# COMBINATÓRIA E TEORIA DE CÓDIGOS
## Exercise List 5

21/03/201

Exercises 8.1 - 8.12 + 9.1 - 9.11 (R. Hill)

**1. a)** Exercise 5.12 in Hill;

**b)** If $G_1$ e $G_2$ are generator matrices for the codes $C_1$ and $C_2$, respectevely, write a generator matrix for $C_1 * C_2$ (Plotkin construction) in terms of $G_1$ and $G_2$. [First, find the number or columns and rows of G.]

**c)** Denote by $G(r, m)$ the generator matrix of $\mathcal{RM}(r, m)$. Write a recursive definition for these matrices. [Consider separately the cases $r = 0$, $r = m$ and $0 < r < m$.]

**2. a)** Show that

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

**b)** Show that $\mathcal{RM}(1, m)$ contains a unique word of weight 0, namely the zero word, a unique word of weight $2^m$, namely the word whose components are all 1, and $2^{m+1} - 2$ words of weight $2^{m-1}$.

**c)** Show that $\mathcal{RM}(1, m)$ is equivalent to the dual of an extended binary Hamming code.

**d)** Conclude that the dual of a Hamming code is a *simplex* code, that is, conclude that the words in the dual of a Hamming code of redundancy $r$ are all equidistant and have weight $2^{r-1}$.

**3.** For each binary vector $\mathbf{x} \in \mathbb{F}_2^n$, consider the corresponding vector $\mathbf{x}^* \in \{+1, -1\}^n$ obtained by replacing each zero component by the real number $+1$ and each 1 by $-1$.

**a)** Show that, if $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, then, using the euclidean inner product in $\mathbb{R}^n$,

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

In particular, if $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{2h}$ with $d(x, y) = h$, then $\langle \mathbf{x}^*, \mathbf{y}^* \rangle = 0$;

**b)** Let $\mathcal{RM}(1, m)^{\pm} = \{\mathbf{c}_1^*, \mathbf{c}_2^*, \ldots, \mathbf{c}_{2^{m+1}}^*\}$ be the code obtained replacing each codeword $\mathbf{c}$ in $\mathcal{RM}(1, m)$ by its $\pm 1$ version $\mathbf{c}^*$. Show that:

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

**(ii)**

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

**c)** Apply part b) to justify the following decoding algorithm: If $\mathbf{y}$ is the received vector, compute the inner products $\langle \mathbf{y}, \mathbf{c}_i^* \rangle$, for $i = 1, \ldots, 2^{m+1}$, and decode $y$ by the codeword $\mathbf{c}_j^*$ which maximizes these products.

**4.** Let $C$ be a $[n, k, d]_2$ binary linear code, with $k \geq 2$, and let $\mathbf{c} \in C$, with $d \leq w(\mathbf{c}) < n$, be such that

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

is a generator matrix for $C$.

If $c_{i_1} = c_{i_2} = \cdots = c_{i_{n-w}} = 0$ are the zero components of $\mathbf{c}$, consider the submatrix of $G'$

$$G_1' = \begin{bmatrix} g'_{1i_1} & g'_{1i_2} & \cdots & g'_{1i_{n-w}} \\ \vdots & \vdots & \ddots & \vdots \\ g'_{(k-1)i_1} & g'_{(k-1)i_2} & \cdots & g'_{(k-1)i_{1n-w}} \end{bmatrix}.$$

The code with $G'$ as a generator matrix is called the *Residual Code* $\mathrm{RES}(C, \mathbf{c})$.

**a)** Justify that we can always choose a codeword satisfying the same conditions as $\mathbf{c}$;

**b)** Show that, for a fixed $\mathbf{c} \in C$, the code $\mathrm{RES}(C, \mathbf{c})$ does not depend on the matrix $G'$;

**c)** Show, with examples, that $\mathrm{RES}(C, \mathbf{c})$ depends on the chosen word $\mathbf{c}$, and, even if $w(\mathbf{c}) = w(\mathbf{c}')$, in general we have $\mathrm{RES}(C, \mathbf{c}) \neq \mathrm{RES}(C, \mathbf{c}')$ and, moreover, these codes may not be equivalent.

**d)** Now fix $\mathbf{c} \in C$ with $w(\mathbf{c}) = w(C) = d$. Show that $\mathrm{RES}(C, \mathbf{c})$ is a $[n - d, k - 1, d']$ code with $d' \geq \left\lceil \frac{d}{2} \right\rceil$;

**e)** Define

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

and show that

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

**f)** Show that the binary simplex codes (the dual of the binary Hamming codes) satisfy the equality in the inequality in part **e)**.