Instituto Superior Técnico
Departamento de Matemática
Secção de Álgebra e Análise

Combinatória e Teoria de Códigos

Teste de Recuperação/Exame – 5 de Julho de 2017

Duração: teste 1h 30m, exame 3h

- **Justifique cuidadosamente todas as suas respostas.**
- **Não é permitido o uso de máquinas calculadoras, telemóveis, nem de outros elementos de consulta.**
- **As cotações indicadas dizem respeito ao exame. Para cada teste, multiplicar os valores por 2.**

Teste 1

1. (1,5 val.) Determine a solução da relação de recorrência

$$\begin{cases} a_n = -a_{n-1} - a_{n-2} - a_{n-3} & \text{para } n \geq 3 \\ a_0 = 1 \\ a_1 = 3 \\ a_2 = -7 \end{cases} .$$

Sugestão: Note que se trata de uma relação linear e homogénea.

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

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

(a) (1 val.) Escreva uma matriz geradora de C.

(b) (2 val.) Justifique que C corrige todos os erros simples e **simultaneamente** detecta todos os erros duplos.
Sugestão: Qual o peso dos sintomas destes erros?

(c) (2 val.) Descodifique se possível, usando descodificação incompleta por distância mínima, os seguintes vectores recebidos

$$y = (1,1,1,1,1,0,0,0) \qquad \text{e} \qquad z = (1,1,0,1,1,0,1,1) .$$

3. Sejam C_1, C_2 e C_3 códigos lineares sobre $\mathbb{F}_q$ de comprimento n e dimensões $\dim C_i = k_i \geq 1$, para $i = 1,2,3$. Considere o código

$$C = \left\{(x, y, x+y+z) \in \mathbb{F}_q^{3n} \mid x \in C_1, y \in C_2, z \in C_3\right\} .$$

(a) (1,5 val.) Mostre que C é linear e escreva uma matriz geradora de C à custa de matrizes geradoras de C_1, C_2 e C_3.

(b) (2 val.) Sejam $C_1 = \mathrm{Ham}(3,2)$, C_2 o código de repetição binário com o mesmo comprimento de C_1 e $C_3 = S(3,2)$. Determine os parâmetros $[N, K, D]$ de C.

Teste 2

4. (2 val.) Considere o sistema de Steiner $S(2,3,9)$ cujo conjunto de pontos é $\mathcal{P} = \mathbb{F}_3^2$ e cujos blocos são os subconjuntos de $\mathcal{P}$ da forma $\{a + \lambda b \in \mathbb{F}_3^2 \mid \lambda \in \mathbb{F}_3\}$, com $a \in \mathbb{F}_3^2$ e $b \in \mathbb{F}_3^2 \setminus \{0\}$. Decida, justificando, se cada uma das seguintes afirmações é verdadeira ou falsa:

   (a) O número de blocos é 12;

   (b) Existe um código binário perfeito associado a $S(2,3,9)$ cuja matriz de incidência é definida à custa das palavras de peso igual à distância mínima do código.

5. (1,5 val.) Seja $\mathrm{Tr} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ a aplicação traço e seja $C \subset (\mathbb{F}_{q^m})^n$ um código cíclico. Mostre que o código traço $\mathrm{Tr}(C)$ também é cíclico.

6. (a) (1 val.) Obtenha a factorização de $t^8 - 1$ em polinómios irredutíveis em $\mathbb{F}_7[t]$.
   Sugestão: Verfique que $t^4 + 1 = (t^2 + 4t + 1)(t^2 + 3t + 1)$.

   (b) (1,5 val.) Mostre que qualquer código cíclico, sobre $\mathbb{F}_7$, de comprimento 8 e dimensão 1 é linearmente equivalente ao código de repetição.

7. Seja C o código Reed Solomon sobre $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, onde $\alpha^2 = \alpha + 1$, com polinómio gerador

$$g(t) = (t-1)(t-\alpha) = t^2 + \alpha^2 t + \alpha \ .$$

   (Pode usar, sem o verificar, que α é um elemento primitivo em $\mathbb{F}_4$.)

   (a) (0,5 val.) Indique os parâmetros $[n, k, d]$ de C.

   (b) (1 val.) Seja $C^{(3)}$ o código entrelaçado de grau 3 de C. Indique os parâmetros $[N, K, D]$ de $C^{(3)}$ e o seu polinómio gerador $g^{(3)}(t)$.

   (c) (1 val.) Justifique que $C^{(3)}$ corrige todos os erros-m acumulados com $m \leq 3$.

   (d) (1,5 val.) Para o código $C^{(3)}$, descodifique, se possível, o vector recebido

$$y(t) = 1 + t + t^2 + \alpha t^3 + \alpha t^4 + \alpha t^5 \ ,$$

   usando o algoritmo caça ao erro acumulado.