

## Combinatória e Teoria de Códigos

Teste 1 – 8 de Abril de 2016

Duração: 1h 30m

- **Justifique cuidadosamente todas as suas respostas.**
- **Não é permitido o uso de máquinas calculadoras, telemóveis, nem de outros elementos de consulta.**

1. Determine o número de soluções inteiras da equação  $x_1 + x_2 + x_3 = 20$  quando

- (a) (1 val.)  $x_i \geq 0$  para  $i = 1, 2, 3$ ;  
(b) (2 val.)  $x_1 \geq 0$ ,  $2 \leq x_2 \leq 5$  e  $1 \leq x_3 \leq 3$ .

2. Seja  $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ , onde  $\alpha^2 = \alpha + 1$ .

- (a) (1 val.) Mostre que o polinómio  $f(t) = t^2 + t + \alpha$  é irredutível em  $\mathbb{F}_4[t]$ .  
(b) Considere o corpo  $\mathbb{F}_{16} = \mathbb{F}_4[t]/\langle f(t) \rangle$ , i.e.,  $\mathbb{F}_{16} = \mathbb{F}_4[\beta]$ , onde  $\beta^2 = \beta + \alpha$ .  
Sejam  $u = (1, 0, \alpha, \alpha, \alpha\beta)$  e  $v = (0, 1, \alpha^2, 0, \alpha^2\beta)$  vectores em  $\mathbb{F}_{16}^5$  e seja  $C$  o código linear sobre  $\mathbb{F}_{16}$  gerado por  $u$  e  $v$ .  
(i) (2 val.) Justifique que  $C$  é um espaço vectorial sobre  $\mathbb{F}_4$  e escreva uma base para  $C$  sobre  $\mathbb{F}_4$ . Será  $C$  um código linear sobre  $\mathbb{F}_4$ ?  
(ii) (3 val.) Determine uma matriz geradora para o código subcorpo  $C|_{\mathbb{F}_4} = C \cap \mathbb{F}_4^5$ .

3. Seja  $C$  o código linear sobre  $\mathbb{F}_7$  com matriz de paridade

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

Pode assumir, sem justificar, que  $d(C) = 4$ .

- (a) (1 val.) Qual a capacidade de correcção de erros de  $C$ ?  
(b) (3 val.) Descodifique por distância mínima, se possível, os seguintes vectores recebidos

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

4. Seja  $C$  o subcódigo das palavras de peso par de um código de Hamming binário  $\text{Ham}(3, 2)$ , i.e.,

$$C = \{x \in \text{Ham}(3, 2) : w(x) \text{ é par} \}.$$

- (a) (3 val.) Justifique que  $C$  é um código linear e escreva uma matriz de paridade para  $C$ .  
(b) (2 val.) Determine, justificando, os parâmetros  $[n, k, d]$  de  $C$ .  
(c) (2 val.) Mostre que  $C$  é o dual de um código de Hamming.