Instituto Superior Técnico
Departamento de Matemática
Secção de Álgebra e Análise

Combinatória e Teoria de Códigos

Teste de Recuperação/Exame – 1 de Julho de 2015

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 o número de polinómios mónicos de grau $n \geq 2$ em $\mathbb{F}_q[t]$ sem raízes em $\mathbb{F}_q$. [Sugestão: Princípio de Inclusão-Exclusão.]

2. (a) (1 val.) Sejam $x, y \in \mathbb{F}_2^n$. Mostre que $x \cdot y = 0$ se e só se $\mathrm{w}(x \cap y)$ é par.
   (b) (1 val.) A menos de equivalência, determine o número de códigos binários $[n, 1]_2$ auto-ortogonais.

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

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

   (a) (1,5 val.) Justifique que C é o dual de um código de Hamming e indique os seus parâmetros.
   (b) (1 val.) Mostre que C corrige todos os erros simples e os erros duplos adjacentes.
   (c) (1,5 val.) Usando a capacidade correctora de C enunciada em (b), descodifique os seguintes vectores

$$y = 1110000 \qquad \text{e} \qquad z = 1111000 .$$

4. Seja C um código linear binário tal que $\vec{1} \notin C$. Seja $C^c = \{x^c \mid x \in C\}$, onde x^c é o complementar de x. Para cada um dos seguintes códigos, decida se este é linear e determine quantas palavras contém:

   (a) (1 val.) C^c;
   (b) (1,5 val.) $C \cup C^c$.

Teste 2

5. Seja C um código binário perfeito de comprimento n e distância mínima $2t+1$, onde $t \geq 1$.

   (a) (1 val.) Mostre que existe um sistema de Steiner $S(t, 2t, n-1)$.

   (b) (1 val.) Seja $\mathring{C}$ o pontuado de C na última coordenada. Determine o número de palavras em $\mathring{C}$ com peso $2t$ em função de t e n.

6. Seja C o código linear sobre $\mathbb{F}_9 = \mathbb{F}_3[\alpha]$, onde $\alpha^2 = 2\alpha + 1$, com a seguinte matriz geradora

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \end{bmatrix}.$$

   (a) (1 val.) Mostre que C é um código cíclico.

   (b) (1,5 val.) Determine o polinómio gerador e os parâmetros $[n, k, d]$ de C, justificando cuidadosamente a sua resposta.

   (c) (1,5 val.) Determine o polinómio de paridade e uma matriz de paridade para C.

7. (2 val.) Seja C o código cíclico de comprimento 9, sobre $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, onde $\alpha^2 = \alpha+1$, com polinómio gerador

$$g(t) = \alpha + \alpha^2 t^3 + t^6 \ .$$

   Sabendo que C corrige todos os erros-m acumulados com $m \leq 3$, descodifique o vector recebido

$$y = (\alpha^2, 0, \alpha, 1, 0, 0, 0, 0, 1) \ .$$

8. (a) (1 val.) Determine as classes ciclotómicas-9 módulo 10.

   (b) (1 val.) Determine o número de códigos cíclicos sobre $\mathbb{F}_9$, de comprimento 10 e dimensão 7.