COMBINATÓRIA E TEORIA DE CÓDIGOS

TPC 3 (para entregar na aula de 4/4/2014)

A. 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 $k \leq mK$.

B. Considere $\mathbb{F}_{16} = \mathbb{F}_2[t]/\langle t^4 + t + 1\rangle$, i.e., $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$ onde $\alpha^4 = \alpha + 1$.

(a) Justifique que $t^4 + t + 1$ é irredutível em $\mathbb{F}_2[t]$.

(b) Identifique $\mathbb{F}_4$ como subcorpo de $\mathbb{F}_{16}$.

(c) Determine um polinómio $f(t) \in \mathbb{F}_4[t]$ tal que $\mathbb{F}_{16} = \mathbb{F}_4[t]/\langle f(t)\rangle$.

1. 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 $\mathrm{Tr}(C)$ um código auto-ortogonal ou auto-dual?

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

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

(e) Justifique que o subcódigo subcorpo $C|_{\mathbb{F}_q}$ é linear sobre $\mathbb{F}_q$.

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

(g) 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.

2. Exercícios 4.6, 4.9 e 4.10.

Obervação:

- Cotações: os exercícios em 1 e 2 valem 20 pontos no total, os exercícios bónus A e B valem 4 pontos extra.
- Pode usar os resultados do exercício bónus A na resolução de outros problemas, mesmo que não o resolva.