COMBINATÓRIA E TEORIA DE CÓDIGOS

TPC 5 (para entregar na aula de 16/5/2014)

Observação: Os exercícios 1 a 4 valem 20 pontos no total, o exercício bónus A vale 4 pontos extra.

1. (a) Factorize $t^{12} - 1$ no produto de polinómios irredutíveis em $\mathbb{F}_2[t]$.
   (b) Quantos códigos cíclicos biários de comprimento 12 existem?
   (c) Determine para que valores de k existe um código cíclico binário $[12, k]$.
   (d) Quantos códigos cíclicos biários com parâmetros $[12, 9]$ existem?
   (e) Determine todos os códigos cíclicos binários auto-duais de comprimento 12, indicando os respectivos polinómios geradores.

2. (Exercício 8.8 das notas.) Seja C um código cíclico 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.

3. (Exercícios 8.14 e 8.15 das notas.)
   (a) Seja $g(t)$ o polinómio gerador de um código de Hamming binário $\mathrm{Ham}(r, 2)$, com $r \geq 3$. Mostre que $C = \langle (t-1)g(t) \rangle$ é um código de parâmetros $[2^r - 1, 2^r - r - 2, 4]$. [Sugestão: use o exercício 2.]
   (b) Mostre que o código C pode ser usado para corrigir todos os erros duplos adjacentes, i.e., em posições consecutivas.
   (c) (Generalização da alínea anterior.) Seja $C = \langle (t+1)f(t) \rangle$ um código cíclico binário de comprimento n, onde $f(t) \mid t^n - 1$, mas $f(t) \nmid t^i - 1$, para $1 \leq i \leq n - 1$. Mostre que C corrige todos os erros simples e também os erros duplos em posições consecutivas.

4. (Exercício 8.16 das notas.) Considere o código cíclico binário de comprimento $n = 15$ gerado pelo polinómio $g(t) = 1 + t^3 + t^4 + t^5 + t^6$.
   (a) Justifique que $g(t)$ é de facto o polinómio gerador daquele código.
   (b) Escreva uma matriz geradora, o polinómio de paridade e uma matriz de paridade para o código.
   (c) Escreva, justificando, uma matriz geradora na forma $G = \begin{bmatrix} R & I \end{bmatrix}$ para aquele código e a correspondente matriz de paridade.
   (d) Codifique sistematicamente o vector mensagem $m = 010010001$.
   (e) Sabendo-se que aquele código tem distância mínima $\mathrm{d}(C) = 5$, descodifique o vector recebido $y = 010011000111010$, justificando convenientemente as suas decisões.

A. (a) Seja C um código cíclico $[n, k, d]_q$ com polinómio gerador $g(t)$. Como C é também um código linear, pela independência linear das colunas de uma matriz de paridade, já sabemos que C corrige todos os erros de apagamento até $d-1$ símbolos, usando descodificação por síndrome.

Usando agora as propriedades cíclicas do código e o Algoritmo Caça ao Erro, quais os tipos de erros de apagamento que C pode corrigir? Considere não só o número de símbolos apagados mas também a sua distribuição na palavra recebida.

(b) Seja C o código binário, de comprimento $n = 15$, com polinómio gerador

$$g(t) = 1 + t^4 + t^6 + t^7 + t^8 \ .$$

A distância mínima deste código é $d = 5$. Descodifique, se possível, os seguintes vectores recebidos:

$$y = 000??????111000 \qquad \text{e} \qquad z = ?0101?0101?0000 \ .$$