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 3: CÓDIGOS LINEALES

Mayo de 2017

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.