Instituto Superior Técnico
Departamento de Matemática
Secção de Álgebra e Análise

Combinatória e Teoria de Códigos
Exame/Teste de Recuperação

27 de Junho de 2011

Duração: exame 3h, teste 1h 30m

Justifique cuidadosamente todas as suas respostas.

As cotações indicadas dizem respeito ao exame. Para obter as cotações do teste, multiplicar os valores por 2.

1º Teste

1. Para cada $x \in \mathbb{F}_{q^m}$, definimos o seu traço por $\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{q^i}$.

   (a) *(1 val.)* Mostre que $\mathrm{Tr}(x) \in \mathbb{F}_q$ para todo o $x \in \mathbb{F}_{q^m}$.

   (b) *(1,5 val.)* Mostre que $\mathrm{Tr} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ é uma aplicação linear sobre $\mathbb{F}_q$.

   (c) *(1,5 val.)* Se C é um código linear $[N, K, D]$ sobre $\mathbb{F}_{q^m}$, definimos o *código traço* por

   $$\mathrm{Tr}(C) = \{(\mathrm{Tr}(x_1), \ldots, \mathrm{Tr}(x_N)) \,:\, (x_1, \ldots, x_N) \in C\} \,.$$

   Mostre que $\mathrm{Tr}(C)$ é um código linear q-ário, de comprimento N e dimensão $k \leq mK$.

   Sugestão para o exercício 1: Recorde que $\mathbb{F}_q$ é um subcorpo de $\mathbb{F}_{q^m}$, e que $x \in \mathbb{F}_{q^m}$ pertence a $\mathbb{F}_q$ se e só se $x^q = x$.

2. Considere o código linear $C = \langle(\alpha, \alpha^2, \alpha^4, 1, \alpha^3, \alpha^6, \alpha^5)\rangle$ sobre $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, onde $\alpha^3 = 1 + \alpha$.

   (a) *(0,5 val.)* Indique os parâmetros de C.

   (b) *(1,5 val.)* Determine uma matriz geradora do código traço $\mathrm{Tr}(C)$.

   (c) *(1 val.)* Indique os parâmetros do código dual $\mathrm{Tr}(C)^\perp$.

   (d) *(1 val.)* Com o código $\mathrm{Tr}(C)^\perp$ da alínea anterior, descodifique o vector recebido
   $$y = 1101101.$$

3. *(2 val.)* Seja C um código de Hamming binário de redundância $r \geq 2$ e seja $\widehat{C}$ a sua extensão por paridade. Para um canal de transmissão binário e simétrico, com probabilidade de troca de símbolos $0 < p < 1$, mostre que $P_{corr}(C) = P_{corr}(\widehat{C})$, onde $P_{corr}(C)$ designa a probabilidade de descodificação correcta para o código C.

2º Teste

4. Seja $C = \mathrm{Ham}(3, 2)$ o código de Hamming binário com polinómio gerador $g(t) = 1 + t + t^3$

   (a) *(1 val.)* Determine os parâmetros $[n, k, d]$ do código entrelaçado $C^{(3)}$.

   (b) *(1 val.)* Determine o polinómio gerador e o de paridade de $C^{(3)}$.

   (c) *(1,5 val.)* Mostre que $C^{(3)}$ corrige todos os erros-m acumulados com $m \leq 3$, mas não corrige todos os erros acumulados de comprimento 4.

   (d) *(1,5 val.)* Usando o algoritmo caça ao erro acumulado, descodifique o vector recebido
   $$y(t) = t + t^3 + t^4 + t^9 + t^{13}.$$

5. Considere o código linear $A = \langle (1, \alpha^2, 0), (\alpha, 0, 1) \rangle$ sobre $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ (onde $\alpha^2 = 1 + \alpha$) e o código linear binário $B = \langle 1010, 0101 \rangle$. Seja A^* a concatenação de A e B em relação à aplicação linear $\phi : \mathbb{F}_4 \longrightarrow \mathbb{F}_2^4$ definida por $\phi(1) = 1010$ e $\phi(\alpha) = 1111$.

   (a) *(1 val.)* Determine uma base para o código A^*.

   (b) *(1 val.)* Determine os parâmetros $[n, k, d]$ do código A^*.

6. Nas seguintes alíneas, desmonstre ou dê um contra-exemplo.

   (a) *(1,5 val.)* O dual de um código Reed-Solomon é ainda um código Reed-Solomon.

   (b) *(1,5 val.)* A extensão por paridade de um código Reed-Solomon é ainda um código Reed-Solomon.