Teoría de Códigos y Criptografía

Justo Peralta López
Juan Antonio López Ramos

Universidad de Almería
Departamento de Álgebra y Análisis Matemático

Definición

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

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.

Definiciones

1. 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.
2. 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 $c \neq 0 \in GF(q)$.
3. El máximo común divisor de dos polinomios, $a(x)$ y $b(x)$, es el polinomio mónico de mayor grado que divide a ambos.
4. 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

Si $a(x)$ y $b(x)$ son dos polinomios con $\mathrm{mcd}(a, b) = 1$, entonces existen dos polinomios $s(x)$ y $t(x)$ tal que

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

Definición

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 $GF(q)$.
2. 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 $f(x)$.

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 $GF(q)[x]/f(x)$

Definición

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

Teorema

1. *$F_q[x]/f(x)$ tiene estructura de anillo (es muy similar a Z_m).*
2. *$F_q[x]/f(x)$, con $f(x)$ irreducible tiene estructura de cuerpo.*
3. *Si $f(x)$ es reducible, entonces $F_q[x]/f(x)$ es un anillo pero no un cuerpo.*

Definición

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

Ejemplo

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 $2x + 2x = 0$. Y la multiplicación se realiza módulo $x^2 + 2x + 2$, es decir, $xx^2 = -2x - 2 = x + 1, x(x + 1) = x^2 + x = 2x + 1$ 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

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. $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$

Ejemplo

1. $f(x) = x^2 + x + 1$
2. $f(x) = x^2 + 2x + 2$ un polinomio irreducible sobre $GF(3)$.

Definición

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

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 $GF(3^2)$.

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

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \text{ en } F[x]/(x^n - 1)$$

Entonces

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

Ahora, si multiplicamos $a(x)$ por x, obtenemos
$xa(x) = a_0 x + a_1 x^2 + a_2 x^3 + \cdots + a_{n-1} x^n = a_{n-1} + a_0 x + a_1 x^2 + a_2 x^3 + \cdots + a_{n-2} x^{n-2}$.
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

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

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

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

Teorema

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 $x^n - 1$*

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

Ejemplo

Códigos cíclicos de longitud 3 en GF(2)

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

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	$\{000\}$

Lema

Sea $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_r x^r$ un polinomio generador de un código cíclico. Entonces $g_0 \neq 0$.

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

Teorema

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

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

Teorema

Si $g(x) = g_0, g_1 x + \cdots + g_r x^r$ es el polinomio generador de C, entonces la matriz generadora G viene dado por

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

Ejemplo

Matrices generadoras de todos los códigos cíclicos ternarios de longitud 4.

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

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	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
$(x-1)(x+1) = x^2 - 1$	$\begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$
$(x-1)(x^2+1) = x^3 - x^2 + x - 1$	$\begin{bmatrix} -1 & 1 & -1 & 1 \end{bmatrix}$
$(x+1)(x^2+1) = x^3 + x^2 + x + 1$	$\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$
$x^4 - 1 = 0$	$\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$

Teorema

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

Teorema

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. $C_1 \cap C_2 = \text{mcm}(g_1(x), g_2(x))$
3. $C_1 + C_2 =< \text{mcd}(g_1(x), g_2(x))$

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 $n-r$.
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

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*

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

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

Un código cíclico detecta todos los errores simples.

Teorema

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.

Definición

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

Teorema

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.

Corolario

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

Un polinomio error (binario) es una ráfaga de longitud s si es posible escribirlo como $x^i(1 + e_1 x + e_2 x^2 + \cdots + x^{s-1}) \bmod x^n - 1$ con $e_j \in GF(2)$ y s es el menor entero con esta propiedad.

Ejemplo

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

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

Ejemplo

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.

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

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.

		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

Ejemplo

Codificación en su forma estandar

$d(x)$	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

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 $e(x)$,

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

Ejemplo

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 **??**.

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	$x^2 + 1$

Ejemplo

Líder	Síndrome
x^6	x^2+1

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

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

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 $e(x) = S(u(x))$