Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Soluciones a los problemas de Pruebas de Autoevaluación

Mayo de 2017

Prueba de autoevaluación: Modelo A

Solución a los problemas

Curso OCW: Introducción a la Teoría de Códigos

1. *Se considera el código lineal $C \subseteq \mathbb{F}_3^8$, cuya matriz generadora es*

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

   (a) **(1,5 ptos.)** *Localiza, si es posible, una matriz generadora de C que esté dada en forma estándar y una matriz de control de C.*

   (b) **(1 pto.)** *Demuestra que la distancia mínima de C es 4.*

   (c) **(1 pto.)** *¿Es C cíclico?. En caso de que lo sea, calcula su polinomio generador.*

Solución

(a) Para localizar una matriz generadora dada en forma estándar aplicamos transformaciones elementales por filas hasta llegar a una matriz de la forma $(I_k|B)$. Así una matriz generadora en forma estándar es

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

y empleando la Proposición 3.4 del Tema 3 con G_1 deducimos que una matriz de control de C es

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

(b) Para probar que la distancia mínima es 4, basta aplicar la Proposición 3.5 del Tema 3 y ver que 3 columnas cualesquiera de H son linealmente independientes y que la primera, quinta, sexta y séptima columna de H son linealmente dependientes.

(c) Si aplicamos la Proposición 1.1 del Tema 4 a la base de C, que extraemos de la matriz generadora, $\mathcal{B} = \{12120100, 01212010, 00121201\}$ sabemos que C es cíclico si y, solo si, 10012120 está en C. Pero, 0012120 no es combinación lineal de los elementos de $\mathcal{B}$ por lo que C no es cíclico.

2. *Se considera el código lineal* $C_1 \subseteq \mathbb{F}_3^8$, *dado por*

$$C_1 =< 00111201, 01220211, 12121212, 10122021 > .$$

(a) **(1.5 ptos.)** *Demuestra que* C_1 *es cíclico y calcula su polinomio de control. ¿Cuál es la dimensión de* C_1*?*

(b) **(1 pto.)** *Calcula una matriz generadora y un polinomio generador de* $C_1^{\perp}$.

(c) **(1 pto.)** *¿Es* C_1 *autoortogonal?*

(d) **(1 pto.)** *Decodifica la palabra 01001110. ¿Es única su decodificación? Razona la respuesta.*

Ayuda: *La descomposición en factores irreducibles sobre* $\mathbb{F}_3$ *de* $x^8 - 1$ *es*

$$(1+x)(2+x)(1+x^2)(2+x+x^2)(2+2x+x^2).$$

Solución

(a) Sabemos que $S = \{00111201, 01220211, 12121212, 10122021\}$ es un sistema generador de C_1. Pero es fácil comprobar que no es $\mathbb{F}_3$-libre ya que 12121212 es $\mathbb{F}_3$-combinación lineal del resto. Ahora, aplicando la Proposición 3.1 del Tema 1, deducimos que

$$S_1 = \{00111201, 01220211, 10122021\}$$

es otro sistema generador de C_1. Además, S_1 es un conjunto $\mathbb{F}_3$-libre, así que S_1 es una base de C_1 y la dimensión de C_1 es 3. Para probar que C_1 es cíclico aplicamos la Proposición 1.1 del Tema 4 a S_1. En efecto, las traslaciones cíclicas de los vectores de S_1 verifican:

i. $10011120 = 2 \cdot 00111201 + 10122021$.
ii. $11012202 = 01220211 + 10122021$.

Por tanto, C_1 es cíclico. Para determinar el polinomio de control de C_1, calculamos en primer lugar su polinomio generador. Para ello, nos damos cuenta que el polinomio generador $g(x)$ debe de ser de grado 5, divisor de $x^8 - 1$ y como $C_1(x) = (\overline{g(x)})$, entonces si llamamos $\mathbf{c}_1 = 00111201$, $\mathbf{c}_2 = 01220211$, $\mathbf{c}_3 = 10122021$, se tiene que verificar que $\mathbf{c}_i(x)$ para $i = 1, 2, 3$ deben ser múltiplos de $g(x)$. Ahora

i. $\mathbf{c}_1(x) = x^2(2+x)(1+x^2)(x^2+x+2)$.
ii. $\mathbf{c}_2(x) = (x+1)(x+2)(x^2+1)(x^2+x+2)$.
iii. $\mathbf{c}_3(x) = (x+1)^2(x+2)(x^2+1)(x^2+x+2)$.

De aquí deducimos que el máximo común divisor de $\mathbf{c}_1(x)$, $\mathbf{c}_2(x)$ y $\mathbf{c}_3(x)$ es $(x+2)(x^2+1)(x^2+x+2)$, que es de grado 5 y divisor de x^8-1, por lo que es el polinomio generador de C_1, esto es,

$$g(x) = (x+2)(x^2+1)(x^2+x+2) = 1+x+x^2+2x^3+x^5.$$

El polinomio de control $h(x)$ de C_1 sabemos que verifica en $\mathbb{F}_3[x]$

$$x^8-1 = g(x)h(x).$$

Por tanto,

$$h(x) = (1+x)(2+2x+x^2) = x^3+x+2.$$

(b) En el apartado anterior hemos calculado el polinomio de control de C_1. Sabemos que una matriz generadora de $C_1^\perp$ es una matriz de control de C_1, que podemos hallar aplicando la Proposición 3.1 del Tema 4,

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

Por otro lado, sabemos que si $h(x) = \sum_{i=0}^{k} h_i x^i$ es el polinomio de control de C_1, entonces el polinomio generador de $C_1^\perp$ viene dado por $h_0^{-1}\sum_{i=0}^{k} h_i x^{k-i}$, que en este caso es $h^\perp(x) = 2+2x^2+x^3$.

(c) C_1 es autoortogonal si $C_1 \subseteq C_1^\perp$ y esto sucede si $h^\perp(x)$ es un divisor de $g(x)$. Como no se cumple, deducimos que C_1 no es autoortogonal.

(d) Si calculamos el síndrome de 01001110, obtenemos

$$S(01001110) = (0\,1\,0\,0\,1\,1\,1\,0)\begin{pmatrix} 1 & 0 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 \end{pmatrix}^t = (0\,0\,0\,0\,2).$$

Pero observamos que $S(01001110)$ coincide con $S(00000001)$, luego una decodificación de 01001110 es

$$01001110 - 00000001 = 01001112.$$

Además, esta decodificación es única porque el resto de palabras de peso 1 de $\mathbb{F}_3^8$ tiene síndrome distinto que el de 01001110.

Prueba de autoevaluación: Modelo B

Solución a los problemas

Curso OCW: Introducción a la Teoría de Códigos

1. *Se considera el código lineal* $C \subseteq \mathbb{F}_5^5$*, cuya matriz de control viene dada por*

$$H = \begin{pmatrix} 0 & 4 & 3 & 2 & 1 \\ 4 & 3 & 2 & 1 & 0 \end{pmatrix}.$$

   a) **(1 pto.)** *Hallar su distancia mínima.*

   b) **(1,5 ptos.)** *Decodificar la palabra* 12031*. ¿Tiene decodificación única?*

   c) **(1 pto.)** *¿Es* C *perfecto? Razona tu respuesta.*

   d) **(2 ptos.)** *¿Es* C *cíclico? En caso de respuesta afirmativa, calcula su polinomio generador y una matriz generadora.*

Solución

a) Para calcular la distancia mínima aplicamos la Proposición 3.5 del Tema 3. Observamos que dos columnas cualesquiera de H son linealmente independientes y que las columnas primera, segunda y quinta son linealmente dependientes, por lo que la distancia mínima es 3.

b) Empleamos el método de decodificación mediante síndromes. Tenemos que:

$$\begin{aligned} S(12031) &= (1\ 2\ 0\ 3\ 1)H^t \\ &= (1\ 2\ 0\ 3\ 1)\begin{pmatrix} 0 & 4 \\ 4 & 3 \\ 3 & 2 \\ 2 & 1 \\ 1 & 0 \end{pmatrix} \\ &= (0\ 3). \end{aligned}$$

Entonces, 12031 no es una palabra del código C. Pero $S(12031)$ coincide con $S(20000)$, así que ambas palabras tienen el mismo síndrome. Además, 20000 es la única palabra de peso 1 que tiene ese síndrome, por lo que es líder en su clase de equivalencia. Por tanto, la decodificación de 12031, que es única, viene dada por

$$\mathbf{c} = 12031 - 20000 = 42031.$$

c) Para que C sea perfecto, debemos comprobar si C alcanza la cota de Hamming. Ahora, C es un código de dimensión 3 porque la matriz de

control H es de tamaño 2×5, luego

$$|C| \sum_{i=0}^{\left[\frac{d-1}{2}\right]} \binom{n}{i} (m-1)^i = 5^3 \sum_{i=0}^{1} \binom{5}{i} (5-1)^i = 5^3(1+20) < 5^5.$$

Por consiguiente, C no es perfecto.

d) Sabemos que C es cíclico si y, solo si, $C^\perp$ es cíclico. Por ello, vamos a estudiar si $C^\perp$ es cíclico. Sabemos que $C^\perp$ tiene por matriz generadora a $H = \begin{pmatrix} 0 & 4 & 3 & 2 & 1 \\ 4 & 3 & 2 & 1 & 0 \end{pmatrix}$, por lo que una base de $C^\perp$ es $\{04321, 43210\}$. Pero $C^\perp$ es cíclico si las traslaciones cíclicas de una base son elementos de $C^\perp$. Ahora, la traslación cíclica de 04321 es 10432 y pertenece a $C^\perp$ ya que podemos encontrar $\alpha, \beta \in \mathbb{F}_5$ tales que

$$10432 = \alpha 04321 + \beta 43210 \Rightarrow \begin{cases} 1 = 4\beta \\ 0 = 4\alpha + 3\beta \\ 4 = 3\alpha + 2\beta \\ 3 = 2\alpha + \beta \\ 2 = \alpha \end{cases} \Rightarrow \alpha = 2,\ \beta = 4.$$

Por otro lado, la traslación cíclica de 43210 es 04321, que también pertenece a $C^\perp$. Por tanto, $C^\perp$ es cíclico y también lo es C. Finalmente, como C es cíclico de dimensión 3 y solo hay un código cíclico en $\mathbb{F}_5^5$ de dimensión 3, que es el que está generado por el polinomio $(x+4)^2 = x^2 + 3x + 1$, una matriz generadora de C es

$$G = \begin{pmatrix} 1 & 3 & 1 & 0 & 0 \\ 0 & 1 & 3 & 1 & 0 \\ 0 & 0 & 1 & 3 & 1 \end{pmatrix}.$$

2. **(2,5 puntos)** *Sea $C \subseteq \mathbb{F}_q^n$ un código lineal de dimensión k que corrige errores $\mathbf{e} \in \mathbb{F}_q^n$ tales que $w(\mathbf{e}) \leq t$. Probar que $2t + k \leq n$.*

Solución

Como C corrije errores de peso hasta t, significa que si d es la distancia mínima de C, entonces

$$t = \left[\frac{d-1}{2}\right] \leq \frac{d-1}{2} \Rightarrow 2t \leq d-1$$

Pero sabemos que $d-1$ es menor o igual que el rango de H matriz de control de C, luego

$$2t \leq d-1 \leq \operatorname{rg} H = n - k \Rightarrow 2t + k \leq n.$$

Prueba de autoevaluación: Modelo C

Solución a los problemas

Curso OCW: Introducción a la Teoría de Códigos

1. *Se considera el código binario C cuya matriz de control es:*

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

   a) **(1,5 ptos.)** *Hallar una matriz generadora de C.*

   b) **(0,5 ptos.)** *Probar que 11101000 pertenece a C.*

   c) **(1,5 pto.)** *¿Es C un código autodual?*

   d) **(1,5 ptos.)** *Calcular un código cíclico C_1 de menor dimensión posible que contenga a 11101000.*

   e) **(1,5 pto.)** *¿Es $\dim(C_1 \cap C) > 1$?*

Solución

a) Sumando a la cuarta fila las otras tres filas, obtenemos otra matriz de control de H que es

$$H_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

y, reordenando las filas de H_1, obtenemos otra matriz de control de C que viene dada por

$$H_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Como H_2 está dada en forma estándar, podemos deducir que una matriz generadora de C es

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

b) La palabra 11101000 está en C ya que es la primera fila de la matriz G (recordemos que en una matriz generadora van los vectores de una base de C). Otra forma de demostrar que 11101000 está en C es comprobar que su síndrome es (0 0 0 0), esto es,

$$S(11101000) = (1\ 1\ 1\ 0\ 1\ 0\ 0\ 0)H^t = (0\ 0\ 0\ 0).$$

c) C es autodual si $C = C^\perp$. Ahora, dado $\mathbf{c} \in C$ sabemos que $\mathbf{c}$ pertenece a $C^\perp$ si

$$\mathbf{c}G^t = (0\ 0\ 0\ 0).$$

Por ello, para estudiar si $C \subseteq C^\perp$, es suficiente con estudiar si $GG^t = 0$ y como esto se cumple, deducimos que $C \subseteq C^\perp$ y al ser la dimensión de ambos códigos 4, deducimos que C es autodual.

d) Tenemos que a 11101000 le corresponde el polinomio $1 + x + x^2 + x^4$, que se escribe como producto de irreducibles sobre $\mathbb{F}_2$ de la manera siguiente:

$$1 + x + x^2 + x^4 = (1 + x)(1 + x^2 + x^3).$$

Por otro lado, la descomposición en factores irreducibles sobre $\mathbb{F}_2$ de $x^8 - 1$ es $(1 + x)^8$. Por tanto,

$$\text{mcd}\{1 + x + x^2 + x^4, x^8 - 1\} = 1 + x$$

y el código cíclico de menor dimensión que contiene a 11101000 es el que tiene por polinomio generador a $1 + x$.

e) $\dim(C_1 \cap C)$ es mayor que 1 ya que la palabra 11010100 de C (y en general cualquiera de peso par de C) también pertenece a C_1 porque

$$1 + x + x^3 + x^5 = (1 + x)(1 + x^3 + x^4)$$

y, como $\{11010100, 11101000\}$ es un conjunto libre, se sigue que $\dim(C_1 \cap C)$, que contiene a $< 11010100, 11101000 >$, es mayor o igual que 2.

2. **(1,5 pto.)** *Sea $C \subseteq \mathbb{F}_q^n$ un código lineal de dimensión k y distancia mínima d. Si $n = 15$ y $k = 6$, probar que C no corrije 5 errores o más.*

Solución

Supongamos, por reducción al absurdo, que C corrije al menos 5 errores. Entonces, la distancia mínima de C es al menos 11. Entonces, por la Cota de Singleton se debe verificar

$$11 \leq 15 - 6 + 1 = 10,$$

lo cual es absurdo. Por tanto, C no corrije 5 errores o más.