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 21 de mayo de 2023

ÍNDICE GENERAL

1

PRELIMINARES

En el desarrollo de este capítulo se explicarán conceptos que nos resultarán útiles durante los demás capítulos. Se ha tomado como referencia **?**.

1.1 CUERPOS FINITOS

Definición 1. Un *cuerpo* es un conjunto $\mathbb{F}$ con dos operaciones: la suma, +, y el producto, $\cdot$ que satisface los siguientes axiomas.

1. El conjunto $\mathbb{F}$ es abeliano con respecto a la operación suma con elemento neutro 0.
2. El conjunto $\mathbb{F}^*$ de todos los elementos no nulos de $\mathbb{F}$ es abeliano con respecto a la operación producto con elemento neutro 1.
3. Cumple la propiedad distributiva : $a \cdot (b + c) = a \cdot b + a \cdot c \ \forall a, b, c \in \mathbb{F}$.

Definición 2. Diremos que un cuerpo $\mathbb{F}$ es **finito** si $\mathbb{F}$ tiene un número finito de elementos y llamaremos **orden** de $\mathbb{F}$ al número de elementos. En general, denotaremos un cuerpo con q elementos como $\mathbb{F}_q$

Si p es primo, los enteros módulos p forman un cuerpo, al que denotaremos $\mathbb{F}_p$. Estos son los ejemplos más sencillos de cuerpos finitos.

La finitud de $\mathbb{F}_q$ implica que existe un entero positivo p tal que $1 + 1 + \cdots + 1$ (p 1s) es 0. Este entero p es primo y lo denominaremos la *característica* de $\mathbb{F}_q$. Si a es un entero positivo, denotamos la suma de 1s en el cuerpo como a. Además, si queremos escribir la suma de α a veces en el cuerpo, escribiremos $a\alpha$ o $a \cdot \alpha$, por tanto, vemos que $p\alpha = 0 \, \forall \alpha \in \mathbb{F}_q$. El conjunto de p elementos distintos $\{0, 1, 2, \cdots, (p-1)\}$ de $\mathbb{F}_q$ es isomorfo al cuerpo $\mathbb{F}_p$ de los enteros módulo p. Como un cuerpo isomorfo a $\mathbb{F}_p$ está contenido en $\mathbb{F}_q$, diremos que $\mathbb{F}_p$ es un subcuerpo de $\mathbb{F}_q$. A este subcuerpo $\mathbb{F}_p$ lo llamaremos *subcuerpo primo* de $\mathbb{F}_q$. El cuerpo $\mathbb{F}_q$ es además un espacio de dimensión finita sobre $\mathbb{F}_p$, digamos de dimensión m. Por lo tanto, $q = p^m$ ya que es el número de vectores en el espacio vectorial de dimensión m sobre $\mathbb{F}_p$.

Resumimos ahora en un teorema los resultados que acabamos de ver.

Teorema 1. *Sea $\mathbb{F}_q$ un cuerpo finito con q elementos. Entonces :*

1. $q = p^m$ *para algún primo p.*
2. $\mathbb{F}_q$ *contiene un subcuerpo* $\mathbb{F}_p$.
3. $\mathbb{F}_q$ *es un espacio vectorial sobre* $\mathbb{F}_p$ *de dimensión m.*
4. $p\alpha = 0 \, \forall \alpha \in \mathbb{F}_q$.
5. $\mathbb{F}_q$ *es único salvo isomorfismo.*

1.1.1 *Polinomios y el Algoritmo de Euclides*

El conjunto de los polinomios en x con coeficientes en $\mathbb{F}_q$ lo denotaremos como $\mathbb{F}_q[x]$. Este conjunto forma un anillo conmutativo unitario bajo la suma y multiplicación de polinomios. Un anillo conmutativo unitario satisface los mismos axiomas que un cuerpo excepto que los elementos no nulos no es necesario que tengan inversos multiplicativos. De hecho, $\mathbb{F}_q[x]$ es un dominio de integridad, ya que es un anillo conmutativo unitario tal que el producto de dos elementos no nulos en el anillo es también no nulo. El anillo $\mathbb{F}_q[x]$ es importante tanto para la construcción de cuerpos finitos como para la construcción de códigos.

Denotaremos a los polinomios en $\mathbb{F}_q[x]$ como $f(x) = \sum_{i=0}^{n} a_i x^i$, donde a_i son coeficientes del término $a_i x^i$ de grado i. El *grado de un polinomio* es el grado más alto de cualquier término con coeficiente no nulo, lo denotaremos como $deg(f(x))$. El coeficiente del término con mayor grado se le conoce como *coeficiente líder*.Diremos que un polinomio es *mónico* si su coeficiente líder es 1.

Sea $f(x)$ y $g(x)$ polinomios en $\mathbb{F}_q[x]$. Decimos que *f(x) divide a g(x)*, denotado por $f(x) \mid g(x)$, si existe un polinomio $h(x) \in \mathbb{F}_q[x]$ tal que $g(x) = f(x)h(x)$. Al polinomio $f(x)$ se le dice factor o divisor de $g(x)$. El *máximo común divisor* de $f(x)$ y $g(x)$, siendo al menos uno de ellos no nulo, es el polinomio mónico de $\mathbb{F}_q[x]$ con coeficiente más alto que divide tanto a $f(x)$ como a $g(x)$. El máximo común divisor es único salvo producto por una unidad y lo denotaremos como $mcd(f(x), g(x))$. Si el $mcd(f(x), g(x)) = 1$, entonces diremos que $f(x)$ y $g(x)$ son primos relativos.

Como con los enteros, también podemos dividir polinomios y obtener un cociente y un resto.

Teorema 2 (Algoritmo de la División). *Sea $f(x)$ y $g(x)$ polinomios en $\mathbb{F}_q[x]$ con $g(x)$ no nulo.*

1. *Existen dos polinomios únicos $h(x), r(x) \in \mathbb{F}_q[x]$ tales que $f(x) = g(x)h(x) + r(x)$ donde $deg(r(x)) < deg(g(x))$ o $r(x) = 0$.*
2. *Si $f(x) = g(x)h(x) + r(x)$ entonces $mcd(f(x), g(x)) = mcd(g(x), r(x))$.*

Si usamos el Algoritmo de la División recursivamente, podemos encontrar el mcd de dos polinomios cualesquiera, a este método se le conoce como el Algoritmo de Euclides.

Teorema 3 (Algoritmo de Euclides). *Sea $f(x)$ y $g(x)$ polinomios en $\mathbb{F}_q[x]$ con $g(x)$ no nulo.*

1. *Repetimos la siguiente secuencia hasta que $r_n(x) = 0$ para algún n:*

   $f(x) = g(x)h_1(x) + r_1(x)$ *donde* $deg(r_1(x)) < deg(g(x))$

   $g(x) = r_1(x)h_2(x) + r_2(x)$ *donde* $deg(r_2(x)) < deg(r_1(x))$

   $r_1(x) = r_2(x)h_3(x) + r_3(x)$ *donde* $deg(r_3(x)) < deg(r_2(x))$

   $\vdots$

   $r_{n-3}(x) = r_{n-2}(x)h_{n-1}(x) + r_{n-1}(x)$ *donde* $deg(r_{n-1}(x)) < deg(r_{n-2}(x))$

   $r_{n-2}(x) = r_{n-1}(x)h_n(x) + r_n(x)$ *donde* $deg(r_n(x)) = 0$

   donde el $mcd(f(x), g(x)) = cr_{n-1}(x)$, *donde* $c \in \mathbb{F}_q$ *es escogido tal que* $cr_{n-1}(x)$ *sea mónico.*
2. *Existen polinomios $a(x), b(x) \in \mathbb{F}_q[x]$ tales que*

   $a(x)f(x) + b(x)g(x) = mcd(f(x), g(x))$.

Ejemplo 1. Vamos a calcular el $mcd(x^8 + x^6 + x^5 + x^3 + x^2 + 1, x^4 + x^3 + 1)$ en el anillo $\mathbb{F}_2[x]$ usando el Algoritmo de Euclides. La parte 1) del algoritmo produce lo siguiente:

$x^8 + x^6 + x^5 + x^3 + x^2 + 1 = (x^4 + x^3 + 1)(x^4 + x^3 + x) + (x^2 + x + 1)$

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

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

$x = 1x + 0$

Por tanto, $1 = mcd(x, 1) = mcd(x^2 + x + 1, x) = mcd(x^4 + x^3 + 1, x^2 + x + 1) = mcd(x^8 + x^6 + x^5 + x^3 + x^2 + 1, x^4 + x^3 + 1)$. Ahora encontramos $a(x), b(x)$ tales que $a(x)(x^8 + x^6 + x^5 + x^3 + x^2 + 1) + b(x)(x^4 + x^3 + 1) = 1$ haciendo a la inversa los pasos anteriores. Luego, tenemos que :

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

Ahora, despejamos x de la segunda ecuación y lo sustituimos en la tercera lo que quedaría de la siguiente forma,

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

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

Despejamos $(x^2 + x + 1)$ de la primera ecuación y lo sustituimos en lo que hemos obtenido en el paso anterior, quedando de la siguiente forma,

$[(x^8 + x^6 + x^5 + x^3 + x^2 + 1) - (x^4 + x^3 + 1)(x^4 + x^3 + x)](x^3 + x^2 + x) + (x^4 + x^3 + 1)(x + 1) = 1$

$(x^3+x^2+x)(x^8+x^6+x^5+x^3+x^2+1)+(x^7+x^3+x^2)(x^4+x^3+1)=1$

Por tanto, tenemos que $a(x)=(x^3+x^2+x)$ y $b(x)=(x^7+x^3+x^2)$.

1.1.2 *Elementos primitivos*

Queremos encontrar una forma sencilla de poder sumar y multiplicar los elementos de un cuerpo $\mathbb{F}_q$. Vimos que $\mathbb{F}_q$ es un espacio vectorial sobre $\mathbb{F}_p$ de dimensión m, luego una forma sencilla de sumar es escribir los elementos como m-tuplas de $\mathbb{F}_p$, sin embargo, la multiplicación no es tan sencilla. Por ello, presentamos el siguiente teorema en donde escribiremos los elementos de otra forma que nos facilite la multiplicación.

Teorema 4. *Se verifica lo siguiente:*

1. *El grupo $\mathbb{F}_q^*$ es cíclico de orden $q-1$ bajo la multiplicación en $\mathbb{F}_q$.*
2. *Si γ es un generador de ese grupo cíclico, entonces*

$$\mathbb{F}_q=\{0,1=\gamma^0,\gamma,\gamma^2,\cdots,\gamma^{q-2}\}$$

donde $\gamma^i=1$ si y solo si $(q-1)\mid i$.

Demostración. Por el Teorema Fundamental de Grupos Abelianos Finitos, sabemos que $\mathbb{F}_q^*$ es producto directo de grupos cíclicos de orden $m_1,m_2,\cdots,m_a$, donde $m_i \mid m_{i+1}$ para $1\leq i<a$ y $m_1m_2\cdots m_a=q-1$. En particular, $\alpha^{m_a}=1\ \forall\alpha\in\mathbb{F}_q^*$. Luego, el polinomio $x^{m_a}-1$ tiene al menos $q-1$ raíces, lo cual no es posible a menos que $a=1$ y $m_a=q-1$. Por tanto, $\mathbb{F}_q^*$ es cíclico, dando lugar a 1). 2) se obtiene como propiedades de los grupos cíclicos. □

Definición 3. Llamaremos **elemento primitivo** de $\mathbb{F}_q$ a cada generador γ de $\mathbb{F}_q^*$

Cuando los elementos no nulos de un cuerpo finito son expresados como potencias de γ, la multiplicación en el cuerpo se puede realizar fácilmente de la siguiente manera, $\gamma^i\gamma^j=\gamma^{i+j}=\gamma^s$, donde $0\leq s\leq q-2$ y $i+j\equiv s\,(mod\,q-1)$.

Sea γ un elemento primitivo de $\mathbb{F}_q$, entonces $\gamma^{q-1}=1$ por definición. Por tanto, $(\gamma^s)^{q-1}=1$ para $0\leq s\leq q-2$, mostrando que los elementos de $\mathbb{F}_q^*$ son raíces de $x^{q-1}-1\in\mathbb{F}_q[x]$ y por tanto, de x^q-x. Como 0 es una raíz de x^q-x, los elementos de $\mathbb{F}_q$ son precisamente las raíces de x^q-x.

Teorema 5. *Los elementos de $\mathbb{F}_q$ son precisamente las raíces de x^q-x.*

Para analizar la estructura de un cuerpo, será útil saber el número de elementos primitivos que hay en $\mathbb{F}_q$ y como encontrarlos todos conociendo uno de ellos. Ya que $\mathbb{F}_q^*$ es cíclico, vamos a recordar algunos hechos de los grupos cíclicos finitos.

En cualquier grupo cíclico finito $\mathcal{G}$ de orden n con generador g, los generadores de $\mathcal{G}$ son precisamente los elementos g^i donde $mcd(i,n)=1$. Sea $\phi(n)$ el número de

enteros i con $1 \leq i \leq n$ tal que $mcd(i,n) = 1$. A ϕ se le conoce como **función ϕ de Euler** o **función totiente de Euler**. Así que, $\phi(n)$ generadores de $\mathcal{G}$. El orden de un elemento $\alpha \in \mathcal{G}$ es le entero positivo más pequeño tal que $\alpha^i = 1$. Un elemento de $\mathcal{G}$ tiene orden d si y solo si $d \mid n$. Además g^i tiene orden $d = n/mcd(i,n)$ y hay tantos $\phi(d)$ elementos de orden d. Cuando hablamos de elementos de un cuerpo $\alpha \in \mathbb{F}_q^*$, el orden de α es su orden en el grupo multiplicativo $\mathbb{F}_q^*$. En particular, los elementos primitivos de $\mathbb{F}_q$ son aquellos con orden $q-1$.

Teorema 6. *Sea γ un elemento primitivo de $\mathbb{F}_q$.*

1. *Hay $\phi(q-1)$ elementos primitivos en $\mathbb{F}_q$, esos son los elementos γ^i donde $mcd(i, q-1) = 1$.*
2. *Para cualquier d donde $d \mid (q-1)$, hay $\phi(d)$ elementos en $\mathbb{F}_q$ de orden d y esos son los elementos $\gamma^{(q-1)i/d}$ donde $mcd(i,q) = 1$.*

Definición 4. Un elemento $\tau \in \mathbb{F}_q$ es una **raíz n-ésima de la unidad** si $\tau^n = 1$ y es una **raíz n-ésima primitiva de la unidad** si además $\tau^s \neq 1$ para $0 < s < n$.

1.1.3 *Construcción de cuerpos finitos*

Un polinomio no contante $f(x) \in \mathbb{F}_q[x]$ es irreducible sobre $\mathbb{F}_q$ si no factoriza en un producto de dos polinomios no constantes en $\mathbb{F}_q[x]$ de menor grado. Los polinomios irreducibles en $\mathbb{F}_q[x]$ toman el rol de los números primos en el anillo de los enteros. Por ejemplo, cada entero mayor que 1 se puede descomponer de forma única en producto de primos positivos. Un resultado similar ocurre en $\mathbb{F}_q[x]$, por lo que tenemos un *dominio de factorización única*.

Teorema 7. *Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio no constante. Entonces,*

$$f(x) = p_1(x)^{a_1} p_2(x)^{a_2} \cdots p_k(x)^{a_k}$$

donde cada $p_i(x)$ es irreducible, los $p_i(x)$s son únicos hasta una multiplicación escalar y los a_is son únicos.

Además de ser un dominio de factorización única, es un dominio de ideales principales. Un **ideal** $\mathcal{I}$ en un anillo conmutativo $\mathcal{R}$ es un subconjunto no vacío del anillo el cual es cerrado para la suma, y para el producto por elementos de $\mathcal{I}$ por un elemento de $\mathcal{R}$ siempre se queda en $\mathcal{I}$. El ideal $\mathcal{I}$ es **principal** si hay un $a \in \mathcal{R}$ tal que $\mathcal{I} = \{ra \mid r \in \mathcal{R}\}$. Un dominio de ideales principales es un dominio de integridad en donde cada ideal es principal.

Para construir un cuerpo con característica p, empezamos con un polinomio $f(x) \in \mathbb{F}_p[x]$ que sea irreducible en $\mathbb{F}_p$. Supongamos que $f(x)$ es de grado m. Usando el Algoritmo de Euclides podemos probar que el anillo cociente $\mathbb{F}_p[x]/(f(x))$ es un cuerpo y por tanto, $\mathbb{F}_q$ es un cuerpo finito con $q = p^m$ elementos.

Cada elemento del anillo cociente es una clase de equivalencia $g(x) + (f(x))$, donde $g(x)$ está determinado por un grado a lo sumo $m-1$. Podemos comprimir la notación escribiendo las clases como un vector en $\mathbb{F}_p^m$ con la siguiente correspondencia :

$$g_{m-1}x^{m-1} + g_{m-2}x^{m-2} + \cdots + g_1x + g_0 + (f(x)) \Leftrightarrow g_{m-1}g_{m-2}\cdots g_1g_0$$

Con esta notación podemos sumar usando la operación de adición ordinario de los vectores.

Para multiplicar $g_1 + (f(x)) \cdot g_2 + (f(x))$, primero usamos el Algoritmo de la División, obteniendo $g_1(x)g_2(x) = f(x)h(x) + r(x)$ con $deg(r(x)) \leq m-1$ o $r(x) = 0$. Entonces $(g_1 + (f(x)))(g_2 + (f(x))) = r(x) + (f(x))$. La notación es un poco engorrosa así que la vamos a simplificar reemplazando x por α tal que $f(\alpha) = 0$. Así tenemos la correspondencia anterior de la siguiente manera :

$$g_{m-1}g_{m-2}\cdots g_1g_0 \Leftrightarrow g_{m-1}\alpha^{m-1} + g_{m-2}\alpha^{m-2} + \cdots + g_1\alpha + g_0$$

Así que para multiplicar en $\mathbb{F}_q$, simplemente multiplicamos polinomios en α de manera ordinaria y usamos que $f(\alpha) = 0$ para reducir las potencias de α mayores que $m-1$ a polinomios en α con menor grado que m.

Ejemplo 2. El polinomio $f(x) = x^3 + x^2 + 1$ es irreducible en $\mathbb{F}_2$, si fuese reducible habría un factor de grado 1 que además sería raíz en $\mathbb{F}_2$ y no lo hay. Así que $\mathbb{F}_8 = \mathbb{F}_2/(f(x))$ y usando ambas correspondencias obtenemos que los elementos de $\mathbb{F}_8$ son

Clases	Vectores	Polinomios en α	Potencias de α
$0 + (f(x))$	000	0	0
$1 + (f(x))$	001	1	$1 = \alpha^0$
$x + (f(x))$	010	α	α
$x + 1 + (f(x))$	011	$\alpha + 1$	α^5
$x^2 + (f(x))$	100	α^2	α^2
$x^2 + 1 + (f(x))$	101	$\alpha^2 + 1$	α^3
$x^2 + x + (f(x))$	110	$\alpha^2 + \alpha$	α^6
$x^2 + x + 1 + (f(x))$	111	$\alpha^2 + \alpha + 1$	α^4

Las potencias de α las hemos obtenido de $f(\alpha) = \alpha^3 + \alpha^2 + 1 = 0$ lo que implica que $\alpha^3 = \alpha^2 + 1$, así $\alpha^4 = \alpha\alpha^3 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha = \alpha^2 + \alpha + 1$, $\alpha^5 = \alpha\alpha^4 = \alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1 + \alpha^2 + \alpha = \alpha + 1$ y $\alpha^6 = \alpha\alpha^5 = \alpha(\alpha + 1) = \alpha^2 + \alpha$.

Luego, si queremos sumar $x^2 + (f(x))$ y $x^2 + 1 + (f(x))$ eso nos da $1 + (f(x))$ que corresponde a sumar 100 y 101 que da 001 en $\mathbb{F}_2^3$.

Si ahora queremos multiplicar $x^2 + x + (f(x))$ y $x^2 + x + 1 + (f(x))$, multiplicamos $\alpha^6 \cdot \alpha^4 = \alpha^3 = \alpha^2 + 1$ lo que nos da $x^2 + 1 + (f(x))$.

Describimos la construcción diciendo que $\mathbb{F}_q$ se obtiene a partir de $\mathbb{F}_p$ "adjuntando" una raíz α de $f(x)$ a $\mathbb{F}_p$. Esta raíz α normalmente viene dado por $\alpha = x + (f(x))$ en el anillo cociente $\mathbb{F}_p[x]/(f(x))$ y por tanto, $g(x) + (f(x)) = g(\alpha)$ y $f(\alpha) = f(x + (f(x))) = f(x) + (f(x)) = 0 + (f(x))$.

En general, α no tiene la necesidad de ser un elemento primitivo. Decimos que un polinomio irreducible en $\mathbb{F}_p$ con grado m es primitivo si tiene una raíz que es un elemento primitivo de $\mathbb{F}_q = \mathbb{F}_{p^m}$. Idealmente, queremos empezar con un polinomio primitivo para construir nuestro cuerpo, pero no es un requisito. Además, el polinomio con el que empezamos si lo multiplicamos por una constante para hacerlo mónico, no influye en el ideal generado por el polinomio o el anillo cociente. Tenemos el siguiente resultado:

Teorema 8. *Para cualquier primo p y cualquier entero positivo m, existe un cuerpo finito, único salvo isomorfismos, tal que tiene $q = p^m$ elementos.*

1.1.4 *Cuerpos de los automorfismos*

El cuerpo de los automorfismos de $\mathbb{F}_q$ forma un grupo con la composición.

Definición 5. Un **automorfismo** σ de $\mathbb{F}_q$ es una aplicación biyectiva $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ tal que $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ y $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)\ \forall \alpha, \beta \in \mathbb{F}_q$.

Definimos $\sigma_p : \mathbb{F}_q \to \mathbb{F}_q$ como

$$\sigma_p(\alpha) = \alpha^p\ \forall \alpha \in \mathbb{F}_q$$

Obviamente, $\sigma_p(\alpha\beta) = \sigma_p(\alpha)\sigma_p(\beta)$ y $\sigma_p(\alpha + \beta) = \sigma_p(\alpha) + \sigma_p(\beta)$. Como σ_p tiene núcleo $\{0\}$, σ_p es un automorfismo de $\mathbb{F}_q$, al que llamaremos **automorfismo de Frobenius**. Análogamente, definimos $\sigma_{p^r}(\alpha) = \alpha^{p^r}$.

El grupo de los automorfimos de $\mathbb{F}_q$, denotado por $Gal(\mathbb{F}_q)$, se le llama grupo de Galois de $\mathbb{F}_q$. Con el siguiente teorema vamos a caracterizar ese grupo.

Teorema 9.
1. *$Gal(\mathbb{F}_q)$ es cíclico de orden m y está generado por el automorfismo de Frobenius σ_p.*
2. *El subcuerpo primo de $\mathbb{F}_q$ es precisamente el conjunto de elementos de $\mathbb{F}_q$ tal que $\sigma_p(\alpha) = \alpha$.*
3. *El subcuerpo $\mathbb{F}_q$ de $\mathbb{F}_{q^t}$ es precisamente el conjunto de elementos de $\mathbb{F}_{q^t}$ tal que $\sigma_p(\alpha) = \alpha$.*

Usamos σ_p para denotar al automorfismo de Frobenius de cualquier cuerpo con característica p. Si $\mathbb{E}$ y $\mathbb{F}$ son cuerpos de característica p con $\mathbb{E}$ siendo un cuerpo de extensión de $\mathbb{F}$, entonces el automorfismo de Frobenius de $\mathbb{E}$ restringido a $\mathbb{F}$ es el automorfismo de Frobenius de $\mathbb{F}$

Definición 6. Un elemento $\alpha \in \mathbb{F}$ es **fijo** si $\sigma(\alpha) = \alpha$ por el automorfismo σ de $\mathbb{F}$.

Sea $r \mid m$. Entonces σ_{p^r} genera un subgrupo cíclico de $Gal(\mathbb{F}_q)$ de orden m/r

1.1.5 *Polinomios mínimos*

Sea $\mathbb{E}$ un cuerpo de extensión finito de $\mathbb{F}_q$, entonces $\mathbb{E}$ es un espacio vectorial sobre $\mathbb{F}_q$ y por tanto, $\mathbb{E} = \mathbb{F}_{q^t}$ para algún entero positivo t. Cada elemento α de $\mathbb{E}$ es una raíz del polinomio $x^{q^t} - x$ como dijimos anteriormente. Por consiguiente, hay un polinomio mónico $\mathcal{M}_\alpha(x)$ en $\mathbb{F}_q[x]$ de menor grado el cual tiene a α como raíz. A este polinomio lo llamaremos **polinomio mínimo** de α sobre $\mathbb{F}_q$. Vamos a dar unas cuantas propiedades sobre los polinomios mínimos.

Teorema 10. *Sea $\mathbb{F}_{q^t}$ un cuerpo de extensión de $\mathbb{F}_q$ y sea α un elemento de $\mathbb{F}_{q^t}$ con polinomio mínimo $\mathcal{M}_\alpha(x)$ en $\mathbb{F}_q[x]$. Tenemos lo siguiente:*

1. *$\mathcal{M}_\alpha(x)$ es irreducible sobre $\mathbb{F}_q$.*
2. *Si $g(x)$ es cualquier polinomio en $\mathbb{F}_q[x]$ satisfaciendo que $g(\alpha) = 0$, entonces $\mathcal{M}_\alpha(x) \mid g(x)$.*
3. *$\mathcal{M}_\alpha(x)$ es único, es decir, solo hay un polinomio mónico en $\mathbb{F}_q[x]$ de menor grado que tiene a α como raíz.*

Si empezamos con un polinomio irreducible $f(x)$ en $\mathbb{F}_q$ de grado r, podemos adjuntar una raíz de $f(x)$ a $\mathbb{F}_q$ para obtener el cuerpo $\mathbb{F}_{q^r}$, en el cual, todas sus raíces se quedan en $\mathbb{F}_{q^r}$

Teorema 11. *Sea $f(x)$ un polinomio mónico irreducible en $\mathbb{F}_q$ con grado r. Entonces :*

1. *Todas las raíces de $f(x)$ se encuentran en $\mathbb{F}_{q^r}$ y en cualquier cuerpo que contenga a $\mathbb{F}_q$ junto a una raíz de $f(x)$.*
2. *$f(x) = \prod_{i=1}^{r}(x - \alpha^i)$, donde $\alpha^i \in \mathbb{F}_{q^r}$ para $1 \leq i \leq r$.*
3. *$f(x) \mid x^{q^r} - x$.*

Demostración. Sea α una raíz de $f(x)$ que adjuntamos a $\mathbb{F}_q$ para formar el cuerpo $\mathbb{E}_\alpha$ con q^r elementos. Si β es una raíz de $f(x)$, que no está en $\mathbb{E}_\alpha$, es raíz de algún factor irreducible en $\mathbb{E}_\alpha$ de $f(x)$. Adjuntando β a $\mathbb{E}_\alpha$ formamos un cuerpo de extensión $\mathbb{E}$ de $\mathbb{E}_\alpha$. Sin embargo, dentro de $\mathbb{E}$, hay un subcuerpo $\mathbb{E}_\beta$ obtenido al adjuntar β a $\mathbb{F}_q$. $\mathbb{E}_\beta$ debe tener q^r elemenetos ya que $f(x)$ es un irreducible de grado r en $\mathbb{F}_q$. Como $\mathbb{E}_\alpha$ y $\mathbb{E}_\beta$ son subcuerpos de $\mathbb{E}$ del mismo tamaño, entonces $\mathbb{E}_\alpha = \mathbb{E}_\beta$, probando que todas las raíces de $f(x)$ se encuentran en $\mathbb{F}_{q^r}$. Luego, como cualquier cuerpo que contenga a $\mathbb{F}_q$ y una raíz de $f(x)$ contiene a $\mathbb{F}_{q^r}$, queda demostrado 1). Para 2), como las α_i son las raíces de $f(x)$ es simplemente su descomposición en factores. Para el apartado 3) lo sacamos a partir del 2) ya que $x^{q^r} - x = \prod_{\alpha \in \mathbb{F}_{q^r}}(x - \alpha)$ por el Teorema 5 □

En particular, este teorema se puede aplicar a polinomios mínimos ya que estos polinomios son mónicos irreducibles.

Lema 1. *Sea $s = p^r$ y $q = p^m$, entonces $(x^s - x) \mid (x^q - x)$ si y solo si $r \mid m$.*

Teorema 12. *Sea $\mathbb{F}_{q^t}$ una extensión de $\mathbb{F}_q$ y sea α un elemento de $\mathbb{F}_{q^t}$ con polinomio mínimo $\mathcal{M}_\alpha(x)$ en $\mathbb{F}_q[x]$. Tenemos lo siguiente:*

1. *$\mathcal{M}_\alpha(x) \mid (x^q - x)$.*
2. *$\mathcal{M}_\alpha(x)$ tiene raíces distintas todas en $\mathbb{F}_{q^t}$.*
3. *El grado de $\mathcal{M}_\alpha(x)$ divide a t.*
4. *$x^{q^t} - x = \prod_\alpha \mathcal{M}_\alpha(x)$, donde α recorre un subconjunto de $\mathbb{F}_{q^t}$ que enumera los polinomios mínimos de todos los elementos de $\mathbb{F}_{q^t}$ exactamente una vez.*
5. *$x^{q^t} - x = \prod_f f(x)$, donde f recorre todos los polinomios mónicos irreducibles de $\mathbb{F}_q$ cuyos grados dividen a t.*

Demostración. El apartado 1) sale del Teorema 10, ya que $\alpha^{q^t} - \alpha = 0$ por el Teorema 5. Como las raíces de $x^{q^t} - x$ son los q^t elementos de $\mathbb{F}_{q^t}$, $x^{q^t} - x$ tiene raíces distintas, luego 1) y por el Teorema 11 se tiene 2). Por el Teorema 7, $x^{q^t} - x = \prod_{i=1}^n p_i(x)$, donde $p_i(x)$ es irreducible en $\mathbb{F}_q$.Como $x^{q^t} - x$ tiene raíces distintas, los factores $p_i(x)$ son distintos. Si los escalamos, podemos asumir que cada uno es mónico ya que $x^{q^t} - x$ es mónico. Así que $p_i(x) = \mathcal{M}_\alpha(x)$ para cualquier $\alpha \in \mathbb{F}_{q^t}$ con $p_i(\alpha) = 0$. Por tanto, tenemos 4). Pero si $\mathcal{M}_\alpha(x)$ tiene grado r, adjuntando α a $\mathbb{F}_q$ obtenemos el subcuerpo $\mathbb{F}_{q^r} = \mathbb{F}_{p^{mr}}$ o $\mathbb{F}_{q^t} = \mathbb{F}_{p^{mt}}$ lo que implica que $mr \mid mt$ y por tanto 3). El apartado 5) se obtiene del 4) si demostramos que cada polinomio mónico irreducible de $\mathbb{F}_q$ de grado r que divide a t es un factor de $x^{q^t} - x$. Pero $f(x) \mid (x^{q^r} - x)$ por el Teorema 11. Y como $mr \mid mt$, $(x^{q^r} - x) | (x^{q^t} - x)$ por el Lema 1.

□

Dos elementos de $\mathbb{F}_{q^t}$ que tienen el mismo polinomio mínimo en $\mathbb{F}_q[x]$ se les llama **conjugados** en $\mathbb{F}_q$. Será importante encontrar todos los conjugados de $\alpha \in \mathbb{F}_q$, ya que, estos son todas las raíces de $\mathcal{M}_\alpha(x)$. Podemos encontrarlos con el siguiente teorema.

Teorema 13. *Sea $f(x)$ un polinomio en $\mathbb{F}_q[x]$ y sea α una raíz de $f(x)$ en una extensión $\mathbb{F}_{q^t}$. Entonces:*

1. *$f(x^q) = f(x)^q$.*
2. *α^q es también una raíz de $f(x)$ en $\mathbb{F}_q$.*

Demostración. Sea $f(x) = \sum_{i=0}^n a_i x^i$. Como $q = p^m$, donde p es la característica de $\mathbb{F}_q$, $f(x)^q = \sum_{i=0}^n a_i^q x^{iq}$. Sin embargo, $a_i^q = a_i$, porque $a_i \in \mathbb{F}_q$ y los elementos de $\mathbb{F}_q$ son raíces de $x^q - x$ por el Teorema 5, hemos probado 1). En particular, $f(\alpha^q) = f(\alpha)^q = 0$ lo que implica 2). □

Si repetimos este teorema vemos que $\alpha, \alpha^q, \alpha^{q^2}, \cdots$ son todas las raíces de $\mathcal{M}_\alpha(x)$. Este proceso termina tras el término r ya que $\alpha^{q^r} = \alpha$.

2

INTRODUCCIÓN A LOS CÓDIGOS LINEALES

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

2.1 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 7. 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 3.
- 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 lineal* 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 8. Una *matriz generadora* de un $[n, k]$ *código lineal* $\mathcal{C}$ es cualquier matriz $k \times n$ cuyas filas forman una base de $\mathcal{C}$.

Para cada conjunto de k filas independientes de una matriz generadora G, se dice que dicho 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 lineal es un subespacio de un espacio vectorial, es el núcleo de alguna transformación lineal.

Definición 9. Una *matriz de paridad* H de dimensión $(n-k) \times k$ es:

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

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 14 (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 4. 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 14, 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*.

2.2 PESOS Y DISTANCIAS

Definición 10. 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 5. Sea $\mathbf{x} = 20110$ y $\mathbf{y} = 10121$ entonces $d(x,y) = 3$.

Teorema 15. *La distancia de Hamming $d(x,y)$ 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 entre dos palabras 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 6. 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 11. El *peso de Hamming*, denotado por $\mathrm{wt}(x)$, 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 7. Sea $\mathbf{x} = 202210$ un vector en $\mathbb{F}_3^6$ entonces $\mathrm{wt}(x) = 4$.

Teorema 16. *Si* $x, y \in \mathbb{F}_q^n$, *entonces* $d(x,y) = \mathrm{wt}(x - y)$. *Si* $\mathcal{C}$ *es un código lineal, la distancia mínima d es igual al peso mínimo 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 $d(x,y) = \mathrm{wt}(x - y) \geq \mathrm{wt}(\mathcal{C})$ para cualesquiera $x, y \in \mathcal{C}$. Se tiene que $d(\mathcal{C}) \geq \mathrm{wt}(\mathcal{C})$.

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

Como resultado de este teorema, para códigos lineales, la *distancia mínima* 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.

2.3 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 12. 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 $i \to i+1 (\, mod\, n)$, está también en $\mathcal{C}$.

Así, un código cíclico contiene las n permutaciones cíclicas 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 $\mathcal{C}$, entonces $xc(x)$ también lo está.

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 $\mathcal{R}_n$. Para este estudio necesitamos factorizar el polinomio $x^n - 1$.

2.3.1 *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, que es equivalente a que q y n son primos relativos.

Como ayuda para factorizar $x^n - 1$ sobre $\mathbb{F}_q^n$, es útil considerar la extensión $\mathbb{F}_{q^t}^n$ 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 se verifica si y solo si $sq^r \equiv s \,(mod\, n)$

Definición 13. Sea $\mathbb{F}_q^n$ un cuerpo finito y $\mathbb{F}_{q^t}^n$ una extensión de $\mathbb{F}_q^n$, 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 8. Vamos a calcular las clases *2-ciclotómicas* para $n = 15$ y $q = 2$:

La primera de todas es $\mathcal{C}_0 = \{0 * 2^r \equiv 0 \,(mod\, 15)\} = \{0\}$ y repetimos este proceso. Luego tenemos:

$\mathcal{C}_1 = \{1 * 2^r \equiv 1 \,(mod\, 15)\} = \{1, 1*2^1 = 2, 1*2^2 = 4, 1*2^3 = 8\} = \{1, 2, 4, 8\}$ ya que $1 * 2^4 = 16 \equiv 1 \,(mod\, 15)$ luego $r = 4$.

$\mathcal{C}_3 = \{3 * 2^r \equiv 3 \,(mod\, 15)\} = \{3, 3*2 = 6, 3*2^2 = 12, 3*2^3 = 9\} = \{3, 6, 9, 12\}$ ya que $3 * 2^4 = 48 \equiv 3 \,(mod\, 15)$ luego $r = 4$.

$\mathcal{C}_5 = \{5 * 2^r \equiv 5 \,(mod\, 15)\} = \{5, 5*2 = 10\} = \{5, 10\}$ ya que $5 * 2^2 = 20 \equiv 5 \,(mod\, 15)$ luego $r = 2$.

$\mathcal{C}_7 = \{7 * 2^r \equiv 7 \,(mod\, 15)\} = \{7, 7*2 = 14, 7*2^2 = 13, 7*2^3 = 11\} = \{7, 11, 13, 14\}$ ya que $7 * 2^4 = 112 \equiv 7 \,(mod\, 15)$ luego $r = 4$.

Ejemplo 9. Vamos a calcular las clases *3-ciclotómicas* para $n = 8$ y $q = 3$ que serán las siguientes :

$\mathcal{C}_0 = \{0 * 3^r \equiv 0 \,(mod\, 8)\} = \{0\}$

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

$\mathcal{C}_2 = \{2 * 3^r \equiv 2 \,(mod\, 8)\} = \{2, 2*3^1 = 6\} = \{2, 6\}$ ya que $2 * 3^2 = 18 \equiv 2 \,(mod\, 8)$ luego $r = 2$.

$\mathcal{C}_4 = \{4 * 3^r \equiv 4 \,(mod\, 8)\} = \{4\}$ ya que $4 * 3^1 = 12 \equiv 4 \,(mod\, 8)$ luego $r = 1$.

$\mathcal{C}_5 = \{5 * 3^r \equiv 5\,(mod\,8)\} = \{5, 5 * 3^1 = 7\} = \{5, 7\}$ ya que $5 * 3^2 = 45 \equiv 5\,(mod\,8)$ luego $r = 2$.

Luego, ya tenemos todas las clases *3-ciclotómicas* para $n = 8$ y $q = 3$.

Teorema 17. *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 10. Vamos a factorizar $x^{15} - 1$ para ello, cogemos las clases *2-ciclotómicas* calculadas en el Ejemplo 8 que son $\mathcal{C}_0 = \{0\}$, $\mathcal{C}_1 = \{1, 2, 4, 8\}$, $\mathcal{C}_3 = \{3, 6, 9, 12\}$, $\mathcal{C}_5 = \{5, 108\}$ y $\mathcal{C}_7 = \{7, 11, 13, 14\}$. Siendo un conjunto de representantes $\{0, 1, 3, 5, 7\}$. Luego el $ord_{15}(2) = 4$ y la raíz primitiva *quince-ésima* de la unidad reside en la extensión $\mathbb{F}_{16}$.

Podemos afirmar que los factores irreducibles de $x^{15} - 1$ tienen grado 1,4,4,2 y 4. Estos polinomios son $\mathcal{M}_1(x) = x + 1$, $\mathcal{M}_\alpha(x)$, $\mathcal{M}_{\alpha^3}(x)$, $\mathcal{M}_{\alpha^5}(x)$ y $\mathcal{M}_{\alpha^7}(x)$ donde α es la raíz primitiva *quince-ésima* de la unidad en $\mathbb{F}_{16}$. Como el único polinomio irreducible de grado dos en $\mathbb{F}_2$ es $x^2 + x + 1$ no queda otra que sea $\mathcal{M}_{\alpha^5}(x)$. Usando la raíz primitiva *quince-ésima* de la unidad α y que $x^4 + x + 1$ es irreducible en $\mathbb{F}_2$ ya que $x^2 + x + 1$ no es un factor suyo y $x + 1$ tampoco, podemos obtener la siguiente tabla,

0000	0	1000	α^3	1011	α^7	1110	α^{11}
0001	1	0011	α^4	0101	α^8	1111	α^{12}
0010	α	0110	α^5	1010	α^9	1101	α^{13}
0100	α^2	1100	α^6	0111	α^{10}	1001	α^{14}

Cuadro 1: $\mathbb{F}_{16}$ con elemento primitivo α donde $\alpha^4 = \alpha + 1$

Aplicamos el Teorema 17 para obtener el resto de factores de $x^{15} - 1$.

$$x^{15} - 1 = \mathcal{M}_1(x)\mathcal{M}_\alpha(x)\mathcal{M}_{\alpha^3}(x)\mathcal{M}_{\alpha^5}(x)\mathcal{M}_{\alpha^7}(x).$$

Calculemos $\mathcal{M}_{\alpha}(x)$,$\mathcal{M}_{\alpha^3}(x)$ y $\mathcal{M}_{\alpha^7}(x)$:

$$\begin{aligned}\mathcal{M}_{\alpha}(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)\\ &= (x^2+\alpha^2x+\alpha x+\alpha^3)(x^2+\alpha^8x+\alpha^4x+\alpha^{12})\\ &= (x^2+(\alpha^2+\alpha)x+\alpha^3)(x^2+(\alpha^2+\alpha)x+\alpha^{12})\\ &= x^4+(\alpha^2+\alpha+\alpha^2+\alpha)x^3+(\alpha^{12}+\alpha^4+\alpha^2+\alpha^3)x^2+(\alpha^{14}+\alpha^{13}+\alpha^5+\alpha^4)x+1\\ &= x^4+x+1\end{aligned}$$

$$\begin{aligned}\mathcal{M}_{\alpha^3}(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12})\\ &= (x^2+\alpha^6x+\alpha^3x+\alpha^9)(x^2+\alpha^{12}x+\alpha^9x+\alpha^6)\\ &= (x^2+\alpha^2x+\alpha^9)(x^2+(\alpha^2+1)x+\alpha^6)\\ &= x^4+(\alpha^2+1+\alpha^2)x^3+(\alpha^6+\alpha^4+\alpha^2+\alpha^9)x^2+(\alpha^8+\alpha^{11}+\alpha^9)x+1\\ &= x^4+x^3+x^2+x+1\end{aligned}$$

$$\begin{aligned}\mathcal{M}_{\alpha^7}(x) &= (x-\alpha^7)(x-\alpha^{11})(x-\alpha^{13})(x-\alpha^{14})\\ &= (x^2+\alpha^7x+\alpha^{11}x+\alpha^3)(x^2+\alpha^{13}x+\alpha^{14}x+\alpha^{12})\\ &= (x^2+(\alpha^2+1)x+\alpha^3)(x^2+\alpha^2x+\alpha^{12})\\ &= x^4+(\alpha^2+\alpha^2+1)x^3+(\alpha^{12}+\alpha^4+\alpha^2+\alpha^3)x^2+(\alpha^{14}+\alpha^{12}+\alpha^5)x+1\\ &= x^4+x^3+1\end{aligned}$$

Por tanto, podemos concluir que la factorización de $x^{15}-1$ es

$$x^{15}-1=(x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1)$$

Ejemplo 11. Ahora vamos a factorizar x^8-1 para ello, cogemos las clases *3-ciclotómicas* calculadas en el Ejemplo 9 que son $\mathcal{C}_0=\{0\}$, $\mathcal{C}_1=\{1,3\}$, $\mathcal{C}_2=\{2,6\}$, $\mathcal{C}_4=\{4\}$ y $\mathcal{C}_5=\{5,7\}$ .Siendo un conjunto de representantes $\{0,1,2,4,5\}$. Luego el $ord_8(3)=2$ y la raíz primitiva *ocho-ésima* de la unidad reside en la extensión $\mathbb{F}_9$.

Podemos afirmar que los factores irreducibles de x^8-1 tienen grado 1,2,2,1 y 2. Estos polinomios son $\mathcal{M}_1(x)$, $\mathcal{M}_{\alpha}(x)$, $\mathcal{M}_{\alpha^2}(x)$, $\mathcal{M}_{\alpha^4}(x)$ y $\mathcal{M}_{\alpha^5}(x)$ donde α es la raíz primitiva *ocho-ésima* de la unidad en $\mathbb{F}_9$. Usando la raíz primitiva *ocho-ésima* de la unidad α y que x^2+x+1 es irreducible en $\mathbb{F}_3$ ya que $x+2$ no es un factor suyo y $x+1$ tampoco, podemos obtener la siguiente tabla,

00	0	21	α^3	12	α^7
01	1	02	α^4		
10	α	20	α^5		
11	α^2	22	α^6		

Cuadro 2: $\mathbb{F}_9$ con elemento primitivo α donde $\alpha^2 = \alpha + 1$

Aplicamos el Teorema 17 para obtener los factores de $x^8 - 1$.

$$x^8 - 1 = \mathcal{M}_1(x)\mathcal{M}_\alpha(x)\mathcal{M}_{\alpha^2}(x)\mathcal{M}_{\alpha^4}(x)\mathcal{M}_{\alpha^5}(x).$$

$$\mathcal{M}_1(x) = (x-1) = x+2$$

$$\begin{aligned}\mathcal{M}_\alpha(x) &= (x-\alpha)(x-\alpha^3)\\ &= x^2 - \alpha x - \alpha^3 x + \alpha^4\\ &= x^2 - (\alpha+\alpha^3)x + 2\\ &= x^2 + 2x + 2\end{aligned}$$

$$\begin{aligned}\mathcal{M}_{\alpha^2}(x) &= (x-\alpha^2)(x-\alpha^6)\\ &= x^2 - \alpha^2 x - \alpha^6 x + 1\\ &= x^2 - (\alpha^2+\alpha^6)x + 1\\ &= x^2 + 1\end{aligned}$$

$$\mathcal{M}_{\alpha^4}(x) = (x-\alpha^4) = x-2 = x+1$$

$$\begin{aligned}\mathcal{M}_{\alpha^5}(x) &= (x-\alpha^5)(x-\alpha^7)\\ &= x^2 - \alpha^5 x - \alpha^7 x + \alpha^4\\ &= x^2 - (\alpha^5+\alpha^7)x + 2\\ &= x^2 + x + 2\end{aligned}$$

Por tanto, podemos concluir que la factorización de $x^8 - 1$ es

$$x^8 - 1 = (x+2)(x^2+2x+2)(x^2+1)(x+1)(x^2+x+2)$$

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

Teorema 18. *El tamaño de cada clase q-ciclotómica es un divisor del $ord_n(q)$. Además, el tamaño de 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 $\mathcal{C}_1 = ord_n(q)$. □

2.3.2 *Teoría básica de los códigos cíclicos*

Anteriormente, comentábamos 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 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 19. *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 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 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).

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 $x^n - 1$ corresponde con la palsbra código 0 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 17. □

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 el Teorema 19. Asumiendo 2), sea $g_1(x)$ un polinomio mónico de menor grado en $\mathcal{C}$. Por la demostración del Teorema 19 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 $\mathbb{F}_q[x]$, son iguales. □

Del teorema, obtenemos que $g(x)$ es un polinomio mónico que divide a $x^n - 1$ y genera a $\mathcal{C}$. Del corolario, obtenemos 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 entre los códigos cíclicos no nulos y los divisores de $x^n - 1$. 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 12. Para el polinomio $x^7 - 1$ en $\mathbb{F}_2$, calculamos sus clases *2-ciclotómicas* que son $\mathcal{C}_0 = \{0\}$, $\mathcal{C}_1 = \{1, 2, 4\}$ y $\mathcal{C}_3 = \{3, 5, 6\}$. Luego, sus tamaños son 1,3 y 3, por tanto, por el corolario anterior sabemos que hay $2^3 = 8$ códigos cíclicos y sus dimensiones son : $0, 1, 3, 3, 4, 4, 6, 7$. Veamos los polinomios generadores de cada uno en la siguiente tabla.

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

2.3.3 *Ceros de un código cíclico*

Definición 14. Sea $\mathcal{C}$ un código cíclico en $\mathcal{R}_n$ con polinomio generador $g(x)$. Luego, $g(x) = \prod_s \mathcal{M}_{\alpha^s}(x) = \prod_s \prod_{i \in \mathcal{C}_s} (x - \alpha^i)$ donde s recorre un subconjunto de los representantes de las clases *q-ciclotómicas* $\mathcal{C}_s$ módulo n. Sea T $= \cup_s \mathcal{C}_s$ la unión de estas clases *q-ciclotómicas*. Llamaremos **ceros** de un código cíclico a $\mathcal{Z} = \{\alpha^i \mid i \in T\}$ y **no-ceros** a $\{\alpha^i \mid i \notin T\}$. Al conjunto T, lo llamaremos **conjunto de definición** de $\mathcal{C}$

Nos damos cuenta de que T y por tanto, el conjunto de ceros y no-ceros, determina completamente al polinomio generador $g(x)$. Por el Teorema 19 , la dimensión de $\mathcal{C}$ es $n -$ | T | y | T | es el grado de $g(x)$

Ejemplo 13. Mostraremos el conjunto de definición para cada código cíclico relativo a la raíz primitiva α

i	dimensión	$g_i(x)$	conjunto de definición
0	0	$x^{10}-1$	$\{0,1,2,3,4,5,6,7,8,9\}$
1	1	$x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$	$\{1,2,3,4,5,6,7,8,9\}$
2	1	$x^9+x^8+x^7+2x^6+x^5+2x^4+x^3+2x^2+x+2$	$\{0,1,2,3,4,6,7,8,9\}$
3	2	$x^8+x^6+x^4+x^2+1$	$\{1,2,3,4,6,7,8,9\}$
4	4	x^6+2x^5+x+2	$\{0,2,4,5,6,8\}$
5	4	x^6+x^5+2x+2	$\{0,1,3,5,7,9\}$
6	5	x^5+1	$\{2,4,5,6,8\}$
7	5	$x^5+x^4+2x^3+x^2+2x+2$	$\{0,2,4,6,8\}$
8	5	$x^5+2x^4+2x^3+2x^2+2x+1$	$\{1,3,5,7,9\}$
9	5	x^5+2	$\{0,1,3,7,9\}$
10	6	$x^4+2x^3+x^2+2x+1$	$\{2,4,6,8\}$
11	6	$x^4+x^3+x^2+x+1$	$\{1,3,7,9\}$
12	8	x^2+3x+2	$\{0,5\}$
13	9	$x+1$	$\{5\}$
14	9	$x+2$	$\{0\}$
15	10	1	$\emptyset$

El siguiente teorema nos da propiedades básicas de los códigos cíclicos en relación a los conjuntos de definición.

Teorema 20. *Sea α la n-ésima raíz primitiva de la unidad en un cuerpo de extensión de $\mathbb{F}_q$. Sea $\mathcal{C}$ un código cíclico de longitud n en $\mathbb{F}_q$ con conjunto de definición T y polinomio generador $g(x)$. Se verifica lo siguiente:*

1. *T es la unión de las clases q-ciclotómicas módulo n.*
2. $g(x) = \prod_{i \in T}(x - \alpha^i)$.
3. $c(x) \in \mathcal{R}_n \Leftrightarrow c(\alpha^i) = 0 \, \forall i \in T$.
4. *La dimensión de $\mathcal{C}$ es $n - \mid T \mid$.*

2.3.4 *Distancia mínima de códigos cíclicos*

Es importante saber cual es la distancia mínima que puede alcanzar cualquier código, para así poder determinar su capacidad de corrección de errores. Luego, es útil encontrar cotas inferiores para la distancia mínima. Una de las cotas más antiguas es la cota de *Bose-Ray-Chaudhuri-Hocquenghem*, normalmente conocida como la *cota BCH* que nos servirá para definir los códigos BCH más adelante.

Antes de definir la cota BCH, vamos a dar un lema sobre el determinante de la matriz de Vandermonde que nos servirá para probar dicha cota.

Lema 2. *det* $V = \prod_{1 \leq i < j \leq s}(\alpha_j - \alpha_i)$ *. En particular, V es regular si los elementos* $\alpha_1, \cdots, \alpha_s$ *son distintos.*

Teorema 21 (Cota inferior BCH). *Sea* $\mathcal{C}$ *un código cíclico de longitud n sobre* $\mathbb{F}_q$ *con conjunto de definición T. Supongamos que d es el peso mínimo de* $\mathcal{C}$*. Asumimos que T contiene los* $\delta - 1$ *elementos consecutivos para un entero* δ*. Entonces* $d \geq \delta$*.*

Demostración. Asumimos que $\mathcal{C}$ tiene ceros que incluye a $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+\delta-2}$. Sea $c(x)$ una palabra código no-nula en $\mathcal{C}$ de peso w y sea

$$c(x) = \sum_{j=1}^{w} c_{i_j} x^{i_j}$$

Asumimos por el contrario que $w < \delta$. Como $c(\alpha^i) = 0$ para $b \leq i \leq b + \delta - 2$, $Mu^T = 0$, donde

$$M = \begin{pmatrix} \alpha^{i_1 b} & \alpha^{i_2 b} & \cdots & \alpha^{i_w b} \\ \alpha^{i_1 (b+1)} & \alpha^{i_2 (b+1)} & \cdots & \alpha^{i_w (b+1)} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{i_1 (b+w-1)} & \alpha^{i_2 (b+w-1)} & \cdots & \alpha^{i_w (b+w-1)} \end{pmatrix}$$

y $u = c_{i_1} c_{i_2} \cdots c_{i_w}$. Como $u \neq 0$, M es una matriz singular y por tanto $det\, M = 0$. Pero $det\, M = \alpha^{(i_1 + i_2 + \cdots + i_w)^b} det\, V$, donde V es la matriz de Vandermonde :

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_w} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{i_1 (w-1)} & \alpha^{i_2 (w-1)} & \cdots & \alpha^{i_w (w-1)} \end{pmatrix}$$

Como los α^{i_j} son distintos, $det\, V \neq 0$ por el Lema 2, contradiciendo que $det\, M = 0$. □

Ejemplo 14. Sea $\mathcal{C}$ el $[10, 2, d]$ código cíclico binario con conjunto de definición $T = \{1, 2, 3, 4, 6, 7, 8, 9\}$. Si aplicamos la cota BCH a $\mathcal{C}$, vemos que $d \geq 5$ ya que el conjunto con más elementos consecutivos es de tamaño 4.

2.4 CÓDIGOS BCH Y REED-SOLOMON

En esta parte examinaremos una de las muchas importantes familias de códigos cíclicos que se conocen como los códigos BCH junto a una subfamilia que se la conoce como códigos Reed-Solomon.

2.4.1 *Códigos BCH*

Los códigos BCH son códigos cíclicos diseñados para aprovecharse de la cota BCH. Queremos construir un código cíclico $\mathcal{C}$ de longitud n sobre $\mathbb{F}_q$ que tenga simultáneamente un peso mínimo alto y una alta dimensión. Tener un peso mínimo alto, con la cota BCH , se puede obtener elegiendo un conjunto de definición T de $\mathcal{C}$ con un número grande de elementos consecutivos. Ya que la dimensión de $\mathcal{C}$ es $n- \mid T \mid$, si tiene distancia mínima al menos δ, podemos elegir un conjunto de definición tan pequeño como nos sea posible tal que sea la unión de las clases q-ciclotómicas con $\delta - 1$ elementos consecutivos.

Definición 15. Sea δ un entero tal que $2 \leq \delta \leq n$. Un **código BCH** $\mathcal{C}$ en $\mathbb{F}_q$ con longitud n y distancia predefinida δ es un código cíclico con conjunto de definición

$$T = \mathcal{C}_b \cup \mathcal{C}_{b+1} \cup \cdots \cup \mathcal{C}_{b+\delta-2}$$

donde $\mathcal{C}_i$ es la clase q-ciclotómica módulo n que contiene a i. Por la cota BCH, este código tiene al menos distancia mínima δ.

Teorema 22. *Un código BCH con distancia predefinida δ tiene peso mínimo al menos δ.*

Demostración. El conjunto de definición T que hemos definido anteriormente tiene $\delta - 1$ elementos consecutivos, luego el resultado lo obtenemos de aplicar la cota BCH. □

Si variamos el valor de b en el conjunto de definición, podemos obtener una variedad de códigos con diferentes distancias mínimas y dimensiones. Cuando $b = 1$, $\mathcal{C}$ se le conoce como **código BCH en sentido estricto**. Como con cualquier código cíclico, si $n = q^t - 1$, entonces $\mathcal{C}$ se le conoce como **código BCH primitivo**.

Ejemplo 15. Vamos construir un código BCH sobre $\mathbb{F}_2$ de longitud 15. Las clases 2-ciclotómicas módulo 15 son las calculadas en el Ejemplo 8 :

$\mathcal{C}_0 = \{0\}$, $\mathcal{C}_1 = \{1, 2, 4, 8\}$, $\mathcal{C}_3 = \{3, 6, 9, 12\}$, $\mathcal{C}_5 = \{5, 108\}$, $\mathcal{C}_7 = \{7, 11, 13, 14\}$.

Como $ord_{15}(2) = 4$, $x^{15} - 1$ tiene todas sus raíces en $\mathbb{F}_{2^4}$. Tenemos que el código BCH en sentido estricto $\mathcal{C}_1$ con distancia predefinida 3, tiene de conjunto de definición $T = \mathcal{C}_1 \cup \mathcal{C}_2 = \{1, 2, 4, 8\}$ y de polinomio generador $g_1(x) = x^4 + x + 1$. Por el Teorema 22, $\mathcal{C}_1$ tiene peso mínimo al menos 3.

2.4.2 *Códigos Reed-Solomon*

Definiremos los códigos Reed-Solomon como una subfamilia de los códigos BCH.

Definición 16. Un **código Reed-Solomon**, abreviado como *código RS*, sobre $\mathbb{F}_q$ es un código BCH de longitud $n = q - 1$.

Luego, $ord_n(q) = 1$ lo que implica que todos los factores irreducibles de $x^n - 1$ son de grado 1 y todas sus clases q-ciclotómicas tienen tamaño 1. De hecho,las raíces de $x^n - 1$ son exactamente los elementos no nulos de $\mathbb{F}_q$, y una n-ésima raíz primitiva de la unidad es un elemento primitivo de $\mathbb{F}_q$. Así que, si $\mathcal{C}$ tiene distancia predefinida δ, el conjunto de definición de $\mathcal{C}$ tiene tamaño $\delta - 1$ y es $T = \{b, b+1, \cdots, b+\delta-2\}$ para algún entero b. Por el Teorema 22 y la cota de Singleton, la dimensión k y la distancia mínima d de $\mathcal{C}$ satisfacen que $k = n - \delta + 1 \geq n - d + 1 \geq k$. Luego, ambas inigualdades son igualdades lo que implica que $d = \delta$ y $k = n - d + 1$.

Teorema 23. *Sea $\mathcal{C}$ un código RS sobre $\mathbb{F}_q$ de longitud $n = q - 1$ y con distancia predefinida δ. Entonces :*

1. *$\mathcal{C}$ tiene como conjunto de definición $T = \{b, b+1, \cdots, b+\delta-2\}$ para algún entero b.*
2. *$\mathcal{C}$ tiene distancia mínima $d = \delta$ y dimensión $k = n - d + 1$.*

Ejemplo 16. Vamos a definir un código Reed-Solomon utilizando el Teorema 23 . Un código de longitud 8 y conjunto de definición $\{1, 2, 3\}$ es un código $\mathcal{C}$ con distancia mínima 4 y es un $[8, 5, 4]$ código.

2.4.3 *Algoritmo de Decodificación de Peterson-Gorensein-Zierler*

Sea $\mathcal{C}$ un código BCH sobre $\mathbb{F}_q$ con longitud n y distancia predefinida δ. Como la distancia mínima de $\mathcal{C}$ es al menos δ, podemos corregir al menos $t = \lfloor (\delta - 1)/2 \rfloor$ errores. El algoritmo de decodificación Peterson-Gorenstein-Zierler puede corregir hasta t errores. Mientras que el algoritmo se puede aplicar a cualquier código BCH, podemos simplicarlo si asumimos que $\mathcal{C}$ es en sentido estricto. Por lo tanto, el conjunto de definición T de $\mathcal{C}$ asumimos que contiene $\{1, 2, \cdots, \delta - 1\}$, con α siendo la n-ésima raíz primitiva de la unidad en un cuerpo de extensión $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$, donde $m = ord_n(q)$, usado para determinar este conjunto de definición. El alogritmo requiere cuatro pasos que vamos a describir en orden y más tarde, resumir.

Supongamos que recibimos $y(x)$, asumimos que $y(x)$ difiere de una palabra código $c(x)$ en al menos t coordenadas. Por tanto, $y(x) = c(x) + e(x)$, donde $c(x) \in \mathcal{C}$ y $e(x)$ es el vector de error con peso $v \leq t$. Supongamos que los errores ocurren en coordenadas desconocidas $k_1, k_2, \cdots, k_v$. Luego,

$$e(x) = e_{k_1} x^{k_1} + e_{k_2} x^{k_2} + \cdots + e_{k_v} x^{k_v}$$

Una vez determinamos $e(x)$, nos falta encontrar donde ocurren los errores k_j y sus magnitudes e_{k_j}, entonces podemos decodificar el vector recibido como $c(x) = y(x) - e(x)$. Recordemos que por el Teorema 20 $c(x) \in \mathcal{C}$ si y solo si $c(\alpha^i) = 0 \, \forall i \in T$. En particular, $y(\alpha^i) = c(\alpha^i) + e(\alpha^i) = e(\alpha^i) \, \forall 1 \leq i \leq 2t$, ya que $2t \leq \delta - 1$. Para $1 \leq i \leq 2t$, definimos el **síndrome** S_i de $y(x)$ como un elemento $S_i = y(\alpha^i)$ en $\mathbb{F}_{q^m}$

El *primer paso* del algoritmo es calcular los síndromes $S_I = y(\alpha^i)$ para $1 \leq i \leq 2t$ del vector recibido.

Teorema 24. $S_{iq} = S_i^q \; \forall i \geq 1$.

Los síndromes dan lugar a un sistema de ecuaciones que envuelven las localizaciones desconocidas de los errores y sus magnitudes. Además, los síndromes satisfacen :

$$S_i = y(\alpha^i) = \sum_{j=1}^{v} e_{k_j}(\alpha^i)^{k_j} = \sum_{j=1}^{v} e_{k_j}(\alpha^{k_j})^i$$

para $1 \leq i \leq 2t$. Para simplicar la notación, para los $1 \leq j \leq v$, llamaremos $E_j = e_{k_j}$ a *la magnitud del error en la coordenada* k_j y a $X_j = \alpha^{k_j}$ como *el número de localización correspondiente a la localización del error* k_j. Por el Teorema si $\alpha^i = \alpha^k$ para i y k entre 0 y $n-1$, entonces $i = k$. Por tanto, sabiendo que X_j determina únicamente la localización del error k_j. Con esta notación tenemos :

$$S_i = \sum_{j=1}^{v} E_j X_j^i \quad para \quad 1 \leq i \leq 2t \tag{1}$$

del cual podemos obtener el siguiente sistema de ecuaciones:

$$S_1 = E_1X_1 + E_2X_2 + \cdots + E_vX_v \tag{2}$$

$$\begin{aligned} S_2 &= E_1X_1^2 + E_2X_2^2 + \cdots + E_vX_v^2 \\ S_3 &= E_1X_1^3 + E_2X_2^3 + \cdots + E_vX_v^3 \\ &\vdots \\ S_{2t} &= E_1X_1^{2t} + E_2X_2^{2t} + \cdots + E_vX_v^{2t} \end{aligned}$$

Este sistema es no-lineal en las X_js con coeficientes desconocidos E_j. La estrategia es usar 1 para crear un sistema lineal que envuelve nuevas variables $\sigma_1, \sigma_2, \cdots, \sigma_v$ por las que obtendremos directamente los números de localización de los errores. Luego, tenemos el sistema 2 que es lineal en las E_js y lo resolvemos para obtener las magnitudes.

Definición 17. Llamamos **polinomio localizador de errores** a

$$\sigma(x) = (1 - xX_1)(1 - xX_2)\cdots(1 - xX_v) = 1 + \sum_{i=1}^{v} \sigma_i x^i$$

Las raíces de $\sigma(x)$ son los inversos de los números de localización de los errores y por tanto,

$$\sigma(X_j^{-1}) = 1 + \sigma_1 X_j^{-1} + \sigma_2 X_j^{-2} + \cdots + \sigma_v X_j^{-v} = 0$$

para $1 \leq j \leq v$. Multiplicando por $E_j X_j^{i+v}$ tenemos,

$$E_j X_j^{i+v} + \sigma_1 E_j X_j^{i+v-1} + \cdots + \sigma_v E_j X_j^{i} = 0$$

para cualquier i. Sumando esto para j con $1 \leq j \leq v$, obtenemos

$$\sum_{j=1}^{v} E_j X_j^{i+v} + \sigma_1 \sum_{j=1}^{v} E_j X_j^{i+v-1} + \cdots + \sigma_v \sum_{j=1}^{v} E_j X_j^{i} = 0 \tag{3}$$

Siempre que $1 \leq i$ y $i + v \leq 2t$, estas sumas son los síndromes obtenidos en 1. Porque $v \leq t$, 3 se convierte en :

$$S_{i+v} + \sigma_1 S_{i+v-1} + \sigma_2 S_{i+v-2} + \cdots + \sigma_v S_i = 0$$

o

$$\sigma_1 S_{i+v-1} + \sigma_2 S_{i+v-2} + \cdots + \sigma_v S_i = -S_{i+v} \tag{4}$$

válido para $1 \leq i \leq v$. Por tanto, podemos encontrar los σ_ks si resolvemos la siguiente ecuación matricial.

$$\begin{pmatrix} S_1 & S_2 & S_3 & \cdots & S_{v-1} & S_v \\ S_2 & S_3 & S_4 & \cdots & S_v & S_{v+1} \\ S_3 & S_4 & S_5 & \cdots & S_{v+1} & S_{v+2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ S_v & S_{v+1} & S_{v+2} & \cdots & S_{2v-2} & S_{2v-1} \end{pmatrix} \begin{pmatrix} \sigma_v \\ \sigma_{v-1} \\ \sigma_{v-2} \\ \vdots \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} -S_{v+1} \\ -S_{v+2} \\ -S_{v+3} \\ \vdots \\ -S_{2v} \end{pmatrix} \tag{5}$$

El *segundo paso* del algoritmo será resolver 5 para $\sigma_1, \cdots, \sigma_v$. Cuando este paso esté completado, los $\sigma(x)$ estarán determinados. Sin embargo, determinar los $\sigma(x)$ es complicado ya que no conocemos v, y por tanto, no podemos saber el tamaño del sistema involucrado. Queremos buscar la solución que tenga el menor valor de v posible y por ello, tenemos el siguiente lema.

Lema 3. *Sea $\mu \leq t$ y sea* $M_\mu = \begin{pmatrix} S_1 & S_2 \cdots & S_\mu \\ S_2 & S_3 & \cdots S_{\mu+1} \\ \vdots & \vdots & \vdots \\ S_\mu & S_{\mu+1} & \cdots \end{pmatrix}$ *$S_{2\mu-1}$*

Entonces M_μ es invertible si $\mu = v$ y singular si $\mu > v$, donde v es el número de errores que han ocurrido.

Demostración. Si $\mu > v$, sea $X_{v+1} = X_{v+2} = \cdots = X_\mu = 0$ y $E_{v+1} = E_{v+2} = \cdots = E_\mu = 0$. Tenemos A_μ y B_μ que son

$$A_\mu = \begin{pmatrix} 1 & 1 \cdots & 1 & \\ X_1 & X_2 & \cdots X_\mu & \\ \vdots & \vdots & \vdots & \vdots \\ X_1^{\mu-1} & X_2^{\mu-1} & \cdots & X_\mu^{\mu-1} \end{pmatrix} \text{ y } B_\mu = \begin{pmatrix} E_1X_1 & 0 \cdots & 0 & \\ 0 & E_2X_2 & \cdots 0 & \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & E_\mu X_\mu \end{pmatrix}$$

entonces $M_\mu = A_\mu B_\mu A_\mu^T$. Por tanto, $det(M_\mu) = det(A_\mu)det(B_\mu)det(A_\mu)$. Si $\mu > v$, $det(B_\mu) = 0$ ya que B_μ es una matriz diagonal con 0 en la diagonal. Si $\mu = v$, entonces $det(B_\mu) \neq 0$, ya que B_μ es una matriz diagonal con elementos no nulos en la diagonal. Además $det(A_\mu) \neq 0$ por el Lema 2 porque A_μ es una matriz de Vandermonde con $X_1, \cdots, X_\mu$ distintos. Por tanto, M_μ es invertible si $\mu = v$. □

Para ejecutar el segundo paso del algoritmo, intentamos adivinar el número v de errores. Llamaremos μ a ese intento y empezaremos con $\mu = t$ que es el número más grande que puede tomar v. La matriz de coeficientes del sistema lineal 5 que intentamos resolver es $M_\mu = M_t$ por el Lema anterior. Si M_μ es singular, entonces reducimos μ a $\mu = t - 1$ y vemos si $M_\mu = M_{t-1}$ es singular. Continuamos con este proceso hasta encontrar alguna M_μ invertible. Con $v = \mu$, resolvemos 5 y por tanto, obtenemos $\sigma(x)$.

El *tercer paso* es encontrar las raíces de $\sigma(x)$ e invertirlas para determinar los números de localización de los errores. Se suele completar haciendo una busca exhaustiva comprobando $\sigma(\alpha^i)$ para $0 \leq i < n$.

El *cuarto paso* es insertar los números obtenidos en el paso tres en 2 y resolver el sistema lineal para las magnitudes de los errores E_j. De hecho, solo necesitamos considerar las primeras v ecuaciones en 2 por el siguiente motivo. La matriz de coeficientes de las primeras v ecuaciones tiene por determinante

$$det \begin{pmatrix} X_1 & X_2 \cdots & X_v & \\ X_1^2 & X_2^2 & \cdots X_v^2 & \\ \vdots & \vdots & \vdots & \vdots \\ X_1^v & X_2^v & \cdots & X_v^v \end{pmatrix} = X_1X_2 \cdots X_\mu \begin{pmatrix} 1 & 1 \cdots & 1 & \\ X_1 & X_2 & \cdots X_v & \\ \vdots & \vdots & \vdots & \vdots \\ X_1^{v-1} & X_2^{v-1} & \cdots & X_\mu^{v-1} \end{pmatrix}$$

El determinante de la matriz de la derecha es el determinante de una matriz de Vandermonde, luego es no nulo y los X_j son distintos.

Resumiendo, el **Algoritmo de Decodificación Peterson-Gorenstein-Zierler** para códigos BCH sigue los siguientes pasos:

1. Calcular los síndromes $S_i = y(\alpha^i)$ para $1 \leq i \leq 2t$.

2. En el orden $\mu = t$, $\mu = t-1$, $\cdots$ decidir si M_μ es singular, parando para el primer valor de μ en el que M_μ es invertible. Cogemos $v = \mu$ y resolvemos 5 para obtener $\sigma(x)$.
3. Encontramos las raíces de $\sigma(x)$, calculando $\sigma(\alpha^i)$ para $0 \leq i < n$. Invertimos esas raíces para obtener los número de localización de errores X_j.
4. Resolvemos las primeras v ecuaciones de 2 para obtener las magnitudes de los errores E_j.

Ejemplo 17. Sea $\mathcal{C}$ el $[15, 5]$ código binario BCH en sentido estricto con distancia predefinida $\delta = 6$, que tiene como conjunto de definición $T = \{3, 5, 6, 7, 9, 10, 11, 12, 13, 14\}$. Usando la raíz primitiva 15-ésima de la unidad α que podemos ver en la siguiente tabla,

0000	0	1000	α^3	0111	α^7	1101	α^{11}
0001	1	1001	α^4	1110	α^8	0011	α^{12}
0010	α	1011	α^5	0101	α^9	0110	α^{13}
0100	α^2	1111	α^6	1010	α^{10}	1100	α^{14}

Cuadro 3: $\mathbb{F}_{16}$ con elemento primitivo α donde $\alpha^4 = \alpha^3 + 1$

Tenemos que el polinomio generador de $\mathcal{C}$ es $g(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$. Supongamos que $\mathcal{C}$ va a transmitir una palabra código y recibimos $y(x) = x^{12} + x^{10} + x^6 + x^4 + x^3 + x + 1$. Usando la tabla anterior y el Teorema 24, aplicando el primer paso obtenemos,

$$S_1 = 1 + \alpha + \alpha^3 + \alpha^4 + \alpha^6 + \alpha^{10} + \alpha^{12} = \alpha^2$$

$$S_2 = S_1^2 = (\alpha^2)^2 = \alpha^4$$

$$S_3 = 1 + \alpha^3 + \alpha^9 + \alpha^{12} + \alpha^{18} + \alpha^{30} + \alpha^{36} = \alpha^4$$

$$S_4 = S_2^2 = (\alpha^4)^2 = \alpha^8$$

Para el paso dos, denotamos

$$M_2 = \begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix} = \begin{pmatrix} \alpha^2 & \alpha^4 \\ \alpha^4 & \alpha^4 \end{pmatrix}$$

que es invertible ya que $det(M_2) = \alpha^2 \cdot \alpha^4 + \alpha^4 \cdot \alpha^4 = 1$ y su inversa es

$$M_2^{-1} = \begin{pmatrix} \alpha^4 & \alpha^4 \\ \alpha^4 & \alpha^2 \end{pmatrix}$$

Luego $v = 2$, por tanto, es el número de errores cometidos y tenemos que resolver :

$$\begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} -S_3 \\ -S_4 \end{pmatrix} \text{ o } \begin{pmatrix} \alpha^2 & \alpha^4 \\ \alpha^4 & \alpha^4 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} \alpha^4 \\ \alpha^8 \end{pmatrix}$$

La solución es $[\sigma_2\,\sigma_1]^T = M_2^{-1}[\alpha^4\,\alpha^8]^T = [\alpha^{11}\,\alpha^2]^T$. Por tanto, el paso dos produce el polinomio de localización de errores $\sigma(x) = \alpha^{11}x^2 + \alpha^2 x + 1$. Por el paso tres, tenemos las raíces de $\sigma(x)$ que son α^9 y α^{10}, por tanto, los números de localización de errores son $X_1 = \alpha^6$ y $X_2 = \alpha^5$.

Nos queda resolver el siguiente sistema:

$$\left.\begin{aligned} E_1\alpha^6 + E_2\alpha^5 &= \alpha^2 \\ E_1\alpha^{12} + E_2\alpha^{10} &= \alpha^4 \end{aligned}\right\}$$

Podemos observar rápidamente que $E_1 = E_2 = 1$, ya tenemos calculadas sus magnitudes. Así que, el vector de error es $e(x) = x^6 + x^5$, y la palabra código transmitida es $c(x) = x^{12} + x^{10} + x^5 + x^4 + x^3 + x + 1$.

2.4.4 *Algoritmo de Sugiyama*

El Algoritmo de Sugiyama es otro método para encontrar el polinomio de localización de errores, luego vamos a presentar una alternativa al paso dos del Algoritmo de Peterson-Gorenstein-Zierler. Este algoritmo es una aplicación relativamente simple pero ingeniosa del Algoritmo de Euclides.

Definición 18. Definimos el **polinomio evaluador de errores** $\omega(x)$ como

$$\omega(x) = \sum_{j=1}^{v} E_j X_j \prod_{j=1}^{v}(1 - xX_i) = \sum_{j=1}^{v} E_j X_j \frac{\sigma(x)}{1 - xX_j}$$

Notamos que $deg(\sigma(x)) = v$ y $deg(\omega(x)) \leq v - 1$. Definimos los polinomios $S(x)$ con grado como mucho $2t - 1$ como

$$S(x) = \sum_{i=0}^{2t-1} S_{i+1}x^i$$

donde los S_i con $1 \leq i \leq 2t$ son los síndromes del vector recibido.

Expandiendo la parte derecha de la definición de polinomio evaluador de errores como una serie formal de potencias y usando 1 junto a la definición de $S(x)$, obtenemos,

$$\omega(x) = \sigma(x)\sum_{j=1}^{v} E_j X_j \frac{\sigma(x)}{1 - xX_j} = \sigma(x)\sum_{j=1}^{v} E_j X_j \sum_{i=0}^{\infty}(xX_j)^i$$

$$= \sigma(x)\sum_{i=0}^{\infty}(\sum_{j=1}^{v} E_j X_j^{i+1})x^i \equiv \sigma(x)\sum_{i=0}^{2t-1}(\sum_{j=1}^{v} E_j X_j^{i+1})x^i \,(mod\, x^{2t})$$

$$\equiv \sigma(x)S(x)\ (mod\, x^{2t})$$

Por tanto, tenemos a lo que llamamos **ecuación clave**

$$\omega(x) \equiv \sigma(x)S(x)\ (mod\, x^{2t})$$

La siguiente observación sobre $\sigma(x)$ y $\omega(x)$ será importante más adelante.

Lema 4. *Los polinomios $\sigma(x)$ y $\omega(x)$ son primos relativos.*

Demostración. Las raíces de $\sigma(x)$ son precisamente los X_j^{-1} para $1 \leq j \leq v$. Pero

$$\omega(X_j^{-1}) = E_j X_j \prod_{i=1\, i\neq j}^{v} (1 - X_j^{-1}X_i) \neq 0$$

lo que prueba el lema. □

El Algoritmo de Sugiyama usa el Algoritmo de Euclides para resolver la ecuación clave, luego sigue de esta forma.

1. Supongamos que $f(x) = x^{2t}$ y $s(x) = S(x)$. Sea $r_{-1}(x) = f(x)$,$r_0(x) = s(x)$,$b_{-1}(x) = 0$ y $b_0(x) = 1$.
2. Repetimos las siguientes dos operaciones para encontrar $h_i(x)$,$r_i(x)$ y $b_i(x)$ por inducción para $i = 1, 2, \cdots, I$ satisfaciendo que $deg(r_{I-1}(x)) \geq t$ y $deg(r_I(x)) < t$:

   $r_{i-2}(x) = r_{i-1}h_i(x) + r_i(x)$, donde $deg(r_i(x)) < deg(r_{i-1}(x))$

   $b_i(x) = b_{i-2}(x) - h_i(x)b_{i-1}(x)$
3. $\sigma(x)$ es algún múliplo escalar no nulo de $b_I(x)$

Notamos que la I del paso dos está bien definida ya que $deg(r_i(x))$ decrece estrictamente con $deg(r_{-1}(x)) > t$. Con el fin de probar que el Algoritmo de Sugiyama funciona, necesitamos el siguiente lema.

Lema 5. *Usando la notación del Algoritmo de Suigyama, sea $a_{-1}(x) = 0$,$a_0(x) = 1$ y $a_i(x) = a_{i-2}(x) - h_i(x)a_{i-1}(x)$ para $i \geq 1$. Tenemos lo siguiente:*

1. $a_i(x)f(x) + b_i(x)s(x) = r_i(x)$ *para* $i \geq -1$
2. $b_i(x)r_{i-1}(x) - b_{i-1}(x)r_i(x) = (-1)^i f(x)$ *para* $i \geq 0$
3. $a_i(x)b_{i-1}(x) - a_{i-1}(x)b_i(x) = (-1)^{i+1}$ *para* $i \geq 0$
4. $deg(b_i(x)) + deg(r_{i-1}(x)) = deg(f(x))$ *para* $i \geq 0$

Demostración. Vamos a probar todos los puntos por inducción. Para 1), los casos $I_0 - 1$ y $i = 0$ se obtienen directamente del conjunto de valores iniciales del paso uno del

Algoritmo de Sugiyama y los valores $a_{-1}(x) = 1$ y $a_0(x) = 0$. Asumimos que se cumple 1) para $i-1$ veamos que se cumple para i, tenemos,

$a_i(x)f(x) + b_i(x)s(x) = [a_{i-2}(x) - h_i(x)a_{i-1}(x)]f(x) + [b_{i-2}(x) - h_i(x)b_{i-1}(x)]s(x)$

$= a_{i-2}(x)f(x) + b_{i-2}(x)s(x) - h_i(x)[a_{i-1}(x)f(x) + b_{i-1}(x)s(x)$

$= r_{i-2}(x) - h_i(x)r_{i-1}(x) = r_i(x)$

completando 1).

De nuevo, cuando $i = 0$, 2) se obtiene del paso uno del Algoritmo de Sugiyama. Asumimos que se cumple 2) para $i-1$ veamos que es cierto para i,

$b_i(x)r_{i-1}(x) - b_{i-1}(x)r_i(x) = [b_{i-2}(x) - h_i(x)b_{i-1}(x)]r_{i-1}(x) - b_{i-1}(x)r_i(x)$

$= b_{i-2}(x)r_{i-1}(x) - b_{i-1}(x)[h_i(x)r_{i-1}(x) + r_i(x)]$

$= b_{i-2}(x)r_{i-1}(x) - b_{i-1}(x)r_{i-2}(x)$

$= -(-1)^{i-1}f(x) = (-1)^i f(x)$

lo que prueba 2).

Cuando $i = 0$, 3) se obtiene del paso uno del Algoritmo de Sugiyama y los valores $a_{-1}(x) = 1$ y $a_0(x) = 0$. Asumimos que se cumple 3) para $i-1$ veamos que es cierto para i,

$a_i(x)b_{i-1}(x) - a_{i-1}(x)b_i(x) = [a_{i-2}(x) - h_i(x)a_{i-1}(x)]b_{i-1}(x) - a_{i-1}(x)[b_{i-2}(x) - h_i(x)b_{i-1}(x)]$

$= -[a_{i-1}(x)b_{i-2}(x) - a_{i-2}(x)b_{i-1}(x)] = -(-1)^i = (-1)^{i+1}$

lo que prueba 3).

Cuando $i = 0$, 4) se obtiene del paso uno del Algoritmo de Sugiyama. Asumimos que se cumple 4) para $i-1$ veamos que es cierto para i, esto es, $deg(b_{i-1}(x)) + deg(r_{i-2}(x)) = deg(f(x))$. En el paso dos del Algoritmo de Sugiyama, tenemos que $deg(r_i(x)) < deg(r_{i-2}(x))$. Así que, $deg(b_{i-1}(x)r_i(x)) = deg(b_{i-1}(x) + deg(r_i(x)) < deg(f(x))$ lo que implica 4) para el caso i usando el apartado 2).

□

Ahora verificamos que el Algoritmo de Sugiyama funciona. Por el Lema 5 apartado 1), tenemos,

$$a_I(x)x^{2t} + b_I(x)S(x) = r_I(x) \tag{6}$$

Por la ecuación clave, también sabemos que,

$$a_I(x)x^{2t} + \sigma(x)S(x) = \omega(x) \tag{7}$$

para algún polinomio $a(x)$. Multiplicando 6 por $\sigma(x)$ y 7 por $b_I(x)$ para obtener,

$$a_I(x)\sigma(x)x^{2t} + b_I(x)\sigma(x)S(x) = r_I(x)\sigma(x) \tag{8}$$

y

$$a_I(x)b_I(x)x^{2t} + \sigma(x)b_I(x)S(x) = \omega(x)b_I(x) \tag{9}$$

Módulo x^{2t} implica que

$$r_I(x)\sigma(x) \equiv \omega(x)b_I(x)\ (mod\ x^{2t}) \tag{10}$$

Como $deg(\sigma(x)) \leq t$, por la elección de I, $deg(r_I(x)\sigma(x)) = deg(r_I(x)) + deg(\sigma(x)) < t + t = 2t$. Por el Lema 5 apartado 4), la elección de I y el hecho de que $deg(\omega(x)) < t$, $deg(\omega(x) \times b_I(x)) = deg(\omega(x)) + deg(b_I(x)) = t + (deg(x^{2t}) - deg(r_{I-1}(x)) \leq 3t - t = 2t$. Por eso, 10 implica que $r_I(x)\sigma(x) = \omega(x)b_I(x)$. Esto, junto a 8 y 9, prueba que

$$a_I(x)\sigma(x) = a(x)b_I(x) \tag{11}$$

Sin embargo, el Lema 5 apartado 3), implica que $a_I(x)$ y $b_I(x)$ son primos relativos y por tanto, $a(x) = \lambda(x)a_I(x)$ por 11. Sustituyendo esto en 11 tenemos,

$$\sigma(x) = \lambda(x)b_I(x) \tag{12}$$

Si ponemos esto en 7 obtenemos $\lambda(x)a_I(x)x^{2t} + \lambda(x)b_I(x)S(x) = \omega(x)$. Luego, 6 implica que

$$\omega(x) = \lambda(x)r_I(x) \tag{13}$$

Por el Lema 4, 12 y 13, $\lambda(x)$ debe ser una constante no-nula, lo que verifica el paso tres del Algoritmo de Sugiyama.

Como solo nos interesan las raíces de $\sigma(x)$, es suficiente encontrar las raíces de $b_I(x)$ del paso dos, ya que así obtenemos los números de localización de errores.

Ejemplo 18. Vamos a obtener un múltiplo escalar del $\sigma(x)$ del Ejemplo 17, usando ahora el Algoritmo de Sugiyama. En el otro ejemplo, teníamos que $t = 2$ y los síndromes eran $S_1 = \alpha^2$, $S_2 = \alpha^4$, $S_3 = \alpha^4$ y $S_4 = \alpha^8$.

El Algoritmo de Sugiyama dice que $r_{-1}(x) = x^{2t} = x^4$, $r_0(x) = S(x) = \alpha^8x^3 + \alpha^4x^2 + \alpha^4x + \alpha^2$, $b_{-1}(x) = 0$ y $b_0(x) = 1$. Tenemos que resolver lo siguiente:

$r_{-1}(x) = r_0(x)h_1(x) + r_1(x)$

$x^4 = (\alpha^8x^3 + \alpha^4x^2 + \alpha^4x + \alpha^2)(\alpha^7x + \alpha^3) + (\alpha^3x^2 + \alpha x + \alpha^5)$

$b_1(x) = b_{-1}(x) - h_1(x)b_0(x) = h_1(x) = (\alpha^7 x + \alpha^3)$

Como $deg(r_1(x))$ no es mejor que t volvemos a aplicar este paso.

$r_0(x) = r_1(x)h_2(x) + r_2(x)$

$\alpha^8 x^3 + \alpha^4 x^2 + \alpha^4 x + \alpha^2 = (\alpha^3 x^2 + \alpha x + \alpha^5)(\alpha^5 x + \alpha^7) + (\alpha^7 x + \alpha^{14})$

$b_2(x) = b_0(x) - h_2(x)b_1(x)$

$b_2(x) = 1 + (\alpha^5 x + \alpha^7)(\alpha^7 x + \alpha^3) = (\alpha^{12} x^2 + \alpha x + \alpha^5)$

La siguiente tabla resume los resultados.

i	$r_i(x)$	$h_i(x)$	$b_i(x)$
-1	x^4		0
0	$\alpha^8 x^3 + \alpha^4 x^2 + \alpha^4 x + \alpha^2$		1
1	$\alpha^3 x^2 + \alpha x + \alpha^5$	$\alpha^7 x + \alpha^3$	$\alpha^7 x + \alpha^3$
2	$\alpha^7 x + \alpha^{14}$	$\alpha^5 x + \alpha^7$	$\alpha^{12} x^2 + \alpha x + \alpha^5$

Luego, el primer índice I donde $deg(r_I(x)) < t = 2$ es $I = 2$. Por tanto, $\sigma(x)$ es múltiplo de $b_2(x) = \alpha^{12} x^2 + \alpha x + \alpha^5$.

Podemos concluir con que tanto el Algoritmo de Peterson-Gorenstein-Zierler y el de Sugiyama se pueden usar para decodificar cualquier código cíclico hasta la cota BCH. Sea $\mathcal{C}$ un código cíclico con conjunto de definición T y supongamos que T contiene δ elementos consecutivos $\{b, b+1, \cdots, b+\delta-2\}$. Sea $\mathcal{B}$ el código BCH con conjunto de definición $\mathcal{C}_b \cup \mathcal{C}_{b+1} \cup \cdots \cup \mathcal{C}_{b+\delta-2}$, que es un subconjunto de T , luego $\mathcal{C} \subseteq \mathcal{B}$. Sea $t = \lfloor (\delta - 1)/2 \rfloor$. Supongamos que transmitimos una palabra código $c(x) \in \mathcal{C}$ y recibimos $y(x)$ donde se han cometido t o menos errores. Entonces $c(x) \in \mathcal{B}$ y cualquier de los algoritmos que apliquemos a $\mathcal{B}$ corregirá $y(x)$ para obtener $c(x)$. Luego, estos algoritmos corregirán una palabra recibida de cualquier código cíclico si se comenten v errores y $2v + 1$ no supera la cota BCH del código. Por supuesto, el número de errores es menor que el número actual de errores que $\mathcal{C}$ es capaz de corregir.

3

POLINOMIOS TORCIDOS

El desarrollo de este capítulo está basado en los siguientes artículos :

3.1 PROPIEDADES BÁSICAS DEL ANILLO DE LOS POLINOMIOS TORCIDOS

En esta sección introduciremos los anillos de polinomios torcidos con coeficientes en un cuerpo. Daremos una breve explicación de resultados teóricos de anillos para más tarde, discutir los códigos cíclicos torcidos.

Definición 19. Sea F cualquier cuerpo y $\sigma \in Aut(F)$. El **anillo de los polinomios torcidos** $F[x;\sigma]$ se define como el conjunto $\{\sum_{i=0}^{N} f_i x^i \mid N \in \mathbb{N}_0\,,\ f_i \in F\}$ dotado por la suma usual, respecto a los coeficientes y la multiplicación sigue la siguiente regla :

$$xa = \sigma(a)x \,\forall a \in F$$

junto a la asociatividad y la distributividad. Entonces $(F[x;\sigma], +, \cdot)$ es un anillo, donde el neutro es $x^0 = 1$. A sus elementos los llamaremos **polinomios torcidos**.

Comentario 1. En general, el anillo de polinomios se define como $F[x;\sigma;\delta]$ y entonces tenemos que $xa = \sigma(a)x + \delta(a)$ donde *delta* es una *sigma*-derivación. Por simplicidad, utilizaremos la definión dada anteriormente.

Si $\sigma = id$, entonces $F[x;\sigma] = F[x]$ y tenemos el anillo de los polinomios conmutativos sobre F. Este caso es el que se ha desarrollado en el capítulo anterior. En el caso general, los grupos aditivos de $F[x;\sigma]$ y $F[x]$ son idénticos, mientras que la multiplicación viene dada por,

$$(\sum_{i=0}^{N} f_i x^i)(\sum_{j=0}^{M} f_j x^j) = \sum_{i,j} f_i \sigma^i(g_j) x^{i+j}$$

Otra forma de escribir los polinomios es $\{\sum_{i=0}^{N} x^i f_i \mid N \in \mathbb{N}_0,\ f_i \in F\}$, la diferencia ahora es que cuando aplicamos σ, los coeficientes los cambiamos de derecha a

izquierda aplicando σ^{-1}. En este capítulo tomaremos la notación de los coeficientes a la izquierda, por ello el **coeficiente líder** es el coeficiente a la izquierda del término de mayor grado.

Por tanto, un polinomio se dice que es **mónico** si su coeficiente líder es 1.

Definición 20. El **grado** de una polinomio torcido se define de manera usual como el mayor exponente de x en el polinomio y $deg(0) = -\infty$. Además, el grado no depende de donde se encuentre el coeficiente ya que σ es un automorfismo, por lo que tenemos las siguientes operaciones:

$deg(f+g) \leq max\{deg(f), deg(g)\}$ y $deg(f*g) = deg(f) + deg(g)$.

Como consecuencia, las unidades de $F[x;\sigma]$ son $F^* = F$ 0.

Definición 21. Sean los polinomios g y f no nulos en $F[x;\sigma]$. Diremos que g es **un dividor por la derecha** de f, denotado por, $g \mid_r f$ si $f = hg$ para algún $h \in F[x;\sigma]$. Diremos que f es **irreducible** si todos sus dividores por la derecha son unidades o polinomios del mismo grado que f. Es claro que los polinomios de grado 1 son irreducibles.

A diferencia de como ocurría en el caso conmutativo, la factorización de un polinomio no tiene por qué ser única.

Ejemplo 19. Sea $F = \mathbb{F}_8 = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$ donde $\alpha^3 = \alpha^2 + 1$. Sea σ el σ_2 automorfismo de Frobenius. Entonces $\sigma^{-1} = \sigma$ y en $\mathbb{F}_8[x,\sigma]$ tenemos que,

En $F[x;\sigma]$ también tenemos división por resto, por tanto, podemos definir el máximo común divisor y el mínimo común múltiplo pero en este anillo tenemos que tener en cuenta el lado por el que dividimos.

Teorema 25. *Sea $F[x,\sigma]$ un dominio Euclídeo a izquierda y a derecha. Se verifica lo siguiente:*

- ***División a derecha con resto:*** *Para todo $f, g \in F[x;\sigma]$ con $g \neq 0$, existen polinomios únicos $s, r \in F[x;\sigma]$ tal que $f = sg + r$ y $deg(r) < deg(g)$. Si $r = 0$, entonces g es un divisor a derecha de f.*
- *Para cualesquiera dos polinomios $f_1, f_2 \in F[x;\sigma]$, siendo al menos uno de ellos no nulo, existe un polinomio mónico único $d \in F[x;\sigma]$ tal que $d \mid_r f_1$, $d \mid_r f_2$ y cuando haya un $h \in F[x;\sigma]$ que cumpla que $h \mid_r f_1$, $h \mid_r f_2$ entonces $h \mid_r d$. Al polinomio d se le llama el **máximo común dividor a derecha** de f_1 y f_2, lo denotaremos por $mcdd(f_1, f_2)$. Además, satisface la identidad de Bezout a la derecha,*

  $$d = uf_1 + vf_2$$

  para algunos $u, v \in F[x;\sigma]$.
  *Claramente el $deg(u) < deg(f_2)$ y $deg(v) < deg(f_1)$. Si $d = 1$, entonces diremos que f_1 y f_2 son **primos relativos a derecha**.*
-