OCW
OpenCourseWare

Universidad del País Vasco
Euskal Herriko Unibertsitatea

Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Ejercicios y Problemas resueltos

Mayo de 2017

Ejercicios Resueltos: Preliminares sobre Álgebra Lineal

1. *Sea $(K,+,\cdot)$ un cuerpo. Demostrar que*

$$K^n = \{(k_1,\ldots,k_n) | k_i \in K, \forall i \in \{1,2,\ldots,n\}\}$$

con la suma definida por: para cualesquiera $(x_1,\ldots,x_n),(y_1,\ldots,y_n) \in K^n$

$$(x_1,\ldots,x_n)+(y_1,\ldots,y_n) = (x_1+y_1,\ldots,x_n+y_n)$$

y la multiplicación por un escalar:

$$\forall \lambda \in K, \forall (x_1,\ldots,x_n) \in K^n,\ \lambda(x_1,\ldots,x_n) = (\lambda x_1,\ldots,\lambda x_n)$$

es un K-espacio vectorial.

Solución

$(K^n,+,.)$ es un K-espacio vectorial ya que

(a) $(K^n,+)$ es un grupo abeliano porque se cumple

i. Asociativa: $\forall (x_1,\ldots,x_n),(y_1,\ldots,y_n),(z_1,\ldots,z_n) \in K^n$, se cumple

$$\begin{array}{l}((x_1,\ldots,x_n)+(y_1,\ldots,y_n))+(z_1,\ldots,z_n) = \\ (x_1+y_1,\ldots,x_n+y_n)+(z_1,\ldots,z_n) = \\ ((x_1+y_1)+z_1,\ldots,(x_n+y_n)+z_n) = \\ (x_1+(y_1+z_1),\ldots,x_n+(y_n+z_n)) = \\ (x_1,\ldots,x_n)+(y_1+z_1,\ldots,y_n+z_n) = \\ (x_1,\ldots,x_n)+((y_1,\ldots,y_n)+(z_1,\ldots,z_n))\end{array}$$

por verificarse la propiedad asociativa en $(K,+)$.

ii. Conmutativa: $\forall (x_1,\ldots,x_n),(y_1,\ldots,y_n) \in K^n$, se cumple

$$\begin{array}{rcl}(x_1,\ldots,x_n)+(y_1,\ldots,y_n) & = & (x_1+y_1,\ldots,x_n+y_n) \\ & = & (y_1+x_1,\ldots,y_n+x_n) \\ & = & (y_1,\ldots,y_n)+(x_1,\ldots,x_n)\end{array}$$

por verificarse la propiedad conmutativa en $(K,+)$.

iii. Existencia de elemento neutro: Si tomamos el elemento $(0_K, \ldots, 0_K)$ resulta que para todo $(x_1, \ldots, x_n) \in K^n$ se cumple

$$(x_1, \ldots, x_n) + (0_K, \ldots, 0_K) = (x_1 + 0_K, \ldots, x_n + 0_K) = (x_1, \ldots, x_n),$$

por ser 0_K el elemento neutro para $(K, +)$.

iv. Existencia de elemento opuesto: Dado $(x_1, \ldots, x_n) \in K^n$, el elemento $(-x_1, \ldots, -x_n)$ está también en K^n y cumple

$$(x_1, \ldots, x_n)+(-x_1, \ldots, -x_n) = (x_1+(-x_1), \ldots, x_n+(-x_n)) = (0_K, \ldots, 0_K),$$

por lo que existe elemento opuesto.

(b) La multiplicación por un escalar verifica:

i. $1_K(x_1, \ldots, x_n) = (1_K x_1, \ldots, 1_K x_n) = (x_1, \ldots, x_n)$, $\forall (x_1, \ldots, x_n) \in K^n$, por ser 1_K el elemento identidad del cuerpo K.

ii. Para todo $\lambda_1, \lambda_2 \in K$ y $(x_1, \ldots, x_n) \in K^n$, se cumple

$$\begin{aligned}(\lambda_1 + \lambda_2)(x_1, \ldots, x_n) &= ((\lambda_1 + \lambda_2)x_1, \ldots, (\lambda_1 + \lambda_2)x_n) \\ &= (\lambda_1 x_1 + \lambda_2 x_1, \ldots, \lambda_1 x_n + \lambda_2 x_n) \\ &= (\lambda_1 x_1, \ldots, \lambda_1 x_n) + (\lambda_2 x_1, \ldots, \lambda_2 x_n) \\ &= \lambda_1(x_1, \ldots, x_n) + \lambda_2(x_1, \ldots, x_n)\end{aligned}$$

por ser $(K, +, .)$ un cuerpo.

iii. Para todo $\lambda \in K$ y $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in K^n$, usando que $(K, +, .)$ es un cuerpo, se tiene

$$\begin{aligned}\lambda((x_1, \ldots, x_n) + (y_1, \ldots, y_n)) &= \lambda(x_1 + y_1, \ldots, x_n + y_n) \\ &= (\lambda(x_1 + y_1), \ldots, \lambda(x_n + y_n)) \\ &= (\lambda x_1 + \lambda y_1, \ldots, \lambda x_n + \lambda y_n) \\ &= (\lambda x_1, \ldots, \lambda x_n) + (\lambda y_1, \ldots, \lambda y_n) \\ &= \lambda(x_1, \ldots, x_n) + \lambda(y_1, \ldots, y_n).\end{aligned}$$

iv. Para todo $\lambda_1, \lambda_2 \in K$ y $(x_1, \ldots, x_n) \in K^n$, se tiene

$$\begin{aligned}(\lambda_1\lambda_2)(x_1, \ldots, x_n) &= ((\lambda_1\lambda_2)x_1, \ldots, (\lambda_1\lambda_2)x_n) \\ &= (\lambda_1(\lambda_2 x_1), \ldots, \lambda_1(\lambda_2 x_n)) \\ &= \lambda_1(\lambda_2 x_1, \ldots, \lambda_2 x_n) \\ &= \lambda_1(\lambda_2(x_1, \ldots, x_n)),\end{aligned}$$

usando que $(K, +, .)$ es un cuerpo.

2. *Estudiar si los siguientes conjuntos son $\mathbb{F}_q$-subespacios vectoriales de $\mathbb{F}_q^n$ y determinar su dimensión.*

(a) $S_1 = \{(a, a, \ldots, a) \mid a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$.

(b) $S_2 = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid x_n = \sum_{i=1}^{n-1} x_i\}$.

Solución

(a) Observamos que S_1 es no vacío. Usando la Proposición 2.1 del Tema 1, el subconjunto

$$S_1 = \{(a, a, \ldots, a) \mid a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$$

es un $\mathbb{F}_q$-subespacio vectorial si para cualesquiera $\alpha, \beta \in \mathbb{F}_q$ y $(a, a, \ldots, a)$, $(b, b, \ldots, b) \in S_1$, la combinación lineal $\alpha(a, a, \ldots, a) + \beta(b, b, \ldots, b)$ es otro elemento de S_1. Ahora,

$$\alpha(a, a, \ldots, a) + \beta(b, b, \ldots, b) = (\alpha a + \beta b, \alpha a + \beta b, \ldots, \alpha a + \beta b),$$

y como $\alpha, \beta, a, b \in \mathbb{F}_q$ y $\mathbb{F}_q$ es un cuerpo, sabemos que $\alpha a + \beta b$ es otro elemento de $\mathbb{F}_q$, por lo que $(\alpha a+\beta b, \alpha a+\beta b, \ldots, \alpha a+\beta b)$ es un elemento de S_1. Consecuentemente, S_1 es un $\mathbb{F}_q$-subespacio vectorial de $\mathbb{F}_q^n$. Además,

$$(a, a, \ldots, a) = a(1_K, 1_K, \ldots, 1_K),$$

y al se $(1_K, 1_K, \ldots, 1_K)$ un vector no nulo, el conjunto $\{(1_K, 1_K, \ldots, 1_K)\}$ es libre, por lo que una base de S_1 es $\{(1_K, 1_K, \ldots, 1_K)\}$ y es S_1 un subespacio de dimensión 1.

(b) De nuevo, observamos que observamos que S_2 es no vacío. Usando la Proposición 2.1 del Tema 1, el subconjunto

$$S_2 = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid x_n = \sum_{i=1}^{n-1} x_i\}$$

es un $\mathbb{F}_q$-subespacio vectorial si se verifican las dos condiciones siguientes:

i. Para todo $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in S_2$, se tiene

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) \in S_2.$$

ii. Para todo $\alpha \in \mathbb{F}_q$ y $(x_1, \ldots, x_n) \in S_2$, se cumple $\alpha(x_1, \ldots, x_n) \in S_2$.

En efecto,

i. Como $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in S_2$, sabemos que

$$x_n = \sum_{i=1}^{n-1} x_i \quad y_n = \sum_{i=1}^{n-1} y_i.$$

Por otro lado,

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

y

$$x_n + y_n = \sum_{i=1}^{n-1} x_i + \sum_{i=1}^{n-1} y_i = \sum_{i=1}^{n-1} (x_i + y_i)$$

por lo que $(x_1, \ldots, x_n) + (y_1, \ldots, y_n)$ es otro elemento de S_1.

ii. Como $(x_1, \ldots, x_n) \in S_2$, se cumple $x_n = \sum_{i=1}^{n-1} x_i$. Por otro lado, si $\alpha \in \mathbb{F}_q$,

$$\alpha(x_1, \ldots, x_n) = (\alpha x_1, \ldots, \alpha x_n)$$

y

$$\alpha x_n = \alpha \sum_{i=1}^{n-1} x_i = \sum_{i=1}^{n-1} \alpha x_i,$$

luego $\alpha(x_1, \ldots, x_n) \in S_2$.

Además, es fácil ver que el conjunto $\{(1_K, 0_K, 0_K, \ldots, 0_K, 1_K), (0_K, 1_K, 0_K, \ldots, 0_K, 1_K), \ldots, (0_K, 0_K, 0_K, \ldots, 0_K, 1_K, 1_K)\}$ es una base de S_2, luego S_2 es de dimensión $n-1$.

3. *Demostrar que el conjunto*

$$\mathcal{B} = \{(1_K, 0_K, \ldots, 0_K), (0_K, 1_K, 0_K, \ldots, 0_K), \ldots, (0_K, \ldots, 0_K, 1_K)\}$$

es una base de K^n. ¿Cuál es la dimensión de K^n?

Solución

El conjunto $\mathcal{B}$ será una base de K^n si es un sistema generador de K^n y es libre. Ahora, $\mathcal{B}$ es un sistema generador ya que dado un elemento $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$ se cumple

$$\begin{aligned}(x_1, \ldots, x_n) &= x_1(1_K, 0_K, \ldots, 0_K) + x_2(0_K, 1_K, 0_K, \ldots, 0_K) + \cdots + \\ &\quad x_n(0_K, \ldots, 0_K, 1_K).\end{aligned}$$

Además,

$$(0_K, \ldots, 0_K) = \alpha_1(1_K, 0_K, \ldots, 0_K) + \alpha_2(0_K, 1_K, 0_K, \ldots, 0_K) + \cdots + \alpha_n(0_K, \ldots, 0_K, 1_K)$$

implica

$$0 = \alpha_1 = \cdots = \alpha_n,$$

por lo que el conjunto $\mathcal{B}$ es también libre. En definitiva, $\mathcal{B}$ es una base de K^n y, por tanto, la dimensión de K^n es precisamente n.

4. *Sea S el subespacio vectorial de $\mathbb{F}_2^7$ definido por*

$$S = < 1101000, 0110100, 0011010, 0001101 >$$

(a) *Halla una base de S y la dimensión de S.*

(b) *Estudia si la palabra $\mathbf{x} = 1000110$ pertenece a S y, en caso de que esté, calcula las coordenadas de $\mathbf{x}$ en la base calculada en el apartado anterior.*

Solución

(a) Por la definición de S, sabemos que

$$T = \{1101000, 0110100, 0011010, 0001101\}$$

es un sistema generador de S. Comprobamos si este conjunto es también libre. Para ello, estudiamos si los únicos escalares de $\mathbb{F}_2$ de una combinación lineal que de el vector 0000000 son todos 0. Tenemos que

$$0000000 = \alpha_1 1101000 + \alpha_2 0110100 + \alpha_3 0011010 + \alpha_4 0001101$$

implica

$$\begin{array}{l} 0 = \alpha_1 \\ 0 = \alpha_1 + \alpha_2 \\ 0 = \alpha_2 + \alpha_3 \\ 0 = \alpha_1 + \alpha_3 + \alpha_4 \ , \\ 0 = \alpha_2 + \alpha_4 \\ 0 = \alpha_3 \\ 0 = \alpha_4 \end{array}$$

por lo que la única solución es

$$0 = \alpha_1 = \alpha_2 = \alpha_3 = \alpha_4.$$

Por tanto, T es también libre, luego T es una base S y la dimensión de S es 4.

(b) La palabra $\mathbf{x} = 1000110$ pertenece a S si $\mathbf{x}$ se puede escribir como una combinación lineal de los vectores de la base. Ahora,

$$1000110 = \alpha_1 1101000 + \alpha_2 0110100 + \alpha_3 0011010 + \alpha_4 0001101$$

implica

$$\begin{array}{l} 1 = \alpha_1 \\ 0 = \alpha_1 + \alpha_2 \\ 0 = \alpha_2 + \alpha_3 \\ 0 = \alpha_1 + \alpha_3 + \alpha_4 \ , \\ 1 = \alpha_2 + \alpha_4 \\ 1 = \alpha_3 \\ 0 = \alpha_4 \end{array}$$

cuya solución es

$$1 = \alpha_1 = \alpha_2 = \alpha_3 \ \ 0 = \alpha_4,$$

esto es,

$$1000110 = 1101000 + 0110100 + 0011010$$

y las coordenadas de 1000110 en la base hallada en el apartado anterior son (1 1 1 0).

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 $a_0 a_1 \dots a_{12}$ el número que queremos comprobar. Entonces,

   (a) Para 9783540283713, se cumple que $3\sum_{i=0}^{5} a_{2i+1} + \sum_{i=0}^{6} a_{2i} \equiv 0 \mod 10$, 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 $a_0 \dots a_{12}$, 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.

Ejercicios Resueltos: Códigos Lineales

1. *Sea $C \subseteq \mathbb{F}_q^n$ un código lineal de dimensión k y distancia mínima d.*

   (a) *Demostrar que* $\sum_{i=0}^{\left[\frac{d-1}{2}\right]} \binom{n}{i} (q-1)^i \leq q^{n-k}$.

   (b) *¿Existe un código lineal $C \subseteq \mathbb{F}_2^6$ con distancia mínima 3 y al menos 9 elementos? Razona la respuesta.*

   Solución

   (a) Basta aplicar la cota de Hamming y tener en cuenta que un código lineal de dimensión k tiene q^k elementos.

   (b) Si sustituimos los valores a $q = 2$, $n = 6$ y $d = 3$ en la desigualdad del apartado (a), tenemos que

   $$\sum_{i=0}^{1} \binom{6}{i} \leq 2^{6-k}.$$

   Por tanto,

   $$7 \leq 2^{6-k},$$

   luego

   $$k \leq 3,$$

   y, por tanto, si existe C binario de longitud 6 y distancia mínima 5, tendrá a lo sumo 8 elementos. Por tanto, no existe un código lineal $C \subseteq \mathbb{F}_2^6$ con distancia mínima 3 y al menos 9 elementos.

2. *Demostrar que los siguientes conjuntos son (n, k)-códigos lineales y determinar su dimensión, su distancia mínima y una matriz generadora:*

   (a) $S_1 = \{aa \dots a \,|\, a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$ *(Código de repetición)*

   (b) $S_2 = \{x_1 \dots x_n \,|\, x_i \in \mathbb{F}_q, i = 1, \dots, n, x_n = \sum_{i=1}^{n-1} x_i\}$ *(Código de paridad)*

Solución

(a) Para que $S_1 = \{aa\dots a \,|\, a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$ sea un $\mathbb{F}_q$-código lineal, debemos comprobar que es un $\mathbb{F}_q$-subespacio vectorial de $\mathbb{F}_q^n$. Para ello, usaremos las caracterizaciones equivalentes de subespacio vectorial que se enuncian en la Proposición 2.1 del Tema 1. Es obvio que S_1 es no vacío. Ahora, dados $\alpha, \beta \in \mathbb{F}_q$ y $aa\dots a, bb\dots b \in S_1$, se tiene

$$\alpha\, aa\dots a + \beta\, bb\dots b = (\alpha a + \beta b)(\alpha a + \beta b)\dots(\alpha a + \beta b) \in S_1,$$

luego S_1 es un $\mathbb{F}_q$-espacio vectorial. Además, para cada $aa\dots a \in S_1$ se verifica

$$aa\dots a = a\,11\dots 1.$$

Por tanto, $\{11\dots 1\}$ es un sistema generador de S_1 y, como solo consta de un único elemento no nulo, es una base de S_1. Así que la dimensión de S_1 es 1 y una matriz generadora es $(1\ 1\ \dots\ 1)$. Por último, la distancia mínima de S_1 es n, ya que toda palabra no nula de S_1 es de peso n.

(b) Para que $S_2 = \{x_1\dots x_n \,|\, x_i \in \mathbb{F}_q, i = 1,\dots,n, x_n = \sum_{i=1}^{n-1} x_i\}$ sea un $\mathbb{F}_q$-código lineal, debemos comprobar que es un $\mathbb{F}_q$-subespacio vectorial de $\mathbb{F}_q^n$. Para ello, usaremos de nuevo la caracterización equivalente de subespacio vectorial que se enuncia en la Proposición 2.1 del Tema 1. Es obvio que S_2 es no vacío. Ahora, dados $\alpha, \beta \in \mathbb{F}_q$ y $x_1\dots x_n, y_1\dots y_n \in S_2$, se tiene

$$\alpha\, x_1\dots x_n + \beta\, y_1\dots y_n = (\alpha x_1 + \beta y_1)\dots(\alpha x_n + \beta y_n)$$

y por estar $x_1\dots x_n$ e $y_1\dots y_n$ en S_2, tenemos

$$\alpha x_n + \beta y_n = \alpha \sum_{i=1}^{n-1} x_i + \beta \sum_{i=1}^{n-1} y_i = \sum_{i=1}^{n-1} (\alpha x_i + \beta y_i),$$

luego $\alpha\, x_1\dots x_n + \beta\, y_1\dots y_n$ es otro elemento de S_2. Además, si $x_1\dots x_n$ es un elemento de S_2, podemos escribirlo de la manera siguiente:

$$x_1\dots x_n = x_1\, 10\dots 01 + x_2\, 010\dots 01 + \dots + x_{n-1} 0\dots 011.$$

Por tanto, $\{10\dots 01, 010\dots 01, \dots, 0\dots 011\}$ es un sistema generador de S_2, que además es libre, luego es una base de S_2 y la dimensión de S_2 es $n-1$. Una matriz generadora de S_2 es

$$G = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 1 & 0 & \dots & 0 & 0 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 & 1 \end{pmatrix}.$$

Por otro lado, como $10\dots 01 \in S_2$, observamos que el peso mínimo de S_2 es menor o igual a 2. Pero, por la definición de S_2, no hay palabras de peso 1 en S_2. Así que el peso mínimo, y consecuentemente la distancia mínima, de S_2 es 2.

3. *Sea* $C \subseteq \mathbb{F}_3^3$ *el código ternario con matriz generadora* $G = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix}$.

   (a) *Demostrar que no tiene ninguna matriz generadora en forma estándar.*

   (b) *Localizar un código lineal* C_1 *equivalente a* C *que sí admita matriz generadora en forma estándar.*

Solución

(a) Basta observar que los pares formados por las dos primeras coordenadas de las palabras del código pueden tomar sólo tres valores: $(0,0), (1,2), (2,1)$, por lo que no es posible construir una matriz generadora de C dada en forma estándar.

(b) Permutando cíclicamente hacia la derecha las coordenadas de las palabras del código obtenemos otro código equivalente C' con matriz generadora $G' = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$. Multiplicando a la izquierda por la matriz $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, que equivale a sumar a la fila 1 la fila 2, obtenemos

$$G'' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix},$$

que está dada en forma estándar. Por tanto, el código C_1 que buscamos será aquel que tenga por matriz generadora a G''.

4. *Sea* $C \subseteq \mathbb{F}_q^n$ *un código lineal y* $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$. *Se define la relación de equivalencia dada por:*

$$\mathbf{x} \sim \mathbf{y} \Longleftrightarrow \mathbf{x} - \mathbf{y} \in C.$$

Probar que $\mathbf{x} \sim \mathbf{y}$ *si y, sólo si,* $S(\mathbf{x}) = S(\mathbf{y})$, *donde* $S(\mathbf{z})$ *denota el síndrome de* $\mathbf{z} \in \mathbb{F}_q^n$.

Solución

$\Rightarrow$) Supongamos que $\mathbf{x} \sim \mathbf{y}$. Entonces, $\mathbf{x} - \mathbf{y} \in C$ y $S(\mathbf{x} - \mathbf{y}) = 0$. Pero, si H es una matriz de control de C, sabemos que

$$S(\mathbf{x} - \mathbf{y}) = (\mathbf{x} - \mathbf{y})H^t = \mathbf{0},$$

por ser $\mathbf{x} - \mathbf{y}$ un elemento de C y como $S(\mathbf{x} - \mathbf{y}) = S(\mathbf{x}) - S(\mathbf{y})$, se sigue

$$S(\mathbf{x}) = S(\mathbf{y}).$$

$\Leftarrow$) Supongamos que $S(\mathbf{x}) = S(\mathbf{y})$. Entonces,

$$S(\mathbf{x} - \mathbf{y}) = S(\mathbf{x}) - S(\mathbf{y}) = 0,$$

lo que implica $\mathbf{x} - \mathbf{y} \in C$, por lo que $\mathbf{x} \sim \mathbf{y}$.

5. *Se considera el código lineal de* $\mathbb{F}_3^4$ *cuya matriz generadora es:* $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}$.

   (a) *Calcular una matriz de control y su distancia mínima.*

   (b) *Decodificar la palabra 2121 empleando el método de los síndromes.*

   (c) *¿Tienen todas las palabras de* $\mathbb{F}_3^4$ *decodificación única? ¿Es un código perfecto? Razona la respuesta.*

Solución

(a) Si intercambiamos en G las filas 1 y 2 y en la matriz resultante le restamos a la segunda fila la primera, obtenemos una matriz G_1 equivalente a G que es matriz generadora del mismo código lineal que genera G y está dada en forma estándar. En concreto, se obtiene

$$G_1 = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 2 \end{pmatrix}.$$

Por consiguiente, aplicando la Proposición 3.4 del Tema 3, deducimos que una matriz de control de C viene dada por:

$$H = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Además, de la Proposición 3.5 del Tema 3, se sigue que la distancia mínima del código definido es 3.

(b) Si calculamos el síndrome de 2121 usando como matriz de control H, se tiene

$$S(2121) = (2\ 1\ 2\ 1)H^t = (1\ 1),$$

que coincide con el síndrome de 0100. Además, el resto de palabras de peso 1 de $\mathbb{F}_3^4$ tienen síndrome distinto a (1 1), luego el líder de la clase de 2121 es precisamente 0100 y es único. Por consiguiente, la decodificación de 2121 es 2021.

(c) Sí, todas las palabras tienen decodificación única por ser C un código perfecto al alcanzar la Cota de Hamming.

6. (a) *Construir un código de Hamming binario* C *de longitud 7 y dimensión 4.*

   (b) *Hallar la decodificación de la palabra:* 1001010, *utilizando el método de decodificación basado en los líderes.*

Solución

Como C es un código de Hamming binario de longitud 7, comprobamos en primer lugar que es posible construirlo buscando el valor de r. Se debe verificar

$$2^r - 1 = 7 \qquad 2^r - 1 - r = 4,$$

y lo anterior se cumple para $r = 3$. Vamos a construir una matriz de control de C siguiendo lo indicado en el apartado 5 del Tema 3. Buscamos de cada subespacio vectorial de dimensión 1 de $\mathbb{F}_2^3$ una base y construimos la matriz que lleve en sus columnas los vectores de las bases de los diferentes subespacios de dimensión 1. Así

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

De aquí podemos calcular una matriz generadora de C que viene dada por

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

y las palabras del código C serán

$$\begin{aligned} C = \; & \{0000000, 0001011, 0010101, 0011110, \\ & 0100110, 0101101, 0110011, 0111000, \\ & 1000111, 1001100, 1010010, 1011001, \\ & 1100001, 1101010, 1110100, 1111111\}. \end{aligned}$$

Por tanto, la clase de equivalencia de 1001010 es

$$\begin{aligned} [1001010] = \; & \{1001010, 1000001, 1011111, 1010100, \\ & 1101100, 1100111, 1111001, 1110010, \\ & 0001101, 0000110, 0011000, 0010011, \\ & 0101011, 0100000, 0111110, 0110101\} \end{aligned}$$

y su líder es 0100000. Por consiguiente, la decodificación de 1001010 es

$$1001010 - 0100000 = 1101010.$$

7. *Sea* $G = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \in \mathrm{Mat}_{2\times 5}(\mathbb{F}_2)$ *la matriz generadora de un código lineal* C.

   (a) *Demostrar que* C *es de dimensión 2 y calcular todas las palabras de* C.

   (b) *Hallar una matriz de control de paridad.*

   (c) *Buscar líderes de las clases de equivalencia del conjunto cociente* $\mathbb{F}_2^5/C$.

Solución

(a) C es de dimensión 2 porque G es de tamaño 2×5 y las filas de G son palabras que forman una base de C. Para calcular todas las palabras de C basta realizar todas las combinaciones lineales de los elementos de una

base de C. Si tomamos como base de C a $\mathcal{B} = \{01111, 10010\}$, que son las filas de G, entonces las palabras de C serán de la forma

$$\mathbf{c} = \alpha 01111 + \beta 10010,$$

siendo $\alpha, \beta \in \mathbb{F}_2$. Por tanto,

$$C = \{00000, 01111, 10010, 11101\}.$$

(b) Si intercambiamos de posición las filas 1 y 2 de G, obtenemos una matriz generadora de C que está dada en forma estandar. Por tanto, aplicando la Proposición 3.4 del tema 3, se tiene que una matriz de control de C será $H = (-B^t|I_3)$, con $B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$, esto es,

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

(c) Obervamos que 10000 y 00010 están en la misma clase de equivalencia porque su diferencia es una palabra del código. El resto de palabras de $\mathbb{F}_2^5$ de peso 1 se encuentran en clases de equivalencia distintas porque no hay ninguna palabra más de peso 2. Por tanto, ya tenemos los siguientes líderes de las clases de equivalencia de $\mathbb{F}_2^5/C$: 00000, 10000, 01000, 00100, 00001. Pero la unión de las clases de equivalencia de estos líderes sólo cubren 20 de las 32 palabras de $\mathbb{F}_2^5$, por lo que necesitamos otros tres líderes. Para buscarlos, nos fijamos que en $[00000] \cup [10000] \cup [01000] \cup [00100] \cup [00001]$ la única palabra de peso 2 que tenemos es 10010, por lo que otro líder es 11000. Ahora, en [11000] también están las palabras de peso 2 01010 y 00101, por lo que otro líder de $\mathbb{F}_2^5/C$ es 10100. Pero a [10100] pertenecen también las palabras de peso 2 00110 y 01001, así que otro líder de $\mathbb{F}_2^5/C$ es 10001 y terminamos de hallar los líderes de $\mathbb{F}_2^5/C$.

8. *Se considera el código lineal binario C con matriz de control* $H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$.

   (a) *Calcular la dimensión de C.*

   (b) *Empleando síndromes, decodificar* 11001.

   (c) *¿Es C perfecto?*

Solución

(a) Como H es de tamaño 3×5, se sigue que C es un código de dimensión 2.

(b) Si calculamos el síndrome de 11001, se tiene

$$S(11001) = (1\,1\,0\,0\,1)H^t = (1\,1\,0\,0\,1)\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (1\,0\,0)$$

y como 00100, que es de peso 1, tiene el mismo síndrome que 11001, se sigue que una decodificación de 11001 es 11101. Además, el resto de palabras de peso 1 tienen síndrome distinto del de 00100, se sigue que la decodificación dada de 11001, esto es 11101, es única.

(c) Observamos que en la matriz H dos columnas cualesquiera son linealmente independientes y hay 3 (p.e., la primera, tercera y cuarta) que son linealmente dependientes, por lo que la distancia mínima de C es 3, según hemos visto en la Proposición 3.5 del tema 3. Entonces, para saber si es perfecto estudiamos si se alcanza la cota de Hamming. Ahora, en el apartado (a) hemos visto que la dimensión de C es 2, así que

$$2^2 \sum_{i=0}^{1} \binom{5}{i} = 4(1+5) = 24 < 32 = 2^5,$$

luego no es C perfecto.

10. *Sea $C \subseteq \mathbb{F}_q^n$ un código lineal de dimensión k y $W_C(x,y)$ su polinomio enumerador de pesos. Demostrar que:*

(a) $W_C(1,1) = q^k$.

(b) $W_C(0,1) = 1$.

(c) *Si $q = 2$, entonces $W_C(1,0) \in \{0,1\}$.*

(d) *Si $q = 2$, entonces $W_C(x,y) = W_C(y,x)$ si y sólo si $W_C(1,0) = 1$.*

Solución

(a) Basta aplicar la definición de polinomio enumerador de pesos dada en el problema propuesto 9 y tener en cuenta que al ser un código lineal de dimensión k el cardinal de C es q^k, ya que

$$W_C(1,1) = \sum_{i=0}^{n} a_i = |C| = q^k.$$

(b) Observamos que

$$W_C(0,1) = \sum_{i=0}^{n} a_i 0^i 1^{n-i} = a_0,$$

y como a_0 es el número de palabras de C con peso 0, sabemos que $a_0 = 1$, puesto que $00\ldots0$ está en C por ser C lineal. Consecuentemente, $W_C(0,1) = 1$.

(c) Tenemos que

$$W_C(1,0) = \sum_{i=0}^{n} a_i 1^i 0^{n-i} = a_n,$$

y a_n es el número de palabras de C que tienen peso n. Como trabajamos sobre $\mathbb{F}_2$, se sigue que en $\mathbb{F}_2^n$ hay una única palabra de peso n, la $11\ldots1$, por lo que

$$a_n = \begin{cases} 0, & \text{si } 11\ldots1 \notin C; \\ 1, & \text{si } 11\ldots1 \in C. \end{cases}$$

Por consiguiente, $W_C(1,0) \in \{0,1\}$.

(d) $\Rightarrow$) Supongamos que $W_C(x,y) = W_C(y,x)$. Entonces, $W_C(1,0) = W_C(0,1)$ y aplicando el apartado (b), deducimos que $W_C(1,0) = 1$.

$\Leftarrow$) Si $W_C(1,0) = 1$, entonces se tiene que $11\ldots1$ es una palabra de C. Debemos probar que $W_C(x,y) = W_C(y,x)$. Para ello, es suficiente con ver que $a_i = a_{n-i}$. Ahora si llamamos $A_i = \{\mathbf{c} \in C \mid w(\mathbf{c}) = i\}$, observamos que si $\mathbf{c} \in A_i$, entonces $11\ldots1 - \mathbf{c}$ es otra palabra de C, por ser diferencia de dos palabras de C y ser C lineal, que además es de peso n_i. Por tanto,

$$a_i = |A_i| \leq |A_{n-i}| = a_{n-i}.$$

El mismo argumento pero sobre A_{n-i} prueba que a_{n-i} es menor o igual que a_i. En definitiva,

$$a_{n-i} = a_i.$$

13. *Sea $C \subseteq \mathbb{F}_q^n$ un (n,k)-código lineal y $C^\perp$ su código dual. Se dice que C es autoortogonal si $C \subseteq C^\perp$ y C es autodual si $C = C^\perp$. Demostrar que C es autodual si y, solo si, C es autoortogonal y $\dim C = n/2$.*

Solución

$\Rightarrow$) Supongamos que C es autodual. Entonces, de la definición se deduce que C es autoortogonal. Por otro lado, como $C = C^\perp$, se sigue que $\dim(C) = \dim(C^\perp)$. Pero sabemos que

$$\dim(C) + \dim(C^\perp) = n,$$

luego

$$n = \dim(C) + \dim(C^\perp) = 2\dim(C) \Rightarrow \dim(C) = \frac{n}{2}.$$

$\Leftarrow$) Como C es autoortogonal, tenemos que $C \subseteq C^\perp$. Pero como la dimensión de $C^\perp$ es $n - \dim(C)$, deducimos que

$$\dim(C^\perp) = n - \frac{n}{2} = \frac{n}{2}.$$

Ahora, tenemos que C es un subespacio vectorial de $C^\perp$ con la misma dimensión que $C^\perp$, así que C coincide con $C^\perp$ y, por consiguiente, C es autodual.

Ejercicios Resueltos: Códigos cíclicos

1. *Localizar los códigos cíclicos de $\mathbb{F}_2^7$, determinando para cada uno de ellos un polinomio generador y una matriz generadora.*

   Solución

   Sabemos que un código cíclico de longitud n tiene por polinomio generador un polinomio mónico que sea divisor de x^n-1. Por tanto, para calcular los códigos cíclicos de longitud 7 de $\mathbb{F}_2^7$, debemos determinar los factores irreducibles sobre $\mathbb{F}_2$ de x^7-1 y a partir de ahí localizar los divisores mónicos de x^7-1. De esta forma calculamos los polinomios generadores de los códigos cíclicos binarios de longitud 7. Por otro lado, usando la Proposición 2.2 del Tema 4, podemos deducir una matriz generadora a partir de los coeficientes del polinomio generador. Ahora, la descomposición en polinomios irreducibles sobre $\mathbb{F}_2$ de x^7-1 es

   $$x^7-1=(x^3+x+1)(x^3+x^2+1)(x+1).$$

   Entonces, hay 2^3 códigos distintos $C_i(x)=(\overline{g_i(x)})$, con $i=1,\ldots,8$, donde

   $$\begin{array}{llll} g_1(x) &= 1, & g_2(x) &= x+1,\\ g_3(x) &= x^3+x+1, & g_4(x) &= x^3+x^2+1,\\ g_5(x) &= x^4+x^2+x+1, & g_6(x) &= x^4+x^3+x^2+1,\\ g_7(x) &= x^6+x^5+x^4+x^3+x^2+x+1, & g_8(x) &= x^7-1. \end{array}$$

   Observamos que

   (a) Si C_1 es el código cíclico con polinomio generador $g_1(x)=1$, entonces $C_1(x)=\mathbb{F}_2[x]/(x^7-1)$ y, por tanto, $C_1=\mathbb{F}_2^7$ y una matriz generadora de C_1 es $G_1=I_7$.

   (b) Si C_2 es el código cíclico con polinomio generador $g_2(x)=x+1$, entonces $C_2(x)=(\overline{x+1})$, por lo que una matriz generadora vendrá dada por

   $$G_2=\begin{pmatrix} 1&1&0&0&0&0&0\\ 0&1&1&0&0&0&0\\ 0&0&1&1&0&0&0\\ 0&0&0&1&1&0&0\\ 0&0&0&0&1&1&0\\ 0&0&0&0&0&1&1 \end{pmatrix}.$$

(c) Si C_3 es el código cíclico con polinomio generador $g_3(x) = x^3 + x + 1$, entonces $C_3(x) = (\overline{x^3 + x + 1})$, por lo que una matriz generadora vendrá dada por

$$G_3 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

(d) Si C_4 es el código cíclico con polinomio generador $g_4(x) = x^3 + x^2 + 1$, entonces $C_4(x) = (\overline{x^3 + x^2 + 1})$, por lo que una matriz generadora vendrá dada por

$$G_4 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

(e) Si C_5 es el código cíclico con polinomio generador $g_5(x) = x^4 + x^2 + x + 1$, entonces $C_5(x) = (\overline{x^4 + x^2 + x + 1})$, por lo que una matriz generadora vendrá dada por

$$G_5 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

(f) Si C_6 es el código cíclico con polinomio generador $g_6(x) = x^4 + x^3 + x^2 + 1$, entonces $C_5(x) = (\overline{x^4 + x^3 + x^2 + 1})$, por lo que una matriz generadora vendrá dada por

$$G_6 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

(g) Si C_7 es el código cíclico con polinomio generador $g_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, entonces $C_7(x) = (\overline{x^6 + x^5 + x^4 + x^3 + x^2 + x + 1})$, por lo que una matriz generadora vendrá dada por

$$G_7 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

(h) Si C_8 es el código cíclico con polinomio generador $g_8(x) = x^7 - 1$, entonces $C_8(x) = (\overline{x^7 - 1})$, por lo que $C_8 = \{0000000\}$.

2. *Encontrar los códigos cíclicos no triviales de $\mathbb{F}_3^4$ y hallar para cada uno de ellos un polinomio de control y una matriz de control.*

Solución

Sabemos que para hallar el polinomio de control de un código cíclico de longitud n, debemos determinar primero su polinomio generador, porque si $g(x)$

es el polinomio generador de este código cíclico, su polinomio de control verifica $x^7 - 1 = g(x)h(x)$. Además, los coeficientes del polinomio de control nos permiten determinar una matriz de control aplicando la Proposición 3.1 del Tema 4. Ahora, la descomposición en factores irreducibles sobre $\mathbb{F}_3$ de $x^4 - 1$ viene dada por

$$x^4 - 1 = (x+1)(x+2)(x^2+1).$$

Por tanto, tenemos los siguientes códigos cíclicos no triviales de longitud 4 sobre $\mathbb{F}_3$:

(a) Si C_1 es el código cíclico con polinomio generador $g_1(x) = x+1$, entonces su polinomio de control es $h_1(x) = (x+2)(x^2+1) = 2 + x + 2x^2 + x^3$ y una matriz de control viene dada por $H_1 = \begin{pmatrix} 1 & 2 & 1 & 2 \end{pmatrix}$.

(b) Si C_2 es el código cíclico con polinomio generador $g_2(x) = x+2$, entonces su polinomio de control es $h_2(x) = (x+1)(x^2+1) = 1 + x + x^2 + x^3$ y una matriz de control viene dada por $H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$.

(c) Si C_3 es el código cíclico con polinomio generador $g_3(x) = x^2+1$, entonces su polinomio de control es $h_3(x) = (x+2)(x+1) = 2 + x^2$ y una matriz de control viene dada por

$$H_3 = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix}.$$

(d) Si C_4 es el código cíclico con polinomio generador $g_1(x) = (x+1)(x+2)$, entonces su polinomio de control es $h_4(x) = x^2+1$ y una matriz de control viene dada por

$$H_4 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

(e) Si C_5 es el código cíclico con polinomio generador $g_1(x) = (x+1)(x^2+1)$, entonces su polinomio de control es $h_1(x) = x+2$ y una matriz de control viene dada por

$$H_5 = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix}.$$

(f) Si C_6 es el código cíclico con polinomio generador $g_1(x) = (x+2)(x^2+1)$, entonces su polinomio de control es $h_1(x) = x+1$ y una matriz de control viene dada por

$$H_6 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

4. *Hallar, si es que existe, un código cíclico de $\mathbb{F}_2^7$ de dimensión 3 y determinar las palabras que lo forman.*

Solución

Para que el código cíclico buscado sea de dimensión 3, sabemos que su polinomio generador tiene que ser de grado 4. En el Ejercicio 1 de este tema hemos calculado los polinomios generadores de códigos cíclicos binarios de longitud 7 y los que tienen polinomio generador de grado 4 son C_5 con polinomio generador $g_5(x) = x^4 + x^2 + x + 1$ y C_6 con polinomio generador $g_6(x) = x^4 + x^3 + x^2 + 1$. Por tanto, hay dos códigos cíclicos binarios de longitud 7 con dimensión 3. Si nos centramos en C_5, entonces una matriz generadora vendrá dada por

$$G_5 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Así que las palabras de C_5 se calcularán mediante

$$(\alpha_1\ \alpha_2\ \alpha_3)G_5 = (\alpha_1\ \alpha_2\ \alpha_3) \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix},$$

siendo $\alpha_1, \alpha_2, \alpha_3 \in F_2$. Entonces, las palabras de C_5 son

$$C_5 = \{0000000, 0011101, 0111010, 0100111, 1110100, 1101001, 1001110, 1010011\}.$$

5. *Determinar, si es que existe, un código cíclico binario con la menor dimensión posible que contenga a*

   (a) 1010011

   (b) 1001011

Solución

(a) Sea C el código cíclico de menor dimensión que contiene a $\mathbf{c}_1 = 1010011$ y sea $g(x)$ el polinomio generador de C. Nos fijamos que si $\mathbf{c}_1 = 1010011$, entonces $\mathbf{c}_1(x) = 1 + x^2 + x^5 + x^6 = (1 + x)(1 + x + x^2)(1 + x^2 + x^3)$ y como $\overline{\mathbf{c}_1(x)} \in C(x)$, sabemos que

$$\overline{\mathbf{c}_1(x)} = \overline{g(x)f(x)} \qquad (1)$$

para algún $f(x)$. Pero si queremos que C sea de menor dimensión posible, esto implica que $g(x)$ sea un divisor de $x^7 - 1$ del mayor grado posible y cumpliendo (1). Entonces, si calculamos el máximo común divisor mónico de $x^7 - 1$ y $\mathbf{c}_1(x)$ en $\mathbb{F}_2[x]$, este polinomio será el polinomio generador del código cíclico que buscamos. En concreto,

$$g(x) = \text{mcd}\{1+x^2+x^5+x^6, x^7-1\} = (1+x)(1+x^2+x^3) = 1+x+x^2+x^4.$$

esto es, C es el código cíclico binario de longitud 7 con polinomio generador $g(x) = 1 + x + x^2 + x^4$.

(b) Aplicando el mismo razonamiento pero para $\mathbf{c}_2 = 1001011$, tenemos que calcular el máximo común divisor de $\mathbf{c}_2(x) = 1 + x^3 + x^5 + x^6$ y $x^7 - 1$ en $\mathbb{F}_2[x]$ para determinar el polinomio generador del código cíclico que estamos buscando. Entonces, el polinomio generador del código cíclico binario de longitud 7 que contiene a 1001011 es

$$\begin{aligned} g(x) &= \text{mcd}\{x^7 - 1, 1 + x^3 + x^5 + x^6\} \\ &= (1 + x)(1 + x + x^3) \\ &= 1 + x^2 + x^3 + x^4. \end{aligned}$$

6. Se considera el código cíclico C de $\mathbb{F}_2^9$ cuyo polinomio generador es $1 + x^3$. Hallar $C^\perp$.

Solución

Como el polinomio generador de C es $1+x^3$, entonces C es de dimensión $k = 6$ y su polinomio de control vendrá dado por $h(x) = \frac{x^9-1}{1+x^3} = 1+x^3+x^6$, que es de grado $k = 6$. El polinomio generador de $C^\perp$ será $h_0^{-1} \sum_{i=0}^{6} h_i x^{6-i} = x^6+x^3+1$ y $C^\perp$ es un código cíclico binario de dimensión 3, longitud 9 y polinomio generador $x^6 + x^3 + 1$.

7. *Demostrar que si C es un código cíclico binario de longitud n impar, entonces $1 \ldots 1 \in C$ si y sólo si C contiene una palabra de peso impar.*

Solución

$\Rightarrow$) Es inmediato. En efecto, supongamos que $1 \ldots 1 \in C$ y que la longitud $n = 2l + 1$. Entonces, el peso de $1 \ldots 1$ es $n = 2l + 1$ y $1 \ldots 1$ es una palabra de C de peso impar.

$\Leftarrow$) Supongamos que $\mathbf{c} = c_0 \ldots c_{n-1}$ es una palabra de C de peso impar. Como C es cíclico, sabemos que también están en C sus traslaciones cíclicas $c_{n-1}c_0 \ldots c_{n-2}$, $c_{n-2}c_{n-1}c_0 \ldots c_{n-3}$, $\ldots$, y $c_1 \ldots c_{n-1}c_0$. Pero al ser lineal, sabemos que las combinaciones lineales de palabras de C también pertenecen a C. En particular, estará en C la palabra

$$c_0 \ldots c_{n-1} + c_{n-1}c_0 \ldots c_{n-2} + c_{n-2}c_{n-1}c_0 \ldots c_{n-3} + \cdots + c_1 \ldots c_{n-1}c_0,$$

que observamos que tiene en todas sus posiciones la letra $c_0 + \cdots + c_{n-1} \bmod 2$. Pero como estamos trabajando en $\mathbb{F}_2$, para cada $i = 0, \ldots n - 1$, se cumple $c_i \in \{0, 1\}$ y

$$c_0 + \cdots + c_{n-1} = w(c_0 \ldots c_{n-1}).$$

Pero $w(c_0 \ldots c_{n-1})$ es un número impar , puesto que hemos elegido $\mathbf{c} = c_0 \ldots c_{n-1}$ de peso impar, así que

$$c_0 + \cdots + c_{n-1} \equiv 1 \bmod 2,$$

por lo que

$$\begin{aligned} &c_0 \ldots c_{n-1} + c_{n-1}c_0 \ldots c_{n-2} + c_{n-2}c_{n-1}c_0 \ldots c_{n-3} + \cdots + c_1 \ldots c_{n-1}c_0 = \\ &(c_0 + \cdots + c_{n-1}) \ldots (c_0 + \cdots + c_{n-1}) = 1 \ldots 1 \end{aligned}$$

es una palabra de C.

8. *Demostrar que si C es un código cíclico binario de longitud n impar, entonces $1\ldots1 \in C$ si y sólo si $g(1) \equiv 1 \bmod 2$, siendo $g(x)$ el polinomio generador de C.*

Solución

Supongamos que $1\ldots1 \in C$. Entonces, $\exists P(x), Q(x) \in \mathbb{F}_2[x]$ tales que

$$g(x)P(x) = 1 + x + \cdots + x^{n-1} + Q(x)(x^n - 1).$$

Evaluando en $x = 1$, obtenemos $g(1)P(1) = n = 1$, ya que n es impar. Esto implica que $g(1) = 1$, ya que si no se tendría $1 = 0$.

Recíprocamente, supongamos que $g(1) = 1$ en $\mathbb{F}_2$. Entonces,

$$\text{mcd}\{g(x), x - 1\} = 1,$$

ya que en caso contrario, $x - 1 | g(x)$, de donde se deduciría que $g(1) = 0$. Ahora,

$$1 + x + \cdots + x^{n-1} = g(x)\frac{x^n - 1}{g(x)(x-1)}$$

donde, obviamente, el segundo factor está en $\mathbb{F}_2[x]$.

9. *Sea C un código cíclico binario de longitud n. Estudiar si el conjunto*

$$C_1 = \{\mathbf{c} \in C \,|\, w(\mathbf{c}) \equiv 0 \bmod 2\}$$

es un código lineal. En caso de respuesta afirmativa, determinar si es cíclico.

Solución

Obervamos que C_1 es un conjunto no vacío ya que la palabra $0\ldots0 \in C$ está también en C_1 por verificar que $w(0\ldots0) = 0$. Para que C_1 sea un código lineal sólo nos falta ver si se cumple que dados $\alpha \in \mathbb{F}_2$ y $\mathbf{c}_1, \mathbf{c}_2 \in C_1$, entonces

(a) $\alpha\mathbf{c}_1$ es un elemento de C_1.

(b) $\mathbf{c}_1 + \mathbf{c}_2$ es un elemento de C_1.

Ahora, (a) se cumple de forma trivial al ser $\alpha = 0, 1$. Nos falta ver si se verifica (b). Pero como C es un código cíclico binario, es en particular un código lineal, por lo que $\mathbf{c}_1 + \mathbf{c}_2 \in C$. Además, como trabajamos en $\mathbb{F}_2$, sabemos que el peso de una palabra de C coincide con la suma de las letras de ésta y

$$w(\mathbf{c}_1 + \mathbf{c}_2) \equiv w(\mathbf{c}_1) + w(\mathbf{c}_2) \equiv 0 \bmod 2,$$

luego C_1 es otro código lineal. Afirmamos que C_1 es cíclico, si C lo es. En efecto, para ver que C_1 es cíclico es suficiente con fijarse que si $\mathbf{c} = c_0 \ldots c_{n-1} \in C_1$, entonces

$$w(c_{n-1}c_0 \ldots c_{n-2}) = w(c_0 \ldots c_{n-1}) \equiv 0 \bmod 2$$

y como C es cíclico, entonces si $c_0 \dots c_{n-1} \in C$, también está en C la palabra $c_{n-1}c_0 \dots c_{n-2}$.

10. Sea $C \subseteq \mathbb{F}_q^n$ un código cíclico con polinomio generador $g(x)$. Si g_0 es el término independiente de $g(x)$, demostrar que $g_0 \neq 0$.

    Solución

    Si fuera $g_0 = 0$ se tendría que $x|g(x)$ en $\mathbb{F}_q[x]$ luego, como $g(x)|(x^n - 1)$, también $x|(x^n - 1)$, y ahora, dado que $x|x^n$, se deduce que $x|(-1)$, lo cual origina una contradicción.