Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Solución a los problemas de la Prueba de Autoevaluación: Modelo A

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.