

# COMBINATÓRIA E TEORIA DE CÓDIGOS

## TPC 5 (para entregar na aula de 10/5/2013)

- Factorize  $t^{12} - 1$  no produto de polinómios irredutíveis em  $\mathbb{F}_2[t]$ .
  - Quantos códigos cíclicos biários de comprimento 12 existem?
  - Determine para que valores de  $k$  existe um código cíclico binário  $[12, k]$ .
  - Quantos códigos cíclicos biários com parâmetros  $[12, 9]$  existem?
  - Determine todos os códigos cíclicos binários auto-duais de comprimento 12, indicando os respectivos polinómios geradores.
- Determine o polinómio gerador e a dimensão do menor código cíclico ternário que contém a palavra  $c = 220211010000 \in \mathbb{F}_3^{12}$ .
- (Exercício 8.8 das notas.) Seja  $C$  um código cíclico binário com polinómio gerador  $g(t)$ .
  - Mostre que, se  $t - 1$  divide  $g(t)$ , então todas as palavras de código têm peso par.
  - Assumindo que o comprimento de  $C$  é ímpar, mostre que  $C$  contém uma palavra de peso ímpar se e só se o vector  $\vec{1} = (1, \dots, 1)$  é uma palavra de código.
- (Exercícios 8.14 e 8.15 das notas.)
  - Seja  $g(t)$  o polinómio gerador de um código de Hamming binário  $\text{Ham}(r, 2)$ , 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 3.]
  - Mostre que o código  $C$  pode ser usado para corrigir todos os erros duplos adjacentes, i.e., em posições consecutivas.
  - (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.
- (Exercício 8.16 das notas.) Considere o código cíclico binário de comprimento  $n = 15$  gerado pelo polinómio  $g(t) = 1 + t^3 + t^4 + t^5 + t^6$ .
  - Justifique que  $g(t)$  é de facto o polinómio gerador daquele código.
  - Escreva uma matriz geradora, o polinómio de paridade e uma matriz de paridade para o código.
  - Escreva, justificando, uma matriz geradora na forma  $G = [R \ I]$  para aquele código e a correspondente matriz de paridade.
  - Codifique sistematicamente o vector mensagem  $m = 010010001$ .
  - Sabendo-se que aquele código tem distância mínima  $d(C) = 5$ , decodifique o vector recebido  $y = 010011000111010$ , justificando convenientemente as suas decisões.