Instituto Superior Técnico
Departamento de Matemática
Secção de Álgebra e Análise

Combinatória e Teoria de Códigos
2º Teste/1º Exame

18 de Junho de 2010

Duração: teste 1h 30m, exame 3h

- Justifique cuidadosamente todas as suas respostas.
- Exame: todas as perguntas. Teste: perguntas 3, 4 e 5.
- As cotações indicadas dizem respeito ao exame. Para obter as cotações do teste, multiplicar os valores por 2.

1. Considere o código linear C, sobre $\mathbb{F}_{11}$, com a seguinte matriz de paridade

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & X \\ 1 & 4 & 9 & 5 & 3 & 3 & 5 & 9 & 4 & 1 \end{bmatrix} .$$

Note que a última linha de H também se pode escrever na forma $\begin{bmatrix} 1^2 & 2^2 & 3^2 & \cdots & 9^2 & X^2 \end{bmatrix}$.

(a) *(1,5 val.)* Determine, justificando, os parâmetros $[n, k, d]$ do código C.

(b) *(1,5 val.)* Mostre que C corrige todos os erros simples e todos os erros de transposição adjacente.

(c) *(1 val.)* Descreva um algoritmo de descodificação incompleta que corrija os erros da alínia anterior.

(d) *(2 val.)* Usando o algoritmo da alínea anterior, descodifique os vectores recebidos

$$y = 0204000910 \quad \text{e} \quad z = 100000X308.$$

2. Considere dois códigos lineares C_1 e C_2 sobre $\mathbb{F}_q$, de comprimento n e dimensões $\dim(C_i) = k_i$, $i = 1, 2$, e defina

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

(a) *(2 val.)* Mostre que C é um código linear de parâmetros $[3n, 2k_1 + k_2]$.

(b) *(2 val.)* Escreva uma matriz geradora de C em termos de matrizes geradoras G_1 e G_2 de C_1 e C_2, respectivamente.

3. Considere a factorização, em factores irredutíveis, de $t^9 - 1$ em $\mathbb{F}_2[t]$

$$t^9 - 1 = (1 + t)(1 + t + t^2)(1 + t^3 + t^6) \ .$$

   (a) *(1 val.)* Diga quantos códigos cíclicos binários de comprimento $n = 9$ existem.

   (b) *(1 val.)* Escreva o polinómio gerador e uma matriz geradora de um código cíclico binário de comprimento $n = 9$ e dimensão $k = 2$.

   (c) *(1 val.)* Determine o polinómio e uma matriz de paridade para o código C da alínea anterior.

   (d) *(1,5 val.)* Indique,justificando, quantas palavras de peso par o código dual $C^{\perp}$ possui.

4. Considere o código Reed-Solomon C sobre $\mathbb{F}_8$ com o seguinte polinómio gerador:

$$g(t) = (t - \alpha)(t - \alpha^2)(t - \alpha^3)(t - \alpha^4) = \alpha^3 + \alpha t + t^2 + \alpha^3 t^3 + t^4 \ ,$$

   onde identificamos $\mathbb{F}_8$ com o quociente $\mathbb{F}_2[t]/\langle 1 + t + t^3 \rangle$, e $\alpha \in \mathbb{F}_8$ é uma raíz de $1 + t + t^3$.

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

   (b) *(2 val.)* Utilize o Algoritmo Caça ao Erro para descodificar os vectores recebidos

   $$y = (0, 1, 0, \alpha^2, 0, 0, 0) \quad \text{e} \quad z = (0, \alpha^3, 0, 1, \alpha^3, 1, 1).$$

   [Sugestão: Verifique que $\alpha^5 + \alpha^4 t + \alpha^3 t^2 + \alpha^4 t^3$ é o resto da divisão de $z(t)$ por $g(t)$.]

   (c) *(1 val.)* Seja $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ um isomorfismo vectorial sobre $\mathbb{F}_2$ à sua escolha. O que pode concluir sobre a capacidade de correcção de erros acumulados do código concatenação $C^* = \phi^*(C)$?

5. *(1,5 val.)* Seja C um código binário MDS com comprimento n e dimensão k tal que $1 < k < n$. Assumindo que C têm uma matriz geradora na forma canónica $G = [I|A]$, mostre que C é o dual do código de repetição.

   [Sugestão: Comece por justificar que um código linear de redundância r é MDS se e só se quaisquer r colunas de uma matriz de paridade H são linearmente independentes.]

Formulário

Tabela de inversos em $\mathbb{F}_{11}$

x	1	2	3	4	5	6	7	8	9	X
x^{-1}	1	6	4	3	9	2	8	7	5	X

Potências em $\mathbb{F}_8$

Se $\alpha \in \mathbb{F}_8$ é uma raíz do polinómio $1+t+t^3$, as potências α^i, com $i = 3, \ldots, 6$, podem-se escrever na seguinte forma:

$$\begin{aligned} \alpha^3 &= 1 + \alpha \\ \alpha^4 &= \alpha + \alpha^2 \\ \alpha^5 &= 1 + \alpha + \alpha^2 \\ \alpha^6 &= 1 + \alpha^2 \end{aligned}$$