Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Ejercicios y Problemas resueltos

Tema 2: NOCIONES BÁSICAS DE LA TEORÍA DE CÓDIGOS

Mayo de 2017

Ejercicios Resueltos: Nociones básicas de la Teoría de Códigos

1. *Estudiar si las siguientes tuplas corresponden a un código EAN:*

   (a) 9783540283713

   (b) 8412345678914

   (c) 9783662479735

   Solución

   Para saber si corresponde a un código EAN, debemos comprobar si $3\sum_{i=0}^{5} a_{2i+1} + \sum_{i=0}^{6} a_{2i} \equiv 0 \bmod 10$, siendo $a_0 a_1 \ldots a_{12}$ el número que queremos comprobar. Entonces,

   (a) Para 9783540283713, se cumple que $3\sum_{i=0}^{5} a_{2i+1} + \sum_{i=0}^{6} a_{2i} \equiv 0 \text{ mod } 10$, luego 9783540283713 corresponde a un código EAN.

   (b) Para 8412345678914 obtenemos $3\sum_{i=0}^{5} a_{2i+1} + \sum_{i=0}^{6} a_{2i} \equiv 2 \bmod 10$, luego 8412345678914 no corresponde a un código EAN.

   (c) Para 9783662479735, tenemos que $3\sum_{i=0}^{5} a_{2i+1} + \sum_{i=0}^{6} a_{2i} \equiv 0 \bmod 10$, luego 9783662479735 corresponde a un código EAN.

2. *Determinar el valor de "a" para que las siguientes tuplas correspondan a un código EAN:*

   (a) 843a554161836

   (b) 4325351455a52

   (c) 978421345667a

   Solución

   Como ya se ha indicado, si la cadena de dígitos correspondiente al producto es $a_0 \ldots a_{12}$, se tiene que satisfacer que

   $$3(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) + a_0 + a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12} \equiv 0 \bmod 10.$$

(a) $3(4+a+5+1+1+3)+8+3+5+4+6+8+6 \equiv 0 \bmod 10$. Pero esto implica que
$$3(4+a) \equiv 0 \bmod 10.$$
y como $3 \cdot 7 \equiv 1 \bmod 10$, se deduce que $4+a \equiv 7 \cdot 0 \equiv 0 \bmod 10$, luego $a = 6$.

(b) Tenemos ahora que buscar a para que
$$3(3+5+5+4+5+5)+4+2+3+1+5+a+2 \equiv 0 \bmod 10.$$
Ahora, esto equivale a resolver
$$3 \cdot 7 + 7 + a \equiv 0 \bmod 10$$
o equivalentemente
$$8 + a \equiv 0 \bmod 10,$$
que se cumple para $a = 2$.

(c) En este caso se debe cumplir
$$3(7+4+1+4+6+7)+9+8+2+3+5+6+a \equiv 0 \bmod 10,$$
o sea,
$$3 \cdot 9 + 3 + a \equiv 0 \bmod 10.$$
Por tanto, $a \equiv 0 \bmod 10$ y $a = 0$.

4. *Sea C un código un código de bloque sobre $\mathbb{F}_q$ de longitud n. Se llama* **polinomio enumerador de pesos** *de C al polinomio*
$$W_C(x,y) = \sum_{i=0}^{n} a_i x^i y^{n-i}, \quad \text{siendo } a_i = |\{c \in C \mid w(c) = i\}|.$$
Calcular $W_C(x,y)$ para el código $C = \{aa\ldots a \mid a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$ (Código de repetición).

Solución

Es claro que en C sólo hay elementos de peso 0 (el $00\ldots0$) y de peso n. Además, hay $q-1$ palabras de C con peso n, por lo que
$$W_C(x,y) = \sum_{i=0}^{n} a_i x^i y^{n-i} = y^n + (q-1)x^n.$$

5. *Sea $A = \{a_1, \ldots, a_m\}$ un alfabeto, $T_n = \{x_1 \ldots x_n \mid x_i \in A, i = 1, \ldots, n\}$ y $d : T_n \times T_n \to \{0, 1, 2, \ldots, n\}$ la aplicación definida por*
$$d(x_1 \ldots x_n, y_1 \ldots y_n) = |\{i \in \{1, \ldots, n\} \mid x_i \neq y_i\}|,$$
para todo $x_1 \ldots x_n, y_1 \ldots y_n \in T_n$. Demostrar que d es una distancia.

Solución

Para que d sea una distancia debe cumplir

(a) $d(x_1 \dots x_n, y_1 \dots y_n) \geq 0$ y $d(x_1 \dots x_n, y_1 \dots y_n) = 0$ si y, solo si, $x_1 \dots x_n = y_1 \dots y_n$: Se deduce que se cumplen ambas afirmaciones de la propia definición de $d(x_1 \dots x_n, y_1 \dots y_n)$

(b) $d(x_1 \dots x_n, y_1 \dots y_n) = d(y_1 \dots y_n, x_1 \dots x_n)$: Es evidente que si x_i es distinto de y_i, entonces y_i no coincide con x_i. Por ello, se deduce de forma inmediata que $d(x_1 \dots x_n, y_1 \dots y_n) = d(y_1 \dots y_n, x_1 \dots x_n)$.

(c) $d(x_1 \dots x_n, y_1 \dots y_n) \leq d(x_1 \dots x_n, z_1 \dots z_n) + d(y_1 \dots y_n, z_1 \dots z_n)$ (desigualdad triangular): Sea $z_1 \dots z_n \in T_n$. Entonces, el conjunto $XY = \{i \in \{1, \dots, n\} \mid x_i \neq y_i\}$ lo podemos escribir como

$$XY = \{i \in \{1, \dots, n\} \mid x_i \neq y_i, x_i \neq z_i\} \dot\cup \{i \in \{1, \dots, n\} \mid x_i \neq y_i, x_i = z_i\}.$$

Pero

$$|\{i \in \{1, \dots, n\} \mid x_i \neq y_i, x_i \neq z_i\}| \leq |\{i \in \{1, \dots, n\} \mid x_i \neq z_i\}|$$

y

$$|\{i \in \{1, \dots, n\} \mid x_i \neq y_i, x_i = z_i\}| = |\{i \in \{1, \dots, n\} \mid z_i \neq y_i\}|.$$

Por consiguiente,

$$d(x_1 \dots x_n, y_1 \dots y_n) \leq d(x_1 \dots x_n, z_1 \dots z_n) + d(y_1 \dots y_n, z_1 \dots z_n).$$

6. *Sean* $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$. *Se define*

$$\mathbf{x} \cap \mathbf{y} = (x_1 y_1, x_2 y_2, \dots, x_n y_n).$$

Demostrar que $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x} \cap \mathbf{y})$, *donde* $d(\mathbf{x}, \mathbf{y})$ *es la distancia de Hamming de las palabras* $\mathbf{x}$ *e* $\mathbf{y}$ *y* $w(\mathbf{z})$ *es el peso de la palabra* $\mathbf{z}$.

Solución

Para cada $i \in \{1, \dots, n\}$, sean

$$a_i = \begin{cases} 1, & \text{si } x_i \neq y_i; \\ 0, & \text{en otro caso,} \end{cases}$$

$$b_i = \begin{cases} 1, & \text{si } x_i \neq 0; \\ 0, & \text{en otro caso,} \end{cases}$$

$$c_i = \begin{cases} 1, & \text{si } y_i \neq 0; \\ 0, & \text{en otro caso,} \end{cases}$$

$$d_i = \begin{cases} 1, & \text{si } x_i y_i \neq 0; \\ 0, & \text{en otro caso.} \end{cases}$$

Basta probar que $a_i = b_i + c_i - 2d_i \ \forall i \in \{1, \dots, n\}$. Ahora,

(a) Si $x_i = 0, y_i = 0$, entonces $a_i = 0, b_i + c_i - 2d_i = 0 + 0 - 2 \cdot 0 = 0$.

(b) Si $x_i = 0, y_i = 1$, entonces $a_i = 1, b_i + c_i - 2d_i = 0 + 1 - 2 \cdot 0 = 1$.

(c) Si $x_i = 1, y_i = 0$, entonces $a_i = 1, b_i + c_i - 2d_i = 1 + 0 - 2 \cdot 0 = 1$.

(d) Si $x_i = 1, y_i = 1$, entonces $a_i = 0, b_i + c_i - 2d_i = 1 + 1 - 2 \cdot 1 = 0$.

Así que en los cuatro casos se da la igualdad buscada.

8. *Sea $C \subseteq T_n$ un código de bloque de longitud n sobre un alfabeto A con distancia mínima d. Demostrar que C es perfecto si y, solo si, $\dot{\bigcup}_{\mathbf{c}\in C}\overline{B}(\mathbf{c}, \left[\frac{d-1}{2}\right]) = T_n$.*

Solución

Primero, observamos que las bolas $\overline{B}(\mathbf{c}, \left[\frac{d-1}{2}\right])$ centradas en las palabras de un código C con distancia mínima d son disjuntas dos a dos, ya que si $x \in \overline{B}(\mathbf{c}_1, \left[\frac{d-1}{2}\right]) \cap \overline{B}(\mathbf{c}_2, \left[\frac{d-1}{2}\right])$, con $c_1, c_2 \in C$ y $c_1 \neq c_2$, entonces

$$d(x, c_1) \leq \left[\frac{d-1}{2}\right] \leq \frac{d-1}{2}, d(x, c_2) \leq \left[\frac{d-1}{2}\right] \leq \frac{d-1}{2},$$

y ahora se deduce de la desigualdad triangular que

$$d(c_1, c_2) \leq \frac{d-1}{2} + \frac{d-1}{2} = d - 1,$$

lo cual contradice que la distancia mínima de C es d.

Por lo que acabamos de probar,

$$\dot{\bigcup}_{\mathbf{c}\in C}\overline{B}(\mathbf{c}, \left[\frac{d-1}{2}\right]) \subseteq T_n,$$

y de ahí se deduce que se da la igualdad si y, solo si, ambos conjuntos tienen el mismo cardinal, es decir, si y, solo si, se da la igualdad en la cota de Hamming, lo cual es equivalente, por definición, a que el código C sea perfecto.