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 4: CÓDIGOS CÍCLICOS

Mayo de 2017

Ejercicios Resueltos: 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.*

   Solución

   Sabemos que un código cíclico de longitud n tiene por polinomio generador un polinomio mónico que sea divisor de x^n-1. Por tanto, para calcular los códigos cíclicos de longitud 7 de $\mathbb{F}_2^7$, debemos determinar los factores irreducibles sobre $\mathbb{F}_2$ de x^7-1 y a partir de ahí localizar los divisores mónicos de x^7-1. De esta forma calculamos los polinomios generadores de los códigos cíclicos binarios de longitud 7. Por otro lado, usando la Proposición 2.2 del Tema 4, podemos deducir una matriz generadora a partir de los coeficientes del polinomio generador. Ahora, la descomposición en polinomios irreducibles sobre $\mathbb{F}_2$ de x^7-1 es

   $$x^7-1=(x^3+x+1)(x^3+x^2+1)(x+1).$$

   Entonces, hay 2^3 códigos distintos $C_i(x)=(\overline{g_i(x)})$, con $i=1,\ldots,8$, donde

   $$\begin{array}{llll} g_1(x) & =1, & g_2(x) & =x+1,\\ g_3(x) & =x^3+x+1, & g_4(x) & =x^3+x^2+1,\\ g_5(x) & =x^4+x^2+x+1, & g_6(x) & =x^4+x^3+x^2+1,\\ g_7(x) & =x^6+x^5+x^4+x^3+x^2+x+1, & g_8(x) & =x^7-1. \end{array}$$

   Observamos que

   (a) Si C_1 es el código cíclico con polinomio generador $g_1(x)=1$, entonces $C_1(x)=\mathbb{F}_2[x]/(x^7-1)$ y, por tanto, $C_1=\mathbb{F}_2^7$ y una matriz generadora de C_1 es $G_1=I_7$.

   (b) Si C_2 es el código cíclico con polinomio generador $g_2(x)=x+1$, entonces $C_2(x)=(\overline{x+1})$, por lo que una matriz generadora vendrá dada por

   $$G_2=\begin{pmatrix} 1&1&0&0&0&0&0\\ 0&1&1&0&0&0&0\\ 0&0&1&1&0&0&0\\ 0&0&0&1&1&0&0\\ 0&0&0&0&1&1&0\\ 0&0&0&0&0&1&1 \end{pmatrix}.$$

(c) Si C_3 es el código cíclico con polinomio generador $g_3(x) = x^3 + x + 1$, entonces $C_3(x) = (\overline{x^3 + x + 1})$, por lo que una matriz generadora vendrá dada por

$$G_3 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

(d) Si C_4 es el código cíclico con polinomio generador $g_4(x) = x^3 + x^2 + 1$, entonces $C_4(x) = (\overline{x^3 + x^2 + 1})$, por lo que una matriz generadora vendrá dada por

$$G_4 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

(e) Si C_5 es el código cíclico con polinomio generador $g_5(x) = x^4 + x^2 + x + 1$, entonces $C_5(x) = (\overline{x^4 + x^2 + x + 1})$, por lo que una matriz generadora vendrá dada por

$$G_5 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

(f) Si C_6 es el código cíclico con polinomio generador $g_6(x) = x^4 + x^3 + x^2 + 1$, entonces $C_5(x) = (\overline{x^4 + x^3 + x^2 + 1})$, por lo que una matriz generadora vendrá dada por

$$G_6 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

(g) Si C_7 es el código cíclico con polinomio generador $g_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, entonces $C_7(x) = (\overline{x^6 + x^5 + x^4 + x^3 + x^2 + x + 1})$, por lo que una matriz generadora vendrá dada por

$$G_7 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

(h) Si C_8 es el código cíclico con polinomio generador $g_8(x) = x^7 - 1$, entonces $C_8(x) = (\overline{x^7 - 1})$, por lo que $C_8 = \{0000000\}$.

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.*

Solución

Sabemos que para hallar el polinomio de control de un código cíclico de longitud n, debemos determinar primero su polinomio generador, porque si $g(x)$

es el polinomio generador de este código cíclico, su polinomio de control verifica $x^7 - 1 = g(x)h(x)$. Además, los coeficientes del polinomio de control nos permiten determinar una matriz de control aplicando la Proposición 3.1 del Tema 4. Ahora, la descomposición en factores irreducibles sobre $\mathbb{F}_3$ de $x^4 - 1$ viene dada por

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

Por tanto, tenemos los siguientes códigos cíclicos no triviales de longitud 4 sobre $\mathbb{F}_3$:

(a) Si C_1 es el código cíclico con polinomio generador $g_1(x) = x+1$, entonces su polinomio de control es $h_1(x) = (x+2)(x^2+1) = 2 + x + 2x^2 + x^3$ y una matriz de control viene dada por $H_1 = \begin{pmatrix} 1 & 2 & 1 & 2 \end{pmatrix}$.

(b) Si C_2 es el código cíclico con polinomio generador $g_2(x) = x+2$, entonces su polinomio de control es $h_2(x) = (x+1)(x^2+1) = 1 + x + x^2 + x^3$ y una matriz de control viene dada por $H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$.

(c) Si C_3 es el código cíclico con polinomio generador $g_3(x) = x^2+1$, entonces su polinomio de control es $h_3(x) = (x+2)(x+1) = 2 + x^2$ y una matriz de control viene dada por

$$H_3 = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix}.$$

(d) Si C_4 es el código cíclico con polinomio generador $g_1(x) = (x+1)(x+2)$, entonces su polinomio de control es $h_4(x) = x^2+1$ y una matriz de control viene dada por

$$H_4 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

(e) Si C_5 es el código cíclico con polinomio generador $g_1(x) = (x+1)(x^2+1)$, entonces su polinomio de control es $h_1(x) = x+2$ y una matriz de control viene dada por

$$H_5 = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix}.$$

(f) Si C_6 es el código cíclico con polinomio generador $g_1(x) = (x+2)(x^2+1)$, entonces su polinomio de control es $h_1(x) = x+1$ y una matriz de control viene dada por

$$H_6 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

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

Solución

Para que el código cíclico buscado sea de dimensión 3, sabemos que su polinomio generador tiene que ser de grado 4. En el Ejercicio 1 de este tema hemos calculado los polinomios generadores de códigos cíclicos binarios de longitud 7 y los que tienen polinomio generador de grado 4 son C_5 con polinomio generador $g_5(x) = x^4 + x^2 + x + 1$ y C_6 con polinomio generador $g_6(x) = x^4 + x^3 + x^2 + 1$. Por tanto, hay dos códigos cíclicos binarios de longitud 7 con dimensión 3. Si nos centramos en C_5, entonces una matriz generadora vendrá dada por

$$G_5 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Así que las palabras de C_5 se calcularán mediante

$$(\alpha_1\ \alpha_2\ \alpha_3)G_5 = (\alpha_1\ \alpha_2\ \alpha_3) \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix},$$

siendo $\alpha_1, \alpha_2, \alpha_3 \in F_2$. Entonces, las palabras de C_5 son

$$C_5 = \{0000000, 0011101, 0111010, 0100111, 1110100, 1101001, 1001110, 1010011\}.$$

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

   (a) 1010011

   (b) 1001011

Solución

(a) Sea C el código cíclico de menor dimensión que contiene a $\mathbf{c}_1 = 1010011$ y sea $g(x)$ el polinomio generador de C. Nos fijamos que si $\mathbf{c}_1 = 1010011$, entonces $\mathbf{c}_1(x) = 1 + x^2 + x^5 + x^6 = (1 + x)(1 + x + x^2)(1 + x^2 + x^3)$ y como $\overline{\mathbf{c}_1(x)} \in C(x)$, sabemos que

$$\overline{\mathbf{c}_1(x)} = \overline{g(x)f(x)} \qquad (1)$$

para algún $f(x)$. Pero si queremos que C sea de menor dimensión posible, esto implica que $g(x)$ sea un divisor de $x^7 - 1$ del mayor grado posible y cumpliendo (1). Entonces, si calculamos el máximo común divisor mónico de $x^7 - 1$ y $\mathbf{c}_1(x)$ en $\mathbb{F}_2[x]$, este polinomio será el polinomio generador del código cíclico que buscamos. En concreto,

$$g(x) = \text{mcd}\{1+x^2+x^5+x^6, x^7-1\} = (1+x)(1+x^2+x^3) = 1+x+x^2+x^4.$$

esto es, C es el código cíclico binario de longitud 7 con polinomio generador $g(x) = 1 + x + x^2 + x^4$.

(b) Aplicando el mismo razonamiento pero para $\mathbf{c}_2 = 1001011$, tenemos que calcular el máximo común divisor de $\mathbf{c}_2(x) = 1 + x^3 + x^5 + x^6$ y $x^7 - 1$ en $\mathbb{F}_2[x]$ para determinar el polinomio generador del código cíclico que estamos buscando. Entonces, el polinomio generador del código cíclico binario de longitud 7 que contiene a 1001011 es

$$\begin{aligned} g(x) &= \text{mcd}\{x^7 - 1, 1 + x^3 + x^5 + x^6\} \\ &= (1 + x)(1 + x + x^3) \\ &= 1 + x^2 + x^3 + x^4. \end{aligned}$$

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

Solución

Como el polinomio generador de C es $1+x^3$, entonces C es de dimensión $k = 6$ y su polinomio de control vendrá dado por $h(x) = \frac{x^9-1}{1+x^3} = 1+x^3+x^6$, que es de grado $k = 6$. El polinomio generador de $C^\perp$ será $h_0^{-1} \sum_{i=0}^{6} h_i x^{6-i} = x^6+x^3+1$ y $C^\perp$ es un código cíclico binario de dimensión 3, longitud 9 y polinomio generador $x^6 + x^3 + 1$.

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.*

Solución

$\Rightarrow$) Es inmediato. En efecto, supongamos que $1 \ldots 1 \in C$ y que la longitud $n = 2l + 1$. Entonces, el peso de $1 \ldots 1$ es $n = 2l + 1$ y $1 \ldots 1$ es una palabra de C de peso impar.

$\Leftarrow$) Supongamos que $\mathbf{c} = c_0 \ldots c_{n-1}$ es una palabra de C de peso impar. Como C es cíclico, sabemos que también están en C sus traslaciones cíclicas $c_{n-1}c_0 \ldots c_{n-2}$, $c_{n-2}c_{n-1}c_0 \ldots c_{n-3}$, $\ldots$, y $c_1 \ldots c_{n-1}c_0$. Pero al ser lineal, sabemos que las combinaciones lineales de palabras de C también pertenecen a C. En particular, estará en C la palabra

$$c_0 \ldots c_{n-1} + c_{n-1}c_0 \ldots c_{n-2} + c_{n-2}c_{n-1}c_0 \ldots c_{n-3} + \cdots + c_1 \ldots c_{n-1}c_0,$$

que observamos que tiene en todas sus posiciones la letra $c_0 + \cdots + c_{n-1} \bmod 2$. Pero como estamos trabajando en $\mathbb{F}_2$, para cada $i = 0, \ldots n - 1$, se cumple $c_i \in \{0, 1\}$ y

$$c_0 + \cdots + c_{n-1} = w(c_0 \ldots c_{n-1}).$$

Pero $w(c_0 \ldots c_{n-1})$ es un número impar , puesto que hemos elegido $\mathbf{c} = c_0 \ldots c_{n-1}$ de peso impar, así que

$$c_0 + \cdots + c_{n-1} \equiv 1 \bmod 2,$$

por lo que

$$\begin{aligned} &c_0 \ldots c_{n-1} + c_{n-1}c_0 \ldots c_{n-2} + c_{n-2}c_{n-1}c_0 \ldots c_{n-3} + \cdots + c_1 \ldots c_{n-1}c_0 = \\ &(c_0 + \cdots + c_{n-1}) \ldots (c_0 + \cdots + c_{n-1}) = 1 \ldots 1 \end{aligned}$$

es una palabra de C.

8. *Demostrar que si C es un código cíclico binario de longitud n impar, entonces $1\ldots1 \in C$ si y sólo si $g(1) \equiv 1 \bmod 2$, siendo $g(x)$ el polinomio generador de C.*

Solución

Supongamos que $1\ldots1 \in C$. Entonces, $\exists P(x), Q(x) \in \mathbb{F}_2[x]$ tales que

$$g(x)P(x) = 1 + x + \cdots + x^{n-1} + Q(x)(x^n - 1).$$

Evaluando en $x = 1$, obtenemos $g(1)P(1) = n = 1$, ya que n es impar. Esto implica que $g(1) = 1$, ya que si no se tendría $1 = 0$.

Recíprocamente, supongamos que $g(1) = 1$ en $\mathbb{F}_2$. Entonces,

$$\text{mcd}\{g(x), x - 1\} = 1,$$

ya que en caso contrario, $x - 1 | g(x)$, de donde se deduciría que $g(1) = 0$. Ahora,

$$1 + x + \cdots + x^{n-1} = g(x)\frac{x^n - 1}{g(x)(x-1)}$$

donde, obviamente, el segundo factor está en $\mathbb{F}_2[x]$.

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

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

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

Solución

Obervamos que C_1 es un conjunto no vacío ya que la palabra $0\ldots0 \in C$ está también en C_1 por verificar que $w(0\ldots0) = 0$. Para que C_1 sea un código lineal sólo nos falta ver si se cumple que dados $\alpha \in \mathbb{F}_2$ y $\mathbf{c}_1, \mathbf{c}_2 \in C_1$, entonces

(a) $\alpha\mathbf{c}_1$ es un elemento de C_1.

(b) $\mathbf{c}_1 + \mathbf{c}_2$ es un elemento de C_1.

Ahora, (a) se cumple de forma trivial al ser $\alpha = 0, 1$. Nos falta ver si se verifica (b). Pero como C es un código cíclico binario, es en particular un código lineal, por lo que $\mathbf{c}_1 + \mathbf{c}_2 \in C$. Además, como trabajamos en $\mathbb{F}_2$, sabemos que el peso de una palabra de C coincide con la suma de las letras de ésta y

$$w(\mathbf{c}_1 + \mathbf{c}_2) \equiv w(\mathbf{c}_1) + w(\mathbf{c}_2) \equiv 0 \bmod 2,$$

luego C_1 es otro código lineal. Afirmamos que C_1 es cíclico, si C lo es. En efecto, para ver que C_1 es cíclico es suficiente con fijarse que si $\mathbf{c} = c_0 \ldots c_{n-1} \in C_1$, entonces

$$w(c_{n-1}c_0 \ldots c_{n-2}) = w(c_0 \ldots c_{n-1}) \equiv 0 \bmod 2$$

y como C es cíclico, entonces si $c_0 \dots c_{n-1} \in C$, también está en C la palabra $c_{n-1}c_0 \dots c_{n-2}$.

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 $g_0 \neq 0$.

    Solución

    Si fuera $g_0 = 0$ se tendría que $x|g(x)$ en $\mathbb{F}_q[x]$ luego, como $g(x)|(x^n - 1)$, también $x|(x^n - 1)$, y ahora, dado que $x|x^n$, se deduce que $x|(-1)$, lo cual origina una contradicción.