esquerda (ou sete desvios cíclcicos para a direita), obtemos um vector $x' = (1, 0, 5, 0, 0, 0, 0, 0, 0)$ com zeros nas últimas 6 coordenadas. Ou seja, no anel R_9, se $x(t) = t^2 + 5t^4$, então $t^{-2} x(t) \equiv t^7 x(t) = 1 + 5t^2$ tem grau $n - k - 1 = 2$.

Lema 8.36. *O vector $x \in \mathbb{F}_q^n$ contém uma sequência cíclica de k zeros se e só se existe $i \in \{0, 1, \ldots, n-1\}$ tal que* $\deg(t^i x(t)) \leq n-k-1$.

Dem. Basta permutar ciclicamente as coordenadas de x até os k zeros consecutivos ocuparem as últimas k componentes de x. O vector assim obtido corresponde a um polinómio em R_n de grau menor ou igual a $n-k-1$. □

Lema 8.37. *Seja $\vec{e} \in \mathbb{F}_q^n$, com peso* $\mathrm{w}(\vec{e}) \leq T$*, contendo uma sequência cíclica de k zeros. Então* $\mathrm{w}(S(t^i e(t))) \leq T$*, para algum $i \in \{0, \ldots, n-1\}$.*

Dem. Pelo lema anterior, seja $i \in \{0, 1, \ldots, n-1\}$ tal que $t^i e(t)$ tem grau menor ou igual a $n-k-1 = r-1$. Portanto, pelo Teorema 8.29, o sintoma do desvio cíclico $t^i e(t)$ é $S(t^i e(t)) = t^i e(t)$. Como permutações das coordenadas não alteram o peso de um vector, também se verifica que

$$\mathrm{w}(S(t^i e(t))) = \mathrm{w}(t^i e(t)) = \mathrm{w}(e(t)) \leq T \ . \qquad \square$$

Podemos finalmente justificar o seguinte algoritmo de descodificação.

Algoritmo Caça ao Erro:

Seja C um código cíclico $[n, k, d]_q$ com polinómio gerador $g(t)$ de grau $r = n-k$. Seja $T = \left\lfloor \frac{d-1}{2} \right\rfloor$. Recebido $y(t) \in R_n$:

1. Calcular os sintomas $s_i(t) := S(t^i y(t))$;
2. Se $\mathrm{w}(s_i(t)) \leq T$ para algum $i \in \{0, 1, \ldots, n-1\}$, então assumimos que $t^{n-i} s_i(t)$ é o vector erro e descodificamos $y(t)$ por $y(t) - t^{n-i} s_i(t)$;
3. Caso contrário, o erro ocorrido não é corrigível.

Antes de mais, convém observar que $y(t) - t^{n-i} s_i(t) \in C$, pois

$$\begin{aligned} t^i(y(t) - t^{n-i} s_i(t)) &= t^i y(t) - t^n s_i(t) \\ &= q(t)g(t) + s_i(t) - t^n s_i(t) \qquad \text{porque } s_i(t) = S(t^i y(t)) \\ &= q(t)g(t) + (1 - t^n) s_i(t) \\ &\equiv q(t)g(t) \pmod{t^n - 1} \end{aligned}$$

donde $t^i(y(t) - t^{n-i} s_i(t)) \in C$ e também $y(t) - t^{n-i} s_i(t) \in C$, porque o código C é cíclico.

Além disso, este algoritmo de caça ao erro corrige todos os vecores erro de peso T no máximo, que contenham uma sequência cíclica de $k = \dim C$ zeros.

Justificação: Seja $x(t) \in C$ o vector enviado e $y(t) \in R_n$ o vector recebido. Pelos resultados anteriores, se o erro ocorrido $e(t) = y(t) - x(t)$ contém uma sequência cíclica de k zeros, então existe i tal que $S(t^i e(t))$ tem peso T no máximo e $S(t^i e(t)) = t^i e(t)$. Logo

$$\begin{aligned} s_i(t) := S(t^i y(t)) &= S(t^i x(t)) + S(t^i e(t)) = 0 + t^i e(t) \\ &= t^i e(t) \ , \end{aligned}$$

e o algoritmo descodifica $y(t)$ correctamente por $y(t) - t^{n-i} s_i(t) = y(t) - e(t) = x(t)$.

Exemplo 8.38. Continuação do Exemplo 8.31: Aplicando o Algoritmo Caça ao Erro ao vector recebido $z(t) = 1 + t^4$, uma vez que já calculámos os sintomas de $t^i z(t)$ no Exemplo 8.33 e que $T = 1$, assumimos que o erro ocorrido é $t^{7-2}s_2(t) = t^5$ e descodificamos $z(t)$ por

$$z(t) - t^5 = 1 + t^4 + t^5 \ ,$$

que foi o que já obtivémos anteriormente.

Exemplo 8.39. Seja C o código binário $[15, 7]$ com polinómio gerador $g(t) = 1 + t + t^2 + t^4 + t^8$. Deixamos como exercício verificar que $\mathrm{d}(C) = 5$. Portanto $T = 2$ e o algoritmo caça ao erro permite corrigir todos os erros simples e duplos que contenham uma sequência cíclica de $k = 7$ zeros.

- Se $\mathrm{w}(\vec{e}) = 1$, então $\vec{e}$ é uma permutação cíclica de $(1, 0, \ldots, 0)$ e, portanto, contém uma sequência cíclica de 14 zeros.
- Se $\mathrm{w}(\vec{e}) = 2$, então $\vec{e}$ é uma permutação cíclica de um vector da forma

  $$\vec{f} = (1, \underbrace{0, \ldots, 0}_{l \text{ zeros}}, 1, \underbrace{0, \ldots, 0}_{13-l \text{ zeros}}) \ .$$

  Se $l \geq 7$, o vector $\vec{f}$ contém obviamente sete zeros seguidos. Se $l \leq 6$, então $13 - l \geq 7$ e $\vec{f}$ também contém sete zeros seguidos. Em qualquer caso, concluimos que $\vec{e}$ contém uma sequência cíclica de sete zeros.

Para este código C, o algoritmo caça ao erro corrige todos os vectores erros $\vec{e}$ com peso $\mathrm{w}(\vec{e}) \leq 2$.

Exemplo 8.40. Seja C o código binário $[15, 7, 5]$ do exemplo anterior. Vamos descodificar o vector recebido $y = 111110110010101$.

Para uma aplicação pragmática do algoritmo caça ao erro, vamos apenas calcular os sintomas $s_i(t) = S(t^i y(t))$, com $i = 0, 1, \ldots, n-1$, até encontrarmos um com peso menor ou igual a $T = 2$. Como $y(t) = 1 + t + t^2 + t^3 + t^4 + t^6 + t^7 + t^{10} + t^{12} + t^{14} = g(t)(t^6 + t^4) + (1 + t + t^2 + t^3 + t^5 + t^6)$, aplicando os Teorema 8.29 e 8.32 (o último várias vezes), obtem-se

$$\begin{aligned}
s_0(t) &= 1 + t + t^2 + t^3 + t^5 + t^6 && \text{tem peso } 6 > T, \\
s_1(t) &= t + t^2 + t^3 + t^4 + t^6 + t^7 && \text{tem peso } 6 > T, \\
s_2(t) &= 1 + t + t^3 + t^5 + t^7 && \text{tem peso } 5 > T, \\
s_3(t) &= 1 + t^6 && \text{tem peso } 2 \leq T,
\end{aligned}$$

por isso assumimos que o erro ocorrido foi $t^{15-3}s_3(t) = t^{12}(1 + t^6) \equiv t^3 + t^{12} \pmod{t^{15} - 1}$, e descodificamos $y(t)$ por $y(t) - t^3 - t^{12} = 1 + t + t^2 + t^4 + t^6 + t^7 + t^{10} + t^{14}$, ou seja, descodificamos o vector y por 111010110010001.

5. Erros Acumulados

Definição 8.41. O vector $e = (e_1, \ldots, e_n) \in \mathbb{F}_q^n$ diz-se um *erro-l acumulado*, ou um *erro acumulado de comprimento l*, se existe $i \in \{1, \ldots, n\}$ tal que $e_i \neq 0$ e $e_{i+l-i} \neq 0$, e $e_j = 0$ para todo o $j \notin \{i, \ldots, i + l - 1\}$, onde os índices são calculados módulo n.

Ou seja, as coordenas não nulas de um vector erro-l acumulado estão contidas numa sequência de comprimento l, sendo a primeira e última coordenadas desta sequência não nulas.

Exemplo 8.42. Os vectores 00111000, 10100000 e 01000001 são erros-3 acumulados em $\mathbb{F}_2^8$.

Exemplo 8.43. Se $l = 2$, um vector erro-2 acumulado é da forma

$$e = (0, \ldots, e_i, e_{i+1}, 0, \ldots, 0) \quad \text{ou} \quad e = (e_1, 0, \ldots, 0, e_n) \ ,$$

com $e_i \neq 0$, $e_{i+1} \neq 0$, $e_1 \neq 0$ e $e_n \neq 0$, e diz-se um *erro duplo adjacente*.

Teorema 8.44. *Seja C um código linear $[n,k]_q$, não necessariamente cíclico, tal que C corrige todos os erros-m acumulados com $m \leq l$. Então*

(i) C não contém nenhum vector erro-m acumulado com $m \leq 2l$;

(ii) ***Estemativa de Reigner:*** *$n - k \geq 2l$.*

Dem. (i) Seja $\vec{e}$ um vector erro-m acumulado com $m \leq 2l$. Então

$$\vec{e} = (\vec{0}, a, \vec{u}, \vec{v}, b, \vec{0}) \ ,$$

com $a, b \in \mathbb{F}_q \setminus \{0\}$ e $\vec{u}, \vec{v}$ vectores de comprimento menor ou igual a $l-1$. Sejam

$$\vec{x} = (\vec{0}, a, \vec{u}, \vec{0}, 0, \vec{0}) \qquad \text{e} \qquad \vec{y} = -(\vec{0}, 0, \vec{0}, \vec{v}, b, \vec{0}) \ .$$

Então $\vec{x}$ e $\vec{y}$ são erros acumulados de comprimento menor ou igual a l. Como C corrige estes erros por hipótese, então $\vec{x}$ e $\vec{y}$ pertencem a classes distintas, i.e., $\vec{x}+C \neq \vec{y}+C$, ou ainda, $\vec{e} = \vec{x} - \vec{y} \notin C$.
(ii) Seja H uma matriz de paridade para C. Sejam $u_1, u_2, \ldots, u_{r+1}$ as primeiras $r+1$ colunas de H. Como pertencem a $\mathbb{F}_q^r$, os $r+1$ vectores $u_1, \ldots, u_{r+1}$ são linearmente dependentes, logo existem escalares $c_1, \ldots, c_{r+1} \in \mathbb{F}_q$, não todos nulos, tais que

$$c_1 u_1 + c_2 u_2 + \cdots + c_{r+1} u_{r+1} = \vec{0} \ .$$

Seja $c = (c_1, c_2, \ldots, c_{r+1}, 0, \ldots, 0) \in \mathbb{F}_q^n$. Então c é um erro-m acumulado com $m \leq r+1$ e, como $Hc = 0$, $c \in C$. Por (i), tem-se $m > 2l$, portanto $r+1 > 2l$, o que é equivalente a $n-k = r \geq 2l$. □

Corolário 8.45. *Um código linear $[n,k]$ corrige no máximo todos os erros-m acumulados com $m \leq \left\lfloor \frac{n-k}{2} \right\rfloor$*

Este corolário é uma consequência directa da Estimativa de Reigner.

Exemplo 8.46. Seja C o código binário cíclico $[15, 9]$, com polinómio gerador $g(t) = 1+t+t^2+t^3+t^6$. Em notação polinomial, os erros-m acumulados com $m \leq 3$ são:

$$t^i \ \text{ para } m = 1, \quad t^i(1+t) \ \text{ para } m = 2, \quad t^i(1+t^2) \ \text{ e } \ t^i(1+t+t^2) \ \text{ para } m = 3,$$

onde $0 \leq i \leq 14$ nos quatro casos. São 60 polinómios no total, mas todos pertencem a classes diferentes pois têm sintomas distintos dois a dois (exercício: verifique esta última afirmação, de preferência com a ajuda de um programa de computador). Portanto C corrige todos os erros-m acumulados com $m \leq 3$. Por outro lado, a Estimativa de Reigner dá $l \leq \left\lfloor \frac{n-k}{2} \right\rfloor = \left\lfloor \frac{15-9}{2} \right\rfloor = 3$. Ou seja, C atinge a igualdade na Estimativa de Reigner, e esta não pode ser melhorada.

Por definição, um erro-l acumulado é um vector da forma

$$e = (0, \ldots, e_i, *, \ldots, *, e_{i+l-1}, 0, \ldots, 0) \ ,$$

onde $e_i \neq 0$, $e_{i+l-1} \neq 0$ e as $l-2$ componentes assinaladas com $*$ podem ser nulas ou não, logo um erro-l acumulado contém uma sequência cíclica de $n-l$ zeros. Se C é um código cíclico $[n,k]_q$ que corrige todos os erros acumulados de comprimento $m \leq l$, então, pela Estimativa de Reigner, $k \leq n-2l \leq n-l$. Vamos, portanto, poder usar o Algoritmo Caça ao Erro, mas ignorando a condição $\mathrm{w}(\vec{e}) \leq T$, para corrigir todos estes erros.

Algoritmo Caça ao Erro Acumulado:

Seja C um código cíclico $[n,k]_q$, corrector de todos os erros-m acumulados com $m \leq l$. Recebido $y(t) \in R_n$:

1. Calcular os sintomas $s_i(t) := S(t^i y(t))$;
2. Se $s_i(t)$ é um erro-m acumulado, com $m \leq l$, para algum $i \in \{0, 1, \ldots, n-1\}$, então assumimos que $t^{n-i} s_i(t)$ é o vector erro e descodificamos $y(t)$ por $y(t) - t^{n-i} s_i(t)$;
3. Caso contrário, o erro ocorrido não é corrigível.

Note que $y(t) - t^{n-i} s_i(t) \in C$, tal como já acontecia com o algoritmo de caça ao erro.

Deixamos como exercício justificar que este algoritmo corrige os erros enunciados.

Exemplo 8.47. Seja C o código cíclico binário $[15, 9]$, do Exemplo 8.46, com polinómio gerador

$$g(t) = 1 + t + t^2 + t^3 + t^6 \ .$$

Já sabemos que este código corrige todos os erros acumulado de comprimento $m \leq 3$, pois estes vectores pertencem a classes distintas. Vamos descodificar o vector recebido

$$y = 110000011101110 \qquad \text{ou} \qquad y(t) = 1 + t + t^7 + t^8 + t^9 + t^{11} + t^{12} + t^{13} \ .$$

Calculemos os sintomas $s_i(t) = S(t^i y(t))$, com $i = 0, \ldots, n-1$, até encontrarmos um que seja um erro-m acumulado com $m \leq 3$:

$$\begin{aligned}
s_0(t) &= 1 + t^2 + t^4 + t^5 && \text{é um erro-6 acumulado,} \\
s_1(t) &= t s_0(t) - g(t) = 1 + t^2 + t^5 && \text{é um erro-6 acumulado,} \\
s_2(t) &= t s_1(t) - g(t) = 1 + t^2 && \text{é um erro-3 acumulado.}
\end{aligned}$$

Portanto assumimos que o erro ocorrido é $e(t) = t^{15-2} s_2(t) = t^{13}(1 + t^2) \equiv 1 + t^{13} \pmod{t^{15} - 1}$, e descodificamos $y(t)$ por $y(t) - e(t)$, ou y por

$$y - 100000000000010 = 010000011101100 \ .$$

6. Entrelaçamento

O entralaçamento de um código é uma construção que permite aumentar a capacidade de correcção de erros acumulados.

Definição 8.48. O *entralaçamento* de s vectores $x_1, \ldots, x_s \in \mathbb{F}_q^n$ é o vector

$$x^{(s)} = (\underbrace{x_{1,1}, x_{2,1}, \ldots, x_{s,1}}_{\text{a } 1^{\text{a}} \text{ coordenada de cada } x_i}, \overbrace{x_{1,2}, x_{2,2}, \ldots, x_{s,2}}^{\text{a } 2^{\text{a}} \text{ coordenada de cada } x_i}, \ldots, \underbrace{x_{1,n}, x_{2,n}, \ldots, x_{s,n}}_{\text{a última coordenada de cada } x_i},) \in \mathbb{F}_q^{ns} \ ,$$

onde $x_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,n})$.

Exemplo 8.49. O entrelaçamento dos três vectores $x_1 = 0000$, $x_2 = 1111$, $x_3 = 3456 \in \mathbb{F}_7^4$ é

$$x^{(3)} = 013014015016 \in \mathbb{F}_7^{12} \ .$$

Se escrevermos uma matriz cujas linhas são vectores x_1, x_2 e x_3

$$X = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 3 & 4 & 5 & 6 \end{bmatrix} \ ,$$

podemos obter o vector entrelaçado lendo as entradas da matriz X de cima para baixo e da esquerda para a direita.

Em geral, escrevendo uma matriz X cujas linhas são os vectores $x_i \in \mathbb{F}_q^n$, com $1 \leq i \leq s$,

$$X = \begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,n} \\ \vdots & \vdots & & \vdots \\ x_{s,1} & x_{s,2} & \cdots & x_{s,n} \end{bmatrix}_{s \times n} \ , \tag{8.5}$$

o vector entrelaçado são as colunas de X escritas consecutivamente como as entradas de um vector em $\mathbb{F}_q^{ns}$

Definição 8.50. Seja C um código linear $[n,k]_q$. O código $C^{(s)}$ obtido entrelaçando quaisquer s palavras do código C diz-se o *código entrelaçado de grau s.*

Exemplo 8.51. Seja $C = \langle 111 \rangle$ o código binário de repetição de comprimento 3. Para obter $C^{(2)}$, vamos descrever o vector entrelaçado dos pares ordenados de palavras de C. Os quatro casos possíveis estão descritos na seguinte tabela:

x_1	000	000	111	111
x_2	000	111	000	111
$x^{(2)}$	000000	010101	101010	111111

Portanto, $C^{(2)} = \langle 010101, 101010 \rangle \subset \mathbb{F}_2^6$ e é um código linear e cíclico. Note que, apesar do código entrelaçado ter comprimento maior, $\mathrm{d}(C^{(2)}) = 3 = \mathrm{d}(C)$, portanto $C^{(2)}$ tem as mesmas capacidades de correcção que C para erros aleatórios.

Teorema 8.52. *(a) Se C é um código linear $[n,k]$, então $C^{(s)}$ é um código linear $[ns, ks]$.*

(b) Se $C \subseteq R_n$ é um código cíclico com polinómio gerador $g(t)$, então $C^{(s)} \subset R_{ns}$ é um código cíclico com polinómio gerador $g(t^s)$.

(c) Se C é um código cíclico corrector de todos os erros-m acumulados com $m \leq l$, então $C^{(s)}$ é um código corrector de todos os erros-m acumulados com $m \leq ls$.

Dem. (a) Por construção, $C^{(s)}$ é um subconjunto de $\mathbb{F}_q^{ns}$ e $|C^{(s)}| = |C|^s = q^{ks}$. Portanto, se $C^{(s)}$ é linear, então $\dim C^{(s)} = \log_q(|C^{(s)}|) = ks$. Para ver que $C^{(s)}$ é linear, basta ver que é fechado para a soma de vectores e produto por um escalar. Seja $x^{(s)} \in C^{(s)}$ o entrelaçado dos vectores $x_1, \ldots, x_s \in C$, seja $y^{(s)} \in C^{(s)}$ o entrelaçado de $y_1, \ldots, y_s \in C$, e seja $a \in \mathbb{F}_q$. Deixamos como exercício verificar que $x^{(s)} + y^{(s)}$ e $ax^{(s)}$ são os entrelçados de $x_1 + y_1, \ldots, x_s + y_s$ e de $ax_1, \ldots, ax_s$, respectivamente — use a notação das matrizes (8.5). Logo $x^{(s)} + y^{(s)}, ax^{(s)} \in C^{(s)}$, porque C é um código linear.

(b) Uma vez que $C^{(s)}$ é linear, pela aínea (a), só falta ver que $C^{(s)}$ é fechado para os desvios cíclicos. Seja $x^{(s)} \in C^{(s)}$ o entrelaçado dos vectores $x_1, \ldots, x_s \in C$. Como C é cíclico, $\sigma(x_s) \in C$ e, portanto, o vector y obtido entrelaçando $\sigma(x_s), x_1, \ldots, x_{s-1}$ é uma palavra do código $C^{(s)}$. Explicitando as coordenadas de y e pondo $x_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,n})$, obtém-se

$$y = (\underbrace{x_{s,n}, x_{1,1}, \ldots, x_{s-1,1}}_{s \text{ coordenadas}}, \underbrace{x_{s,1}, x_{1,2}, \ldots, x_{s-1,2}}_{s \text{ coordenadas}}, \ldots, \underbrace{x_{s,n-1}, x_{1,n}, \ldots, x_{s-1,n}}_{s \text{ coordenadas}}) \ ,$$

ou seja, $y = \sigma(x) \in C^{(s)}$.

Para determinarmos o polinómio gerador, temos de encontrar um polinómio mónico de grau $ns - ks$ (a redundância de $C^{(s)}$), que divida $t^{ns} - 1$, e que pertença ao código $C^{(s)}$. Seja $g(t) = g_0 + g_1 t + \cdots + g_r t^r$, com $r = n - k$, o polinómio gerador de C, e seja $g = (g_0, g_1, \ldots, g_r, 0, \ldots, 0) \in \mathbb{F}_q^n$ o vector correspondente. Então, o entrelaçado de g com $s - 1$ vectores nulos $\vec{0} \in \mathbb{F}_q^n$ é um elemento de $C^{(s)}$ e as suas coordenadas são

$$g^{(s)} = (\underbrace{g_0, 0, \ldots, 0}_{s \text{ coord.}}, \underbrace{g_1, 0, \ldots, 0}_{s \text{ coord.}}, \ldots, g_r, 0, \ldots, 0) \ ,$$

que, em notação polinomial, se escreve

$$g^{(s)}(t) = g_0 + g_1 t^s + g_2 t^{2s} + \cdots + g_r t^{rs} = g(t^s) \ .$$

Portanto $g(t^s) \in C^{(s)}$ é mónico ($g_r = 1$ porque $g(t)$ é mónico), tem grau $rs = ns - ks$ e divide $t^{ns} - 1$ porque

$$g(t)h(t) = t^n - 1 \quad \Longrightarrow \quad g(t^s)h(t^s) = (t^s)^n - 1 = t^{sn} - 1 \ .$$

(c) Seja $\vec{e} \in \mathbb{F}_q^{ns}$ um erro-m de acumulação com $m \leq ls$. O vector $\vec{e}$ é da forma

$$\vec{e} = (0, \ldots, 0, \underbrace{e_i, \ldots, e_{i+ls-1}}_{ls \text{ coordenadas}}, 0, \ldots, 0) \ .$$

Seja E a matriz $s \times n$ que se obtem escrevendo as coordendas de $\vec{e}$ por ordem ao longo das colunas, ou seja, o entrelaçado das linhas de E é o vector erro $\vec{e}$. Portanto, cada linha não nula de E contém no máximo l entradas não nulas. Portanto, C corrige os vectores erro correspondentes às linhas de E, logo $C^{(s)}$ corrige o vector erro-m acumulado $\vec{e}$. □

Exemplo 8.53. Continuação do Exemplo 8.49: As palavras de $C^{(2)}$ correspondem aos polinómios

$$0 \ , \quad t + t^3 + t^5 \ , \quad 1 + t^2 + t^4 \quad \text{e} \quad 1 + t + t^2 + t^3 + t^4 + t^5 \ ,$$

logo $g_2(t) = 1 + t^2 + t^4$ é o polinómio gerador de $C^{(2)}$, ou, aplicando o Teorema 8.52, como $g(t) = 1 + t + t^2$ é o polinómio gerador de C, então $g_2(t) = g(t^2) = 1 + t^2 + t^4$ é o polinómio gerador do

código entrelaçado. Quanto às capaciadades correctoras, C corrige apenas os erros simples, pois $\mathrm{d}(C) = 3$ e C é um código perfeito mas, pelo Teorema 8.52, $C^{(2)}$ pode ser usado para corrigir todos os erros simples e todos os erros duplos adjacentes.

Exercícios

8.1. Resolva a Ficha 6.

8.2. (a) Mostre que a aplicação *desvio cíclico* $\sigma : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ definida por $\sigma(x_1, \ldots, x_{n-1}, x_n) = (x_n, x_1, \ldots, x_{n-1})$ é linear e bijectiva.
(b) Mostre que um código linear C é cíclico se e só se $\sigma^i(C) = C$ para todo o $i \in \mathbb{Z}$.

8.3. (a) No Exemplo 8.6, mostre que $\langle 2, t\rangle$ não é um ideal principal em $\mathbb{Z}[t]$.
(b) Mostre que $\langle x, y\rangle$ não é um ideal principal no anel dos polinómios de duas variáveis[5] $\mathbb{F}_q[x, y]$.

8.4. Para $a \in \mathbb{F}_q$ fixo, mostre que o conjunto $I = \{f(t) \in \mathbb{F}_q[t] \,:\, f(a) = 0\}$ é um ideal em $\mathbb{F}_q[t]$. Determine um gerador de I.

8.5. Os ideais nas seguintes alíneas são ideais do anel $R_n = \mathbb{F}_q[t]/\langle t^n - 1\rangle$. Assumindo que $g(t)|t^n - 1$ em $\mathbb{F}_q[t]$, mostre que
(a) $\langle f_1(t)\rangle \subseteq \langle f_2(t)\rangle$ se e só se $f_2(t)$ divide $f_1(t)$ em R_n;
(b) $\langle f(t)\rangle = \langle g(t)\rangle$ se e só se existe $a(t) \in \mathbb{F}_q[t]$ tal que $f(t) \equiv a(t)g(t) \pmod{t^n - 1}$ e $\mathrm{MDC}(a(t), h(t)) = 1$, onde $h(t)g(t) = t^n - 1$;

8.6. (a) Factorize $t^{12} - 1$ no produto de polinómios irredutíveis em $\mathbb{F}_3[t]$.
(b) Quantos códigos cíclicos ternários de comprimento 12 existem?
(c) Determine para que valores de k existe um código cíclico ternário $[12, k]$.
(d) Quantos códigos cíclicos ternários com parâmetros $[12, 9]$ existem?

8.7. (a) Determine o polinómio gerador e a dimensão do menor código cíclico binário que contém a palavra $c = 1110010 \in \mathbb{F}_2^7$.
(b) Escreva uma matriz geradora, o polinómio de paridade e uma matriz de paridade para o código que determinou na alínea anterior.

8.8. Seja C um código cíclico, de comprimento n, com polinómio gerador $g(t)$. Mostre que, se $C = \langle f(t)\rangle$, i.e., se $f(t)$ é um gerador do ideal C, então $g(t) = \mathrm{MDC}(f(t), t^n - 1)$. Em particular, conclua que o polinómio gerador do menor código cíclico, de comprimento n, que contém $f(t)$ é $g(t) = \mathrm{MDC}(f(t), t^n - 1)$.

8.9. Se $g(t)$ é o polinómio gerador de um código cíclico, mostre que $\langle g(t)\rangle$ e $\langle \bar{g}(t)\rangle$ são códigos equivalentes. Conclua que o código gerado pelo polinómio de paridade de um código cíclico C é equivalente ao código dual $C^\perp$.

8.10. Resolva a Ficha 7.

8.11. Mostre que o código entrelaçado se grau s, $C^{(s)}$, é equivalente ao código soma $C \oplus \cdots \oplus C$ de s cópias de C. Conclua que $\mathrm{d}(C^{(s)}) = \mathrm{d}(C)$.

[5] Podia ser $K[x, y]$, com K um corpo qualquer.

8.12. Seja $C = \mathrm{Ham}(3,2)$ o código de Hamming binário de redundância 3, com polinómio gerador $g(t) = 1 + t + t^3$.

(a) Determine os parâmetros e o polinómio gerador de $C^{(3)}$.

(b) Mostre que o código $C^{(3)}$ corrige todos os erros-m acumulados com $m \leq 3$.

(c) Usando o Algoritmo Caça ao Erro Acumulado, descodifique o vector recebido

$$y(t) = t + t^3 + t^5 + t^7 + t^8 + t^9 + t^{11} \ .$$

8.13. Um código cíclico q-ário de comprimento n diz-se *degenerado* se existe $r \in \mathbb{N}$ tal que r divide n e cada palavra do código se escreve na forma $c = c'c' \cdots c'$ com $c' \in \mathbb{F}_q^r$, isto é, cada palavra do código consiste em n/r cópias idênticas de uma sequência c' de comprimento r.

(a) Mostre que o entrelaçamento $C^{(s)}$ de um código de repetição C é um código degenerado.

(b) Mostre que o polinómio gerador de um código cíclico degenerado de comprimento n é da forma

$$g(t) = a(t)(1 + t^r + t^{2r} + \cdots + t^{n-r}) \ .$$

(c) Mostre que um código cíclico de comprimento n e polinómio de paridade $h(t)$ é degenerado se e só se existe $r \in \mathbb{N}$ talque r divide n e $h(t)$ divide $t^r - 1$.

8.14. Seja C o código binário linear com a seguinte matriz de paridade

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

(a) Determine a distância mínima $\mathrm{d}(C)$ e indique a capacidade de detecção e de correcção de erros aleatórios deste código.

(b) Mostre que C detecta todos os erros-m acumulados com $m \leq 3$.

(c) Seja C' o pontuado, na última coordenada, do código dual $C^{\perp}$. Mostre que C' é um código cíclico e degenerado, e determine o seu polinómio gerador.

8.15. Determine todos os códigos binários, cíclicos e degenerados de comprimento 9, indicando os respectivos polinómios geradores e a correspondente sequência de comprimento r.