Combinatória e Teoria de Códigos
2º Teste/1º Exame
18 de Junho de 2010

RESOLUÇÃO

1. (a) Como H tem 10 colunas e 3 linhas, $n = 10$ e $k = 10 - 3 = 7$.
Quaisquer três colunas i, j, k de H formam uma matriz de Vandermonde

$$V_{ijk} = \begin{bmatrix} 1 & 1 & 1 \\ i & j & k \\ i^2 & j^2 & k^2 \end{bmatrix} ,$$

cujo determinante é $\det(V_{ijk}) = (i-j)(i-k)(j-k)$. Se as colunas forem distintas, as entradas da segunda linha de V_{ijk} são distintas e portanto $\det(V_{ijk}) \neq 0$, ou seja, as colunas i, j, k de H são linearmente independentes. Logo $\mathrm{d}(C) \geq 4$. Por outro lado, como H tem 3 linhas, quaisquer 4 colunas são linearmente dependentes (bastava existirem apenas 4 colunas linearmente dependentes), portanto $\mathrm{d}(C) \leq 4$. Conclusão: $d = \mathrm{d}(C) = 4$.

(b) Erros simples são vectores do tipo

$$\vec{e_1} = (0, \ldots, 0, a, 0, \ldots, 0)$$

com $a \in \mathbb{F}_{11} \setminus \{0\}$ na coordenada i.
Se $x = (x_1, \ldots, x_{10}) \in C$ é a palavra enviada e ocorre um erro de transposição adjacente, então $y = (x_1, \ldots, x_{i-1}, x_{i+1}, x_i, x_{i+2}, \ldots, x_{10})$ é a palavra recebida, i.e., as duas coordenadas consecutivas x_i e x_{i+1} de $x \in C$ foram trocadas. Portanto o erro ocorrido foi $y - x = (0, \ldots, 0, x_{i+1} - x_i, x_i - x_{i+1}, 0, \ldots, 0)$ com entradas não nulas nas coordendas i e $i + 1$. Ou seja, ocorreu um erro do tipo

$$\vec{e_2} = (0, \ldots, 0, -a, a, 0, \ldots, 0)$$

com $a \in \mathbb{F}_{11} \setminus \{0\}$.
O código C corrige todos os erros simples e de transposição adjacentes sse todos os vectores do tipo $\vec{e_1}$ e do tipo $\vec{e_2}$ tiverem sintomas distintos.
Cálculo dos sintomas:

$$S(\vec{e_1}) = H\vec{e_1} = (a, ia, i^2a) \quad (1)$$
$$S(\vec{e_2}) = H\vec{e_2} = (0, a, (2i+1)a) \quad (2)$$

Como a é invertível em $\mathbb{F}_{11}$, $(a, ia, i^2a) = (b, jb, j^2b)$ sse $a = b$ e $i = j$, portanto os sintomas do tipo (1) são distintos entre si. (Também se podia ter concluído que os sintomas dos erros simples são todos distintos porque $T = \lfloor (\mathrm{d}(C) - 1)/2 \rfloor = 1$.)

Analogamente, como a é invertível em $\mathbb{F}_{11}$, $(0, a, (2i+1)a) = (0, b, (2j+1)b)$ sse $a = b$ e $2i + 1 = 2j + 1$ sse $a = b$ e $i = j$ (pois 2 também é invertível em $\mathbb{F}_{11}$). Portanto os sintomas do tipo (2) são distintos entre si.

Claramente qualquer sintoma de tipo (1) não pode ser igual a um de tipo (2), basta olhar para a primeira coordenada.

(c) Recebido $y \in \mathbb{F}_{11}^{10}$, calcular o sintoma $S(y) = Hy$.

(1º) Se $S(y) = (0, 0, 0)$ então assumimos que não ocorreu nenhum erro e descodificamos y por y.

(2º) Se $S(y) = (s_1, s_2, s_3)$ com $s_i \neq 0$ para $i = 1, 2, 3$, então assumimos que ocorreu um erro simples de amplitude $s_1 \neq 0$ na posição $i = s_2 s_1^{-1} \in \{1, 2, \ldots, 10\}$ e descodificamos y por

$$y - (0, \ldots, 0, s_1, 0, \ldots, 0) \qquad \text{com } s_1 \text{ na coordenada } i.$$

(3º) Se $S(y) = (0, s_2, s_3)$ com s_2 e s_3 não nulos, então assumimos que ocorreu um erro de transposição adjacente com vector erro

$$\vec{e} = (0, \ldots, 0, -s_2, s_2, 0, \ldots, 0)$$

de coordenadas i e $i+1$ não nulas, onde $i = (s_2^{-1} s_3 - 1) \times 2^{-1}$ é calculado módulo 11. Decodificamos y por $y - \vec{e}$.

(4º) Caso não se verifique nenhuma das condições dos primeiros três passos, pedimos retransmissão.

(d) $Sy = (5, 2, 3) \Rightarrow$ aplicamos o 2º passo do algoritmo. Ocorreu um erro simples na posição $2 \times 5^{-1} \equiv 2 \times 9 \equiv 7 \pmod{11}$ de amplitude 5. O vector y é descodificado por

$$y - 0000005000 = 0204006910 \ .$$

$Sz = (0, X, 9) \Rightarrow$ aplicamos o 3º passo do algoritmo. O vector erro é $\vec{e} = (0, \ldots, 0, -X, X, 0, \ldots, 0)$ com $-X = 1$ na coordenada $(X^{-1}9 - 1) \times 2^{-1} \equiv -X \times 2^{-1} \equiv -5 \equiv 6 \pmod{11}$. O vector z é descodificado por

$$x = z - \vec{e} = 100000X308 - 000001X000 = 10000X0308 \ .$$

(Note que de facto x é obtido de z trocando as coordenadas z_6 e z_7.)

2. (a) O comprimento de C é $3n$, directamente pela definição.

Linearidade:

Como $C \subseteq F_q^{3n}$, para ver que C é um código linear, basta verificar o fecho da soma de vectores e do produto de um vector por um escalar.

Sejam $a, a', b, b' \in C_1$, $x, x' \in C_2$ e $\lambda \in \mathbb{F}_q$.

$$\begin{aligned}&(a+x, b+x, a+b+x) + (a'+x', b'+x', a'+b'+x') = \\ &\quad = ((a+a')+(x+x'), (b+b')+(x+x'), (a+a')+(b+b')+(x+x')) \quad (*)\end{aligned}$$

Como $a+a' \in C_1$, $b+b' \in C_1$ e $x+x' \in C_2$ porque C_1 e C_2 são códigos lineares, então o vector (*) pertence a C.
Analogamente, como $\lambda a \in C_1$, $\lambda b \in C_1$ e $\lambda x \in C_2$, então

$$\lambda(a+x, b+x, a+b+x) = (\lambda a + \lambda x, \lambda b + \lambda x, \lambda a + \lambda b + \lambda x) \in C \ .$$

Dimensão:
Dados dois vectores $(a+x, b+x, a+b+x)$ e $(a'+x', b'+x', a'+b'+x')$ em C, então $(a+x, b+x, a+b+x) = (a'+x', b'+x', a'+b'+x')$ sse

$$\begin{cases} a+x = a'+x' \\ b+x = b'+x' \\ a+b+x = a'+b'+x' \end{cases} \Leftrightarrow \begin{cases} a+x = a'+x' \\ b+x = b'+x' \\ a = a' \end{cases} \Leftrightarrow \begin{cases} x = x' \\ b = b' \\ a = a' \end{cases}$$

Ou seja, escolhas diferentes de $a, b \in C_1$ e de $x \in C_2$ dão palavras diferentes em C. Portanto C contém $|C_1| \cdot |C_1| \cdot |C_2| = q^{2k_1+k_1}$ palavras e

$$\dim(C) = \log_q |C| = 2k_1 + k_2 \ .$$

(b) Qualquer palavra do código C é da forma $(a,0,a)+(0,b,b)+(x,x,x)$ com $a, b \in C_1$ e $x \in C_2$. Seja

$$G = \begin{bmatrix} G_1 & 0 & G_1 \\ 0 & G_1 & G_1 \\ G_2 & G_2 & G_2 \end{bmatrix} \ .$$

As primeiras k_1 linhas de G geram os vectores $(a,0,a)$ com $a \in C_1$. As segundas k_1 linhas de G geram os vectores $(0,b,b)$ com $b \in C_1$. As últimas k_2 linhas de G geram os vectores (x,x,x) com $x \in C_2$. Portanto as linhas de G formam um conjunto gerador de C. Como já vimos que $\dim(C) = 2k_1 + k_2$, que é precisamente o número de linhas de G, então estas formam uma base de C e, podemos concluir que G é uma matriz geradora do código C.

3. (a) O polinómio gerador $g(t)$ de um tal código tem de ser mónico e um divisor de $t^9 - 1$. Logo $g(t) = (1+t)^i(1+t+t^2)^j(1+t^3+t^6)^k$ com $i, j, k \in \{0,1\}$, logo há $2^3 = 8$ códigos cíclicos binários de comprimento 9.

(b) Como o grau do polinómio gerador $g(t)$ é $n-k=7$ e $g(t)$ divide t^9-1 então $g(t)=(t+1)(1+t^3+t^6)=1+t+t^3+t^4+t^6+t^7$ e

$$G=\begin{bmatrix}1&1&0&1&1&0&1&1&0\\0&1&1&0&1&1&0&1&1\end{bmatrix}$$

é uma matriz geradora. (A primeira linha de G é $\begin{bmatrix}g_0 & g_1 & \cdots & g_7 & 0\end{bmatrix}$.)

(c) O polinómio de paridade é $h(t)=\dfrac{t^9-1}{g(t)}=1+t+t^2$, portanto

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

é uma matriz de paridade. (A primeira linha de H é $\begin{bmatrix}h_2 & h_1 & h_0 & 0 & \cdots & 0\end{bmatrix}$.)

(d) Seja C' o subcódigo de $C^\perp$ formado pelas palavras de $C^\perp$ de peso par.
$\bar{h}(t)=h_0^{-1}t^2h(t^{-1})=h(t)\Rightarrow C^\perp=\langle 1+t+t^2\rangle$.
$x(t)$ tem peso par sse $x(1)\equiv 0 \pmod 2$ sse $t+1$ divide $x(t)$. Logo

$$C'=\langle (1+t)(1+t+t^2)\rangle\ .$$

Como $g'(t)=(1+t)(1+t+t^2)$ divide t^9-1 (e é mónico), então $g'(t)$ é de facto o polinómio gerador de C' e, portanto, C' contém $2^6=64$ palavras, pois $\dim(C')=n-\text{grau}(g'(t))=9-3=6$.

Outra resolução:

A matriz geradora de C da alínea (b) é uma matriz de paridade de $C^\perp$.

$x\in\mathbb{F}_2^9$ tem peso par se e só se $\displaystyle\sum_{i=1}^{9}x_1\equiv 0 \pmod 2$.

Portanto o subcódigo C' das palavras de peso par de $C^\perp$ é o núcleo da matriz

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

Como as linhas de H' são linearmente independentes (porquê?), então H' é uma matriz de paridade para C' e $r=3$ é a redundância de C', portanto $C^\perp$ contém $2^{n-r}=2^6=64$ palavras de peso par.

4. (a) C é um código Reed-Solomon com $\delta = \mathrm{grau}(g(t)) + 1 = 5$.
   O comprimento é $n = q - 1 = 7$.
   A dimensão é $k = n - \mathrm{grau}(g(t)) = 3$ (ou $k = q - \delta$).
   A distância mínima é $\delta = 5$ porque qualquer código Reed Solomon é MDS.

   (b) $T = \left\lfloor \frac{\mathrm{d}(C) - 1}{2} \right\rfloor$=2.
   Como o grau de $y(t) = t + \alpha^2 t^3$ é estritamente menor que o grau de $g(t)$, o resto da divisão de $y(t)$ por $g(t)$ é o próprio $y(t)$. Logo $S(y(t)) = y(t)$ tem peso $2 \leq T$, logo o vector erro é $y(t)$ e descodificamos y pelo vector nulo.

   Aplicando o algoritmo de divisão para polinómios obtém-se

$$z(t) = (\alpha^2 + \alpha t + t^2)g(t) + \alpha^5 + \alpha^4 t + \alpha^3 t^2 + \alpha^4 t^3 \ ,$$

   portanto $S(z(t)) = \alpha^5 + \alpha^4 t + \alpha^3 t^2 + \alpha^4 t^3$ tem peso $4 > T$.
   $S(tz(t)) = tS(z(t) - \alpha^4 g(t) = 1 + \alpha t^3$ tem peso $2 \leq T$, portanto o vector erro é $t^{n-1} S(tz(t)) = t^6 + \alpha t^9 \equiv \alpha t^2 + t^6$ (mod $t^7 - 1$) e descodificamos z por

$$z - (0, 0, \alpha, 0, 0, 0, 1) = (0, \alpha^3, \alpha, 1, \alpha^3, 1, 0) \ .$$

   (c) C é um código Reed Solomon portanto C^* corrige todos os erros acumulados de comprimento até $m(T-1) + 1 = 3(2-1) + 1 = 4$, onde $m = 3$ é a dimensão de $\mathbb{F}_8$ sobre $\mathbb{F}_2$.
   C tem parâmetros $[7, 3, 5]_8$, $\mathbb{F}_2^3$ tem parâmetros $[3, 3, 1]_2$, portanto a concatenação tem parâmetros $[7 \times 3, 3 \times 3]_2 = [21, 9]_2$. Aplicando a Estimativa de Reiger, concluímos que C^* corrige no máximo erros-l acumulados com $l \leq \left\lfloor \frac{n-k}{2} \right\rfloor = \left\lfloor \frac{21-9}{2} \right\rfloor = 6$.

5. Ver as notas das aulas.