Combinatória e Teoria de Códigos
1º Teste
11 de Abril de 2013

RESOLUÇÃO

1. (a) Seja $p_i : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ a aplicação (obviamente linear) projecção na coordenada i e seja $p_{i|_C} : C \longrightarrow \mathbb{F}_q$ a restrição a C. Como C é um espaço vectorial e $p_{i|_C}$ é linear, então o núcleo $\mathcal{N}(p_{i|_C}) = C_{0,i}$ é um subespaço vectorial de C, i.e., $C_{0,i}$ é um código linear.

   Se $p_{i|_C} \equiv 0$, então $C_{0,i} = C$ e $\dim C_{0,i} = k$.

   Se $p_{i|_C} \not\equiv 0$, então $p_i|_C$ é sobrejectiva e, da igualdade

$$\dim C = \dim \mathcal{N}(p_{i|_C}) + \dim \mathcal{I}(p_{i|_C}) \ ,$$

   obtém-se que $\dim C_{0,i} = k - 1$.

   (b) Para cada i fixo, os conjuntos $C_{a,i}$, com $a \in \mathbb{F}_q$, formam uma partição de C.

   Caso 1: Se $C = C_{0,i}$, então $C_{a,i} = \varnothing$ para qualquer $a \neq 0$. Portanto $|C_{0,i}| = q^k$ e $|C_{a,i}| = 0$, para $a \neq 0$.

   Caso 2: Se $C \neq C_{0,i}$, então $|C_{0,i}| = q^{\dim C_{0,i}} = q^{k-1}$. Neste caso sabemos que existe $b \in \mathbb{F}_q \setminus \{0\}$ tal que $C_{b,i} \neq \varnothing$, i.e., existe $\vec{x}_b \in C_{b,i}$. Como $a = ab^{-1}b$, para todo o $a \in \mathbb{F}_q$, então $\vec{x}_a = ab^{-1}\vec{x}_b \in C_{a,i}$, donde $C_{a,i} \neq \varnothing$. Por outro lado, $C_{a,i}$ é o conjunto das soluções $x \in C$ da equação linear (não homogénea) $x_i = a$. Como este conjunto é não vazio, então $C_{a,i} = \vec{x}_a + C_{0,i}$, pois todas as soluções são da forma $\vec{x}_a + \vec{v}$ com $\vec{v} \in C_{0,i}$. Ou, equivalentemente, a aplicação

$$\begin{aligned} C_{0,i} &\longrightarrow C_{a,i} \\ \vec{v} &\longmapsto \vec{x}_a + \vec{v} \end{aligned}$$

   é bijectiva. Portanto $|C_{a,i}| = |C_{0,i}| = q^{k-1}$ para todo o $a \in \mathbb{F}_q$.

   (c) Por definição $C' = C \setminus \left(\bigcup_{i=1}^{6} C_{1,i} \right)$.

   C é um código $[6,5]$ sobre $\mathbb{F}_7$ e $C \neq C_{0,i}$ para todo o $i \in \{1, \ldots, 6\}$, portanto $|C_{1,i}| = 7^{k-1} = 7^4$.

   $C_{1,i} \cap C_{1,j} = \{x \in C \,:\, x_i = x_j = 1\}$ é o conjunto das soluções do sistema linear

$$\begin{cases} Hx = 0 \\ x_i = 1 \\ x_j = 1 \end{cases}$$

   que tem $n - 3 = k - 2$ variáveis livres, se $i \neq j$, portanto $|C_{1,i} \cap C_{1,j}| = 7^{k-2} = 7^3$.

   Analogamente, $|C_{1,i_1} \cap \cdots \cap C_{1,i_l}| = 7^{k-l} = 7^{5-l}$, para $1 \leq l \leq 5$, se os l conjuntos C_{1,i_j} forem distintos entre si.

   Por último, $C_{1,1} \cap \cdots \cap C_{1,6} = \{x \in C \,:\, x_1 = \cdots = x_6 = 1\} = \{\vec{1}\}$ ou $\varnothing$. Mas como $H\vec{1} = 0$, então $\vec{1} \in C$ e $|C_{1,1} \cap \cdots \cap C_{1,6}| = 1$.

Aplicando o Princípio de Inclusão-Exclusão, e simplificando as contas, obtém-se

$$
\begin{aligned}
|C'| &= |C| - \sum_{i=1}^{6} |C_{1,i}| + \sum_{i<j} |C_{1,i} \cap C_{1,j}| + \cdots + (-1)^6 |C_{1,1} \cap \cdots \cap C_{1,6}| \\
&= 7^5 + \sum_{l=1}^{5} (-1)^l \tbinom{6}{l} 7^{5-l} + 1 = \sum_{l=0}^{5} (-1)^l \tbinom{6}{l} 7^{5-l} + 1 = \frac{1}{7} \sum_{l=0}^{5} \tbinom{6}{l} (-1)^l 7^{6-l} + 1 \\
&= \frac{1}{7}\big((-1+7)^6 - 1\big) + 1 = \frac{6^6 - 1}{7} + 1 = 6666 \ .
\end{aligned}
$$

2. (a) Directamente da definição de C: $n = 5$ e $k = 1$. Seja $\vec{u} = (1, \alpha, \alpha^2, 1, \alpha^2)$. Então $C = \{a\vec{u} \ : \ a \in \mathbb{F}_4\}$ e a distância mínima de C é $d(C) = \mathrm{w}(C) = 5$, porque $\mathrm{w}(a\vec{u}) = \mathrm{w}(\vec{u}) = 5$, para todo o $a \in \mathbb{F}_4 \setminus \{0\}$. Portanto C é um código $[5, 1, 5]_4$.
Como $G = \begin{bmatrix} 1 & \alpha & \alpha^2 & 1 & \alpha^2 \end{bmatrix}$ é uma matriz geradora de C na forma canónica, i.e., na forma $\begin{bmatrix} I_1 & A \end{bmatrix}$, então

$$
H = \begin{bmatrix} -A^T & | & I_4 \end{bmatrix} = \begin{bmatrix} \alpha & 1 & & & \\ \alpha^2 & & 1 & & \\ 1 & & & 1 & \\ \alpha^2 & & & & 1 \end{bmatrix}
$$

é uma matriz de paridade para o código C.

(b) Sim. A equivalência pode ser obtida aplicando a operação (ii) da definição com $\lambda_1 = 1$, $\lambda_2 = \alpha^{-1} = \alpha^2$, $\lambda_3 = \alpha^{-2} = \alpha$, $\lambda_4 = 1$ e $\lambda_5 = \alpha$, i.e.,

$$
\begin{aligned}
C &\xrightarrow{\cong} \langle \vec{1} \rangle \\
(x_1, x_2, x_3, x_4, x_5) &\longmapsto (x_1, \alpha^2 x_2, \alpha x_3, x_4, \alpha x_5) \ .
\end{aligned}
$$

(c) C é um espaço vectorial sobre $\mathbb{F}_4$ e $\mathbb{F}_2$ é um subcorpo de $\mathbb{F}_4$, por isso C satisfaz a restrição a $\mathbb{F}_2$ dos axiomas de espaço vectorial sobre $\mathbb{F}_4$.
$\{\vec{u}\}$ é uma base de C sobre $\mathbb{F}_4$, $\{1, \alpha\}$ é uma base de $\mathbb{F}_4$ sobre $\mathbb{F}_2$, donde $\{\vec{u}, \alpha\vec{u}\} = \{(1, \alpha, \alpha^2, 1, \alpha^2), (\alpha, \alpha^2, 1, \alpha, 1)\}$ é uma base de C sobre $\mathbb{F}_2$.

(d) Seja $x = (x_1, x_2, x_3, x_4, x_5) \in \mathbb{F}_2^5 \subset \mathbb{F}_4^5$.

$$
\begin{aligned}
x \in C^\perp &\iff x \cdot \vec{u} = 0 \iff x_1 + \alpha x_2 + (1+\alpha) x_3 + x_4 + (1+\alpha) x_5 = 0 \\
&\iff (x_1 + x_3 + x_4 + x_5) 1 + (x_2 + x_3 + x_5) \alpha = 0
\end{aligned}
$$

Como $\{1, \alpha\}$ é uma base de $\mathbb{F}_4$ sobre $\mathbb{F}_2$ e ambos os coeficiente $x_1 + x_3 + x_4 + x_5$ e $x_2 + x_3 + x_5$ estão em $\mathbb{F}_2$, a última igualdade implica que

$$
\begin{cases} x_1 + x_3 + x_4 + x_5 = 0 \\ x_2 + x_3 + x_5 = 0 \end{cases}
$$

ou seja, $x_1 = x_3 + x_4 + x_5$ e $x_2 = x_3 + x_5$, donde se conclui que

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

é uma matriz geradora de $C^\perp|_{\mathbb{F}_2}$. (Note que as linhas de G são de facto linearmente independentes pois as 3 últimas colunas formam a matriz identidade 3×3, isto porque x_3, x_4 e x_5 foram escolhidas como variáveis livres do sistema.)

3. O código linear $C \subset \mathbb{F}_2^4$ é auto-dual se e só se $C = C^\perp$, portanto $\dim C = 2$, porque $\dim C + \dim C^\perp = 4$, donde $|C| = 2^2 = 4$ e podemos escrever $C = \{\vec{0}, \vec{u}, \vec{v}, \vec{u}+\vec{v}\}$.

   Por outro lado, $x \cdot x = 0$ para qualquer $x \in C = C^\perp$, portanto $\mathrm{w}(x) \equiv \sum_i x_i = x \cdot x = 0 \mod 2$, ou seja $\mathrm{w}(x)$ é par. (Claro que $\vec{0}$ e $\vec{1}$ são os únicos vectores em $\mathbb{F}_2^4$ de peso 0 e 4, respectivamente.)

   Caso 1: Se $\vec{1} \in C$, então $C = \{\vec{0}, \vec{1}, \vec{v}, \vec{1}+\vec{v}\}$ com $\mathrm{w}(\vec{v}) = 2$. Note que o vector $\vec{1}+\vec{v}$ é o "complementar" de $\vec{v}$, i.e., a coordenada i de $\vec{1}+\vec{v}$ é 1 se e só se $v_i = 0$, portanto $\mathrm{w}(\vec{1}+\vec{v}) = 4 - \mathrm{w}(\vec{v}) = 2$. E como $\mathbb{F}_2^4$ contém $\binom{4}{2} = 6$ palavras de peso 2, há precisamente três pares $\{\vec{v}, \vec{1}+\vec{v}\}$ distintos. Conclusão: neste caso há três códigos auto-duais

$$\langle 1100, 0011 \rangle \quad , \qquad \langle 1010, 0101 \rangle \quad \text{e} \qquad \langle 1001, 0110 \rangle \ .$$

   Caso 2: Se $\vec{1} \notin C$, então $\vec{u}$, $\vec{v}$ e $\vec{u}+\vec{v}$ têm peso 2. A fórmula

$$\mathrm{w}(\vec{u}+\vec{v}) = \mathrm{w}(\vec{u}) + \mathrm{w}(\vec{v}) - 2\,\mathrm{w}(\vec{u} \cap \vec{v})$$

   implica que $\mathrm{w}(\vec{u} \cap \vec{v}) = 1$. Por outro lado, como

$$\mathrm{w}(\vec{u} \cap \vec{v}) \equiv \sum_{i=1}^{n} u_i v_i = \vec{u} \cdot \vec{v} = 0 \mod 2 \ ,$$

   obtemos uma contradição, portanto este segundo caso nunca ocorre e os únicos códigos binários auto-duais são os determinados no caso 1.

4. (a) $n =$ (número de colunas de H) $= 7$; $n - k =$ (número de linhas de H) $= 3$, logo $k = 4$.
   Quanto à distância mínima d: nehuma das colunas de H é nula, donde $d \geq 2$. Por outro lado, a primeira e terceira colunas de H são iguais, donde $d \leq 2$.
   Conclusão: C é um código $[7, 4, 2]$.

   (b) Seja $\vec{e}_i$ o vector erro do enunciado com $\mathrm{w}(\vec{e}_i) = i$. Os sintomas destes vectores são

$$\begin{aligned} &H\vec{e}_1 = 001 \ , \quad H\vec{e}_2 = 010 \ , \quad H\vec{e}_3 = 011 \ , \quad H\vec{e}_4 = 100 \ , \\ &H\vec{e}_5 = 101 \ , \quad H\vec{e}_6 = 110 \ , \quad H\vec{e}_7 = 111 \ . \end{aligned}$$

   Portanto os sintomas são todos distintos entre si e nenhum é 000, ou seja, os sete vectores $\vec{e}_i$ pertencem a classes $a + C$ distintas e nenhum é uma palavra do código C. Logo o código C pode ser usado para corrigir estes sete erros.

   Descodificar $y = 0011111$ e $z = 0100011$:

$$\begin{aligned} Hy = 101 = H\vec{e}_5 \quad &\Longrightarrow \quad \text{descodificar } y \text{ por } y - \vec{e}_5 = 1100011 \ ; \\ Hz = 001 = H\vec{e}_1 \quad &\Longrightarrow \quad \text{descodificar } z \text{ por } z - \vec{e}_1 = 1100011 \ . \end{aligned}$$

   (c) O número de classes $a + C$ é $|\mathbb{F}_2^n|/|C| = 2^{n-k} = 8$, portanto C corrige no máximo sete erros simultaneamente (note que uma das classes é $\vec{0} + C = C$) e não é possível corrigir mais erros que os da alínea anterior.