Combinatória e Teoria de Códigos

Teste 1 – 20 de Abril de 2017

RESOLUÇÃO

1. Trata-se de uma relação de recorrência linear e homogénea com polinómio característico $p(t) = t^3 - 3t + 2$ (vindo de $a_n - 3a_{n-2} + 2a_{n-3} = 0$), cujas raízes são $r = 1$ (dupla) e $r = -2$ (simples). Portanto, a solução geral do problema é $a_n = A \cdot 1^n + Bn \cdot 1^n + C(-2)^n = A + Bn + C(-2)^n$, com A, B e C constantes. Impondo as condições iniciais obtém-se

$$\begin{cases} a_0 = 0 \\ a_1 = 0 \\ a_2 = 9 \end{cases} \Leftrightarrow \begin{cases} A + C = 0 \\ A + B - 2C = 0 \\ A + 2B + 4C = 9 \end{cases} \Leftrightarrow \begin{cases} C = -A \\ B = 2C - A = -3A \\ A - 6A - 4A = 9 \end{cases} \Leftrightarrow \begin{cases} C = 1 \\ B = 3 \\ A = -1 \end{cases} .$$

   A solução do problema dado é $a_n = -1 + 3n + (-2)^n$, para qualquer $n \geq 0$.

2. Como $x, y \in \mathbb{F}_2^n$, temos a seguinte igualdade $\mathrm{w}(x - y) = \mathrm{w}(x) + \mathrm{w}(y) - 2\,\mathrm{w}(x \cap y)$. Por hipótese temos que $\mathrm{w}(x) = \mathrm{w}(y) = \mathrm{w}(x \cap y)$, portanto

$$\mathrm{d}(x, y) = \mathrm{w}(x - w) = 0 \Leftrightarrow x = y \ .$$

3. (a) Como $f(t) = t^2 + 1$ tem grau 2, basta ver que não tem raízes em $\mathbb{F}_3$. Temos que $f(0) = 1 \neq 0$, $f(1) = 2 \neq 0$ e $f(2) = 2 \neq 0$, donde podemos concluir que $f(t)$ é irredutível.

   (b) Uma vez que $|\mathbb{F}_9 \setminus \{0\}| = 8$, temos que $|x| \mid 8$ para qualquer $x \in \mathbb{F}_9 \setminus \{0\}$ (ou seja $|x| \in \{1, 2, 4, 8\}$), e x é primitivo sse $|x| = 8$. Como $1 \in \mathbb{F}_9$ é o único elemento de ordem 1, e $\alpha \neq 1$, $\beta \neq 1$, basta calcular x^2 e x^4 para $x = \alpha, \beta$.

$$\begin{aligned} &\alpha^2 = -1 = 2 \neq 1 \ , \\ &\alpha^4 = (\alpha^2)^2 = 2^2 = 1 && \text{donde } |\alpha| = 4 \text{ e } \alpha \text{ não é primitivo;} \\ &\beta^2 = (2 + \alpha)^2 = 1 + \alpha + \alpha^2 = \alpha \neq 1 \ , \\ &\beta^4 = (\beta^2)^2 = \alpha^2 = 2 \neq 1 && \text{donde } |\beta| = 8 \text{ e } \beta \text{ é primitivo.} \end{aligned}$$

   (c) Dado que H_a é uma matriz 2×10, tem-se directamente que $n = 10$, $r = 2$ e $k = n - r = 10 - 2 = 8$ para ambos os códigos.

   Como $\alpha^4 = 1$, a terceira e sétima colunas de H_α são iguais. Daqui sai que $\mathrm{d}(C_\alpha) \leq 2$ (há duas colunas em H_α linearmente depententes). Como tambem se têm que nenhuma coluna é o vector nulo, tem-se que $\mathrm{d}(C_\alpha) \geq 2$, donde se conclui que $\mathrm{d}(C_\alpha) = 2$ e, portanto, C_α não é um código de Hamming porque $\mathrm{d}(\mathrm{Ham}(r, q)) = 3$ se $r \geq 2$.

   Um código de Hamming com $r = 2$ sobre $\mathbb{F}_9$ tem comprimento $n = \frac{9^2 - 1}{9 - 1} = 10$. Como β é primitivo em $\mathbb{F}_9$, as colunas de H_β são linearmente independentes duas as duas. Conclusão: $C_\beta = \mathrm{Ham}(2, 9)$, tendo parâmetros $[10, 8, 3]$.

(d) O sintoma de y usando o código C_α é

$$S_\alpha(y) = H_\alpha y = \begin{bmatrix}0\\ \alpha\end{bmatrix} + \begin{bmatrix}2\\ 0\end{bmatrix} + \begin{bmatrix}2\\ 2\alpha\end{bmatrix} + \begin{bmatrix}1\\ \alpha^6\end{bmatrix} \underset{(\alpha^6=\alpha^2\alpha^4=2)}{=} \begin{bmatrix}2\\ 2\end{bmatrix} = 2\begin{bmatrix}1\\ 1\end{bmatrix} .$$

Portanto $y \notin C_\alpha$, pois $S_\alpha(y) \neq 0$, e um chefe de classe de $y + C_\alpha$ tem peso pelo menos 1. Como $S_\alpha(2\vec{e}_3) = S_\alpha(2\vec{e}_7) = S_\alpha(y)$ (onde $\vec{e}_i$ denota os vectores da base canónica de $\mathbb{F}_9^{10}$) e $\mathrm{w}(2\vec{e}_3) = \mathrm{w}(2\vec{e}_7) = 1$, os vectores $2\vec{e}_3$ e $2\vec{e}_7$ são ambos chefes de classe de $y + C_\alpha$. Não há unicidade, não se descodifica y.

O sintoma de y usando o código C_β é

$$\begin{aligned} S_\beta(y) = H_\beta y &= \begin{bmatrix}0\\ \alpha\end{bmatrix} + \begin{bmatrix}2\\ 0\end{bmatrix} + \begin{bmatrix}2\\ 2(2+\alpha)\end{bmatrix} + \begin{bmatrix}1\\ \beta^6\end{bmatrix} \underset{(\beta^6=\beta^2\beta^4=2\alpha)}{=} \begin{bmatrix}2\\ 1+2\alpha\end{bmatrix} \\ &= 2\begin{bmatrix}1\\ 2+\alpha\end{bmatrix} = 2\begin{bmatrix}1\\ \beta\end{bmatrix} = S(2\vec{e}_4) . \end{aligned}$$

Portanto $y \notin C_\beta$, pois $S_\beta(y) \neq 0$, e um chefe de classe de $y + C_\beta$ tem peso pelo menos 1, tal como no caso anterior de C_α. Como $\mathrm{d}(C_\beta) = 3$, este código corrige todos os erros de peso $t = \lfloor \frac{3-1}{2} \rfloor = 1$ e, portanto, todos os vectores de peso 1 são chefes de classe distintas. Como $S_\beta(y) = S_\beta(2\vec{e}_4)$ e $\mathrm{w}(S(2\vec{e}_4)) = 1$, o vector $2\vec{e}_4$ é o único chefe de classe de $y + C_\beta$ e descodifica-se y por $y - 2\vec{e}_4 = (\alpha, 2, 0, 0, 0, 0, 0, 0, 1, 0)$.

4. (a) Uma matriz de paridade para $C^\perp$ é uma matriz geradora para C. Como a matriz de paridade dada está na forma $H = [I \;\; A]$, uma matriz de paridade para $C^\perp$ é

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

(b) Um vector $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ tem peso par sse $x_1 + \cdots + x_n = 0$ sse $\vec{1} \cdot x = 0$, onde $\vec{1}$ denota o vector com todas as componentes iguais a 1. Portanto $x \in C'$ sse $Hx = 0$ e $\vec{1} \cdot x = 0$ sse $H'x = 0$, onde

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

Para H' ser uma matriz de paridade para C' é preciso que as suas linhas sejam linearmente independentes. Aplicando o método de eliminação de Gauss a H' (denotanto por l_i a linha i da matriz) obtém-se

$$H \underset{l_4 \mapsto l_1+l_2+l_3+l_4}{\longrightarrow} \begin{bmatrix}1&0&0&1&0&1\\ 0&1&0&1&0&1\\ 0&0&1&1&1&0\\ 0&0&0&0&0&1\end{bmatrix} ,$$

donde se conclui que as quatro linhas são linearmente independentes e, portanto, H' é de facto uma matriz de paridade para o subcódigo C'.