MATEMATICA DISCRETA II-2006

códigos cíclicos

Por motivos que resultaran claros en breve, en vez de subscribir las palabras como $w_1...w_n$, las subscribiremos como $w_0...w_{n-1}$.

**1.Definicion :**

*Dada una palabra $w = w_0...w_{n-1}$, definimos la rotación (o* cyclic shift*) de $w$ como la palabra $rot(w) = w_{n-1}w_0...w_{n-2}$. Diremos que un código $C$ es* cíclico *si $C$ es lineal y $rot(w) \in C$ para toda $w \in C$. (A veces a los códigos cíclicos se los llama CRC (Cyclic redundancy code o cyclic redundancy check).*

**2.Ejemplo :**

El código $\{000, 011, 101, 110\}$ es cíclico, pero el código $\{000, 001, 110, 111\}$ no lo es.

Como $rot$ es lineal, tenemos que un código es cíclico sii existe una base de $C$ tal que $rot(w) \in C$ para toda palabra $w$ de la base. En particular, es facil construir códigos cíclicos: basta tomar una palabra $w$ cualquiera, y tomar el espacio vectorial generado por el conjunto $\{w, rot(w), rot^2(w), ..., rot^{n-1}(w)\}$, ,pues como $rot^n(w) = w$, ese conjunto es cerrado por la operacion $rot$, y como genera $C$, podemos extraer una base del mismo que cumple la propiedad anterior. El problema con hacer esto es que no tenemos la menor idea de cual sera la dimension de $C$, por ejemplo. Veremos que podemos elejir la palabra $w$ mas cuidadosamente, de forma tal de obtener una base que consitira basicamente, en las primeras $k$ rotaciónes de $w$. Ademas, esta palabra $w$ especial tendra otras porpiedades que la haran muy efectiva.

Antes de poder seguir, identificaremos las palabras de lonitud $n$ con polinomios de grado menor a $n$:

Dada una palabra $w = w_0...w_{n-1}$, identificaremos $w$ con el polinomio $w(x) = w_o + w_1x + w_2x^2 + ... + w_{n-1}x^{n-1}$, el cual tiene grado menor o igual a $n - 1$.

**3.Ejemplo :**

El código $\{0000, 1010, 0101, 1111\}$ se identifica con el código $\{0, 1 + x^2, x + x^3, 1 + x + x^2 + x^3\}$

**4.WARNING :**

*Existen otras identificaciones posibles, por ejemplo, algunos autores identifican $w = w_0...w_{n-1}$ con $w_0x^{n-1} + w_1x^{n-2} + ... + w_{n-2}x + w_{n-1}$, en este caso,* 1010 *es identificado con $x^3 + x$ en vez de con $1 + x^2$. Moraleja: leer bien las convenciones del libro o articulo que esten leyendo.*

La operacion de suma de palabras miradas como vectores en $\boldsymbol{Z}_2^n$ es la misma que la suma de palabras miradas como polinomios, pues los polinomios tambien se suman coeficiente a coeficiente. ¿Cual es la ventaja entonces de mirarlas como polinomios? Que, miradas como polinomios, podemos *multiplicar y dividir* palabras. Por ejemplo, podemos multiplicar las palabras 1010000 y 0100100 de la siguiente forma:

$$\begin{aligned} 1010000.0100100 &\simeq (1 + x^2)(x + x^4) \\ &= x + x^4 + x^3 + x^6 = x + x^3 + x^4 + x^6 \\ &\simeq 0101101 \end{aligned}$$

Hay un pequeño problema sin embargo: la multiplicacion de dos palabras de longitud $n$ puede dar una palabra de longitud mayor a $n$, por ejemplo, $1010.0110 = (1 + x^2)(x + x^2) = x + x^2 + x^3 + x^4 = 01111$. Pero para eso existen los restos:

**5.Definicion :**

*Si $p(x)$ y $h(x)$ son polinomios, entonces "$p(x)$ mod $h(x)$" denotara el resto de la division de $p(x)$ por $h(x)$.*

Demos un ejemplo y de paso repasemos como se dividian polinomios. Si bien la mayoria lo habra visto en la secundaria para polinomios enteros, el mismo algoritmo es valido para polinomios con coeficientes en $\boldsymbol{Z}_2$, solo que las cuentas son mas faciles:

$$
\begin{array}{l}
x^8+x^7+x^6+x^2+x \quad |\underline{x^4+x^2+x+1} \\
x^8+\quad x^6+x^5+x^4 \qquad x^4+x^3 \\
--------- \\
\quad x^7+x^5+x^4+x^2+x \\
\quad x^7+x^5+x^4+x^3 \\
---------- \\
\qquad\quad x^3+x^2+x
\end{array}
$$

Esto significa que $x+x^2+x^6+x^7+x^8 \bmod (1+x+x^2+x^4) = x+x^2+x^3$.

Tambien diremos que $p(x) \equiv q(x)_{(\bmod\ h(x))}$ si $p(x) \bmod h(x) = q(x) \bmod h(x)$.

Por lo tanto, si queremos multiplicar dos palabras de logitud $n$ y que obtengamos otra vez una palabra de longitud $n$, i.e., multiplicar dos polinomios de grado menor que $n$ y que obtengamos otro polinomio de grado menor que $n$, bastara con multiplicar los polinomios, y luego tomar modulo algun polinomio de grado $n$. Por ejemplo, podriamos tomar el producto modulo $x^n$. Pero sera mejor tomar el producto modulo $1+x^n$.

**6.Definicion :**

*Dadas dos palabras $v$ y $w$, definimos su producto como la palabra equivalente al resto de la division del producto de sus polinomios por $1+x^n$, en simbolos:*

$$v \odot w = v(x)w(x) \bmod (1+x^n)$$

**7.Ejemplos :**

*:*

Observemos que $x^n = 1 \bmod 1+x^n$, que $x^{n+1} = x \bmod 1+x^n$, etc.

$$
\begin{aligned}
1010 \odot 0110 &= (1+x^2)(x+x^2) \bmod 1+x^4 \\
&= x+x^2+x^3+x^4 \bmod 1+x^4 \\
&= 1+x+x^2+x^3 \\
&= 1111
\end{aligned}
$$

$$
\begin{aligned}
10011 \odot 11100 &= (1+x^3+x^4)(1+x+x^2) \bmod 1+x^5 \\
&= 1+x+x^2+x^3+x^4+x^5+x^4+x^5+x^6 \bmod 1+x^5 \\
&= 1+x+x^2+x^6 \bmod 1+x^5 \\
&= 1+x+x^2+x \\
&= 1+x^2 \\
&= 10100
\end{aligned}
$$

**8.Propiedad :**

$$rot(w) = x \odot w(x)$$

*Prueba:*

$$\begin{aligned} x \odot w(x) =& x(w_0 + w_1 x + ... + w_{n-2}x^{n-2} + w_{n-1}x^{n-1}) \bmod 1 + x^n \\ =& w_0 x + w_1 x^2 + ... + w_{n-2}x^{n-1} + w_{n-1}x^n \bmod 1 + x^n \\ =& w_0 x + w_1 x^2 + ... + w_{n-2}x^{n-1} + w_{n-1} \\ =& w_{n-1} + w_0 x + w_1 x^2 + ... + w_{n-2}x^{n-1} \\ =& rot(w) \end{aligned}$$

QED.

**9.Corolario :**

*Sea $C$ un código cíclico y $w \in C$. Si $a(x)$ es un polinomio cualquiera. Entonces $a(x)w(x) \bmod 1 + x^n$ es una palabra de $C$. En particular si $v$ es una palabra cualquiera de $n$ bits (no necesariamente en $C$), entonces $v \odot w \in C$.*

*Prueba:*

Por la propiedad anterior, $x^i w(x) \bmod 1 + x^n = rot^i(w)$, por lo tanto esta en $C$. Y por lo tanto la suma de cosas de la forma $x^i w(x) \bmod 1 + x^n$ esta en $C$, pues $C$ es lineal. Entonces, al ser $a(x)w(x) \bmod 1 + x^n$ suma de cosas de la forma $x^i w(x) \bmod 1 + x^n$, esta en $C$. QED.

**10.Comentario :**

*El hecho de que $C$ es lineal y tiene la propiedad de que $v \odot w \in C$ para toda palabra $w$ de $C$ y toda palabra $v$ de $n$ bits dice que $C$ es lo que se llama en matematica un IDEAL. Entonces, todo código cíclico es un ideal. Pero la reciproca tambien vale: todo ideal es un código cíclico, pues es lineal por la primera propiedad, y $v \odot w \in C$ para toda $v$ implica en particular que $x \odot w \in C$, es decir, $rot(w) \in C$ para toda $w$ en $C$, por lo tanto, $C$ es cíclico.*

**11.Propiedad :**

*Si $C$ es lineal, entonces existe* **un unico** *polinomio no nulo en $C$ de grado minimo.*

*Prueba:*

Supongamos que hubiera dos: $g_1$ y $g_2$. Como son distintos, $g_1 + g_2 \neq 0$. Como $C$ es lineal, $g_1 + g_2$ esta en $C$. Pero el grado de $g_1 + g_2$ es estrictamente menor que el grado de $g_1$ o $g_2$, pues al ser ambos del mismo grado, digamos, $t$, entonces ambos son de la forma $x^t$+cosas de grado mas chico. Por lo tanto, al sumarlos, queda $x^t + x^t$+cosas de grado mas chico, y como estamos en $\mathbb{Z}_2$, $x^t + x^t = 0$.

Entonces, tenemos un polinomio no nulo $g_1 + g_2$ de grado mas chico que el menor grado posible, absurdo. QED.

Esto vale para todo código lineal, en particular para los cíclicos. En el caso de los cíclicos, este único polinomio recibe un nombre especial: se llama el **polinomio generador**. Este nombre viene del hecho de que, en los cíclicos, el genera todo el código, en el siguiente sentido:

**12.Teorema :**

*Sea $g(x)$ el polinomio generador de un código cíclico $C$. Entonces $C$ esta formado por los multiplos de $g(x)$ de grado menor que $n$, es decir:*

$$C = \{p(x) : gr(p) < n \& g(x) | p(x)\}$$

*Prueba:*

Supongamos que $gr(p) < n \& g(x) | p(x)$. Entonces, existe $a(x)$ tal que $p(x) = a(x)g(x)$. Como $gr(p) < n$, entonces $p(x) = p(x) \bmod 1 + x^n$, y asi $p(x) = a(x)g(x) \bmod 1 + x^n \in C$. Con lo que hemos probado una inclusion.

Para ver la otra, sea $p(x) \in C$. Dividamos $p(x)$ por $g(x)$, obteniendo polinomios $q(x)$ y $r(x)$, con $gr(r) < gr(g)$ tal que $p(x) = q(x)g(x) + r(x)$.

Pero entonces, $r(x) = p(x) + q(x)g(x)$. Como $gr(r) < gr(g) < n$, entonces $r(x) = r(x) \bmod 1 + x^n$, por lo tanto $r(x) = p(x) + (q(x)g(x) \bmod 1 + x^n)$, y como tanto $p(x)$ como $q(x)g(x) \bmod 1 + x^n$ estan en $C$,

obtenemos que $r(x)$ esta en $C$. Pero como $gr(r) < gr(g)$, debe ser $r(x) = 0$, es decir, $p(x) = q(x)g(x)$, lo cual dice que $g(x)|p(x)$. QED.

Vemos entonces que el polinomio generador es analogo a la matriz generadora: antes las palabras del codigo eran de la forma $uG$ y ahora son de la forma $u(x)g(x)$. Pero la ventaja es que antes debiamos guardar una matriz $k \times n$, i.e., $kn$ entradas, y luego realizar la multiplicacion matricial, mientras que ahora solo hay que guardar un polinomio (i.e., a lo sumo $n$ entradas, incluso veremos que es menos que eso), y mas aun, multiplicacion por un polinomio es muy facil de implementar, sobre todo en hardware, con shift registers. Por eso son tan populares los códigos cíclicos. Queremos ver "que pinta" debe tener un polinomio generador, en particular, cual es su grado.

**13.Propiedades :**

*Sea $C$ un código cíclico de dimension $k$ y longitud $n$ y sea $g(x)$ su polinomio generador. Entonces:*

a) $gr(g(x)) = n - k$
b) $g(x)$ divide a $1 + x^n$.
c) $g_0 = 1$.

*Prueba:*

a): Sea $t$ el grado de $g(x)$. Observemos que por la propiedad anterior, todo elemento de $C$ es de la forma $q(x)g(x)$ para algun polinomio $q(x)$. Pero como el grado de $q(x)g(x)$ debe ser menor que $n$, debemos tener que el grado de $q(x)$ debe ser menor que $n - t$. Entonces tenemos que para cada polinomio de grado menor que $n - t$ corresponde un polinomio del coidigo, y vicecersa. Asi, la cardinalidad de $C$ es igual a la cardinalidad del conjunto de polinomios de grado menor que $n - t$. Esa cardinaldidad es $2^{n-t}$. Por lo tanto, como la cardinalidad de $C$ es $2^k$, tenemos que $2^k = 2^{n-t}$, por lo tanto $k = n - t$, y el grado de $g(x)$ es $t = n - k$.

b) Dividamos $1 + x^n$ por $g(x)$: $1 + x^n = g(x)q(x) + r(x)$, con grado de $r$ menor que el de $g$. Tomando congruencia módulo $1 + x^n$, tenemos que $0 = (g(x)q(x) \bmod 1 + x^n) + r(x)$ (como el grado de $r$ es menor que el de $g$, que es $n - k$, tenemos que $r(x) \bmod (1 + x^n) = r(x)$). Es decir, $r(x) = g(x)q(x) \bmod 1 + x^n$ que es un elemento de $C$. Como tiene grado menor que $g$, debe ser $r(x) = 0$, y $g$ divide a $1 + x^n$.

c)Por b), sabemos que $1 + x^n = p(x)g(x)$ para algun $p(x)$. Entonces, igualando los coeficientes independientes de $1 + x^n$ y $p(x)g(x)$, tenemos que $1 = p_0 g_0$, lo cual dice que no puede ser $g_0 = 0$, asi que debe ser $g_0 = 1$. QED.

De la propiedad a) deducimos entonces que una base de $C$ viene dada por:
$\{g(x), xg(x), ..., x^{k-1}g(x)\}$, es decir, las primeras $k$ rotaciónes de $g(x)$ (empezando por la rotación "nula"). Con lo cual, una matriz generadora de $C$ es:

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & \cdots & \cdots & \cdots & g_{n-k-1} & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & \cdots & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & \cdots & \cdots & \cdots & \cdots & g_{n-k-1} & g_{n-k} & \cdots & 0 \\ 0 & 0 & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & g_0 & g_1 & \cdots & \cdots & \cdots & \cdots & g_{n-k-1} & g_{n-k} \end{pmatrix}$$

**14.Ejemplo :**

Sea $g(x) = 1 + x^2 + x^3$ con $n = 7$. La matriz geneardora sera:

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

Observar que $G$ no esta en forma estandard, pero es facil llevarla a una forma, ya sea si la queremos con la identidad al comienzo o al final, simplemente reduciendo por filas en la forma obvia (de abajo para arriba

pivoteando en las primeras columnas si queremos la identidad al principio, y de arriba para abajo pivoteando en las ultimas columnas si la queremos al final):

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Por otro lado, seria bueno poder obtener la matriz directamente, sin tener que reducir. Para ellos, observemos que para todo polinomio $p(x)$, el polinomio $p(x) + (p(x) \bmod g(x))$ es claramente congruente a cero modulo $g(x)$, y por lo tanto, si su grado es menor que $n$, esta en el código. En particular, cada uno de los polinomios $f_i(x) = x^{n-k+i-1} + (x^{n-k+i-1} \bmod g(x))$ $i = 1, ..., k$ tienen grado a lo sumo $n-k+k-1 = n-1$ menor que $k$, por lo tanto estan en el código. Y como el grado de $x^{n-k+i-1} \bmod g(x)$ es menor que $n-k$, entonces el grado de cada $f_i$ es exactamente $n-k+i-1$, es decir, los grados son crecientes, por lo que los polinomios son linealmente independientes. Como son $k$, forman una base de $C$. Y si tomamos la matriz generadora cuyas filas son los $f_i$, justamente por ser suma de un $x^j$ mas algo de grado menor que $n-k$, para $j = n-k, ..., n-1$, la matriz nos dara con la identidad a derecha.

Veamos un ejemplo: tomando como antes $g(x) = 1 + x^2 + x^3$ con $n = 7$, debemos calcular los $f_i$. Observemos que $x^3 \equiv 1 + x^2$ (modulo $g(x)$), por lo tanto tenemos, multiplicando sucesivamente por $x$:

$$\begin{aligned} &x^3 \equiv 1 + x^2 \Rightarrow f_1 = (x^3 \bmod g(x)) + x^3 = 1 + x^2 + x^3 \\ &x^4 \equiv x + x^3 \equiv 1 + x + x^2 \Rightarrow f_2 = (x^4 \bmod g(x)) + x^4 = 1 + x + x^2 + x^4 \\ &x^5 \equiv x + x^2 + x^3 \equiv 1 + x \Rightarrow f_3 = (x^5 \bmod g(x)) + x^5 = 1 + x + x^5 \\ &x^6 \equiv x + x^2 \Rightarrow f_4 = (x^6 \bmod g(x)) + x^6 = x + x^2 + x^6 \end{aligned}$$

por lo que la matriz es:

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

que es la misma matriz que habiamos obtenido antes.

Observemos que de $x^6 \equiv x + x^2$ obtenemos $x^7 \equiv x^2 + x^3 \equiv 1$, que es como debe ser porque si $g(x)$ no divide a $1 + x^n$ entonces no puede ser polinomio generador. (i.e., no podemos empezar a hacer esto con cualquier $g$: debe ser un divisisor de $1 + x^n$).

Observemos que si obtenemos la matriz de chequeo de este código a partir de la generadora, tenemos la matriz:

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

i.e., esta es la matriz de un código de Hamming. Asi pues, los Hamming (en algun orden de las columnas) son cíclicos.

Veamos otro ejemplo para que quede claro:

$g(x) = 1 + x^2 + x^3 + x^4$, $n = 7$.

Tenemos:

$$\begin{aligned} x^4 \equiv& 1 + x^2 + x^3 (\sim 1011) \\ x^5 \equiv& x + x^3 + x^4 \equiv 1 + x + x^2 (\sim 1110) \\ x^6 \equiv& x + x^2 + x^3 (\sim 0111) \end{aligned}$$

con lo cual la matriz generadora es:

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

Podemos obtener la matriz de chequeo directamente? En realidad, del teorema que teniamos de como transformar una matriz generadora en una de chuqueo, y de la propiedad anterior, sale directamente:

**15.Teorema :**

*Una matriz de chequeo para $C$ viene dada por la matriz cuyas columnas son los polinomios $x^j \bmod g(x)$, $j = 0, ..., n-1$.*

*Prueba:*

Como dije, mirando la propiedad anterior, sale esta directa. Pero por las dudas, incluyamos una prueba independiente:

Sea $H$ esa matriz. Entonces, (algebra lineal) $(Hw)_i = \sum_j H_{i,j} w_j = (\sum_j H^{(j)} w_j)_i$, es decir la columna $Hw$ es suma de las columnas $w_j H^{(j)}$. Mirando ahora cada columna como un polinomio, tenemos:

$$\begin{aligned} Hw &= \sum_j w_j H^{(j)} \\ &= \sum_j w_j x^j \bmod g(x) \\ &= w(x) \bmod g(x) \end{aligned}$$

Por lo tanto, si $w$ es una palabra de $n$ bits: $w \in Nu(H) \iff Hw = 0 \iff w(x) \bmod g(x) = 0 \iff g(x)|w(x) \iff w(x) \in C$, asi que hemos probado que $H$ es una matriz de chequeo de $C$. QED.

**16.Ejemplo :**

Tenemos que las potencias $x^j \bmod (1 + x^2 + x^3)$ son: $1, x, x^2, 1 + x^2, 1 + x + x^2, 1 + x, x + x^2$ por los calculos realizados anteriormente. Asi,

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

Dijimos que en realidad no queremos tanto la matriz genradora como el polinomio generador puesto que es mas facil guardarlo y operar con el. En realidad, tambien existe un polinomio de chequeo:

**17.Propiedad :**

*Sea $g(x)$ el polinomio generador de un codigo ciclico $C$, y sea $h(x) = \frac{1+x^n}{g(x)}$. ($h(x)$ es un polinomio pues $g(x)|(1 + x^n)$). Entonces $h(x)$ es un polinomio de chequeo de $C$, es decir, $w(x) \in C$ sii $w \odot h = 0$.*

*Prueba:*

Por la definición de $p(x)$, tenemos que $g(x)p(x) = 1 + x^n$. Entonces:

a) Si $w(x) \in C$, existe $p(x)$ tal que $w(x) = p(x)g(x)$. Por lo tanto, $w(x)h(x) = p(x)g(x)h(x) = p(x)(1 + x^n) = 0 \bmod (1 + x^n)$.

b) Sea ahora $w(x)$ de grado menor que $n$ tal que $w(x)h(x) = 0 \bmod (1 + x^n)$. Entonces, existe un polinomio $p(x)$ tal que $w(x)h(x) = p(x)(1 + x^n)$, es decir $w(x)h(x) = p(x)g(x)h(x)$. Dividiendo por $h(x)$, tenemos que $w(x) = p(x)g(x)$ esta en $C$. QED.

**18.Ejemplo :**

Tomando como ejemplo a $g(x) = 1 + x^2 + x^3$ con $n = 7$, y haciendo la division, obtenemos que $h(x) = 1 + x^2 + x^3 + x^4$.