Instituto Superior Técnico
Departamento de Matemática
Secção de Álgebra e Análise

Combinatória e Teoria de Códigos

Teste 2 – 19 de Junho de 2017

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. Seja $C \subset \mathbb{F}_2^{10}$ um código linear binário com o seguinte polinómio enumerador de pesos
$$w_C(t) = 1 + 8t^3 + 7t^4 + 7t^6 + 8t^7 + t^{10} \ .$$
Determine o polinómio enumerador de pesos e os parâmetros $[n, k, d]$ de cada um dos seguintes códigos:
   (a) (2 val.) a extensão por paridade $\widehat{C}$;
   (b) (2 val.) o código soma $C \oplus D$, onde $D \subset \mathbb{F}_2^{10}$ é o código de repetição.

2. (3,5 val.) Sejam C e D códigos cíclicos q-ários com o mesmo comprimento. Em cada uma das alíneas, demonstre ou dê um contra-exemplo:
   (a) $C \cap D$ é um código cíclico;
   (b) $C \oplus D$ é um código cíclico.

3. Seja $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, onde $\alpha^2 = \alpha + 1$, e considere a factorização em $\mathbb{F}_4[t]$
$$t^{10} - 1 = (t-1)^2(t^2 + \alpha t + 1)^2(t^2 + \alpha^2 t + 1)^2 \ .$$
   (a) (2 val.) Determine o número de códigos cíclicos sobre $\mathbb{F}_4$ com comprimento 10 e dimensão 5.
   (b) (2,5 val.) Escreva o polinómio gerador de um código cíclico sobre $\mathbb{F}_4$, auto-dual, com comprimento 10.

4. Seja $\mathbb{F}_9 = \mathbb{F}_3[\alpha]$, onde $\alpha^2 = 2\alpha + 1$. Seja $C \subset \mathbb{F}_9^8$ o código cíclico com polinómio gerador
$$\begin{aligned} g(t) &= (t-\alpha)(t-\alpha^2)(t-\alpha^3)(t-\alpha^4)(t-\alpha^5)(t-\alpha^6) \\ &= 2\alpha + 2t + \alpha t^2 + (\alpha+1)t^3 + (2\alpha+1)t^4 + (\alpha+2)t^5 + t^6 \ . \end{aligned}$$
   (a) (2 val.) Justifique que C é um código Reed-Solomon e indique os seus parâmetros $[n, k, d]$.
   (b) (3 val.) Usando o Algoritmo Caça ao Erro, descodifique, se possível, o seguinte vector recebido
$$y = (2\alpha + 1, 2, 2\alpha + 2, \alpha + 1, \alpha, 0, 0, 0) \ .$$
   (c) (3 val.) Seja C^* o código concatenação de C com $B = \mathbb{F}_3^2$ usando o isomorfismo linear $\phi : \mathbb{F}_9 \to B$ definido por $\phi(a_0 + a_1\alpha) = (a_0, a_1)$, para $a_0, a_1 \in \mathbb{F}_3$. Determine uma base para C^*.