UNIVERSIDAD DE GRANADA

ALGORITMO DE SUGIYAMA PARA CÓDIGOS REED-SOLOMON TORCIDOS

VÍCTOR ESTEBAN BOTA

Trabajo Fin de Grado

Doble Grado en Ingeniería Informática y Matemáticas

Tutores

Gabriel Navarro Garulo

FACULTAD DE CIENCIAS

E.T.S. INGENIERÍAS INFORMÁTICA Y DE TELECOMUNICACIÓN

Granada, a 25 de marzo de 2023

ÍNDICE GENERAL

1

INTRODUCCIÓN A LOS CÓDIGOS LINEALES

Todo el desarrollo de este capítulo está basado en **?** .

1.1 CÓDIGOS LINEALES

Sea $\mathbb{F}_q$ el cuerpo finito de q elementos, denotamos $\mathbb{F}_q^n$ al espacio vectorial de las n-tuplas sobre el cuerpo finito $\mathbb{F}_q$. A los vectores $(a_1, a_2, \cdots, a_n)$ de $\mathbb{F}_q$ generalmente los escribiremos como $a_1 a_2 \cdots a_n$.

Definición 1. Un (n, M) *código* $\mathcal{C}$ sobre $\mathbb{F}_q$ es un subconjunto de $\mathbb{F}_q^n$ de tamaño M. Llamaremos *palabras código* a los elementos de $\mathcal{C}$.

Ejemplo 1.
- En el cuerpo $\mathbb{F}_2$, a los códigos se les conoce como *códigos binarios* y un ejemplo sería $\mathcal{C} = \{00, 01, 10, 11\}$.
- En el cuerpo $\mathbb{F}_3$, a los códigos se les conoce como *códigos ternarios* y un ejemplo sería $\mathcal{C} = \{01, 12, 02, 10, 20, 21, 22\}$.

Si $\mathcal{C}$ es un espacio k-dimensional de $\mathbb{F}_q^n$, entonces decimos que $\mathcal{C}$ es un $[n, k]$ *código linear* sobre $\mathbb{F}_q$ y tiene q^k palabras código. Las dos formas más comunes de representar un código lineal son con la *matriz generadora* o la *matriz de paridad*.

Definición 2. Una *matriz generadora* de un $[n, k]$ *código linear* $\mathcal{C}$ es cualquier matriz $k \times n$ cuyas columnas forman una base de $\mathcal{C}$.

Para cada conjunto de k columnas independientes de una matriz generadora G, se dice que el conjunto de coordenadas forman un *conjunto de información* de $\mathcal{C}$. Las $r = n - k$ coordenadas restantes forman el *conjunto de redundancia* y el número r es la *redundancia* de $\mathcal{C}$.

En general no hay una única matriz generadora pero si las primeras k coordenadas forman un conjunto de información, entonces el código tiene una única matriz generado de la forma $[I_k|A]$, donde I_k es la matriz identidad $k \times k$. Esta matriz se dice que está en *forma estándar*.

Como un código linear es un subespacio de un espacio vectorial, es el núcleo de alguna transformación lineal.

Definición 3. Una *matriz de paridad* H de dimensión $(n-k) \times k$ de un $[n,k]$ *código linear* $\mathcal{C}$ es una matriz que verifica :

$$C = \{x \in \mathbb{F}_q^n | Hx^T = 0\}$$

Como ocurría con la matriz generadora, la matriz de paridad no es única. Con el siguiente resultado podremos obtener una de ellas cuando $\mathcal{C}$ tiene una matriz generadora en forma estándar.

Teorema 1 (Matriz de paridad a partir de la generadora)**.** *Si $G = [I_k|A]$ es una matriz generadora del $[n,k]$ código $\mathcal{C}$ en su forma estándar, entonces $H = \left[-A^T|I_{n-k}\right]$ es la matriz de paridad de $\mathcal{C}$.*

Demostración. Sabemos que $HG^T = -A^T + A^T = 0$, luego $\mathcal{C}$ está contenido en el núcleo de la transformación lineal $x \mapsto Hx^T$. Como H tiene rango $n-k$, el núcleo de esta transformación es de dimensión k que coincide con la dimensión de $\mathcal{C}$. □

Ejemplo 2. Sea la matriz $G = [I_4|A]$, donde

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

es la matriz generadora en forma estándar del $[7,4]$ código binario que denotaremos por $\mathcal{H}_3$. Por el teorema, la matriz de paridad de $\mathcal{H}_3$ es

$$H = \left[A^T|I_3\right] = \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

Este código se le conoce como el $[7,4]$ *código de Hamming*.

1.2 CÓDIGOS DUALES

La matriz generadora G de un $[n,k]$ código $\mathcal{C}$ es simplemente una matriz cuyas filas son independientes y que expanden el código. Las filas de la matriz de paridad H también son independientes, luego H es la matriz generadora del mismo código al que llamaremos *código dual u ortogonal* y lo denotaremos como $\mathcal{C}^\perp$. Notamos que $\mathcal{C}^\perp$ es un $[n, n-k]$ código. Otra forma de verlo es de la siguiente manera:

Definición 4. $\mathcal{C}$ es un subespacio de un espacio vectorial luego a su ortogonal es a lo que llamamos *espacio dual u ortogonal* de $\mathcal{C}$ y viene dado por

$$\mathcal{C}^{\perp} = \left\{ \mathbf{x} \in \mathbb{F}_q^n \;:\; \mathbf{x} \cdot \mathbf{c} = 0 \quad \forall \mathbf{c} \in \mathcal{C} \right\}$$

Vamos a obtener ahora la matriz generadora y de paridad de $\mathcal{C}^{\perp}$ a partir de las de $\mathcal{C}$

Proposición 1. *Si G y H son las matrices generadora y de paridad de $\mathcal{C}$ respectivamente, entonces H y G son las matrices generadora y de paridad de $\mathcal{C}^{\perp}$.*

Demostración. Sea $G = [I_k|A]$ la matriz generadora y $H = \left[-A^T|I_{n-k}\right]$ la matriz de paridad del $[n,k]$ código $\mathcal{C}$.

Sabemos que $HG^T = GH^T = 0$ luego

$$\mathcal{C}^{\perp} = \left\{ \mathbf{x} \in \mathbb{F}_q^n \;:\; \mathbf{x} \cdot \mathbf{c} = 0 \quad \forall \mathbf{c} \in \mathcal{C} \right\} = \left\{ \mathbf{x} \in \mathbb{F}_q^n \;:\; \mathbf{x} \cdot G^T = 0 \quad \forall \mathbf{c} \in \mathcal{C} \right\} =$$
$$= \left\{ \mathbf{x} \in \mathbb{F}_q^n \;:\; G \cdot \mathbf{x}^T = 0 \quad \forall \mathbf{c} \in \mathcal{C} \right\}$$

Luego $\mathcal{C}^{\perp}$ está contenido en el núcleo de la transformación lineal $x \mapsto Gx^T$. Como G tiene rango k, el núcleo de esta transformación es de dimensión $n-k$ que coincide con la dimensión de $\mathcal{C}^{\perp}$. Por tanto, G es la matriz de paridad de $\mathcal{C}^{\perp}$.

Por último, como $HG^T = 0$ entonces H es la matriz generadora de $\mathcal{C}^{\perp}$. $\square$

Tras este resultado se ve claramente que $\mathcal{C}^{\perp}$ es un $[n, n-k]$ código.

Definición 5. Diremos que un código $\mathcal{C}$ es auto-ortogonal si $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ y diremos que es autodual si $\mathcal{C} = \mathcal{C}^{\perp}$

Ejemplo 3. Tenemos una matriz generadora del código de Hamming $[7,4]$ dada en el ejemplo 2. Ahora definimos $\mathcal{H}_3'$ como el $[8,4]$ código en donde hemos añadido una columna a la paridad de G. Sea

$$G' = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right)$$

donde G' es la matriz generadora de $\mathcal{H}_3'$. Veamos que es autodual:

Sabemos que $G' = [I_4|A']$ y en este caso A' es la siguiente matriz:

$$A' = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

y $(A')^T$ es la misma matriz. Luego como $A'(A')^T = I_4$ entonces $\mathcal{H}_3'$ es autodual.

1.3 PESOS Y DISTANCIAS

Definición 6. La *distancia de Hamming* $d(x,y)$ entre dos vectores $x, y \in \mathbb{F}_q^n$ es el número de coordenadas en las que x e y difieren.

Ejemplo 4. Sea $\mathbf{x} = 20110$ y $\mathbf{y} = 10121$ entonces $d(x,y) = 3$.

Teorema 2. *La función distancia $d(x,y)$ satisface las siguientes cuatro propiedades:*

1. *No negatividad:* $d(x,y) \geq 0 \quad \forall x,y \in \mathbb{F}_q^n$.
2. $d(x,y) = 0 \Leftrightarrow x = y$.
3. *Simetría:* $d(x,y) = d(y,x) \quad \forall x,y \in \mathbb{F}_q^n$.
4. *Desigualdad triangular:* $d(x,z) \leq d(x,y) + d(y,z) \quad \forall x,y,z \in \mathbb{F}_q^n$

Demostración. Las tres primeras propiedades son evidentes por la definición de la distancia, comprobemos la última propiedad.

Distinguimos dos casos, si $x = z$ tenemos que $d(x,z) = 0$ y por tanto se verifica la desigualdad. Si $x \neq z$ entonces, no puede ocurrir que $x = y = z$, por tanto $d(x,y) \neq 0$ o $d(y,z) \neq 0$ y por la no negatividad se tendría la desigualdad, en el caso de que $x = y$ o $y = z$ tendríamos la igualdad. □

Llamaremos *distancia mínima* de un código $\mathcal{C}$ a la menor distancia no-nula entre dos palabras cualquiera del código. Además, esta distancia es un invariante y es importante a la hora de determinar la capacidad de corrección de errores del código $\mathcal{C}$.

Ejemplo 5. Sea $\mathcal{C} = \{201310, 311210, 202210, 312100\}$ un código. Sus distancias son:

$$d(201310, 311210) = 3, \quad d(201310, 202210) = 2, \quad d(201310, 312100) = 5,$$

$$d(311210, 202210) = 3, \quad d(311210, 312100) = 3, \quad d(202210, 312100) = 4$$

Luego, la distancia mínima es $d(\mathcal{C}) = 2$.

Definición 7. El *peso de Hamming* o $\mathrm{wt}(x)$ de un vector $x \in \mathbb{F}_q^n$ es el número de coordenadas no-nulas en x. Llamaremos *peso de* $\mathcal{C}$ a $\mathrm{wt}(\mathcal{C}) = \mathrm{mín}(\mathrm{wt}(x))$ con $x \neq 0$.

Ejemplo 6. Sea $\mathbf{x} = 202210$ un vector en $\mathbb{F}_3^6$ entonces $\mathrm{wt}(x) = 4$.

Teorema 3. *Si $x, y \in \mathbb{F}_q^n$, entonces $d(x,y) = \mathrm{wt}(x-y)$. Si $\mathcal{C}$ es un código linear, la mínima distancia d es igual al mínimo peso de $\mathcal{C}$.*

Demostración. Como $\mathcal{C}$ es lineal, tenemos que $0 \in \mathcal{C}$ y además $\mathrm{wt}(x) = d(x,0) \quad \forall x \in \mathcal{C}$, luego $d(\mathcal{C}) \leq \mathrm{wt}(\mathcal{C})$.

Por otro lado, sea $x, y \in \mathcal{C}$ entonces $x - y \in \mathcal{C} \quad \forall x, y \in \mathcal{C}$ y sabemos que $d(x, y) = \text{wt}(x - y) \geq \text{wt}(\mathcal{C})$ para cualesquiera $x, y \in \mathcal{C}$. Se tiene que $d(\mathcal{C}) \geq \text{wt}(\mathcal{C})$.

Hemos conseguido así la igualdad, $d(\mathcal{C}) = \text{wt}(\mathcal{C})$. □

Como resultado de este teorema, para códigos lineales, la *mínima distancia* también se denomina el *peso mínimo* de un código. Si se conoce el peso mínimo de un código, entonces nos referiremos a él como el $[n, k, d]$ código.

1.4 CÓDIGOS CÍCLICOS

Vamos a estudiar los códigos cíclicos de longitud n, por ello, denotaremos las coordenadas de sus posiciones como $0, \cdots, n-1$ que son los enteros módulo n.

Definición 8. Un código lineal $\mathcal{C}$ de longitud n sobre $\mathbb{F}_q$ es *cíclico* si para cada vector $c = c_0, \cdots, c_{n-2}, c_{n-1}$ en $\mathcal{C}$, el vector $c_{n-1}, c_0, \cdots, c_{n-2}$ obtenido de **c** por la permutación de las coordenadas $i \to i + 1 (modn)$, está también en $\mathcal{C}$.

Así, un código cíclico contiene las n permutaciones de cada palabra código. Por tanto, es conveniente pensar que las coordenadas cuando alcanzan $n - 1$, vuelven a la coordenada 0.

Cuando hablemos de códigos cíclicos sobre $\mathbb{F}_q$, normalmente las palabras códigos las representaremos en su forma polinómica, ya que hay una correspondencia biyectiva entre los vectores $c = c_0, c_1, \cdots, c_{n-1}$ en $\mathbb{F}_q^n$ y los polinomios $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ en $\mathbb{F}_q[x]$ con grado como mucho $n - 1$. Notemos que si **c** es el polinomio dado, entonces $xc(x) = c_{n-1} x^n + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1}$ representa una permutación de **c** si x^n es igual a 1. Más formalmente, el hecho de que el código cíclico $\mathcal{C}$ sea invariante por permutaciones, implica que $c(x)$ está en $\mathcal{C}$, luego $xc(x)$ también lo está multiplicando módulo $x^n - 1$.

Esto sugiere que para un mejor estudio de los códigos cíclicos, desarrollemos el anillo cociente

$$\mathcal{R}_n = \mathbb{F}_q[x] / (x^n - 1)$$

bajo la correspondencia vectores-polinomios dada anteriormente, los códigos cíclicos son ideales de $\mathcal{R}_n$ y los ideales de $\mathcal{R}_n$ son códigos cíclicos. Luego, el estudio de códigos cíclicos en $\mathbb{F}_q^n$ es equivalente al estudio de los ideales de $\mathcal{R}_n$ que se basa en factorizar el polinomio $x^n - 1$

1.4.1 *Factorización de $x^n - 1$*

Queremos encontrar los factores irreducibles de $x^n - 1$. Encontramos dos posibilidades: que $x^n - 1$ tenga factores irreducibles repetidos o no los tenga. En el caso de los códigos cíclicos, se centra más en el segundo caso, por ello, hacemos la asumpción de que $x^n - 1$ no tiene factores repetidos si y solo si q y n son primos relativos.

Como ayuda para factorizar $x^n - 1$ sobre $\mathbb{F}_q^n$, es útil encontrar una extensión del cuerpo $\mathbb{F}_{q^t}^n$ sobre $\mathbb{F}_q^n$ que contiene todas las raíces del polinomio. En otras palabras, $\mathbb{F}_{q^t}^n$ debe contener las raíces primitivas *n-ésimas* de la unidad, que ocurre cuando $n \mid (q^t - 1)$. Definimos el orden, $ord_n(q)$ de q módulo n, como el entero positivo más pequeño a tal que $q^a \equiv 1 \, (mod\, n)$. Notemos que si $t = ord_n(q)$, entonces $\mathbb{F}_{q^t}^n$ contiene la raíz primitiva *n-ésima* de la unidad α , pero ninguna extesión del cuerpo $\mathbb{F}_q^n$ contiene esa raíz. Como los α^i son distintos para $0 \leq i < n$ y $(\alpha^i)^n = 1$, entonces $\mathbb{F}_{q^t}^n$ contiene todas las raíces de $x^n - 1$. Consecuentemente, llamaremos a $\mathbb{F}_{q^t}^n$ el *cuerpo de descomposición* de $x^n - 1$ sobre $\mathbb{F}_q^n$. Así que los factores irreducibles de $x^n - 1$ sobre $\mathbb{F}_q^n$ deben de ser productos de los distintos polinomios mínimos de las raíces *n-ésimas* en $\mathbb{F}_{q^t}^n$. Supongamos que γ es un elemento primitivo, es decir, el elemento generador de $\mathbb{F}_{q^t}^n$, entonces $\alpha = \gamma^d$ es una raíz primitiva *n-ésima* de la unidad en donde $d = (q^t - 1)/n$. Las raíces de $\mathcal{M}_{\alpha^s}(x)$ son $\{\gamma^{ds}, \gamma^{dsq}, \gamma^{dsq^2}, \cdots, \gamma^{dsq^{r-1}}\} = \{\alpha^s, \alpha^{sq}, \alpha^{sq^2}, \cdots, \alpha^{sq^{r-1}}\}$ donde r es el entero positivo más pequeño que cumple que $dsq^r \equiv ds \, (mod\, q-1)$ pero esto solo se verifica si y solo si $sq^r \equiv s \, (mod\, n)$

Definición 9. Sea $\mathbb{F}_q^n$ un cuerpo finito y $\mathbb{F}_{q^t}^n$ un cuerpo de extensión suyo, llamaremos *clase q-ciclotómica de s módulo n* al conjunto :

$$\mathcal{C}_s = \{s, sq, \cdots, sq^{r-1}\} \, (mod\, n)$$

donde r es el menor entero positivo tal que $sq^r \equiv s \, (mod\, n)$.

Las distintas clases *q-ciclotómicas* modulo n forman una partición del conjunto de los enteros $\{0, 1, 2, \cdots, n-1\}$.

Ejemplo 7. Vamos a calcular las clases *2-ciclotómicas* para $n = 9$ y $q = 2$:

La primera de todas es $\mathcal{C}_0 = \{0 * 2^r \equiv 0 \, (mod\, 9)\} = \{0\}$ y repetimos este proceso. Luego tenemos:

$\mathcal{C}_1 = \{1 * 2^r \equiv 1 \, (mod\, 9)\} = \{1, 1 * 2^1 = 2, 1 * 2^2 = 4, 1 * 2^3 = 8, 1 * 2^4 = 7, 1 * 2^5 = 5\} = \{1, 2, 4, 8, 7, 5\}$ ya que $1 * 2^6 = 64 \equiv 1 \, (mod\, 9)$ luego $r = 6$

$\mathcal{C}_3 = \{3 * 2^r \equiv 3 \, (mod\, 9)\} = \{3, 3 * 2 = 6\} = \{3, 6\}$ ya que $3 * 2^2 = 12 \equiv 3 \, (mod\, 9)$ luego $r = 2$

Ejemplo 8. Vamos a calcular las clases *3-ciclotómicas* para $n = 13$ y $q = 3$ que serán las siguientes :

$\mathcal{C}_0 = \{0 * 3^r \equiv 0 \, (mod\, 13)\} = \{0\}$

$\mathcal{C}_1 = \{1 * 3^r \equiv 1 \, (mod\, 13)\} = \{1, 1 * 3^1 = 3, 1 * 3^2 = 9 = \{1, 3, 9\}$ ya que $1 * 3^3 = 27 \equiv 1 \, (mod\, 13)$ luego $r = 3$

$\mathcal{C}_2 = \{2 * 3^r \equiv 2\,(mod\,13)\} = \{2, 2 * 3^1 = 6, 2 * 3^2 = 5\} = \{2, 6, 5\}$ ya que $2 * 3^3 = 54 \equiv 2\,(mod\,13)$ luego $r = 3$

$\mathcal{C}_4 = \{4 * 3^r \equiv 4\,(mod\,13)\} = \{4, 4 * 3^1 = 12, 4 * 3^2 = 10\} = \{4, 12, 10\}$ ya que $4 * 3^3 = 108 \equiv 4\,(mod\,13)$ luego $r = 3$

$\mathcal{C}_7 = \{7 * 3^r \equiv 7\,(mod\,13)\} = \{7, 7 * 3^1 = 8, 7 * 3^2 = 11\} = \{7, 8, 11\}$ ya que $7 * 3^3 = 189 \equiv 7\,(mod\,13)$ luego $r = 3$

Luego, ya tenemos todas las clases *3-ciclotómicas* para $n = 13$ y $q = 3$.

Teorema 4. *Sea n un entero positivo, primo relativo con q. Sea $t = ord_n(q)$ y sea α la raíz primitiva n-ésima de la unidad en $\mathbb{F}_{q^t}$.*

1. *Por cada entero s con $0 \leq s < n$, el polinomio mínimo de α^s sobre $\mathbb{F}_q$ es*

$$\mathcal{M}_{\alpha^s}(x) = \prod_{i \in \mathcal{C}_s} (x - \alpha^i)$$

   donde $\mathcal{C}_s$ es la clase q-ciclotómica de s módulo n

2. *Los conjugados de α^s son los elementos α^i con $i \in \mathcal{C}_s$*
3. $$x^n - 1 = \prod_s \mathcal{M}_{\alpha^s}(x)$$

   es la factorización de $x^n - 1$ en factores irreducibles sobre $\mathbb{F}_q$ donde s recorre un conjunto de los representantes de la clase q-ciclotómica modulo n.

Ejemplo 9. Vamos a factorizar $x^9 - 1$ para ello, cogemos las clases *2-ciclotómicas* calculadas en el ejemplo 7 que son $\mathcal{C}_0 = \{0\}$, $\mathcal{C}_1 = \{1, 2, 4, 8, 7, 5\}$ y $\mathcal{C}_3 = \{3, 6\}$. Luego el $ord_9(2) = 6$ y la *nueve-ésima* raíz primitiva de la unidad reside en el cuerpo de extensión $\mathbb{F}_{64}$ y no en ningún otro más pequeño cuerpo de extensión de $\mathbb{F}_2$.

Podemos afirmar que los factores irreducibles de $x^9 - 1$ tienen grado 1,2 y 6. Estos polinomios son $\mathcal{M}_1(x) = x - 1$, $\mathcal{M}_\alpha(x)$ y $\mathcal{M}_{\alpha^3}(x)$ donde α es la *nueve-ésima* raíz primitiva de la unidad en $\mathbb{F}_{64}$. Como el único polinomio irreducible de grado dos en $\mathbb{F}_2$ es $x^2 + x + 1$ no queda otra que sea $\mathcal{M}_{\alpha^3}(x)$. Por tanto, así tenemos la factorización que es $x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$ y $\mathcal{M}_\alpha(x) = x^6 + x^3 + 1$.

Ejemplo 10. Ahora vamos a factorizar $x^13 - 1$ para ello, cogemos las clases *3-ciclotómicas* calculadas en el ejemplo 8 que son $\mathcal{C}_0 = \{0\}$, $\mathcal{C}_1 = \{1, 3, 9\}$, $\mathcal{C}_2 = \{2, 6, 5\}$, $\mathcal{C}_4 = \{4, 12, 10\}$ y $\mathcal{C}_7 = \{7, 8, 11\}$. Luego el $ord_13(3) = 3$ y la *trece-ésima* raíz primitiva de la unidad reside en el cuerpo de extensión $\mathbb{F}_{27}$ y no en ningún otro más pequeño cuerpo de extensión de $\mathbb{F}_3$.

Podemos afirmar que los factores irreducibles de $x^13 - 1$ tienen grado 1,3,3,3 y 3. Estos polinomios son $\mathcal{M}_1(x) = x - 1$, $\mathcal{M}_\alpha(x)$ y $\mathcal{M}_{\alpha^2}(x)$, $\mathcal{M}_{\alpha^4}(x)$ y $\mathcal{M}_{\alpha^7}(x)$ donde α es la *trece-ésima* raíz primitiva de la unidad en $\mathbb{F}_{27}$.

Como el único polinomio irreducible de grado dos en $\mathbb{F}_2$ es $x^2 + x + 1$ no queda otra que sea $\mathcal{M}_{\alpha^3}(x)$. Por tanto, así tenemos la factorización que es $x^9 - 1 = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1)$ y $\mathcal{M}_\alpha(x) = x^6 + x^3 + 1$.

Viendo estos ejemplos podemos sacar que el tamaño de cada clase *q-ciclotómica* es un divisor del $ord_n(q)$.

Teorema 5. *El tamaño de cada clase q-ciclotómica es un divisor del $ord_n(q)$. Además, el tamaño de $\mathcal{C}_1$ es justamente el $ord_n(q)$.*

Demostración. Sea $t = ord_n(q)$ y sea m el tamaño de $\mathcal{C}_s$. Entonces $\mathcal{M}_{\alpha^s}(x)$ es un polinomio de grado m donde α es la *n-ésima* raíz primitiva de la unidad. Así que, $m \mid t$. Por definición de orden y clase *q-ciclotómica* sale que el tamaño de $\mathcal{C}_1 = ord_n(q)$. □

1.4.2 *Teoría básica de los códigos cíclicos*

Anteriormente, denotamos que los códigos cíclicos sobre $\mathbb{F}_q$ son precisamente los ideales de

$$\mathcal{R}_n = F_q[x]/(x^n - 1)$$

Además cada ideal de $\mathbb{F}_q[x]$ es un ideal principal, luego los ideales de $\mathcal{R}_n$ son también principales y por eso, los códigos cíclicos son ideales principales de $\mathcal{R}_n$.

Los elementos de $\mathcal{R}_n$ son los polinomios de $\mathbb{F}_q$ con grado menor que n y la multiplicación la realizamos módulo $x^n - 1$. Así, cuando trabajamos en $\mathcal{R}_n$, al multiplicar dos polinomios, los multiplicamos como lo hacemos en $\mathbb{F}_q[x]$ y reemplazamos los términos de la forma ax^{ni+j}, con $0 \leq j < n$ por ax^j.

Para distinguir el ideal principal $(g(x))$ de $\mathbb{F}_q[x]$ del ideal principal de $\mathcal{R}_n$, denotamos $< g(x) >$ como el ideal principal de $\mathcal{R}_n$ generado por $g(x)$. Vemos ahora con el siguiente teorema que hay una correspondencia biyectiva entre los códigos cíclicos en $\mathcal{R}_n$ y los polinomios mónicos divisores de $x^n - 1$.

Teorema 6. *Sea $\mathcal{C}$ un código cíclico no-nulo en $\mathcal{R}_n$. Existe un polinomio $g/x) \in \mathcal{C}$ que cumple las siguientes propiedades:*

1. *$g(x)$ es el único polinomio mónico de menor grado en $\mathcal{C}$.*
2. *$\mathcal{C} =< g(x) >$*
3. *$g(x)|(x^n - 1)$*

   Sea $k = n - deg(g(x))$ y sea $g(x) = \sum_{i=0}^{n-k} g_i x^i$ donde $g_{n-k} = 1$. Entonces:
4. *La dimensión de $\mathcal{C}$ es k y $\{g(x), xg(x), \cdots, x^{k-1}g(x)\}$ forman una base de $\mathcal{C}$.*
5. *Cada elemento de $\mathcal{C}$ se puede expresar particularmente como el producto de $g(x)f(x)$, donde $f(x) = 0$ o $deg(f(x)) < k$*

6. $\mathcal{G} = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & \cdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} \end{pmatrix} \Leftrightarrow \begin{pmatrix} g(x) & & & \\ & xg(x) & & \\ & & \ddots & \\ & & & x^{k-1}g(x) \end{pmatrix}$
   es una matriz generadora de $\mathcal{C}$.
7. *Si α es la n-ésima raíz de la unidad en el cuerpo de extensión $\mathbb{F}_q^n$ entonces*

$$g(x) = \prod_s \mathcal{M}_{\alpha^s}(x)$$

   donde el producto es en un subconjunto representativo de las clases q-ciclotómicas módulo n.

Demostración. Sea $g(x)$ un polinomio mónico de menor grado en $\mathcal{C}$. Como $\mathcal{C}$ es no-nulo, ese polinomio existe. Si $c(x) \in \mathcal{C}$, entonces por el algoritmo de la división en $\mathbb{F}_q[x]$, $c(x) = g(x)h(x) + r(x)$, donde $r(x) =$ o $deg(r(x)) < deg(g(x))$. Como $\mathcal{C}$ es un ideal en $\mathcal{R}_n$, $r(x) \in \mathcal{C}$ y como el grado de $g(x)$ es mínimo, implica que $r(x) = 0$. Esto prueba 1 y 2.

De nuevo, por el algoritmo de la división, $x^n - 1 = g(x)h(x) + r(x)$, donde de nuevo $r(x) = 0$ o $deg(r(x)) < deg(g(x))$ en $\mathbb{F}_q[x]$. Como $x^n - 1$ correponde con la palbra código o en $\mathcal{C}$ y $\mathcal{C}$ es un ideal en $\mathcal{R}_n$, entonces $r(x) \in \mathcal{C}$ que es una contradicción, a menos que $r(x) = 0$, lo que prueba 3.

Supongamos que $deg(g(x)) = n - k$. Por 2 y 3 , si $c(x) \in \mathcal{C}$ con $c(x) = 0$ o $deg(c(x)) < n$, entonces $c(x) = g(x)f(x)$ en $\mathbb{F}_q[x]$. Si $c(x) = 0$, entonces $f(x) = 0$. Si $c(x) \neq 0$, $deg(c(x)) < n$ y el grado del producto de dos polinomio es la suma de los grados de los polinomios y sabemos que $deg(g(x)) = n - k$ lo que implica que $deg(f(x)) < k$. Por tanto,

$$\mathcal{C} = \{g(x)f(x) | f(x) = 0 \, o \, deg(f(x)) < k\}$$

Así que $\mathcal{C}$ tiene como mucho dimensión k y $\{g(x), xg(x), \cdots, x^{k-1}g(x)\}$ expande a $\mathcal{C}$. Como estos k polinomios son de distinto grado, son independientes en $\mathbb{F}_q[x]$. Como su grado es como mucho $n-1$, son también independientes en $\mathcal{R}_n$, por lo que queda demostrado 4 y 5. Para 6, basta colocar por filas los elementos de la base y así obtenemos $\mathcal{G}$. El último punto se obtiene del teorema 4. □

A partir de este teorema podemos extraer el siguiente corolario.

Corolario 1. *Sea $\mathcal{C}$ un código cíclico no-nulo en $\mathcal{R}_n$. Son equivalentes:*

1. *$g(x)$ es el único polinomio mónico de menor grado en $\mathcal{C}$.*
2. *$\mathcal{C} =< g(x) >$, $g(x)$ es mónico y $g(x)|(x^n - 1)$.*

Demostración. 1 implica 2 se ha demostrado en 6. Asumiendo 2, sea $g_1(x)$ un polinomio mónico de menor grado en $\mathcal{C}$. Por la demostración del teorema 6 apartados 1 y 2,

$g_1(x)|g(x)$ en $\mathbb{F}_q[x]$ y $\mathcal{C} =< g_1(x) >$. Como $g_1(x) \in \mathcal{C} =< g(x) >$, entonces $g_1(x) = g(x)a(x) + (x^n - 1)b(x)$ en $\mathbb{F}_q[x]$. Como $g(x)|(x^n - 1)$, $g(x)|g(x)a(x) + (x^n - 1)b(x)$ y por tanto $g(x)|g_1(x)$. Como $g_1(x)$ y $g(x)$ son mónicos y se dividen entre ellos en $\mathbb{F}_q[x]$, luego son iguales. □

Del teorema, sacamos que $g(x)$ es un polinomio mónico que divide a $x^n - 1$ y genera a $\mathcal{C}$. Del corolario, sacamos que además $g(x)$ es único. Luego, a este polinomio lo llamaremos el *polinomio generador* del código cíclico $\mathcal{C}$.

Así que hay una correspondencia uno a uno de los códigos cíclicos no-nulos y los divisores de $x^n - 1$ no iguales a $x^n - 1$. Con el fin de tener una correspondencia biyectiva entre todos los códigos cíclicos de $\mathcal{R}_n$ y todos los divisores mónicos de $x^n - 1$, definimos que el *polinomio generador* del código cíclico cero 0 sea $x^n - 1$. Esto da lugar al siguiente corolario.

Corolario 2. *El número de códigos cíclicos en $\mathcal{R}_n$ es igual a 2^m donde m es el número de clases q-ciclotómicas módulo n. Además, las dimensiones de los códigos cíclicos son todas las posibles sumas de los tamaños de las clases q-ciclotómicas módulo n.*

Ejemplo 11. Para el polinomio $x^9 - 1$ en $\mathbb{F}_2$, calculamos sus clases *2-ciclotómicas* en el ejemplo 7 que eran $C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8, 7, 5\}$ y $C_3 = \{3, 6\}$. Luego, sus tamaños son 1,2 y 6, por tanto, por el corolario anterior sabemos que hay $2^3 = 8$ códigos cíclicos y sus dimensiones son : $0, 1, 2, 3, 6, 7, 8, 9$. Veamos los polinomios generadores de cada uno en la siguiente tabla.

i	dimensión	$g_i(x)$
0	0	$x^9 + 1$
1	1	$(x^2 + x + 1)(x^6 + x^3 + 1) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
2	2	$(x + 1)(x^6 + x^3 + 1) = x^7 + x^6 + x^4 + x^3 + x + 1$
3	3	$x^6 + x^3 + 1$
4	6	$(x + 1)(x^2 + x + 1) = x^3 + 1$
5	7	$x^2 + x + 1$
6	8	$x + 1$
7	9	1

Veamos ahora un resultado con respecto a los códigos duales.

Teorema 7. *El código dual de un código cíclico es también cíclico.*

Demostración. Damos primero la definición de código dual $\mathcal{C}^{\perp} = \left\{ \mathbf{x} \in \mathbb{F}_q^n \ : \ \mathbf{x} \cdot \mathbf{c} = 0 \quad \forall \mathbf{c} \in \mathcal{C} \right\}$. Lo que tenemos que probar es que dado un $c \in \mathcal{C}$ entonces $xc \in \mathcal{C}^{\perp}$. Tomamos $c' \in \mathcal{C}^{\perp}$

$$c' \cdot y = 0 \, \forall y \in \mathcal{C} \Rightarrow x \cdot c' \cdot y = 0 \Longrightarrow x \cdot c' \in \mathcal{C}^{\perp}$$

Y por tanto, hemos probado que $\mathcal{C}^\perp$ es cíclico. $\square$

Podemos dar la matriz generado de un código cíclico dual que, en efecto, es también la matriz de paridad de un código cíclico.

Teorema 8. *Sea $\mathcal{C}$ $[n,k]$ código cíclico con polinomio generador $g(x)$. Sea $h(x) = (x^n - 1)/g(x) = \sum_{i=0}^{k} h_i x^i$. Entonces el polinomio generador de $\mathcal{C}^\perp$ es $g(x)^\perp = x^k h(x^{-1})/h(0)$. Además, la matriz generadora de $\mathcal{C}^\perp$ y por tanto, la matriz de paridad de $\mathcal{C}$ es*

$$\mathcal{H} = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & h_k & h_{k-1} & h_{k-2} & \cdots & \cdots & h_0 \end{pmatrix}$$

Demostración. Como sabemos cual es el polinomio generador de $\mathcal{C}^\perp$, podemos calcular su matriz generadora.

$$\begin{pmatrix} g(x)^\perp & & & \\ & xg(x)^\perp & & \\ & & \ddots & \\ & & & x^{k-1}g(x)^\perp \end{pmatrix} =$$

$$\begin{pmatrix} x^k h(x^{-1})/h(0) & & & \\ & xx^k h(x^{-1})/h(0) & & \\ & & \ddots & \\ & & & x^{k-1}x^k h(x^{-1})/h(0) \end{pmatrix}$$

Haciendo cuentas en $\mathcal{R}_n$ obtenemos la matriz $\mathcal{H}$. $\square$

1.5 IDEMPOTENTES Y MULTIPLICADORES

Además del polinomio generador, podemos encontrar otros polinomios que también se pueden usar para generar un código cíclico. Otro polinomio muy común es el que llamaremos *generador idempotente*.

Definición 10. Un elemento e de un anillo lo llamaremos *idempotente* si satisface que $e^2 = e$.

Teorema 9. *Sea $\mathcal{C}$ un código cíclico en $\mathcal{R}_n$. Entonces :*

1. *Existe un único elemento idempotente $e(x) \in \mathcal{C}$ tal que $\mathcal{C} =< e(x) >$,*
2. *si $e(x)$ es un elemento idempotente no-nulo en $\mathcal{C}$, entonces $\mathcal{C} =< e(x) >$ si y solo si es una unidad de $\mathcal{C}$.*

Demostración. Sea $\mathcal{C}$ un código cero, entonces el idempotente es el polinomio cero y se verifica 1) y 2) no se puede aplicar.

Asumimos que $\mathcal{C}$ es no-nulo. Probaremos 2) primero, supongamos que $e(x)$ es una unidad en $\mathcal{C}$. Luego $< e(x) > \in \mathcal{C}$ viendo a $\mathcal{C}$ como un ideal. Si $c(x) \in \mathcal{C}$, entonces $c(x)e(x) = c(x)$ en $\mathcal{C}$, lo que implica que $< e(x) >= \mathcal{C}$. Por el contrario, supongamos que $e(x)$ es el idempotente no-nulo tal que $\mathcal{C} =< e(x) >$. Luego, cada elemento $c(x) \in \mathcal{C}$ se puede escribir de la forma $c(x) = f(x)e(x)$, pero $c(x)e(x) = f(x)e(x)^2 = f(x)e(x) = c(x)$ lo que implica que $e(x)$ es una unidad en $\mathcal{C}$.

Como $\mathcal{C}$ es no-nulo, por 2) si $e_1(x)$ y $e_2(x)$ son generadores idempotentes, entonces ambos son unidades y $e_1(x) = e_2(x)e_1(x) = e_2(x)$. Solo nos falta probar la existencia. Si $g(x)$ es el polinomio generador de $\mathcal{C}$, entonces $g(x)|x^n - 1$. Sea $h(x) = (x^n - 1)/g(x)$, entonces el $mcd(g(x), h(x)) = 1$ en $\mathbb{F}_q[x]$ ya que $x^n - 1$ tiene distintas raíces. Por el Algoritmo de Euclídes, sabemos que existen $a(x), b(x) \in \mathbb{F}_q[x]$ tal que $a(x)g(x) + b(x)h(x) = 1$. Sea $e(x) \equiv a(x)g(x)\ (mod\, x^n - 1)$, donde $e(x)$ es el representante de $a(x)g(x) + (x^n - 1)$ en $\mathcal{R}_n$. Luego en $\mathcal{R}_n$, $e(x)^2 \equiv (a(x)g(x))(1 - b(x)h(x)) \equiv a(x)g(x) \equiv e(x)\ (mod\, x^n - 1)$ ya que $g(x)h(x) = x^n - 1$. Además si $c(x) \in \mathcal{C}$, $c(x) = f(x)g(x)$ implica que $c(x)e(x) \equiv f(x)g(x)(1 - b(x)h(x)) \equiv f(x)g(x) \equiv c(x)\ (mod\, x^n - 1)$, por tanto, $e(x)$ es una unidad de $\mathcal{C}$ y 1) se prueba a partir de 2). □

Gracias a la demostración, hemos encontrado una forma de calcular el polinomio $e(x)$ a partir del polinomio generador $g(x)$. Basta con resolver $1 = a(x)g(x) + b(x)h(x)$ donde $h(x) = (x^n - 1)/g(x)$. Luego, reduciendo $a(x)g(x)$ módulo $x^n - 1$ se tiene $e(x)$. Veamos ahora una forma de obtener $g(x)$ a partir de $e(x)$.

Teorema 10. *Sea $\mathcal{C}$ un código cíclico sobre $\mathbb{F}_q$ con generador idempotente $e(x)$. Entonces, el polinomio generador de $\mathcal{C}$ es $g(x) = mcd(e(x), x^n - 1)$ en $\mathbb{F}_q[x]$.*

Demostración. Sea $d(x) = mcd(e(x), x^n - 1)$ en $\mathbb{F}_q[x]$ y sea $g(x)$ el polinomio generador de $\mathcal{C}$. Como $d(x)|e(x)$, $e(x) = d(x)k(x)$ implica que cada elemento de $\mathcal{C} =< e(x) >$ es también un múltiplo de $d(x)$, así que $\mathcal{C} \subseteq < d(x) <$. Por el teorema 6, sabemos que $g(x)|(x^n - 1)$ y por tanto, $g(x)|e(x)$ porque $e(x) \in \mathcal{C}$. Luego $g(x)|d(x)$ y por tanto, $d(x) \in \mathcal{C}$. Como $d(x)$ es un divisor mónico de $x^n - 1$ que genera a $\mathcal{C}$, entonces por el corolario 1, $d(x) = g(x)$. □

Ejemplo 12. Vamos a calcular las clases *2-ciclotómicas* para $n = 7$ y ver cuáles son sus códigos cíclicos, dando su polinomio generador e idempotente.

Las clases 2-*ciclotómicas* son : $\mathcal{C}_0 = \{0\}$, $\mathcal{C}_1 = \{1 * 2^r \equiv 1\,(mod\, 7)\} = \{1, 2, 4\}$, $\mathcal{C}_3 = \{3 * 2^r \equiv 3\,(mod\, 7)\} = \{3, 6, 5\}$.

Por tanto, tenemos tres clases 2-*ciclotómicas* de tamaños, 1,3 y 3 y la factorización de $x^7 - 1 = (x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)$ Sabemos que hay 8 códigos cíclicos cuyas dimensiones son 0,1,3,3,4,4,6,7. En la siguiente tabla veremos los polinomios generadores e idempotentes.

i	dimensión	$g_i(x)$
0	0	x^7+1
1	1	$(x^3+x+1)(x^3+x^3+1) = x^6+x^5+x^4+x^3+x^2+x+1$
2	3	$(x+1)(x^3+x^2+1) = x^4+x^2+x+1$
3	3	$(x+1)(x^3+x+1) = x^4+x^3+x^2+1$
4	4	x^3+x^2+1
5	4	x^3+x+1
6	6	$x+1$
7	7	1

i	dimensión	$e_i(x)$
0	0	0
1	1	$x^6+x^5+x^4+x^3+x^2+x+1$
2	3	$x^6+x^5+x^3+1$
3	3	$x^4+x^3+x^2+1$
4	4	x^4+x^2+x
5	4	$x^6+x^5+x^3$
6	6	$x^6+x^5+x^4+x^3+x^2+x$
7	7	1

Los polinomios idempotentes los hemos calculado como indicamos anteriormente. Además, los dos códigos de dimensión cuatro son los $[7,4,3]$ códigos Hamming.

Veamos ahora que al igual que los polinomios generadores podíamos sacar la matriz generadora, también podemos hacerlo con los idempotentes.

Teorema 11. *Sea $\mathcal{C}$ un $[n,k]$ código cíclico con polinomio idempotente $e(x) = \sum_{i=0}^{n-1} e_i x^i$, la matriz $k \times n$*

$$\begin{pmatrix} e_0 & e_1 & e_2 & \cdots & e_{n-2} & e_{n-1} & & \\ e_{n-1} & e_0 & e_1 & \cdots & e_{n-3} & e_{n-2} & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ e_{n-k+1} & e_{n-k+2} & e_{n-k+3} & \cdots & e_{n-k-1} & e_{n-k} & & \end{pmatrix}$$

es la matriz generadora de $\mathcal{C}$.

Demostración. Esto es equivalente a decir que $\{e(x), xe(x), \cdots, x^{k-1}e(x)\}$ es una base de $\mathcal{C}$. Por tanto, es suficiente ver que si $a(x) \in \mathbb{F}_q[x]$ tiene menor grado que k tal que $a(x)e(x) = 0$, entonces $a(x) = 0$. Sea $g(x)$ el polinomio generador de $\mathcal{C}$. Si $a(x)e(x) = 0$, entonces $0 = a(x)e(x)g(x) = a(x)g(x)$ ya que $e(x)$ es una unidad de $\mathcal{C}$, contradiciendo así el teorema **??** 5) a menos que $a(x) = 0$. □