COMBINATÓRIA E TEORIA DE CÓDIGOS

TPC 4

(para entregar na aula de 2/5/2014)

Observação: Os exercícios 1 a 4 valem 20 pontos no total, o exercício bónus A vale 4 pontos extra.

1. **Considere a construção C_λ do Problema 4 do Teste 1: Dado um código binário C de parâmetros (n, M, d), com $d \geq 3$, define-se**

$$C_\lambda = \{(x, x+c, \pi(x)+\lambda(c)) : x \in \mathbb{F}_2^n, c \in C\},$$

onde $\lambda : C \longrightarrow \mathbb{F}_2$ é uma aplicação qualquer e $\pi : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ é definido por

$$\pi(x) = \begin{cases} 0 & \text{se w}(x) \text{ é par,} \\ 1 & \text{se w}(x) \text{ é ímpar.} \end{cases}$$

Pode usar, sem demonstrar novamente, que $\mathrm{d}(C_\lambda) = 3$ e os resultados do teste.

(a) Mostre que, se C é um código per-

feito com $\mathrm{d}(C) = 3$, então C_λ é perfeito.

(b) Seja $C = \mathrm{Ham}(r, 2)$, com $r \geq 2$, e seja λ a aplicação nula. Será C_λ um código de Hamming? Justifique.

(c) Seja $C = \mathrm{Ham}(r, 2)$, com $r \geq 2$, e seja λ a aplicação constante igual a $1 \in \mathbb{F}_2$. Será C_λ um código de Hamming? Justifique.

(d) Seja

$$\begin{aligned} C &= \vec{e}_1 + \mathrm{Ham}(r, 2) \\ &:= \{\vec{e}_1 + c : c \in \mathrm{Ham}(r, 2)\}, \end{aligned}$$

com $r \geq 2$ e $\vec{e}_1 = (1, 0, \ldots, 0)$, e seja λ a aplicação nula. Será C_λ um código de Hamming? Justifique.

2. Para qualquer código C define-se o *polinómio enumerador de pesos* por

$$W_C(t) = \sum_{i \geq 0} A_i t^i \ ,$$

onde $A_i = \#\{x \in C : \mathrm{w}(x) = i\}$. (Note

que o polinómio $W_C(t)$ não é mais que a função geradora da sucessão $\{A_i\}_{i\in\mathbb{N}_0}$.)
Se C é um código binário, de comprimento n, mostre que

(a) $W_{C'}(t) = \frac{1}{2}\big(W_C(t) + W_C(-t)\big)$, onde $C' = \{x \in C : \mathrm{w}(x) \text{ é par}\}$;

(b)

$$W_{\widehat{C}}(t) = \frac{1}{2}\big((1+t)W_C(t) + (1-t)W_C(-t)\big),$$

onde $\widehat{C}$ é a extensão por paridade de C.

3. (Exercício 7.4.) Seja C um código binário perfeito de comprimento n e distância mínima $2t+1$. Mostre que existe um sistema de Steiner $S(t+2, 2t+2, n+1)$.

4. Determine o polinómio enumerador de pesos do código C quando

(a) (Exercício 7.8.) $C = G_{24}$ [sugestão: mostre que $\vec{1} \in G_{24}$];

(b) $C = G_{23}$.

A. Seja p um primo e seja $\zeta \in \mathbb{C}$ uma raíz-p primitiva da unidade, i.e.,

$$\zeta^p = 1 \text{ e } \zeta^i \neq 1 \text{ para } 1 \leq i \leq p-1 \ .$$

Dada uma função $f\colon \mathbb{F}_p^n \to V$ qualquer, onde V é um espaço vectorial complexo, define-se $\widehat{f}\colon \mathbb{F}_p^n \to V$ por[1]

$$\widehat{f}(x) = \sum_{y \in \mathbb{F}_p^n} f(y)\zeta^{x \cdot y} \ ,$$

onde $x \cdot y$ denota o produto interno euclideano em $\mathbb{F}_p^n$.

Dado um código linear $C \subset \mathbb{F}_p^n$, define-se $C_i(y) = \{x \in C \ : \ x \cdot y = i\}$, para $y \in \mathbb{F}_p^n$ e $i \in \mathbb{F}_p$.

(a) Mostre que $C = \cup_{i \in \mathbb{F}_p} C_i(y)$. Mostre também que $C_i(y)$ é uma classe de $C_0(y)$ em C se e só se $y \notin C^\perp$,

[1] Neste exercício, identificamos uma classe em $\mathbb{F}_p = \mathbb{Z}_p$ com o respectivo representante inteiro entre 0 e $p-1$.

ou seja, mostre que

$$\Big(\forall\, i \in \mathbb{F}_p \,\exists\, c_i \in C \,\text{t.q.}\, C_i(y) = c_i + C_0(y)\Big) \iff y \notin C^\perp \ .$$

(b) Mostre que

$$\sum_{x\in C} \zeta^{x\cdot y} = \begin{cases} |C| & \text{se } y \in C^\perp, \\ 0 & \text{se } y \notin C^\perp. \end{cases}$$

(c) Mostre que, para $y \in \mathbb{F}_p^n$,

$$f(y) = \frac{1}{p^n} \sum_{x\in\mathbb{F}_p^n} \widehat{f}(x)\zeta^{-x\cdot y} \ .$$

(d) Mostre que

$$\sum_{y\in C^\perp} f(y) = \frac{1}{|C|} \sum_{x\in C} \widehat{f}(x) \ .$$

(e) Seja $f(y) = t^{\mathrm{w}(y)} \in \mathbb{C}[t]$. Mostre que, para $x \in \mathbb{F}_p^n$,

$$\widehat{f}(x) = \big(1+(p-1)t\big)^{n-\mathrm{w}(x)}(1-t)^{\mathrm{w}(x)} \ .$$

(f) **Prove a *Identidade de MacWilliams*[2] para os polinómios enumeradores de pesos de C e do seu dual $C^{\perp}$:**

$$W_{C^{\perp}}(t) = \frac{1}{|C|}(1+(p-1)t)^n W_C\Big(\frac{1-t}{1+(p-1)t}\Big).$$

Uma aplicação: dado que

$$\mathrm{Ham}\,(r,p) = S(r,p)^{\perp}$$

e que

$$W_{S(r,p)}(t) = 1 + (p^r - 1)t^{p^{r-1}}$$

(como consequência da Proposição 6.12), obtém-se $W_{\mathrm{Ham}(r,p)}(t)$ através de da Identidade de MacWilliams.

---

[2] **A Identidades de MacWilliams é válida para o corpo $\mathbb{F}_q$, com q não necessariamente um primo. Para uma demonstração geral pode consultar o livro de S. Roman. No livro de R. Hill, apenas é feito o caso binário.**