Combinatória e Teoria de Códigos
2º Exame

2 de Julho de 2010

RESOLUÇÃO

1. (a) Seja

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

As colunas de H' são todos os vectores não nulos em $\mathbb{F}_2^3$, portanto H' é uma matriz de paridade para um código de Hamming $\mathrm{Ham}(3,2)$, com parâmetros $[7,4,3]$ – a distância mínima é 3 porque a redundância é $3 \geq 2$.

Como

$$H = \left[\begin{array}{ccc|c} & & & 0 \\ & H' & & 0 \\ & & & 0 \\ \hline 1 & \cdots & 1 & 1 \end{array}\right] ,$$

o código C é a extensão por paridade de $\mathrm{Ham}(3,2)$ e, portanto, tem parâmetros $[8,4,d]$ com $3 \leq d \leq 4$. Por ser uma extensão por paridade, a distância mínima de C é par, logo $d = 4$.

(b) Seja $\vec{e_i}$ o vector com a coordenada i igual a 1 e as restantes coordenadas iguais a 0.
Os vectores erro do enunciado desta alínea são $\vec{e_i}$, com $i \in \{1, \dots 8\}$, e $\vec{e_j} + \vec{e_8}$, com $j \in \{1, \dots, 7\}$.
Sejam $c_1, \dots, c_7$ as colunas de H'. Então

$$S(\vec{e_i}) = (c_i, 1) \qquad \text{e}$$
$$S(\vec{e_j} + \vec{e_8}) = (c_j, 1) + (0,0,0,1) = (c_j, 0) .$$

Portanto estes vectores têm sintomas distintos porque as colunas de H' são distintas ($\Rightarrow$ sintomas distintos para erros com o mesmo peso) e a última coordenada dos sintomas é diferente para erros de peso diferente.

Como há $|\mathbb{F}_2^8/C| = 2^{8-k} = 2^4 = 16$ classes $x + C$, este código C corrige no máximo 15 vectores erro (um por cada classe diferente de $\vec{0} + C = C$). Há 8 vectores da forma $\vec{e_i}$ e 7 da forma $\vec{e_j} + \vec{e_8}$, portanto C não pode ser usado para corrigir mais nenhum vector erro, independentemente do peso deste.

(c) Algoritmo de descodificação:
Recebido $y \in \mathbb{F}_2^8$, calcular o sintoma $S(y) = Hy$.
(1º) Se $S(y) = \vec{0}$ então assumimos que não ocorreu nenhum erro e descodificamos y por y.
(2º) Se $S(y)$ é a coluna i de H (em particular, a última coordenada de $S(y)$ é 1), então assumimos que ocorreu um erro na coordenada i e descodificamos y por $y - \vec{e_i}$.

(3º) Se $S(y) = (c, 0)$ com $c \in \mathbb{F}_2^3 \setminus \{\vec{0}\}$, então c é uma coluna de H'. Assumimos que ocorreu um erro na última coordenada e também na coordenada $j \in \{1, \ldots, 7\}$ correspondente à posição de c em H'. Descodificamos y por $y - \vec{e_j} - \vec{e_8}$.

Nota: no 3º passo o vector c é a representação na base dois de j, uma vez que as colunas de H' estão escritas por "ordem crescente".

Nota: não é necessário acrescentar um 4º passo no algoritmo a pedir retransmissão, pois, pela alínea (b), todos os possíveis sintomas já estão incluídos nos outros três passos.

Descodificar $y = 10111011$:

$S(y) = 1000 \Rightarrow$ aplicamos o 3º passo do algoritmo. Como 100 é o número 4 em base 2 (ou $S(y)$ é a 4ª coluna de H'), o vector erro é $\vec{e} = 00010001$ e descodificamos y por $y - \vec{e} = 10101010$.

2. (a) $\vec{x} \in C \Rightarrow \vec{x} \in C^\perp \Rightarrow \vec{x} \cdot \vec{x} = 0 \ , \quad \forall \vec{x} \in C$

   Por outro lado, $\vec{x} \cdot \vec{x} = \sum_i x_i^2 = \sum_i x_i$ pois $1^2 = 1$ e $0^2 = 0$. Donde se conclui que $\mathrm{w}(\vec{x}) \equiv \vec{x} \cdot \vec{x}$ (mod 2). Logo $\mathrm{w}(\vec{x})$ é par para cada $\vec{x} \in C$.

   (b) (i) $C \subseteq C^\perp$ por hipótese.
   Como $\dim C + \dim C^\perp = n$, então $\dim C^\perp = n - \frac{n-1}{2} = \frac{n+1}{2}$, ou seja, $\dim C^\perp = \dim C + 1$, portanto $C^\perp = \langle C, \vec{v} \rangle$ para algum vector $\vec{v} \in C^\perp \setminus C$. Como

$$\begin{aligned}\langle C, \vec{v} \rangle &= \{\vec{x} + \lambda \vec{v} \ : \ \vec{x} \in C, \lambda \in \mathbb{F}_2\} \\ &= \{\vec{x} \ : \ \vec{x} \in C\} \cup \{\vec{x} + \vec{v} \ : \ \vec{x} \in C\} \\ &= C \cup (\vec{v} + C) \ ,\end{aligned}$$

   só falta ver que $\vec{1} \in C^\perp \setminus C$.
   n é ímpar $\Rightarrow \vec{1}$ tem peso n ímpar $\Rightarrow \vec{1} \notin C$ pela alínea (a).
   Seja $\vec{x} \in C$. Ainda pela alínea (a), pois $\mathrm{w}(\vec{x}) \equiv \sum_i x_i$ (mod 2),

$$\vec{1} \cdot \vec{x} = \sum_i x_i = 0 \ , \quad \forall \vec{x} \in C \qquad \Rightarrow \qquad \vec{1} \in C^\perp \ .$$

   (ii) A extensão por paridade de $C^\perp$ é
   $\widehat{C^\perp} = \{(x_1, \ldots, x_n, x_{n+1}) \ : \ (x_1, \ldots, x_n) \in C^\perp, x_{n+1} \equiv \sum_{i=1}^n x_i \text{ (mod 2)}\}$.
   É preciso ver que $\vec{x} \cdot \vec{y} = 0$ para quaisquer $\vec{x}, \vec{y} \in \widehat{C^\perp}$.
   Seja $x' = (x_1, \ldots, x_n) \in C^\perp$. Pela alínea (b)(i), ou $x' \in C$ ou $x' \in \vec{1} + C$. No primeiro caso $\mathrm{w}(x')$ é par (por (a)) e $\vec{x} = (x', 0) \in \widehat{C^\perp}$. No segundo caso $x' = y' + \vec{1}$ com $y' \in C$, logo $\mathrm{w}(x')$ é ímpar e $\vec{x} = (x', 1) = (y' + \vec{1}, 1) = (y', 0) + \vec{1} \in \widehat{C^\perp}$. Portanto qualquer $\vec{x} \in \widehat{C^\perp}$ é da forma $\vec{x} = (x', 0) + \alpha \vec{1}$ com $\alpha \in \mathbb{F}_2$. [Note que este último vector $\vec{1}$ tem comprimento $n+1$.] Logo

$$\begin{aligned}\vec{x} \cdot \vec{y} &= ((x', 0) + \alpha \vec{1}) \cdot ((y', 0) + \beta \vec{1}) \\ &\equiv x' \cdot y' + \alpha \, \mathrm{w}(y') + \beta \, \mathrm{w}(x') + \alpha\beta \, \mathrm{w}(\vec{1}) \text{ (mod 2)} \ ,\end{aligned}$$

   onde $\vec{1} \in \mathbb{F}_2^{n+1}$. Os pesos $\mathrm{w}(y')$ e $\mathrm{w}(x')$ são pares, $x' \cdot y' = 0$ porque C é auto-ortogonal, $\mathrm{w}(\vec{1}) = n + 1$ é par, logo $\vec{x} \cdot \vec{y} = 0$ como queriamos mostrar.

Alternativamente, em vez de justificarmos que qualquer palavra em $\widehat{C^\perp}$ é da forma $\vec{x} = (x', 0) + \alpha\vec{1}$, podiamos calcular os produtos internos $\vec{x} \cdot \vec{y}$ para $\vec{x}, \vec{y} \in \widehat{C^\perp}$, considerando 3 casos: $\vec{x} = (x', 0)$ e $\vec{y} = (y', 0)$ com $x', y' \in C$, ou $\vec{x} = (x', 0)$ e $\vec{y} = (y', 1)$ com $x' \in C$ e $y' \in \vec{1} + C$, ou $\vec{x} = (x', 1)$ e $\vec{y} = (y', 1)$ com $x', y' \in \vec{1} + C$. Dado que o produto interno é simétrico, não é necessário considerar mais nenhum caso.

3. (a) Basta verificar que C' é fechado para a soma de vectores, pois qualquer subconjunto de $\mathbb{F}_2^n$ que contenha o vector nulo é fechado para o produto de vectores por escalres. Como se trata de códigos binários,

$$\mathrm{w}(x + y) = \mathrm{w}(x) + \mathrm{w}(y) - 2\,\mathrm{w}(x \cap y) \ , \qquad (*)$$

portanto, se $x, y \in C'$ então $\mathrm{w}(x)$ e $\mathrm{w}(y)$ são números pares e, por (*), $\mathrm{w}(x + y)$ é par. Como $x + y \in C$ porque C é linear, então $x + y \in C'$.

(b) Seja $P : C \to \mathbb{F}_2$ a aplicação definida por $P(x) = \mathrm{w}(x) \pmod 2$. Então

- P é uma transformação linear sobre $\mathbb{F}_2$, pois $\mathrm{w}(x+y) \equiv \mathrm{w}(x) + \mathrm{w}(y) \pmod 2$ por (*),
- $C' = \mathcal{N}(P)$ por definição de C',
- A imagem de P é $\mathcal{I}(P) = \mathbb{F}_2$, pois $\mathrm{d}(C) = 2t + 1$ é ímpar, logo existe $c \in C$ tal que $\mathrm{w}(c) = 2t + 1 \equiv 1 \pmod 2$.

Como

$$\dim \mathcal{N}(P) + \dim \mathcal{I}(P) = \dim C$$

então $\dim C' = \dim C - 1 = k - 1$.

4. Seja $c(t) = 1+2t+2t^2+2t^3+t^4$. Seja $g(t)$ o polinómio gerador do menor código ternário cíclico, de comprimento 8, que contém $c(t)$. Então $g(t) \in \mathbb{F}_3[t]$ é mónico e é um divisor de $t^8 - 1$, porque é um polinómio gerador. Por outro lado, $c(t) \in \langle g(t) \rangle$ sse $g(t) | c(t)$ no quociente $R_8 = \mathbb{F}_3[t]/\langle t^8 - 1 \rangle$. Mas como $g(t)$ divide $t^8 - 1$ (em $\mathbb{F}_3[t]$), a condição $g(t)|c(t)$ em R_8 é equivalente a $g(t)|c(t)$ em $\mathbb{F}_3[t]$. Logo $g(t) | \operatorname{MDC}(t^8 - 1, c(t))$.

Como $|C| = 3^{\dim C}$ e $\dim C = n - \operatorname{grau}(g(t))$, o menor código C corresponde ao maior grau possível de $g(t)$. Portanto $g(t) = \operatorname{MDC}(t^9 - 1, c(t))$.

Cálculo do máximo divisor comum:

Comecemos por verificar se as raízes de $t^9 - 1$ são também raízes de c(t).

$$c(1) = 2 \neq 0 \Rightarrow t - 1 \not| c(t)$$
$$c(-1) = 0 \Rightarrow t + 1 \,|\, c(t)$$

Calculando o quociente de $c(t)$ por $t + 1$ obtém-se $c(t) = (t + 1)(1 + t + t^2 + t^3)$. É fácil de ver que -1 é uma raíz de $1 + t + t^2 + t^3$ e, fazendo a divisão por $t + 1$, obtém-se $1 + t + t^2 + t^3 = (t + 1)(t^2 + 1)$. Como $t^2 + 1$ é irredutível em $\mathbb{F}_3[t]$, porque tem grau 2 e não possui raízes em $\mathbb{F}_3$, conclui-se que a factorização de $c(t)$ em termos irredutíveis é $c(t) = (t + 1)^2(t^2 + 1)$ e, portanto,

$$g(t) = \operatorname{MDC}(t^9 - 1, c(t)) = (t + 1)(t^2 + 1) \ .$$

Nota: Nas duas divisões de polinómios efectuadas neste exercício podemos aplicar a Regra de Rufini, pois o polinómio divisor em ambos os casos é $t+1$.

5. (a) Um elemento primitivo em $\mathbb{F}_7$ tem ordem 6. A ordem de qualquer elemento em $\mathbb{F}_7 \setminus \{0\}$ é um divisor de 6.

$$\begin{aligned} 3 \neq 1 \Rightarrow &\text{ a ordem de } 3 \text{ não é 1.} \\ 3^2 = 2 \neq 1 \Rightarrow &\text{ a ordem de } 3 \text{ não é 2.} \\ 3^3 = 6 \neq 1 \Rightarrow &\text{ a ordem de } 3 \text{ não é 3.} \end{aligned}$$

Portanto a ordem de 3 é 6 e concluímos que $3 \in \mathbb{F}_7$ é primitivo.

(b) C é um código Reed-Solomon com $\delta = \mathrm{grau}(g(t)) + 1 = 5$.
O comprimento é $n = q - 1 = 6$.
A dimensão é $k = n - \mathrm{grau}(g(t)) = 2$ (ou $k = q - \delta$).
A distância mínima é $\delta = 5$ porque qualquer código Reed Solomon é MDS.

(c) $T = \left\lfloor \dfrac{\mathrm{d}(C) - 1}{2} \right\rfloor$=2.
Como $y(t) = 1 + 2t^3 + 3t^4$ e $g(t)$ têm o mesmo grau, o resto da divisão de $y(t)$ por $g(t)$ é $y(t) - 3g(t) = 3 + t + 5t^2 + 5t^3$.
$S(y(t))$ = resto da divisão tem peso $4 \geq T$
$S(ty(t)) = tSy(t) - 5g(t) = tS(y(t)) + 2g(t) = 1 + 3t^3$ tem peso $2 \leq T \Rightarrow$ descodificamos $y(t)$ por

$$\begin{aligned} x(t) &= y(t) - t^{n-1} S(ty(t)) \\ &= y(t) - t^5(1 + 3t^3) \equiv 1 + 4t^2 + 2t^3 + 3t^4 + 6t^5 \pmod{t^6 - 1} , \end{aligned}$$

ou seja, descodificamos y por $x = (1, 0, 4, 2, 3, 6)$.

(d) O Algoritmo Caça ao Erro corrige qualquer erro de peso menor ou igual a $T = 2$ contendo uma sequência de $k = 2$ zeros.
Qualquer erro de peso 2 é uma permutação cíclica de um vector com a primeira coordenada não nula, portanto é uma permutação cíclica de um dos seguintes vectores:

$$(\alpha, \beta, 0, 0, 0, 0) , \qquad (\alpha, 0, \beta, 0, 0, 0) \qquad \text{ou} \qquad (\alpha, 0, 0\beta, 0, 0) ,$$

com $\alpha, \beta \in \mathbb{F}_7 \setminus \{0\}$. Todos contêm uma sequência de dois zeros, portanto o Algoritmo Caça ao Erro corrige todos os erros de peso 2. A percentagem pedia é 100%.

6. (a) C é um código cíclico $\Rightarrow$ o entrelaçado $C^{(s)}$ também é cíclico.
As palavras de C são da forma $\alpha(1, \ldots, 1) = (\alpha, \ldots, \alpha)$ com $\alpha \in \mathbb{F}_q$. Sejam $\vec{x}_1 = (\alpha_1, \ldots, \alpha_1)$, $\vec{x}_2 = (\alpha_2, \ldots, \alpha_2)$, ..., $\vec{x}_s = (\alpha_s, \ldots, \alpha_s)$ s palavras em C. Então

$$\vec{x}^{(s)} = (\alpha_1, \alpha_2, \ldots, \alpha_s, \alpha_1, \alpha_2, \ldots, \alpha_s, \ldots, \alpha_1, \alpha_2, \ldots, \alpha_s) \in \mathbb{F}_q^{ns}$$

é uma palavra arbitrária em $C^{(s)}$, por definição de entrelaçamento. Portanto $\vec{x}^{(s)} = c'c' \ldots c'$ onde $c' = (\alpha_1, \alpha_2, \ldots, \alpha_s) \in \mathbb{F}_q^s$ é repetida n vezes. Conclui-se que $C^{(s)}$ é um código degenerado com $r = s$.

(b) Seja $c = c'c' \cdots c' \in C$ a palavra de código correspondente ao polinómio gerador $g(t)$ de C, onde c' tem comprimento r. Seja $a(t)$ o polinómio correspondente a c'. A palavra c também se pode escrever na forma

$$c = (c', 0, \ldots, 0) + (0, c', 0, \ldots, 0) + (0, 0, c', 0, \ldots, 0) + \cdots + (0, \ldots, 0, c') \ ,$$

onde 0 denota o vector nulo de comprimento r. Como o segundo vector na decomposição acima é o desvio cíclico iterado r vezes do primeiro, o terceiro é o desvio cíclico iterado $2r$ vezes do primeiro, etc, passando para notação polinomial fica

$$\begin{aligned} g(t) &= a(t) + t^r a(t) + t^{2r} a(t) + \cdots + t^{n-r} a(t) \\ &= a(t)(1 + t^r + t^{2r} + \cdots + t^{n-r}) \ . \end{aligned}$$

(c) ($\Rightarrow$) O inteiro r é o que se obtém da definição de código degenerado, portanto r divide n. Seja $l = n/r$. Pela alínea (b), o polinómio gerador de C é da forma $g(t) = a(t)(1 + t^r + t^{2r} + \cdots + t^{n-r})$. Então

$$t^n - 1 = h(t)g(t) = h(t)a(t)(1 + t^r + t^{2r} + \cdots + t^{n-r}) \ .$$

Por outro lado

$$\begin{aligned} t^n - 1 = (t^r)^l - 1 &= (t^r - 1)(1 + t^r + (t^r)^2 + \cdots + (t^r)^{l-1}) \\ &= (t^r - 1)(1 + t^r + t^{2r} + \cdots + t^{n-r}) \ . \end{aligned} \qquad (**)$$

Comparando as duas factorizações de $t^n - 1$ conclui-se que $h(t)a(t) = t^r - 1$, ou seja, $h(t)$ divide $t^r - 1$.

($\Leftarrow$) Como $h(t)$ divide $t^r - 1$, existe um polinómio $a(t)$ de grau menor do que r tal que $h(t)a(t) = t^r - 1$.
Usando a factorização (**), fica

$$h(t)a(t) = \frac{t^n - 1}{1 + t^r + t^{2r} + \cdots + t^{(l-1)r}} \ ,$$

onde $l = n/r \in \mathbb{N}$ (r divide n por hipótese). Portanto o polinónio gerador é

$$g(t) = \frac{t^n - 1}{h(t)} = a(t)(1 + t^r + t^{2r} + \cdots + t^{(l-1)r}) \ .$$

Só falta mostrar que $\langle g(t) \rangle$ é um código degenerado.
Como $\mathrm{grau}(a(t)) < r$, os polinómios $a(t)$, $t^r a(t)$, $t^{2r} a(t)$, ..., $t^{(l-1)r} a(t)$ não têm termos em comum, o vector correspondente a $g(t)$ é $(c', c', \ldots, c')$ onde c' é a sequência de comprimento r correspondente ao polinómio $a(t)$. Também se verifica a seguinte correspondência

$$\begin{aligned} &\lambda g(t) \text{ é da forma } (\lambda c', \lambda c', \ldots, \lambda c') \ , \quad \forall \lambda \in \mathbb{F}_q \\ &t^i g(t) \text{ é da forma } (\sigma^i(c'), \sigma^i(c'), \ldots, \sigma^i(c')) \ , \quad \forall i \in \mathbb{N} \end{aligned}$$

onde $\sigma^i(c')$ denota o desvio cíclico iterado i vezes de c'. Portanto $f(t)g(t)$ é da forma $(c'', c'', \ldots, c'')$ para qualquer polinómio $f(t)$, donde se conclui que $\langle g(t) \rangle$ é um código degenerado.