Tema 4. Códigos Cíclicos

Justo Peralta López

Juan Antonio López Ramos
Dpto. Álgebra y Análisis Matemático

Resumen: *En este tema se introduce la familia de códigos más importante que veremos en esta asignatura. Esta importancia radica en su rica estructura algebraica. Si hasta ahora los códigos eran subespacios, ahora, si son invariantes respecto rotaciones, veremos que dicho subespacio es isomorfo a un ideal en un anillo de polinomios del tipo $\mathbf{F_q[x]/(x^n-1)}$. En el punto 1 se muestran todos los conocimientos algebraicos de utilidad en la Teoría de Códigos Cíclicos. Entre otros, será de especial utilidad la descripción de la estructura de anillos de polinomios y sus ideales. Cómo construir la extensión de un cuerpo a partir de polinomios irreducibles, el cálculo de polinomios mínimos de un elemento tan necesario para la construcción de códigos BCH, y la factorización de x^n-1 imprescindible para el estudio de todos los códigos cíclicos de longitud n. En el punto 2 aplicaremos los conocimientos adquiridos en el punto 1 para el cálculo de los códigos cíclicos en un anillo de polinomios del tipo $F_q[x]/(x^n-1)$. Mostraremos cómo las operaciones básicas de codificación y decodificación se puede plasmar en un circuito digital y veremos las conexiones de los códigos cíclicos como ideales en anillos de polinomios con códigos cíclicos como subespacios vectoriales. Veremos también que al igual que ocurre con los códigos lineales como subespacios vectoriales, los códigos cíclicos en el anillo de polinomios se puede transformar para que sean códigos sistemáticos. Además, definiremos algunos teoremas que nos permitirán discutir sobre los parámetros más importantes de los códigos cíclicos.*

5.1. Introducción

Códigos cíclicos son una importante clase de códigos por su rica estructura algebraica, por su eficiente implementación y por ser equivalente a un gran número de códigos clásicos.

Definición 5.1.1. *Un código C es cíclico si y sólo si C es lineal y si para cualquier palabra $(a_0, a_1, \ldots, a_{n-1}) \in C$, $a_{n-1}, a_0, \ldots, a_{n-2}) \in C$.*

Ejemplo 5.1.1. *Los siguientes dos códigos son códigos cíclicos o equivalentes a códigos cíclicos.*

- $C = \{000, 101, 011, 110\}$
- $C = \{0000, 1001, 0110, 1111\}$. *Es equivalente a un código cíclico.*

Ahora consideremos la palabra $c_0 \ldots c_{n-1} \in C$ como el siguiente polinomio $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$

5.1.1. Polinomios

Sea $F_q[x]$ el anillo de polinomios con coeficientes en F_q un cuerpo finito de q elementos. Si $f(x) = f_0 + f_1 x + \ldots f_m x^m$ es un polinomio y $f_m \neq 0$, entonces m es llamado el grado de $f(x)$, y a f_m se le llama el líder del polinomio. Si $f_m = 1$, entonces decimos que el polinomio es mónico.

Un polinomio $b(x)$ es divisible por $d(x)$ y $d(x)$ es un factor de $b(x)$ si existe un $q(x)$ tal que $b(x) = q(x)d(x)$. Si $d(x)$ es un factor de $b(x)$, entonces $cd(x)$ también es un factor para $c \neq 0 \in GF(q)$.

Definición 5.1.2. *El máximo común divisor de dos polinomios, $a(x)$ y $b(x)$, es el polinomio mónico de mayor grado que divide a ambos.*

Definición 5.1.3. *El mínimo común múltiplo de dos polinomios, $a(x)$ y $b(x)$, es el polinomio mónico de menor grado tal que $a(x)$ y $b(x)$ lo dividen.*

Teorema 5.1.1. *Si $a(x)$ y $b(x)$ son dos polinomios con $mcd(a, b) = 1$, entonces existen dos polinomios $s(x)$ y $t(x)$ tal que*

$$s(x)a(x) + t(x)b(x) = 1$$

Sea $f(x)$ un polinomio de grado m sobre $GF(q)$ para $m \geq 2$. Si $(x - a)$ es un factor de $f(x)$ con $a \in GF(q)$, entonces a es una raíz de $f(x)$ y $f(a) = 0$. Un polinomio *irreducible* no tiene raíces en $GF(q)$.

Definición 5.1.4. *Dos polinomios $g(x), h(x)$ en $F_q[x]$, se dicen que son congruentes módulo $f(x)$, y se denota por*

$$g(x) \equiv_{f(x)} h(x)$$

si y sólo si $g(x) - h(x)$ es divisible por $f(x)$.

5.1.2. Cuerpo de Galois

Sea $f(x)$ un polinomio irreducible de grado m sobre $GF(q)$. Sea $S = \{b(x)|deg(b(x)) < m\}$, con la adición y multiplicación módulo $f(x)$. A S lo notaremos por $F_q[x]/f(x)$ o $GF(q)[x]/f(x)$

Veamos algunas propiedades

Definición 5.1.5. *Un polinomio es irreducible si no se puede escribir como productos de polinomios de menor grado.*

Teorema 5.1.2. *$F_q[x]/f(x)$ tiene estructura de anillo (es muy similar a Z_m).*

Teorema 5.1.3. *$F_q[x]/f(x)$, con $f(x)$ irreducible tiene estructura de cuerpo.*

Demostración. Veamos que $a(x) \in F_q[x]/f(x)$ tiene inverso. Ya que $f(x)$ es irreducible, mcd$(a(x), f(x)) = 1$, luego existe un $s(x), t(x)$ tal que $a(x)s(x) + t(x)f(x) = 1$. Por definición de polinomios congruentes, $a(x)s(x) \text{mod} f(x) = 1$. Si el grado de $s(x)$ es mayor que $m = gr(f(x))$, sea $s'(x) = s(x) \ mod \ f(x)$. Luego, si $a(x)s(x) \text{ mod } f(x) = 1 \Rightarrow a(x)(s(x) \text{ mod } f(x)) \text{ mod } f(x) = 1 \Rightarrow a(x)s'(x) \text{ mod } f(x) = 1$ y $gr(s'(x)) < m$ □

Teorema 5.1.4. *Si $f(x)$ es reducible, entonces $F_q[x]/f(x)$ es un anillo pero no un cuerpo.*

Demostración. Si $f(x)$ es reducible, entonces $f(x) = a(x)b(x)$. Entonces $a(x)b(x) \equiv_{f(x)} 0$ con $a(x) \neq 0 \neq b(x)$. Si $a(x)$ tuviera inverso, entonces $a^{-1}(x)a(x) \equiv_{f(x)} 1$ y $a^{-1}(x)a(x)b(x) \equiv_{f(x)} 0$ y $b(x) \equiv_{f(x)} 0$. □

Definición 5.1.6. *Un anillo tiene característica n si n es el menor natural tal que $1 + 1 + \overset{n}{\ldots} + 1$. Si ésto último nunca ocurre, entonces decimos que la característica es cero.*

Obsérvese que $Char(GF(q^n)) = q$.

Ejemplo 5.1.2. 1. *Sea $f(x) = x^2 + x + 1$ sobre $GF(2)$. Entonces*

$$GF(2^2) = GF(2)[x]/f(x) = \{0, 1, x + 1\}$$

2. *Sea $f(x) = x^2 + 2x + 2$ sobre $GF(3)$, entonces*

$$GF(3^2) = GF(3)[x]/f(x) = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}$$

Nótese que la adición se realiza con característica 3, es decir, $1 + 2 = 0, 2 + 2 = 1, 2x + x = 0$ y $2x + 2x = x$. Y la multiplicación se realiza módulo $x^2 + 2x + 2$, es decir, $x^2 = -2x - 2 = x + 1, x(x + 1) = x^2 + x = 2x + 1$ y $(x + 1)(x + 2) = x^2 + 2 = x + 1 + 2 = x$. Complete la tabla de la suma y la multiplicación para este cuerpo.

Lema 5.1.1. *Cualquier polinomio verifica las siguientes propiedades*

1. *Un polinomio $f(x)$ tiene como factor a $(x - a)$ si y sólo si $f(a) = 0$.*
2. *Un polinomio de grado 2 o 3 es irreducible si y sólo si $f(a) \neq 0$ para cualquier $a \in F_q$.*
3. $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$

Veamos ahora otra forma de representar los cuerpos.

Ejemplo 5.1.3. *Sea $f(x) = x^2 + x + 1$ sobre $GF(2)$. Como se puede observar no tiene raíces en $GF(2)$, pero si en la extensión del cuerpo $GF(2^2)$. Llamemos α a dicha raíz. Luego $f(\alpha) = 0 = \alpha^2 + \alpha + 1$, es decir, $\alpha^2 = -\alpha - 1 = \alpha + 1$ ($GF(2^2)$ tiene característica 2). A esta última ecuación le llamamos ecuación característica. Luego $GF(2^2) = \{0, \alpha^0 = 1, \alpha^1 = \alpha, \alpha^2 = \alpha + 1\}$. Obsérvese que $GF(2^2)^*$ es un grupo multiplicativo generado por α, lo cual simplifica la búsqueda del inverso de cualquier elemento del cuerpo.*

Ejemplo 5.1.4. *Sea ahora $f(x) = x^2 + 2x + 2$ un polinomio irreducible sobre $GF(3)$. Sea α su raíz en $GF(3^2)$. Entonces*

$$\begin{aligned}
\alpha^0 &= 1 \\
\alpha^1 &= \alpha \\
\alpha^2 &= 1 + \alpha \\
\alpha^3 &= \alpha(1+\alpha) = \alpha + \alpha + 1 = 2\alpha + 1 \\
\alpha^4 &= \alpha\alpha^3 = 2\alpha^2 + \alpha = 2(\alpha+1) + \alpha = 2\alpha + 2 + \alpha = 2 \\
\alpha^5 &= \alpha\alpha^4 = 2\alpha \\
\alpha^6 &= \alpha\alpha^5 = 2 + 2\alpha \\
\alpha^7 &= \alpha\alpha^6 = \alpha(2\alpha+2) = 2\alpha^2 + 2\alpha = 2(\alpha+1) + 2\alpha = 2\alpha + 2 + 2\alpha = \alpha + 2 \\
\alpha^8 &= \alpha\alpha^7 = \alpha^2 + 2\alpha = \alpha + 1 + 2\alpha = 1
\end{aligned}$$

Luego $GF(3^2) = \{0, 1, \alpha, \alpha^2 = 1+\alpha, \alpha^3 = 2\alpha+1, \alpha^4 = 2, \alpha^5 = 2\alpha, \alpha^6 = 2\alpha+2, \alpha^7 = \alpha+2\}$. Escrito de esta forma y teniendo en cuenta que $\alpha^8 = 1$, la búsqueda de cualquier inverso es muy sencillo. Por ejemplo, el inverso de $2\alpha + 2 = \alpha^6$ es $\alpha^2 = 1 + \alpha$. Ya que $\alpha^6\alpha^2 = (2+2\alpha)\alpha^2 = 2\alpha^2 + 2\alpha^3 = 2(1+\alpha) + 2(2\alpha+1) = 2 + 2\alpha + 4\alpha = 6\alpha + 4 = 1$

Definición 5.1.7. *Sea α una raíz de $f(x)$, un polinomio irreducible de grado m sobre $GF(q)$. Si α genera $GF(q^m)^*$, todos los elementos no nulos de $GF(q^m)$, entonces α es un elemento primitivo de $GF(q^m)$ y $f(x)$ un polinomio primitivo.*

Ejemplo 5.1.5. *Sea $f(x) = x^2 + 1$ irreducible en $GF(3)$. Si α es su raíz en $GF(3^2)$, entonces $f(\alpha) = 0 = \alpha^2 + 1$ y la ecuación característica es $\alpha^2 = 2$. El grupo cíclico generado por α viene dado por*

$$< \alpha >= \{\alpha, \alpha^2 = 2, \alpha^3 = 2\alpha, \alpha^4 = 1\}$$

Luego α no genera a $GF(3^2)^*$ y por lo tanto no es un elemento primitivo. Aun así, el conjunto

$$S = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$$

bajo la adición y multiplicación módulo $f(x) = \alpha^2 + 1$, tiene la misma estructura que $GF(3^2)$.

5.2. Códigos Cíclicos

Sea ahora $f(x) = x^n - 1$ y consideremos el anillo de polinomios $F_q[x]/(x^n - 1)$. Entonces $x^n \equiv 1 \ (mod\ x^n - 1)$. Luego podemos reducir cualquier polinomio módulo $x^n - 1$ reemplazando x^n por 1, x^{n+1} por x, etc.

Ahora identifiquemos un vector $a_0, a_1, ..., a_{n-1} \in V(n, q)$ con el polinomio

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \text{ en } F[x]/(x^n - 1)$$

Entonces

$$V(n, q) \cong F[x]/(x^n - 1)$$

Ahora, si multiplicamos $a(x)$ por x, obtenemos $xa(x) = a_0x + a_1x^2 + a_2x^3 + \cdots + a_{n-1}x^n = a_{n-1} + a_0x + a_1x^2 + a_2x^3 + \cdots + a_{n-2}x^{n-2}$. Es decir, si consideramos $a(x)$ como una palabra de un código cíclico, multiplicar por x^i es equivalente a ciclar dicha palabra i veces.

Teorema 5.2.1. *Un código C en $F[x]/(x^n - 1)$ es cíclico si y solo si verifica*

Polinomio Generador	Código en $F[x]/(x^3-1)$	Código en $V(3,2)$
1	Todo $F[x]/(x^3-1)$	Todo $V(3,2)$
$x+1$	$\{0, 1+x, x+x^2, 1+x^2\}$	$\{000, 110, 011, 101\}$
x^2+x+1	$\{0, 1+x+x^2\}$	$\{000, 111\}$
x^3-1	0	$\{000\}$

Cuadro 5.1: Códigos cíclicos en $F[x]/(x^3-1)$

i) $a(x), b(x) \in C \Rightarrow a(x)+b(x) \in C$

ii) $a(x) \in C$ *y* $r(x) \in F[x]/(x^n-1) \Rightarrow r(x)a(x) \in C$

Corolario 5.2.1. *Todo ideal en* $F[x]/(x^n-1)$ *es un código cíclico.*

Teorema 5.2.2. *Sea* C *un código cíclico. Entonces*

i) Existe un uńico polinomio mónico $g(x)$ *de menor grado in* C

ii) $C =< g(x) >$

iii) $g(x)$ *es un factor de* x^n-1

Demostración.

1. Supongamos que C tiene dos polinomios mónicos de menor grado r, $g_1(x)$ y $g_2(x)$. Entonces $g_1(x)-g_2(x)$ es un elemento de C de grado menor que r. Si multiplicamos $g_1(x)-g_2(x)$ por el inverso del coeficiente, obtenemos un polinomio mónico de C de grado menor que r.

2. Sea $g(x)$ el polinomio mónico de menor grado de C, con $gr(g(x))=r$. Sea $a(x) \in C$. Veamos que $a(x)$ es un múltiplo de $g(x)$. De no ser así, $a(x)=q(x)g(x)+r(x)$ con $a(x), q(x)g(x) \in C$, luego $r(x)=a(x)-q(x)g(x) \in C$ y $gr(r(x)) < r$. Luego existiría un polinomio mónico de menor grado de r, por lo que $r(x)=0$.

3. De no ser así, $x^n-1=q(x)g(x)+r(x)$. Ahora bien, en $F_q[x]/(x^n-1)$, $x^n-1 \equiv 0$ y $q(x)g(x)=r(x) \in C$. Luego $r(x)=0$.

□

Al polinomio $g(x)$ del teorema anterior se le llama polinomio generador de C.

Ejemplo 5.2.1. *Códigos cíclicos de longitud 3 en GF(2) (ver tabla 5.1).*

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

Lema 5.2.1. *Sea* $g(x)=g_0+g_1x+g_2x^2+\cdots+g_rx^r$ *un polinomio generador de un código cíclico. Entonces* $g_0 \neq 0$.

Demostración. Sea $g_0=0$, entonces $x^{n-1}g(x)=x^{-1}g(x)$ es una palabra de C de grado $r-1$, pero si $g(x)$ es el generador, entonces $g(x)$ debería ser el polinomio de menor grado de C. □

5.3. Codificación

En $F[x]/(x^n-1)$ basta con multiplicar por el polinomio de datos por el polinomio generador módulo (x^n-1) generador.

Teorema 5.3.1. *Si C es un código cíclico con polinomio generador $g(x)$, y $gr(g(x)) = r$, entonces C tiene dimensión $n-r$. Es decir,*

$$C =< g(x) >= \{f(x)g(x) | deg(f(x)) < n-r\}$$

Demostración.

$$< g(x) >= \{f(x)g(x) | f(x) \in F_q[x]/x^n - 1\}$$

. Veamos que podemos restringir $f(x)$ a los polinomios de grado menor que $n-r$.

Sabemos que $g(x)|x^n-1$, luego $x^n-1 = g(x)h(x)$. Dividamos $f(x)$ por $h(x)$. Entonces

$$f(x) = q(x)h(x) + r(x)$$

con $gr(r(x)) < n-r$. Ahora bien, $f(x)g(x) = q(x)h(x)g(x) + r(x)g(x) = q(x)(x^n-1) + r(x)g(x)$. Si hacemos los cálculos en $F_q[x]/x^n-1$, $f(x)g(x) = r(x)g(x)$ módulo x^n-1 □

Ya que todo código cíclico es lineal, como espacio vectorial, tendrá una matriz generadora.

Teorema 5.3.2. *Si $g(x) = g_0, g_1x + \cdots + g_rx^r$ es el polinomio generador de C, entonces la matriz generadora G viene dado por*

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & g_2 & \dots & g_r & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & & & \ddots & \\ 0 & 0 & \dots & 0 & g_0 & g_1 & g_2 & \dots & g_r \end{bmatrix}$$

Demostración. Como hemos visto por el Teorema 5.3.1, $Dim(C) = n-r$. Luego como $S = \{g(x), xg(x), \dots, x^{n-r-1}g(x)\}$ son linealmente independientes, el conjunto S es una base como espacio vectorial para C. Si representamos cada uno de estos elementos como vectores, obtenemos la matriz del teorema. □

Ejemplo 5.3.1. *Matrices generadoras de todos los códigos cíclicos ternarios de longitud 4 (ver tabla 5.2).*

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

Teorema 5.3.3. *Un polinomio mónico $p(x) \in F_q[x]/x^n - 1$ es el generador de un código cíclico si y sólo si $p(x)|x^n - 1$*

Demostración. Ya sabemos que si C es cíclico, entonces $p(x)|x^n-1$. Veamos la otra implicación. Supongamos que $C =< p(x) >$ tiene otro generador, y llamémoslo $g(x) \neq p(x)$. Ya que ambos polinomio son mónicos y $g(x)$ es el de menor grado, $gr(p(x)) > gr(g(x))$. Por hipótesis

$$x^n - 1 = p(x)f(x)$$

Polinomio Generador	Matriz generadora
1	$[I_1]$
$x-1$	$\begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}$
$x+1$	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$
x^2+1	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
$(x-1)(x+1)=x^2-1$	$\begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$
$(x-1)(x^2+1)=x^3-x^2+x-1$	$\begin{bmatrix} -1 & 1 & -1 & 1 \end{bmatrix}$
$(x+1)(x^2+1)=x^3+x^2+x+1$	$\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$
$x^4-1=0$	$\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$

Cuadro 5.2: Matrices generadoras de los códigos cíclicos en $F_2[x]/(x^4-1)$

Por otra parte, ya que $g(x) \in < p(x) >$, tenemos que

$$g(x) \equiv a(x)p(x)$$

para algún polinomio $a(x)$. Ahora si multiplicamos por $f(x)$, $g(x)f(x) \equiv a(x)p(x)f(x) \equiv a(x)(x^n-1) \equiv 0$. Pero $gr(g(x)f(x)) < gr(p(x)f(x)) = n$ y $g(x)f(x) = 0$, lo cual es imposible. Luego $p(x) = g(x)$. □

Teorema 5.3.4. *Sea $C_1 =< g_1(x) >$ y $C_2 =< g_2(x) >$ dos códigos cíclicos en $F_q[x]/x^n-1$. Entonces*

1. *$C_1 \subset C_2$ si y sólo si $g_2(x)|g_1(x)$.*
2. *$C_1 \cap C_2 = mcm(g_1(x), g_2(x))$*
3. *$C_1 + C_2 =< mcd(g_1(x), g_2(x))$*

5.4. Decodificación

Sea $g(x)$ el polinomio generador de un $[n, n-r]$-código (r grado de $g(x)$). Entonces $x^n - 1 = g(x)h(x)$ y $h(x)$ es el **polinomio de chequeo** con grado $n-r$.

Como se puede observar, si $c(x)$ es una palabra del código cíclico, entonces $c(x)h(x) = 0$. Esto mismo no tiene porqué ocurrir en $V(n,q)$, ya que el producto de polinomios no es equivalente al producto de vectores en un espacio vectorial.

Teorema 5.4.1. *Sea $h(x)$ el polinomio de chequeo de un código cíclico.*

1. *El código C puede describirse por*

$$C = \{p(x) \in F[x]/(x^n-1) | p(x)h(x) \equiv 0\}$$

2. *Si* $h(x) = h_0 + h_1 x + \cdots + h_{n-r}x^{n-r}$*, su matriz de paridad será*

$$H = \begin{bmatrix} h_{n-r} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_{n-r} & \dots & h_0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & & & \ddots & \\ 0 & 0 & \dots & 0 & h_{n-r} & \dots & h_0 \end{bmatrix}$$

3. $C^{\perp}$ *tiene como polinomio generador a*

$$h^{\perp}(x) = x^{n-r}h(x^{-1}) = h_0 x^{n-r} + h_1 x^{n-r-1} + \cdots + h_{n-r}$$

Demostración.

1. Sea $g(x)$ el polinomio generador de C.Si $p(x) \in C$, entonces $p(x) = f(x)g(x)$ para algún polinomio $f(x) \in F_q[x]/x^n - 1$. Luego

$$p(x)h(x) = f(x)g(x)h(x) = p(x)(x^n - 1) \equiv 0$$

Por otro lado, si $p(x) \in F_q[x]/(x^n - 1)$ y $p(x)h(x) \equiv 0$, supongamos que $p(x)$ no es divisible por $g(x)$, entonces

$$p(x) = q(x)g(x) + r(x)$$

con $gr(r(x)) < r$ ($gr(g(x)) = r$. Si multiplicamos por $h(x)$ tenemos

$$p(x)h(x) = q(x)g(x)h(x) + r(x)h(x)$$

Es decir, $r(x)h(x) \equiv 0$. Pero $gr(r(x)h(x)) < r + (n - r) = n$, de lo que se deduce que $r(x)h(x) = 0$ y $r(x) = 0$

2. Si $c(x) \in C$, entonces $c(x)h(x) \equiv 0$. Ahora, $gr(c(x)h(x)) < 2n - r$, luego los coeficientes de $x^{n-r}, x^{n-r+1}, \dots, x^{n-1}$ deben ser ceros, lo cual nos proporciona el siguiente sistema de ecuaciones

$$\begin{aligned} c_0 h_{n-r} + c_1 h_{n-r-1} + \cdots + c_{n-r} h_0 &= 0 \\ c_1 h_{n-r} + c_2 h_{n-r-1} + \cdots + c_{n-r+1} h_0 &= 0 \\ \vdots \quad & \vdots \\ c_{r-1} h_{n-r} + c_r h_{n-r-1} + \cdots + c_{n-1} h_0 &= 0 \end{aligned}$$

Lo cual es equivalente a $(c_0 c_1 \dots c_{n-1})H^T = 0$. Esto quiere decir que H genera un código C' ortogonal a C, pero no sabemos si es el dual, es decir, $C' \subset C^{\perp}$. Pero ya que $h_{n-r} \neq 0$, la dimensión de C' es r, luego tiene la misma dimensión del dual y $C' = C$

3. Si $h^{\perp}(x)$ divide a $x^n - 1$, entonces el código cíclico $< h^{\perp}(x) >$ tendrá como matriz de paridad a H, y por lo tanto $< h^{\perp}(x) >= C^{\perp}$. Ahora bien,

$$h(x)g(x) = x^n - 1$$

Luego

$$h(x^{-1})g(x^{-1} = x^{-n} - 1$$

Lo cual se puede escribir como

$$x^{n-r}h(x^{-1})x^r g(x^{-1}) = 1 - x^n$$

lo cual demuestra que $h^{\perp}(x) | x^n - 1$

□

Al polinomio del último punto del teorema anterior, lo llamamos polinomio recíproco y posee las siguientes propiedades

1. $(h^{\perp})^{\perp}(x) = h(x)$
2. Si $h(x)$ es irreducible $h^{\perp}(x)$ también lo es.
3. Si α es un cero de $h(x)$ de multiplicidad n, entonces α^{-1} es un cero de $h^{\perp}(x)$ con la misma multiplicidad.

Teorema 5.4.2. *Un código cíclico detecta todos los errores simples.*

Demostración. Sea $u(x) \in C =< g(x) >$, entonces $u(x) = a(x)g(x)$ con $gr(a(x)) < n - r$. Luego si α es una raíz de $g(x)$, $g(\alpha) = 0$, también de $u(x)$.

Por otra parte, ocurre que los polinomios de un código cíclico son los polinomios no nulos que tienen las mismas raíces que el polinomio generador del código con la misma o mayor multiplicidad.

Ahora sea $e(x) = x^i$ el error cometido. La única raíz de $e(x^i)$ es $x = 0$. Por otra parte, $g(x)$ tiene como término independiente $g_0 \neq 0$, $g(0) \neq 0$. Si $b(x) = a(x) + e(x)$ es la palabra recibida, $S(b(x)) = S(e(x)) = e(x) \bmod g(x) \neq 0$ □

Teorema 5.4.3. *Si el polinomio generador de un código cíclico binario C es de la forma $g(x) = (x^h - 1)m(x)$ para algún $h > 0$, entonces todos los errores de peso impar son detectables.*

Demostración. Si $g(x) = (x^h - 1)m(x)$, entonces $g(1) = 0$, pero $e(1) \neq 0$. Luego $g(x)$ no puede ser un múltiplo de $g(x)$ y $S(e(x)) = e(x) \bmod g(x) \neq 0$ □

Definición 5.4.1. *Un polinomio de error de la forma $e(x) = x^i + x^j$ se denomina un error doble de distancia $|i - j|$.*

Teorema 5.4.4. *Si el polinomio generador es múltiplo de un polinomio primitivo de grado s, todos los errores dobles de distancia menor que $2^s - 1$ son detectables.*

Demostración. Si $e(x) = x^i + x^j = x^j(x^{i-j} + 1)$, como ni x^j ni $x^{i-j} + 1$ (cuando $i - j < 2^s - 1$) son, por definición, múltiplos de $g(x)$, $e(x)$ no es divisible por $g(x)$ □

Corolario 5.4.1. *Si $g(x)$ contiene como factor a un polinomio primitivo de grado s con $n \neq 2^s - 1$, todos los errores dobles son detectados.*

Definición 5.4.2. *Un polinomio error (binario) es una ráfaga de longitud s si es posible escribirlo como $x^i(1 + e_1x + e_2x^2 + \cdots + x^{s-1}) \bmod x^n - 1$ con $e_j \in GF(2)$ y s es el menor entero con esta propiedad.*

Ejemplo 5.4.1. 010001 *($e(x) = 1 + x^4$) no es una ráfaga de longitud 5, sino 3 ya que* 101000 *o* 000101 *son otras formas de escribirlo, $e(x) = x^4(1 + x^2) \bmod x^6 - 1$.*

Teorema 5.4.5. *Un código cíclico binario con parámetros $[n, k]$ detecta todas las ráfagas de longitud menor a $n - k$.*

Demostración. Sea $x^i(1 + e_1x + e_2x^2 + \cdots + x^{s-1}) \bmod x^n - 1$. Su síndrome será

$$S(e(x)) = x^i(1 + e_1x + e_2x^2 + \cdots + x^{s-1}) \bmod g(x)$$

x^i no es un factor de $g(x)$ y $(1 + e_1x + e_2x^2 + \cdots + x^{s-1})$ para $s < n - k$ tampoco. Luego $e(x)$ no es divisible por $g(x)$. Nótese que en este caso, $gr(g(x)) = n - k$ ya que estamos hablando de un $[n, k]$-código cíclico. □

Ejemplo 5.4.2. *Sea*

$$g(x) = x^{16} + x^{12} + x^5 + 1 = (x+1)(x^{15} + x^{14} + x^{13} + x^{12} + x^4 + x^3 + x^2 + x + 1$$

Además $(x+1)|x^{2^{15}-1} + 1$ *y* $2^{15-1} = 32767$. *Luego,* $C =< g(x) >$ *(*$n = 32767$*).*

1. *Detecta errores simples.*
2. *Detecta los errores impares (contiene* $x + 1$*)).*
3. *Detecta los errores dobles ya que* $x^{15} + x^{14} + \cdots + x^2 + x + 1$ *es un polinomio primitivo de grado* 15 *y* $2^{15} - 1 \geq 32767$.
4. *Detecta las ráfagas de longitud* ≤ 16.

5.5. Códigos cíclicos en su forma estándar

Las matrices generadoras y de paridad obtenidas para los códigos cíclicos no están en su forma estándar. Es decir, si codificamos la palabra $u(x) = d(x)g(x)$, donde $d(x)$ es el polinomio de datos y $g(x)$ el polinomio generador, el resultado son palabras que no están en su forma estándar o sistemática. Veamos de que forma podemos obtener un código cíclico sistemático.

Sea $d(x)$ el dato que queremos codificar en un (n, k)-código cíclico C, cuyo polinomio generador es $g(x)$ de grado r.

Multiplicamos $d(x)$ por x^r y dividimos por $g(x)$.

$$d(x)x^r = g(x)q(x) + r(x)$$

con $gr(r(x)) < r$ Si llamamos $u(x) = g(x)q(x)$ y despejamos

$$u(x) = d(x)x^r - r(x) = g(x)q(x)$$

y $u(x)$ es una palabra del código ya que es un múltiplo del polinomio generador, donde $d(x)x^r$ forman los bits de información y $r(x)$ los de paridad (fíjese que $d(x)x^r$ ocupa siempre las posiciones más significativas de $u(x)$, y $r(x)$ las menos significativos).

Ejemplo 5.5.1. *Sea* $x^7 - 1 = (x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$ *y* $g(x) = x^3 + x + 1$ *el polinomio generador del código en cuestión. En la tabla 5.3 y 5.4 podemos observar la codificación de los datos en su forma estándar y no estándar.*

5.6. Decodificación

El algoritmo de decodificación sigue siendo el mismo que para códigos lineales, salvo que ahora, el síndrome viene dado por

$$S(y(x)) = y(x) mod g(x)$$

Obsérvese, que si $u(x) \in C$, entonces $u(x) = a(x)g(x)$ y al dividir por $g(x)$ el resto será cero. Si a $u(x)$ le a nadimos un error $e(x)$,

$$S(u(x) + e(x)) = (a(x)g(x) + e(x))\text{mod}g(x) = a(x)g(x)\text{mod}g(x) + e(x)\text{mod}g(x) = S(e(x))$$

		Código como polinomios	Código como vectores
$0.g(x)$	$=$	0	0000000
$1.g(x)$	$=$	x^3+x+1	0001011
$x.g(x)$	$=$	x^4+x^2+x	0010110
$(x+1)g(x)$	$=$	$x^4+x^3+x^2+1$	0011101
$x^2.g(x)$	$=$	$x^5+x^3+x^2$	0101100
$(x^2+1).g(x)$	$=$	x^5+x^2+x+1	0100111
$(x^2+x).g(x)$	$=$	$x^5+x^4+x^3+x$	0111010
$(x^2+x+1).g(x)$	$=$	x^5+x^4+1	0110001
$x^3.g(x)$	$=$	$x^6+x^4+x^3$	1011000
$(x^3+1).g(x)$	$=$	x^6+x^4+x+1	1010011
$(x^3+x)g(x)$	$=$	$x^6+x^3+x^2+x$	1001110
$(x^3+x+1).g(x)$	$=$	x^6+x^2+1	1000101
$(x^3+x^2).g(x)$	$=$	$x^6+x^5+x^4+x^2$	1101001
$(x^3+x^2+1).g(x)$	$=$	$x^6+x^5+x^4+x^3+x^2+x+1$	1111111
$(x^3+x^2+x).g(x)$	$=$	x^6+x^5+x	1100010
$(x^3+x^2+x+1).g(x)$	$=$	$x^6+x^5+x^3+1$	1101001

Cuadro 5.3: Codificación no estándar

$d(x)$	d	$u(x)=d(x)x^3-r(x)$	u
0	0000	0	0000000
1	0001	$(1)x^3+x+1$	0001011
x	0010	$(x)x^3+x^2+x$	0010110
$x+1$	0011	$(x+1)x^3+x^2+1$	0011101
x^2	0100	$(x^2)x^3+x^2+x+1$	0100111
x^2+1	0101	$(x^2+1)x^3+x^2$	0101100
x^2+x	0110	$(x^2+x)x^3$	0110001
x^2+x+1	0111	$(x^2+x+1)x^3$	0111010
x^3	1000	$(x^3)x^3$	1000101
x^3+1	1001	$(x^3+1)x^3$	1001110
x^3+x	1010	$(x^3+x)x^3$	1010011
x^3+x+1	1011	$(x^3+x+1)x^3$	1011000
x^3+x^2	1100	$(x^3+x^2)x^3$	1100010
x^3+x^2+1	1101	$(x^3+x^2+1)x^3$	1101001
x^3+x^2+x	1110	$(x^3+x^2+x)x^3$	1110100
x^3+x^2+x+1	1111	$(x^3+x^2+x+1)x^3$	1111111

Cuadro 5.4: Codificación estándar o sistemática

Líder	Síndrome
0	0
1	1
x	x
x^2	x^2
x^3	$x+1$
x^4	x^2+x
x^5	x^2+x+1
x^6	x^2+1

Cuadro 5.5: Array de síndromes

Líder	Síndrome
x^6	x^2+1

Cuadro 5.6: Tabla de Síndromes para un SEC cíclico

Ejemplo 5.6.1. *Sea $g(x) = x^3 + x + 1$ el generador de un código en $F_2[x]/(x^7 - 1)$. El array de síndromes de todos los errores de peso 1 se pueden observar en la tabla 5.5.*

5.7. Decodificación de un SEC

Si nuestro código es del tipo SEC, podemos simplificar la decodificación. La idea consiste en que si es posible detectar si hay un error en el último bit,entonces si no lo hay, podemos ciclar la palabra enviada y pasar el mismo test al último bit de la nueva palabra. En este caso, la decodificación es más óptima ya que sólo tenemos que almacenar un error o líder y su síndrome. Aunque el número de comparaciones sigue siendo el mismo, el requerimientos de almacenamiento son mucho menores. El array de síndromes a la que hacemos referencia se puede observar en la tabla 5.6

Si recibimos $u(x) = x^6 + x + 1$.

$S(u(x)) = x^2 + x$, luego el último bit es correcto.

$x.u(x)$módulo$(x^7 - 1) = x^2 + x + 1$ y $S(x.u(x)) = x^2 + x + 1$, luego no hay un error en la posición 5.

$S(x^2.u(x)) = x^2 + 1$, luego se ha producido un error la cuarta posición.

Teorema 5.7.1. *Sea $C =< g(x) >$. Para cualquier polinomio $u(x) \in F_q[x]/(x^n - 1)$,*

$$syn(x.u(x))mod(x^m - 1)) = syn(x.syn(u(x)))$$

Lema 5.7.1. *Sea C un código cíclico capaz de corregir t errores. Supongamos que se producen menos de t errores en la palabra del código $c(x)$. Si la palabra recibida, $u(x)$ tiene peso menor que t, entonces $e(x) = S(u(x))$.*

5.8. Ejercicios

1. Decidir si los siguientes códigos son cíclicos o equivalentes a un cíclico.
   a) $\{0000, 1100, 0110, 0011, 1001\}$
   b) $\{00000, 10110, 01101, 11011\}$
   c) $\{0000, 1122, 2211\}$
   d) Un código de repetición sobre cualquier alfabeto.
   e) Código binario con todas las palabras de peso par.
   f) Código ternario $\{x \in V(n,3) | w(x) \cong 0(mod 3)\}$
2. Factorizar $x^5 - 1$ sobre $GF(2)$ y determinar todos los códigos cíclicos posibles.
3. Factorizar $x^7 - 1$ sobre $GF(2)$ y determinar todos los códigos binarios de longitud 7.
4. Hacer lo mismo para $x^8 - 1$ sobre $GF(3)$
5. Sea $C =< x + 1 >$ en $F_2[x]/x^3 - 1$. Mostrar que $x^2 + 1$ también lo genera.
6. Calcular todos los códigos cíclicos ternarios de longitud 4. Calcular sus matrices generadoras.
7. Mostrar que el $[7, 4]$-código binario generado por x^3+x+1 y le $[7, 3]$-código binario generado por $x^4 + x^3 + x^2 + 1$ son duales.
8. Mostrar que un polinomio irreducible sobre $GF(2)$ tiene un número impar de coeficientes no nulos.
9. Razonar que para demostrar que un polinomio $p(x)$ es irreducible basta con demostrar que no tiene factores irreducibles de grado $\leq gr(p(x))$.
10. Calcular todos los polinomios irreducibles sobre $GF(2)$ de grado menor o igual a 4. Construir un cuerpo finito de orden 8.
11. Sea $g(x)$ el polinomio generador de un código cíclico binario. ¿ El conjunto de palabras del código $< g(x) >$ es cíclico?. Si lo es, calcular su polinomio generador.
12. Ya que $x^7 - 1$ factoriza en $(x - 1)(x^3 + x + 1)(x^3 + x^2 + 1)$. Calcular los parámetros de todos los códigos cíclicos binarios de longitud 7.
13. Calcular el número de códigos cíclicos de longitud 8 que existen sobre $GF(3)$.
14. Sea $g(x)$ el polinomio generador de un código cíclico binario $Ham(r, 2)$,con $r \geq 3$. Mostrar que $< (x - 1)g(x) >$ genera un código cíclico con parámetros $[2^r - 1, 2^r - 1 - r, 4]$.