COMBINATÓRIA E TEORIA DE CÓDIGOS
Ficha de revisão para o 2º teste

1/6/2010

1. Como $1+t+t^3$ e $1+t^2+t^3$ são polinómios irredutíveis em $\mathbb{F}_2[t]$, os quocientes $A = \mathbb{F}_2[t]/\langle 1+t+t^3\rangle$ e $B = \mathbb{F}_2[t]/\langle 1+t^2+t^3\rangle$ são ambos isomorfos ao corpo $\mathbb{F}_8$. Escreva um isomorfismo $\phi : A \to B$.

   [Sugestão: Seja $\alpha \in A$ uma raíz de $1+t+t^3$ e $\beta \in B$ uma raíz de $1+t^2+t^3$. Encontre uma relação entre α e β ou, mais precisamente, determine uma raíz de $1+t^2+t^3$ em A.]

2. Seja $h(t)$ o polinómio de paridade de um código cíclico C.

   (a) Mostre que $C^\perp$ e $\langle h(t)\rangle$ são códigos equivalentes.

   (b) Dê um exemplo de C que verifique $C^\perp \neq \langle h(t)\rangle$.

3. (a) Factorize $t^{12}-1$ no produto de polinómios irredutíveis em $\mathbb{F}_3[t]$

   (b) Quantos códigos cíclicos ternários de comprimento 12 existem?

   (c) Determine para que valores de k existe um código cíclico ternário $[12, k]$.

   (d) Quantos códigos cíclicos ternários com parâmetros $[12, 9]$ existem?

4. Seja C um código binário com polinómio gerador $g(t)$.

   (a) Mostre que, se $t-1$ divide $g(t)$, então todas as plavras de código têm peso par.

   (b) Assumindo que o comprimento de C é ímpar, mostre que C contém uma palavra de peso ímpar se e só se o vector $\vec{1} = (1, \ldots, 1)$ é uma palavra de código.

5. Determine o polinómio gerador e a dimensão do menor código binário que contém a palavra $c = 1000111 \in \mathbb{F}_2^7$.

6. (a) Exercícios 2 da Ficha 7 e 3 da Ficha 8.
   (b) Exercício 1 da Ficha 8.

7. Seja C um código linear. Justifique que o código entrelaçado de grau s $C^{(s)}$ é equivalente ao código soma $\underbrace{C \oplus \cdots \oplus C}_{\text{s vezes}}$.

8. Seja C o código de Hamming binário de redundância 3 com polinómio gerador $g(t) = 1 + t + t^3$
   (a) Determine os parâmetros de $C^{(3)}$.
   (b) Determine o polinómio gerador de $C^{(3)}$.
   (c) Mostre que o código $C^{(3)}$ corrige todos os erros acumulados de comprimento menor ou igual a 3.

9. Seja C um código Reed-Solomon q-ário com polinómio gerador
$$(t - \alpha^a)(t - \alpha^{a+1}) \cdots (t - \alpha^{a+\delta-1}) \ .$$
   Mostre que $c(t) \in \mathbb{F}_q[t]/\langle t^{q-1} - 1\rangle$ é uma palavra de código se e só se $c(\alpha^i) = 0$ para qualquer $i = a, \ldots, a + \delta - 1$.

10. Seja C o código Reed-Solomon sobre $\mathbb{F}_8$ com polinómio gerador $g(t) = (t - \alpha)(t - \alpha^2)(t - \alpha^3)$, onde $\alpha \in \mathbb{F}_8$ é uma raíz de $1 + t + t^3$.
   (a) Justifique que α é um elemento primitivo de $\mathbb{F}_8$.
   (b) Determine os parâmetros de C.
   (c) Determine os parâmetros do código dual $C^\perp$.
   (d) Determine os parâmetros da extensão $\widehat{C}$.
   (e) Determine os parâmetros de $C^* = \phi^*(C)$, onde $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ é a aplicação linear definida por $\phi(1) = 100$, $\phi(\alpha) = 010$ e $\phi(\alpha^2) = 101$. [Sugestão: Calcule $w(\phi^*(g(t)))$.]