Instituto Superior Técnico
Departamento de Matemática
Secção de Álgebra e Análise

Combinatória e Teoria de Códigos

Exame/Teste de Recuperação – 22 de Junho de 2013

Duração: teste 1h 30m, exame 3h

(Justifique cuidadosamente todas as suas respostas.)

1º teste

1. (a) (1 val.) Escreva o polinómio característico e a solução geral da relação de recorrência linear e homogénea

$$a_n = a_{n-1} + 2a_{n-2} \quad \forall\, n \geq 2 \ .$$

   (b) (1 val.) Escreva uma relação de recorrência linear e homogénea, com o menor grau possível, cujo espaço das soluções contém as soluções da relação da alínea (a) e a sucessão $n2^n$.

2. Seja C o código linear ternário com a seguinte matriz de paridade

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

   (a) (0,5 val.) Justifique que a distância mínima é $\mathrm{d}(C) = 3$.

   (b) (1 val.) Qual a capacidade de correcção de erros do código C? Descodifique o vector recebido $y = 200201$.

   (c) (1 val.) Se C for usado para corrigir erros de apagamento apenas, indique, justificando detalhadamente, qual a capacidade de correcção deste erros.

   (d) (1,5 val.) Descodifique, se possível, os vectores recebidos

$$z = 1??111 \qquad \text{e} \qquad w = ??1?01 \ .$$

3. Sejam C_1, C_2 e C_3 códigos lineares q-ários de comprimento n, dimensões $\dim C_i = k_i$ e distâncias mínimas $\mathrm{d}(C_i) = d_i$, para $i = 1, 2, 3$, e considere o código

$$C = \{(a, a+b, a+c) \,:\, a \in C_1\,, b \in C_2\,, c \in C_3\} \ .$$

   (a) (1,5 val.) Mostre que C é um código linear e determine a sua dimensão.

   (b) (1 val.) Escreva uma matriz geradora de C à custa de matrizes geradoras dos códigos C_i, $i = 1, 2, 3$.

   (c) (1,5 val.) Mostre que $\mathrm{d}(C) = \min\{3d_1, d_2, d_3\}$.

2º teste

4. Seja C o código cíclico binário, de comprimento 15, com polinómio gerador

$$f(t) = t^4 + t + 1 \ .$$

   (a) (0,5 val.) Justifique que C é um código de Hamming.

   (b) (1 val.) Verifique que $x(t) = t^2(1 + t^4 + t^6 + t^7 + t^8)$ é uma palavra do código C e determine o polinómio gerador $g(t)$ do menor código cíclico $C' \subset \mathbb{F}_2^{15}$ que contém $x(t)$.

   (c) (1,5 val.) Sabendo que $\mathrm{d}(C') = 5$, descodifique o vector recebido

$$y = 000011001110000 \ ,$$

   usando o Algoritmo Caça ao Erro para o código C'.

   Sugestão para o exercício 4: Pode usar, sem justificar, que a factorização de $t^{15} - 1$ em polinómios irredutíveis em $\mathbb{F}_2[t]$ é

$$t^{15} - 1 = (t-1)(t^2+t+1)(t^4+t+1)(t^4+t^3+1)(t^4+t^3+t^2+t+1) \ .$$

5. Seja C o código Reed-Solomon sobre $\mathbb{F}_5$ com polinómio gerador $g(t) = (t-2)(t-4)$.

   (a) (0,5 val.) Indique os parâmetros e uma matriz geradora de C.

   (b) (0,5 val.) Indique os parâmetros e uma matriz geradora da extensão $\widehat{C}$.

   (c) (1,5 val.) Determine os polinómios geradores e as dimensões de todos os códigos cíclicos de comprimento 5 sobre $\mathbb{F}_5$.

   (d) (1,5 val.) Seja $\widetilde{C}$ um código cíclico de comprimento 5 e dimensão 2. Escreva uma matriz geradora para $\widetilde{C}$ e mostre que este código é linearmente equivalente a $\widehat{C}$.

   (e) (1,5 val.) Conclua que qualquer código cíclico, não nulo, de comprimento 5 sobre $\mathbb{F}_5$ é MDS.

6. (1,5 val.) Seja C o código de repetição de comprimento n sobre $\mathbb{F}_{q^m}$ e seja C^* o código concatenação de C com o código trivial q-ário $(\mathbb{F}_q)^m$. Mostre que C^* é um código q-ário cíclico e indique os seus parâmetros $[N, K, D]$.