COMBINATÓRIA E TEORIA DE CÓDIGOS

TPC 3 (para entregar na aula de 5/4/2013)

1. Para cada $x \in \mathbb{F}_{q^m}$, definimos o seu traço por $\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{q^i}$.

   (a) Mostre que $(a+b)^{q^i} = a^{q^i} + b^{q^i}$ para quaisquer $a, b \in \mathbb{F}_{q^m}$ e $i \in \mathbb{N}$.
   Sugestão: Mostre primeiro que $(a+b)^p = a^p + b^p$, onde p é a característica de $\mathbb{F}_{q^m}$.

   (b) Justifique que, para qualquer $a \in \mathbb{F}_{q^m}$, $a \in \mathbb{F}_q \subset \mathbb{F}_{q^m}$ se e só se $a^q = a$.

   (c) Mostre que $\mathrm{Tr}(x) \in \mathbb{F}_q$ para todo o $x \in \mathbb{F}_{q^m}$.

   (d) Mostre que $\mathrm{Tr} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ é uma aplicação linear sobre $\mathbb{F}_q$.

   (e) Se C é um código linear $[N, K, D]$ sobre $\mathbb{F}_{q^m}$, definimos o *código traço* por

   $$\mathrm{Tr}(C) = \{(\mathrm{Tr}(x_1), \ldots, \mathrm{Tr}(x_N)) \,:\, (x_1, \ldots, x_N) \in C\} \ .$$

   Mostre que $\mathrm{Tr}(C)$ é um código linear q-ário, de comprimento N e dimensão $k \leq mK$.

2. Considere o código linear $C = \langle(\alpha, \alpha^2, \alpha^4, 1, \alpha^3, \alpha^6, \alpha^5)\rangle$ sobre $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, onde $\alpha^3 = 1+\alpha$.

   (a) Indique os parâmetros de C.

   (b) Determine uma matriz geradora do código traço $\mathrm{Tr}(C)$.

   (c) Indique os parâmetros do código dual $\mathrm{Tr}(C)^\perp$.

   (d) Será $Tr(C)$ um código auto-ortogonal ou auto-dual?

   Se C é um código linear sobre $\mathbb{F}_{q^m}$, definimos o *subcódigo subcorpo* por

   $$C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^N \ .$$

   Pode usar, sem o demonstrar, que o subcódigo subcorpo $C|_{\mathbb{F}_q}$ é linear sobre $\mathbb{F}_q$.

   (e) Determine uma matriz geradora para o código dual $C^\perp$ e para o subcódigo subcorpo $(C^\perp)|_{\mathbb{F}_2}$.

   (f) Verifique que $(C^\perp)|_{\mathbb{F}_2} = \mathrm{Tr}(C)^\perp$.
   Nota: Esta relação entre os códigos traço e subcorpo é válida para qualquer código linear C sobre $\mathbb{F}_{q^m}$, é o Teorema de Delsarte.

3. (a) Para um código linear q-ário de comprimento n e distância mínima d, mostre que os vectores $x \in \mathbb{F}_q^n$ com peso $\mathrm{w}(x) \leq \lfloor \frac{d-1}{2} \rfloor$ são chefes de classes distintas deste código.

   (b) Seja C um código perfeito com $\mathrm{d}(C) = 2t+1$. Mostre que os únicos chefes de classe de C são os determinados na alínea anterior.

   (c) Assumindo que o código perfeito C da alínia (b) é binário, seja $\widehat{C}$ o código obtido de C acrescentando um dígito de paridade, i.e.,

$$\widehat{C} = \left\{ (x_1, \ldots, x_n, x_{n+1}) \in \mathbb{F}_2^{n+1} : (x_1, \ldots, x_n) \in C \,,\, \sum_{i=1}^{n+1} x_i = 0 \right\} .$$

   Mostre que qualquer chefe de classe de $\widehat{C}$ tem peso menor ou igual a $t+1$.

4. Seja C o código linear, sobre $\mathbb{F}_3 = \{0, 1, 2\}$, com a seguinte matriz de paridade

$$H = \begin{bmatrix} 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 \end{bmatrix} .$$

   (a) Determine, justificando, os parâmetros $[n, k, d]$ do código C.

   (b) Determine uma matriz geradora de C.

   (c) Mostre que C corrige todos os erros simples de amplitude 1 e ainda os erros duplos da forma

$$aa000000\,, \quad 0aa00000\,, \quad 00aa0000\,, \quad 000aa000\,,$$
$$0000aa00\,, \quad 00000aa0\,, \quad 000000aa \quad \text{e} \quad a000000a\,,$$

   com $a \in \{1, 2\}$.

   (d) Descodifique os seguintes vectores recebidos

$$y = 11111112 \qquad \text{e} \qquad z = 11211200\,.$$