Instituto Superior Técnico
Departamento de Matemática
Secção de Álgebra e Análise

Combinatória e Teoria de Códigos
2º Exame

2 de Julho de 2010

Duração: 3h

Justifique cuidadosamente todas as suas respostas.

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

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

   (a) *(1.5 val.)* Justifique que C é a extensão de paridade de um código de Hamming, e determine os seus parâmetros $[n, k, d]$.

   (b) *(1.5 val.)* Mostre que C pode ser usado para corrigir todos os erros de peso 1 e todos os erros de peso 2 com a última coordenada não nula. Poderá este código ser usado para corrigir simultaneamente os erros anteriores e mais algum erro de peso 2?

   (c) *(1.5 val.)* Descreva um algoritmo de descodificação que corrija os erros indicados na alínea anterior e descodifique o vector recebido $y = 10111011$.

2. Um código linear C diz-se *auto-ortogonal* se $C \subseteq C^{\perp}$.

   (a) *(1 val.)* Mostre que o peso de qualquer palavra num código auto-ortogonal binário é par.

   (b) Seja C um código auto-ortogonal binário de parâmetros $\left[n, \frac{n-1}{2}\right]$, onde n é ímpar.

      (i) *(1 val.)* Mostre que $C^{\perp} = C \cup (\vec{1} + C)$, onde $\vec{1}$ denota o vector com todas as coordenadas iguais a 1 e $\vec{1} + C = \{\vec{1} + \vec{x} : \vec{x} \in C\}$.

      (ii) *(1 val.)* Mostre que a extensão por paridade de $C^{\perp}$ é auto-dual.

3. Seja C um código linear binário de parâmetros $[n, k, 2t+1]$ e seja $C' = \{x \in C : \mathrm{w}(x) \text{ é par}\}$ o subcódigo de C das palavras de peso par.

   (a) *(1 val.)* Justifique que C' é um código linear.

   (b) *(1.5 val.)* Determine, justificando detalhadamente, a dimensão de C'.

4. *(1.5 val.)* Considere a factorização, em termos irredutíveis, de $t^8 - 1$ em $\mathbb{F}_3[t]$

$$t^8 - 1 = (t-1)(t+1)(t^2+1)(t^2+t-1)(t^2-t-1) \ .$$

Escreva o polinómio gerador do menor código cíclico ternário, de comprimento 8, que contenha o vector $c = 12221000$.

5. Considere o código Reed-Solomon C sobre $\mathbb{F}_7$ com o seguinte polinómio gerador:

$$g(t) = (t-3)(t-3^2)(t-3^3)(t-3^4) = 4 + 2t + 3t^2 + 6t^3 + t^4 \ .$$

(a) *(1 val.)* Justifique que 3 é um elemento primitivo de $\mathbb{F}_7$.

(b) *(1 val.)* Indique, justificando, os parâmetros $[n, k, d]$ de C.

(c) *(1.5 val.)* Utilize o Algoritmo Caça ao Erro para descodificar o vector recebido $y = 100230$.

(d) *(1.5 val.)* Qual a percentagem de vectores erro de peso 2 que o Algoritmo Caça ao Erro corrige? Justifique.

6. 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) *(1 val.)* Mostre que o entrelaçamento $C^{(s)}$ de um código de repetição C é um código degenerado.

(b) *(1 val.)* 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) *(1.5 val.)* 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 $t^r - 1$.
[Sugestão: use o resultado da alínea anterior.]