COMBINATÓRIA E TEORIA DE CÓDIGOS
Ficha 8

9/5/2011

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

2. 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

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

3. 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 $t^r - 1$.

4. 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 $\mathrm{dist}(C)$ 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.

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

6. Seja α uma raiz 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 $\phi^*(A)$?

7. Seja α uma raiz 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 $C = \phi^*(A)$?

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

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

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

11. Seja C um código Reed-Solomon q-ário com polinómio gerador

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

Mostre que $c(t) \in \mathbb{F}_q[t]/\langle t^{q-1} - 1 \rangle$ é uma palavra de código se e só se $c(\alpha^i) = 0$ para qualquer $i = a, \ldots, a + \delta - 1$.

12. 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.

13. 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 $\mathbb{F}_q$.

14. 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 $\phi(\alpha^2) = 101$.

15. (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 $\hat{\phi} : \mathbb{F}_8 \to \mathbb{F}_2^4$ definida por $\hat{\phi}(a_0 + a_1\alpha + a_2\alpha^2) = (a_0, a_1, a_2, a_0 + a_1 + a_2)$. Determine os parâmetros de $C' = \hat{\phi}^*(C)$.

    (d) O que pode concluir acerca da capacidade de correcção de erros aleatórios e/ou erros acumulados de C^* e de C'?

16. 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 $\mathbb{F}_2$ à sua escolha. O que pode concluir sobre a capacidade de correcção de erros acumulados do código concatenação $C^* = \phi^*(C)$?