Teoria de Códigos

Época normal — 14 de Junho de 2006

A duração do exame é de 2 (duas) horas. **Não** é permitida a utilização de máquinas de calcular.

Justifique todas as suas respostas convenientemente.

1. Mostre que um código de Hamming é corrector de erros singulares e que é perfeito. Conclua, justificando[1], que $A_2(2^k-1,3)=2^{2^k-1-k}$.

2. Seja C o código linear binário gerado pela matriz $G=\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$.

   (a) Indique os parâmetros (n, M, d) de C e a sua taxa de informação.

   (b) Calcule o número de vectores corrigíveis e conclua, justificando, se o código é perfeito.

   (c) Sabendo que se usa um canal simétrico binário com a probabilidade p de um símbolo ser recebido erradamente, calcule a probabilidade (em função de p) de uma palavra recebida ser corrigível.

   (d) Considere o código $C^\perp$ dual de C. Corrija em $C^\perp$, se possível, o(s) erro(s) do vector recebido $r=\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$.

3. Seja C o código BCH obtido do polinómio primitivo $\pi(x)=x^4+x+1\in\mathbb{Z}_2[x]$, considerando as primeiras 4 potências de α.

   (a) Encontre o polinómio gerador de C.

   (b) Corrija, em C, o seguinte bloco recebido por um canal binário simétrico:

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

4. Usando o polinómio primitivo $\pi(x)=x^4+x+1\in\mathbb{Z}_2[x]$, calcule, justificando convenientemente, a codificação do bloco **binário** a enviar por um canal simétrico com ruído

$$\left[\begin{array}{cccc|cccc|cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \end{array}\right]$$

   no código Reed-Solomon $RS[15,2]$ obtido de $\pi(x)$, apresentando o resultado na forma de um polinómio sobre $\mathbb{F}=\mathbb{Z}_2[x]/(\pi(x))$.

   [Recorde que o código $RS[15,2]$ é corrector de 2 erros no corpo quociente. Cada $\beta\in\mathbb{F}$ pode-se escrever de forma única como um 4-uplo sobre $\mathbb{Z}_2$.]

Cotação:

1. ~ 2; 2. $\sim (2+2+2+3)$; 3. $\sim (3+4)$; 4. ~ 2

[1] Faça uso da desigualdade de Hamming.