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 propuestos

Mayo de 2017

Ejercicios Propuestos: 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.

2. $*$ Estudiar si los siguientes conjuntos son $\mathbb{F}_q$-subespacios vectoriales de $\mathbb{F}_q^n$ y determinar su dimensión.
   (a) $\{aa \ldots a | a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$.
   (b) $\{x_1 \ldots x_n | x_i \in \mathbb{F}_q, i = 1, \ldots, n, x_n = \sum_{i=1}^{n-1} x_i\}$.

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?

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.

5. Estudiar si el conjunto
$$\begin{aligned} S \ = \{&0000000, 0110100, 0011010, 0001101, \\ &1000110, 1001011, 1011100, 0010111, \\ &1010001, 1110010, 0111001, 1111111, \\ &0101110, 1101000, 0100011, 1100101\} \end{aligned}$$
es un $\mathbb{F}_2$-subespacio vectorial de $\mathbb{F}_2^7$. En caso de que lo sea, calcula la dimensión de S.

Ejercicios Propuestos: Nociones básicas de la Teoría de Códigos

1. $*$ Estudiar si las siguientes tuplas corresponden a un código EAN:
   (a) 9783540283713
   (b) 8412345678914
   (c) 9783662479735

2. $*$ Determinar el valor de "a" para que las siguientes tuplas correspondan a un código EAN:
   (a) 843a554161836
   (b) 4325351455a52
   (c) 978421345667a

3. Determinar la distancia mínima del código EAN. Deducir cuántos errores detecta y corrige. Probar que el código detecta la transposición de dos dígitos consecutivos, es decir, del cambio de la palabra $a_0 \dots a_i a_{i+1} \dots a_{12}$ del código por $a_0 \dots a_{i+1} a_i \dots a_{12}$, con $i \in \{0, \dots, 11\}$.

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

$$W_C(x,y) = \sum_{i=0}^{n} a_i x^i y^{n-i}, \quad \text{siendo } a_i = |\{c \in C \,|\, w(c) = i\}|.$$

   Calcular $W_C(x,y)$ para los siguientes códigos:
   (a) $\{aa \dots a \,|\, a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$ (Código de repetición)
   (b) $\{x_1 \dots x_n \,|\, x_i \in \mathbb{F}_q, i = 1, \dots, n, x_n = \sum_{i=1}^{n-1} x_i\}$ (Código de paridad)

5. $*$ Sea $A = \{a_1, \dots, a_m\}$ un alfabeto, $T_n = \{x_1 \dots x_n \,|\, x_i \in A, i = 1, \dots, n\}$ y $d : T_n \times T_n \to \{0, 1, 2, \dots, n\}$ la aplicación definida por

$$d(x_1 \dots x_n, y_1 \dots y_n) = |\{i \in \{1, \dots, n\} \,|\, x_i \neq y_i\}|,$$

   para todo $x_1 \dots x_n, y_1 \dots y_n \in T_n$. Demostrar que d es una distancia.

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

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

donde $\mathbf{x} = x_1 \ldots x_n$ e $\mathbf{y} = y_1 \ldots y_n$. 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 $\mathbf{z} \in \mathbb{F}_2^n$.

7. Sea $C \subseteq T_n$ un código de longitud n sobre el alfabeto $A = \{a_1, \ldots, a_m\}$ con distancia mínima d. Demostrar que si $\mathbf{c}, \mathbf{c}' \in C$ son dos palabras distintas de C, entonces $\overline{B}(\mathbf{c}, \left[\frac{d-1}{2}\right]) \cap \overline{B}(\mathbf{c}', \left[\frac{d-1}{2}\right]) = \emptyset$.

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

9. Demostrar que no existen códigos perfectos de longitud n sobre un alfabeto A con distancia mínima par.

10. Sea A un alfabeto, $T_n = \{a_1 ... a_n \,|\, a_i \in A, i \in \{1, 2, \ldots, n\}\}$ y $C \subseteq T_n$ un código de bloque de longitud n con distancia mínima d sobre el alfabeto A.

    (a) Demostrar que si $g : A \to A$ es una aplicación biyectiva y $\psi_{g,i} : T_n \to T_n$ está definida por $\psi_{g,i}(a_1 \ldots a_n) = a_1 \ldots a_{i-1} g(a_i) a_{i+1} \ldots a_n$, entonces $\psi_{g,i}(C)$ es un código equivalente a C con la misma distancia mínima que C.

    (b) Sea $1 \leq i < j \leq n$. Si $\phi_{i,j} : T_n \to T_n$ es la aplicación definida por $\phi_{ij}(a_1 \ldots a_n) = (a_1 \ldots a_{i-1} a_j a_{i+1} \ldots a_{j-1} a_i a_{j+1} \ldots a_n)$. Probar que $\phi_{ij}(C)$ es un código equivalente a C con la misma distancia mínima que C.

    (c) Demostrar que si $C' \subseteq T_n$ es un código equivalente a C, entonces la distancia mínima de C', denotada por $d(C')$, coincide con la distancia mínima de C.

Ejercicios Propuestos: 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.

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

   (a) $\{aa\ldots a | a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$ (Código de repetición)

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

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.

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

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.

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.

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 $\mathbb{F}_2^5/C$.

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 y 01110.

   (c) ¿Es C perfecto?

9. Sea C un código de bloque sobre $\mathbb{F}_q$ de longitud n. Se llama **polinomio enumerador de pesos** de C al polinomio

$$W_C(x,y) = \sum_{i=0}^{n} a_i x^i y^{n-i}, \quad \text{siendo } a_i = |\{c \in C | w(c) = i\}|.$$

   (a) Demostrar que si C es un código lineal, entonces el número de palabras de C que se encuentran a distancia i de $c \in C$ es a_i.

   (b) Si $C \in \mathbb{F}_2^5$ es el código lineal cuya matriz generadora viene dada por $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$, calcular su polinomio enumerador de pesos y el de su código dual.

10. $*$ Sea $C \subseteq \mathbb{F}_q^n$ un (n,k)-código lineal 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 $W_C(1,0) = 1$.

11. Sea $C \subseteq \mathbb{F}_2^n$ un código lineal. Demostrar que se verifica una de las dos afirmaciones siguientes:

(a) Todas las palabras son de peso par.

(b) La mitad de las palabras son de peso par y la otra mitad de peso impar.

12. Sea $C \subseteq \mathbb{F}_2^n$ un código lineal. Demostrar que se verifica una de las dos afirmaciones siguientes:

    (a) Todas las palabras empiezan por 0.

    (b) La mitad de las palabras empiezan por 0 y la otra mitad por 1.

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 $\dim C = n/2$.

14. Sea $C_i^\perp$ el código dual del código lineal C_i, $i = 1, 2$. Demostrar que:

    (a) $(C_i^\perp)^\perp = C_i$.

    (b) $(C_1 + C_2)^\perp = C_1^\perp \cap C_2^\perp$.

15. Para $i = 1, 2$, consideramos $C_i \in \mathbb{F}_2^{n_i}$ código lineal de dimensión k, distancia mínima d_i y matriz generadora G_i.

    (a) Demostrar que el código lineal con matriz generadora $\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$ tiene longitud $n_1 + n_2$, dimensión $2k$ y distancia mínima $d = \min\{d_1, d_2\}$.

    (b) Demostrar que el código lineal con matriz generadora $\begin{pmatrix} G_1 & G_2 \end{pmatrix}$ tiene longitud $n_1 + n_2$, dimensión k y distancia mínima $d \geq d_1 + d_2$.

16. Demostrar que si un código lineal admite una matriz generadora en forma estándar, entonces esta es única.

Ejercicios Propuestos: 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.

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.

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

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

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

   (a) 1010011

   (b) 1001011

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

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.

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

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

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

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

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 $g_0 \neq 0$.

11. Sea $C \subseteq \mathbb{F}_q^n$ un código cíclico de dimensión k con polinomio generador $g(x)$. Demostrar que $C^\perp$ es un código cíclico de dimensión $n-k$ y hallar el polinomio generador de $C^\perp$.

12. Se considera el código $C \subseteq \mathbb{F}_3^6$ tal que $C =< 122100, 012210, 120021 >$.

    (a) Demuestra que C es un código cíclico.

    (b) Halla el polinomio generador de C y el polinomio generador de $C^\perp$.

    (c) Calcula una matriz de control de C.

    (d) Utilizando el método de decodificación cíclica, decodifica la palabra 222022. ¿Es única su decodificación?

    (e) Usando una matriz de control de C, deduce cuál es la distancia mínima de C. ¿Cuántos errores detecta C? ¿Cuántos errores corrige C? ¿Es C perfecto? Razona tu respuesta.

13. Hallar un código cíclico BCH de longitud 16 y distancia mínima prevista 9 en el cuerpo $\mathbb{F}_3$.