COMBINATÓRIA E TEORIA DE CÓDIGOS
Ficha 5

14/04/2008

Exercícios 8.1 - 8.12 + 9.1 - 9.11 de R. Hill

1. a) Exercício 5.12 do Hill;

b) Se G_1 e G_2 são, respectivamente, as matrizes geradoras dos códigos C_1 e C_2, exprima a matriz geradora G de $C_1 * C_2$ (Construção de Plotkin) em termos de G_1 e G_2.[Comece por identificar as dimensões da matriz G.];

c) Chamando $G(r, m)$ à matriz geradora do código $RM(r, m)$, obtenha definições recursivas para essas matrizes.
[Considere separadamente os casos $r = 0$, $r = m$ e $0 < r < m$.]

2. a) Mostre que

$$RM(r, m)^{\perp} = RM(m - r - 1, m), \ \forall 0 \leq r < m;$$

b) Mostre que $RM(1, m)$ contém uma única palavra de peso 0, nomeadamante a palavra nula, uma única de peso 2^m, nomeadamente a palavra com 1 em todas as posições, e $2^{m+1} - 2$ palavras de peso 2^{m-1}.

c) Mostre que $RM(1, m)$ é equivalente ao dual de um Código de Hamming binário estendido.

d) Conclua que o dual de um código de Hamming binário é um código *simplex*, mais concretamente, que o dual de um código de Hamming binário de redundância r tem todas as palavras equidistantes e de peso igual a 2^{r-1}

3. Para cada vector binário $\mathbf{x} \in \mathbb{F}_2^n$ considere o correspondente vector $\mathbf{x}^* \in \{+1,-1\}^n$ obtido substituindo cada 0 pelo número real $+1$ e cada 1 por -1:

a) Mostre que, se $\mathbf{x},\mathbf{y} \in \mathbb{F}_2^n$, então, usando o produto interno canónico em $\mathbb{R}^n$

$$\langle \mathbf{x}^*, \mathbf{y}^* \rangle = n - 2d(x,y)$$

Em particular, se $\mathbf{x},\mathbf{y} \in \mathbb{F}_2^{2h}$ com $d(x,y) = h$, então $\langle \mathbf{x}^*, \mathbf{y}^* \rangle = 0$;

b) Seja $RM(1,m)^{\pm} = \{\mathbf{c}_1^*, \mathbf{c}_2^*, \ldots, \mathbf{c}_{2^{m+1}}^*\}$ o código obtido substituindo cada palavra de código $\mathbf{c}$ de $RM(1,m)$ pela sua versão ± 1, $\mathbf{c}^*$. Mostre que então:

(i) $\mathbf{c}^* \in RM(1,m)^{\pm} \Rightarrow -\mathbf{c}^* \in RM(1,m)^{\pm}$;

(ii)

$$\langle \mathbf{c}_i^*, \mathbf{c}_j^* \rangle = \begin{cases} 2^m & \text{se} \quad \mathbf{c}_i^* = \mathbf{c}_j^* \\ -2^m & \text{se} \quad \mathbf{c}_i^* = -\mathbf{c}_j^* \\ 0 & \text{se} \quad \mathbf{c}_i^* \neq \pm \mathbf{c}_j^* \end{cases}$$

c) Use a alínea anterior como base justificativa para o seguinte algoritmo de descodificação. Recebido um vector $\mathbf{y}$ calculam-se os produtos internos $\langle \mathbf{y}, \mathbf{c}_i^* \rangle$ para $i = 1, \ldots, 2^{m+1}$ e descodifica-se para a palavra de código $\mathbf{c}_j^*$ que maximiza esse produto.

4. Seja $C : [n,k,d]_2$, $k \geq 2$, um código linear binário, $\mathbf{c} \in C : d \leq w(\mathbf{c}) < n$ e

$$G_{k\times n} = \begin{bmatrix} - & \mathbf{c} & - \\ & G'_{(k-1)\times n} & \end{bmatrix}$$

uma matriz geradora para C.

Se as componentes nulas de $\mathbf{c}$ são $c_{i_1} = c_{i_2} = \cdots = c_{i_{n-w}} = 0$, tome-se a submatriz de G'

$$G'_1 = \begin{bmatrix} g'_{1i_1} & g'_{1i_2} & \cdots & g'_{1i_{n-w}} \\ \vdots & \vdots & \ddots & \vdots \\ g'_{(k-1)i_1} & g'_{(k-1)i_2} & \cdots & g'_{(k-1)i_{1n-w}} \end{bmatrix}.$$

Chama-se *Código Residual* $RES(C,\mathbf{c})$ ao código que tem G'_1 como matriz geradora.

a) Justifique que se pode sempre escolher uma palavra de código nas condições de $\mathbf{c}$;

b) Mostre que, fixada $\mathbf{c} \in C$, $\mathrm{RES}(C, \mathbf{c})$ não depende da matriz G';

c) Mostre, através de exemplos, que, contudo, $\mathrm{RES}(C, \mathbf{c})$ depende essencialmente da palavra $\mathbf{c}$ escolhida e que mesmo que $w(\mathbf{c}) = w\left(\mathbf{c}'\right)$, em geral, $\mathrm{RES}(C, \mathbf{c}) \neq \mathrm{RES}\left(C, \mathbf{c}'\right)$, podendo mesmo não ser sequer equivalentes.

d) Tomando agora $\mathbf{c} \in C : w(\mathbf{c}) = w(C) = d$: demonstre que $\mathrm{RES}(C, \mathbf{c}) : \left[n - d, k - 1, d'\right]$, com $d' \geq \left\lceil \frac{d}{2} \right\rceil$;

e) Definindo

$$n^*(k, d) = \min\{n \in \mathbb{N} : \exists C_2 [n, k, d]\},$$

mostre que

$$n^*(k, d) \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil;$$

f) Mostre que os códigos simplex binários (duais dos códigos de Hamming), atingem a igualdade na desigualdade da alínea **e)**.