Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Ejercicios y Problemas propuestos
Tema 3: CÓDIGOS LINEALES

Mayo de 2017

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.