UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICA

EQUIVALENCIA ENTRE CÓDIGOS LINEALES Y CÓDIGOS CÍCLICOS

Autor: Br. Reinaldo Villanueva

Tutora: Dra. Irene Santos

Trabajo Especial de Grado presentado ante la ilustre Universidad Central de Venezuela para optar al título de Licenciado en Matemática.

Caracas, Venezuela

Mayo 2015

Nosotros, los abajo firmantes, designados por la Universidad Central de Venezuela como integrantes del Jurado Examinador del Trabajo Especial de Grado titulado "**Equivalencia entre Códigos Lineales y Códigos Cíclicos**", presentado por el **Br. Reinaldo Arturo Villanueva Blanco** titular de la Cédula de Identidad **16.970.363**, certificamos que este trabajo cumple con los requisitos exigidos por nuestra Magna Casa de Estudios para optar al título de **Licenciado en Matemática**.

Dra. Irene Santos
Tutora

Dr. Manuel Maia
Jurado

Dr. Mauricio Angel
Jurado

Para mi Hermosa y Amada Vieja...

Agradecimientos

- A Dios por encaminarme en la vida.

- A mi tutora, Dra. Irene Santos por su invaluable ayuda.

- A mi madre María y a toda mi familia por su infinito e incondicional apoyo.

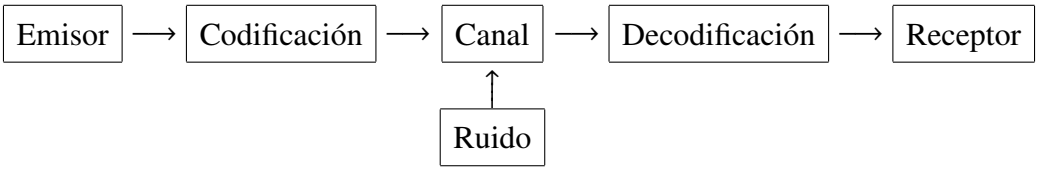
- A todas aquellas personas que de alguna u otra manera contribuyeron en la realización del presente trabajo.

CONTENIDO

Introducción

En la vida cotidiana, usamos muchos códigos aunque a veces no nos demos cuenta. Por ejemplo los más comunes son el código de barras, ISBN usado en los libros y el código ASCII usado en informática. Los primeros ejemplos de códigos usados en la práctica son el código Morse, usado en telegrafía en el siglo XIX, y el sistema Braille para no-videntes. Además, cualquier artefacto tecnológico que transmita o almacene mensajes digitales, sonidos e imágenes, involucra al menos un código. Ejemplos típicos de ello son los computadores, los teléfonos celulares, las transmisiones por satélites, los CD's y DVD's, la televisión, etc.

La situación general es la siguiente. Supongamos que queremos enviar un mensaje, el cual es enviado por un canal de comunicación (fibra óptica, ondas), cuyas características dependen de la naturaleza del mensaje a ser enviado (sonido, imagen, datos). Luego hay que hacer una traducción entre el mensaje original (palabra fuente) y el mensaje que el canal está capacitado para enviar (palabra código). Este proceso se llama codificación. Una vez codificado el mensaje lo enviamos a través del canal, y nuestro receptor recibe un mensaje codificado (palabra recibida) que puede tener errores, ya que en todo proceso de comunicación se presentan interferencias o ruido (atmósfera, lluvia, nubes densas). Finalmente el mensaje recibido es traducido nuevamente a términos originales, es decir, decodificado. Del estudio de este proceso se ocupa lo que se conoce como Teoría de Códigos, la cual es una de las aplicaciones más recientes del Algebra Lineal. La Teoría de Códigos forma parte de la Teoría de la Información, encargada de todo el proceso, es decir, el diseño de canales a usar, estudio de como el ruido afectan los mensajes, entre otros. Se resume todo el procedimiento concerniente a la Teoría de Códigos en el siguiente esquema:



A continuación enunciaremos algunos conceptos básicos para mayor compresión de la relación entre el Algebra Lineal y los códigos. Un alfabeto es un conjunto finito $\mathcal{A} = \{a_1, a_2, \ldots, a_q\}$ y los

elementos de $\mathcal{A}$ los llamaremos símbolos. Una palabra de longitud n ó n-cadena sobre $\mathcal{A}$ es una sucesión

$$a_{i_1}a_{i_2}\dots a_{i_n} \quad \text{donde} \quad a_{i_k} \in \mathcal{A}, \quad i \in \{1, 2, \dots, q\}, \quad 1 \leq k \leq n$$

de n símbolos de $\mathcal{A}$. Denotaremos por $\mathcal{A}^n$ al conjunto de todas las n-cadenas y por $\mathcal{A}^*$ al conjunto de todas las palabras sobre $\mathcal{A}$, es decir,

$$\mathcal{A}^n = \{a_{i_1}a_{i_2}\dots a_{i_n} : a_{i_k} \in \mathcal{A},\ 1 \leq k \leq n\}, \quad \mathcal{A}^* = \bigcup_{n\in\mathbb{N}} \mathcal{A}^n.$$

Dado un alfabeto $\mathcal{A}_q$ de q símbolos, se define un código q-ario sobre $\mathcal{A}_q$ como un subconjunto $C \subset \mathcal{A}_q^*$. Si $q \in \{2, 3, 4\}$ decimos que C es un código binario, ternario y cuaternario respectivamente. Los elementos de C se llaman palabras código y el tamaño de C se define como $M = |C|$. Si todas las palabras código tienen la misma longitud fija n, es decir, si $C \subset \mathcal{A}^n$ decimos que C es un código bloque con parámetros (n, M); si C no es un código bloque, se dice entonces que es un código de longitud variable, un ejemplo de este ultimo es el código Morse. El presente trabajo sólo considera códigos bloque ya que su decodificación es única. Los códigos de bloque que vamos a trabajar son los códigos lineales (códigos de Hamming y Reed-Muller) y los códigos cíclicos (códigos BCH, Reed-Solomon y algunos códigos de Hamming).

Para codificar y decodificar de manera más práctica y eficiente, es común dotar al alfabeto $\mathcal{A}$ de cierta estructura algebraica adicional, por ejemplo se pide que $\mathcal{A}$ sea un cuerpo finito (como en la teoría clásica) o incluso un anillo finito (como en tiempos más recientes). De ahora en adelante fijamos $\mathcal{A} = \mathbb{F}_q$, el cuerpo finito de q elementos, así el conjunto de n-cadenas $\mathcal{A}^n$ es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión n, que identificamos naturalmente con

$$\mathbb{F}_q^n = \{(x_1, \dots, x_n) : x_i \in \mathbb{F}_q,\ 1 \leq i \leq n\}$$

mediante la asignación $x_1x_2\dots x_n \leftrightarrow (x_1, x_2, \dots, x_n)$. Un código lineal q-ario de longitud n y rango k es un subespacio $L \subset \mathbb{F}_q^n$ de dimensión k. Un código C es cíclico si, y sólo si

$$c_1c_2\dots c_n \in C \quad \Rightarrow \quad c_nc_1\dots c_{n-1} \in C.$$

El trabajo que se plantea es el estudio de las equivalencias existentes entre códigos lineales y códigos cíclicos, ya que las equivalencias establecen un isomorfismo de un código con otro. Así como un análisis comparativo de algunos códigos clásicos que se obtienen como códigos cíclicos.

CAPíTULO 1

Generalidades sobre códigos

1. Definiciones básicas

Definición 1.1. Un alfabeto es un conjunto finito

$$\mathcal{A} = \{a_1, a_2, \ldots, a_q\}.$$

Los elementos de $\mathcal{A}$ son llamados símbolos o letras y el número q es la raíz u orden de $\mathcal{A}$. Una n-cadena o palabra de longitud n sobre $\mathcal{A}$ es una sucesión de n elementos en $\mathcal{A}$. Se denota como $\mathcal{A}^n$ el conjunto de todas las n-cadenas y $\mathcal{A}^*$ el conjunto de todas las palabras sobre $\mathcal{A}$, es decir

$$\mathcal{A}^* = \bigcup_{n\in\mathbb{N}} \mathcal{A}^n.$$

Definición 1.2. Si $\mathcal{A} = \{a_1, a_2, \ldots, a_q\}$ es un alfabeto, un código q-ario sobre $\mathcal{A}$ es un subconjunto C de $\mathcal{A}^*$. Los elementos de C son llamados palabras código (codewords). El número $M = |C|$ es conocido como el tamaño del código. Si todas las palabras código tienen longitud fija n se dice que C es un código de bloque y se denota por $(n, M)_q$-código y sus n-cadenas o palabras código se escriben

$$x = x_1x_2 \ldots x_n = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n.$$

Definición 1.3. La tasa de información de un $(n, M)_q$-código C se define como

$$Tasa(C) = \frac{\log_q(M)}{n}.$$

El número anterior da una medida de la cantidad de informacíon que se está transmitiendo. Se buscan códigos con tasa de información alta, por ejemplo, $Tasa(C) > 0,6$ ó $Tasa(C) > \frac{3}{4}$.

2. Distancia de Hamming y peso

Definición 1.4. Sean x, y palabras de igual longitud sobre el mismo alfabeto $\mathcal{A}$. La distancia de Hamming entre x, y se define como el número de coordenadas en que la palabra x difiere de la palabra y, es decir, sea $d : \mathcal{A}^n \times \mathcal{A}^n \longrightarrow [0, n] \subset \mathbb{N}$, con

$$d(x, y) = \Big|\{1 \leq i \leq n : x_i \neq y_i\}\Big|$$

en donde $d(x, y)$ es la distancia de Hamming entre las palabras x, y.

Ejemplo 1.1. Si se tienen las 6-cadenas $x = 210100$, $y = 110211$ entonces $d(x, y) = 4$.

Proposición 1.1. *La función d es una distancia en $\mathcal{A}^n$, es decir, satisface las propiedades:*

(1) *No negativa:* $d(x, y) \geq 0,\ \forall x, y \in \mathbb{F}_q^n \wedge d(x, y) = 0$ *si, y sólo si* $x = y,\ \forall x, y \in \mathbb{F}_q^n$.
(2) *Simétrica:* $d(x, y) = d(y, x),\ \forall x, y \in \mathbb{F}_q^n$.
(3) *Desigualdad triángular:* $d(x, z) \leq d(x, y) + d(y, z),\ \forall x, y, z \in \mathbb{F}_q^n$.

Definición 1.5. Sean $x, y \in \mathbb{F}_q^n$. Se define la distancia del código C como la menor distancia no nula entre sus palabras código y se denotada por

$$d = d(C) = \min_{\substack{x,y \in C \\ x \neq y}} d(x, y).$$

Un $(n, M, d)_q$-código es un código sobre $\mathbb{F}_q$ de longitud n con tamaño M y distancia d.

Definición 1.6. Sea $x \in \mathbb{F}_q^n$. Se define el peso de x como el número de coordenadas no nulas de x, es decir, el peso de x es la distancia de x al $\mathbf{0}$, esto se traduce como $w(x) = d(x, \mathbf{0})$ en donde $w(x)$ es el peso de x. Se define el peso de C como

$$w(C) = \min_{\substack{x \in C \\ x \neq \mathbf{0}}} w(x).$$

De las definiciones 1.5 y 1.6 se tiene que la relación entre la distancia y el peso es

$$d(x, y) = \left|\{1 \leq i \leq n : x_i \neq y_i\}\right| = \left|\{1 \leq i \leq n : x_i - y_i \neq 0\}\right| = w(x - y).$$

Definición 1.7. Sean $x, y \in \mathbb{F}_2^n$, es decir, si $x = x_1 x_2 \ldots x_n,\ y = y_1 y_2 \ldots y_n$ son palabras binarias, la intersección de x con y se define como la palabra

$$x \cap y = (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$$

en donde $(x \cap y)_i = 1$ si, y sólo si $x_i = 1, y_i = 1, \forall i \in \{1, 2, \ldots, n\}$.

Definición 1.8. Un $(n, M, d)_q$-código C es un código de peso constante si cada palabra tiene el mismo peso w. Por ejemplo, las palabras código con peso fijo de un código lineal forman un código de peso constante. Si x, y son palabras distintas de peso w entonces $d(x, y) \leq 2w$. Por tanto se tiene el siguiente teorema.

TEOREMA 1.1. (**La Cota Superior de Johnson**). *Si C es un $(n, M, d)_q$-código con $M > 1$ de peso constante, es decir, el peso de las palabras es igual a w entonces $d \leq 2w$.*

EJEMPLO 1.2. El código Simplex con parámetros $[\frac{q^r-1}{q-1}, r]_q$ es un código de peso constante, en donde todas sus palabras tienen peso constante, $w = q^{r-1}$.

OBSERVACIÓN 1. La única métrica que se usará es la distancia de Hamming.

Cuando se trabaja con códigos sobre $\mathbb{F}_2$ tenemos un resultado elemental sobre el peso de las palabras código en la siguiente proposición:

PROPOSICIÓN 1.2. *El peso w satisface las siguientes propiedades:*

(1) *Si $x, y \in \mathbb{F}_2^n$ entonces $w(x + y) = w(x) + w(y) - 2w(x \cap y)$.*
(2) *Si $x, y \in \mathbb{F}_2^n$ entonces $w(x \cap y) \equiv x \cdot y \ (mod\ 2)$.*
(3) *Si $x \in \mathbb{F}_2^n$ entonces $w(x) \equiv x \cdot x \ (mod\ 2)$.*

DEMOSTRACIÓN.

(1) Si $x, y \in \mathbb{F}_2^n$ entonces

$$\begin{aligned} w(x + y) &= w(x - y) \\ &= \left|\{1 \leq i \leq n : x_i \neq 0\}\right| + \left|\{1 \leq i \leq n : y_i \neq 0\}\right| - 2\left|\{1 \leq i \leq n : x_i y_i \neq 0\}\right| \\ &= w(x) + w(y) - 2w(x \cap y). \end{aligned}$$

(2) Si $x, y \in \mathbb{F}_2^n$ entonces si $w(x \cap y)$ es par entonces el producto interno $x \cdot y$ es cero, así $w(x \cap y) = 2k$ para algún $k \in \mathbb{Z}$. Pero si $w(x \cap y)$ es impar, el producto interno $x \cdot y$ es igual a uno, luego existe $k \in \mathbb{Z}$ tal que $w(x \cap y) = 2k + 1$. Luego, $w(x \cap y) \equiv x \cdot y \ (mod\ 2)$.
(3) Si $x, y \in \mathbb{F}_2^n$ entonces tomando $x = y$ en el caso (2) se tiene el resultado.

□

3. Códigos lineales

Para codificar y decodificar de manera más práctica y eficiente será útil dotar el alfabeto $\mathcal{A}$ con cierta estructura algebraica. Se considerará que $\mathcal{A}$ tiene estructura de cuerpo finito aunque también se lo puede considerar como un anillo. A partir de ahora, se denota $\mathcal{A} = \mathbb{F}_q$ como el cuerpo finito de q elementos, en donde q es potencia de un número primo, es decir, $q = p^r$ para algún primo p y

$r \in \mathbb{N}$. Si q es un número primo, se tiene que el alfabeto $\mathcal{A} = \mathbb{Z}_q$ es el cuerpo de los enteros módulo q.

El conjunto de todas las n-cadenas $\mathcal{A}^n$ es un espacio vectorial sobre $\mathbb{F}_q$ con dimensión n, se identificará con

$$\mathbb{F}_q^n = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{F}_q,\ 1 \leq i \leq n\}$$

mediante la asignación:

$$x_1 x_2 \ldots x_n \quad \longleftrightarrow \quad (x_1, x_2, \ldots, x_n).$$

Definición 1.9. Un código lineal q-ario de longitud n y rango k es un subespacio $C \subset \mathbb{F}_q^n$ de dimensión k ó k-dimensional. En este caso se dice que C es un $[n, k]_q$-código. Si C tiene distancia mínima d entonces se dice que C es un $[n, k, d\,]_q$-código. El tamaño de un $[n, k, d]_q$-código C es $M = q^k$. En este caso la tasa de información es

$$Tasa(C) = \frac{\log_q(q^k)}{n} = \frac{k}{n}.$$

En códigos lineales, la tasa de información es una medida de la cantidad de información de coordenadas relativas al número total de coordenadas. Cuanto mayor sea la tasa, mayor es la proporción de coordenadas en una palabra código, realmente contienen información en lugar de redundancia. Las $r = n - k$ coordenadas restantes se denominan redundancia.

Definición 1.10. Si C no es lineal, un subcódigo de C es cualquier subconjunto de C. Si C es lineal, un subcódigo es un subconjunto de C que también es lineal, en este caso un subcódigo de C es un subespacio de C.

A continuación se presentan varios ejemplos de códigos lineales.

Ejemplo 1.3. Los códigos $\{\mathbf{0}\}$ y $V = \mathbb{F}_q^n$ con parámetros $[n, 0, -]$ y $[n, n, 1]_q$ respectivamente, son los dos códigos lineales triviales.

Ejemplo 1.4. El código de repetición q-ario

$$Rep_q(n) = \{\underbrace{0 \ldots 0}_{n-veces}, \underbrace{1 \ldots 1}_{n-veces}, \underbrace{(q-1) \ldots (q-1)}_{n-veces}\}$$

es un $[n, 1, n]_q$-código lineal.

Ejemplo 1.5. Un vector $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ se dice even-like si $\sum_{i=1}^n x_i = 0$, si ocurre lo contrario se dice odd-like. Un vector x binario es even-like si, y sólo si $w(x)$ es par, así el concepto de vectores even-like es de hecho una generalización de los vectores binarios con peso par. Los vectores even-like de un código C forman un subcódigo $C_e \subseteq C$ sobre $\mathbb{F}_q$ como las palabras de peso par en un código binario (si $C = \mathbb{F}_q^n$, entonces $C_e = P_q(n)$, en donde $P_q(n)$ aparece definido en el ejemplo 2.3). Los vectores even-like no necesitan tener peso par, excepto para el caso binario. Un código se dice even-like si, y sólo si tiene palabras código even-like sino se dirá que es un código odd-like. Si C es un código $[n, k]_q$ entonces el subcódigo $C_e \subset C$ con palabras even-like del código C es lineal y tiene parámetros $[n, k-1]_q$.

Ejemplo 1.6. Si $C = \mathbb{F}_q^n$ con $q = 2$ en el ejemplo anterior, se tiene el subcódigo $C_e = E(n) \subset \mathbb{F}_2^n$ de todas las palabras con peso par en $\mathbb{F}_2^n$ definido por

$$E(n) = \{x \in \mathbb{F}_2^n : w(x) \equiv 0 \ (mod\ 2)\} \subset \mathbb{F}_2^n$$

es un código lineal binario con parámetros $[n, n-1, 2]_2$.

Ejemplo 1.7. El código de Hamming binario de orden r, denotado por $\mathcal{H}_2(r)$ con parámetros $[2^r - 1, 2^r - r - 1, 3]_2$ es lineal.

Proposición 1.3. *Si C es un código lineal entonces se cumple que $d(C) = w(C)$.*

Demostración. Como el código C es lineal y teniendo en cuenta que la palabra nula $\mathbf{0} \in C$, $\forall\, C$ lineal se tiene que

$$d(C) = \min_{\substack{x,y \in C \\ x \neq y}} d(x, y) = \min_{\substack{x,y \in C \\ x \neq y}} w(x - y) = \min_{\substack{x \in C \\ x \neq \mathbf{0}}} w(x) = x(C).$$

(Demostración alternativa). Supongamos que existen $x, y \in C$ tales que $d(C) = d(x, y)$. Usando la relación entre peso y distancia se tiene

$$d(C) = w(x - y) \geq w(C) \tag{1.1}$$

ya que $x - y$ es una palabra en el código lineal C.

Para la otra desigualdad, se cumple que para algún x en el código

$$w(C) = w(x) = d(x, \mathbf{0}) \geq d(C) \tag{1.2}$$

ya que la palabra nula $\mathbf{0}$ pertenece al código lineal C.

De las desigualdades (1.1) y (1.2) se tiene que $d(C) = w(C)$.

□

Ejemplo 1.8. El código ternario $C_1 = \{000, 111, 222\} = Rep_3(3)$ es lineal y por lo tanto se cumple que $d(C_1) = w(C_1) = 3$. Si el código no es lineal, la proposición anterior no es válida. Por ejemplo, se tiene que el código 5-ario $C_2 = \{11, 21, 12, 22, 32, 23, 33\}$ tiene distancia $d(C_2) = 1 < 2 = w(C_2)$. El código binario $C_3 = \{100, 010, 001\}$ tiene $d(C_3) = 2 > 1 = w(C_3)$.

Observación 2. Sea C un $(n, M, d)_q$-código. Los números n, M, d, q son parámetros básicos del código. El parámetro $Tasa(C)$ es secundario y tiene que ver con la eficiencia del código durante la transmisión de mensajes. En general, fijada la longitud n, interesan códigos con un tamaño M grande (para transmitir muchos mensajes distintos) y una distancia d grande (para que detecte y corrija el mayor número de errores). Estas metas son intrínsecamente contradictorias entre sí, y se busca entonces un equilibrio entre estos parámetros.

4. Canales y decodificación

Sean $\mathcal{A} = \{a_1, a_2, \ldots, a_q\}$ y $\mathcal{B} = \{b_1, b_2, \ldots, b_r\}$ alfabetos con $\mathcal{A} \subset \mathcal{B}$. Un canal discreto aleatorio es un canal de comunicación que envía símbolos de $\mathcal{A}$ y recibe símbolos en $\mathcal{B}$. Se asumirá que transmitimos en un canal discreto aleatorio simétrico, es decir, en donde se cumple que $\mathcal{A} = \mathcal{B}$.

Sea $C \subset \mathcal{A}^n$ un código q-ario y supongamos que al transmitir la palabra código $c \in C$ recibimos la palabra $x \notin C$. El método que usaremos para decodificar consiste en asignarle a x la palabra código c más cercana. Es decir, si

$$d(x, c) = \min_{y \in C} d(x, y)$$

donde d es una distancia en C, entonces se decodificará la palabra x por la palabra código c. Este método es llamado decodificación por distancia mínima.

5. Equivalencias y automorfismos de códigos

Existen varias nociones de equivalencias entre códigos. Una de ellas es la siguiente. Dos códigos con la misma longitud n y sobre el mismo alfabeto se dicen equivalentes si uno puede ser obtenido del otro por permutaciones de coordenadas y símbolos, es decir, por una combinación de operaciones del siguiente tipo:

- Permutaciones de las coordenadas en el código (**C**).
- Permutaciones de los símbolos en una posición fija o en varias (**S**).

Ejemplo 1.9. $C_1 = \{00100, 00011, 11111, 11000\}, C_2 = \{00000, 01101, 10110, 11011\}$ son códigos equivalentes en $\mathbb{F}_2^5$. Ya que haciendo una operación del tipo (**C**) intercambiando las coordenadas 2 con 4 y luego una operación del tipo (**S**) intercambiando los símbolos 0 y 1 en la tercera coordenada se obtiene el código C_2, a partir de C_1. Aquí lo vemos:

$$C_1 = \left\{ \begin{array}{c} 0\underline{0}1\underline{0}0 \\ 0\underline{0}0\underline{1}1 \\ 1\underline{1}1\underline{1}1 \\ 1\underline{1}0\underline{0}0 \end{array} \right\} \overset{\mathbf{C}}{\rightarrow} \left\{ \begin{array}{c} 00\bar{1}00 \\ 01\bar{0}01 \\ 11\bar{1}11 \\ 10\bar{0}10 \end{array} \right\} \overset{\mathbf{S}}{\rightarrow} \left\{ \begin{array}{c} 00000 \\ 01101 \\ 11011 \\ 10110 \end{array} \right\} = C_2 \quad \Rightarrow \quad C_1 \simeq C_2.$$

La definición formal se presenta a continuación.

Definición 1.11. Dos códigos $C_1, C_2 \subset \mathbb{F}_q^n$ se dicen **equivalentes** si existe una permutación $\varepsilon \in \mathbb{S}_n$ de las n coordenadas y permutaciones $\pi_1, \pi_2, \ldots, \pi_n \in Biy(\mathcal{A})$ de los símbolos del alfabeto, tales que

$$c_1c_2 \ldots c_n \in C_1 \quad \Longleftrightarrow \quad \pi_1(c_{\varepsilon(1)})\pi_2(c_{\varepsilon(2)}) \ldots \pi_n(c_{\varepsilon(n)}) \in C_2.$$

y se denotará $C_1 \simeq C_2$. En donde, $\mathbb{S}_n$ es el conjunto de todas las permutaciones de las n coordenadas.

Observación 3. Si tenemos que $C_1 \simeq C_2$ entonces $(n_1, M_1, d_1)_q = (n_2, M_2, d_2)_q$ y por lo tanto corregirán el mismo número de errores.

Una definición alternativa de equivalencia entre códigos es la siguiente.

Definición 1.12. Dos códigos C_1, $C_2 \subset \mathbb{F}_q^n$ se dicen **múltiplo escalar equivalente** si C_2 se obtiene de C_1, aplicando operaciones del tipo:

- Permutaciones de las coordenadas en el código (**C**).
- Multiplicación de los símbolos en una coordenada fija, o en varias, por un escalar no nulo $\lambda \in \mathbb{F}_q^*$ (**M**).

Notar que para el caso binario no hay operaciones del tipo (**M**).

Observación 4. Si dos códigos son múltiplo escalar equivalente entonces son equivalentes, ya que si $\lambda \in \mathbb{F}_q^*$, la aplicación $x \longmapsto \lambda x$ es una biyección de $\mathbb{F}_q$ con $\mathbb{F}_q$ un cuerpo. La recíproca no es cierta como se mostrará en el ejemplo a continuación.

Ejemplo 1.10. El código ternario $C = \{012, 120, 201\}$ es equivalente al código ternario de repetición $Rep_3(3) = \{000, 111, 222\}$. En efecto, aplicando las permutaciones del alfabeto $\pi_2 = (012)$ y $\pi_3 = (012)$ en la segunda y tercera coordenada, respectivamente, se obtiene

$$C = \left\{ \begin{array}{c} 0\bar{1}2 \\ 1\bar{2}0 \\ 2\bar{0}1 \end{array} \right\} \overset{\pi_2}{\to} \left\{ \begin{array}{c} 00\bar{2} \\ 11\bar{0} \\ 22\bar{1} \end{array} \right\} \overset{\pi_3}{\to} \left\{ \begin{array}{c} 000 \\ 111 \\ 222 \end{array} \right\} = Rep_3(3).$$

Sin embargo C y $Rep_3(3)$ no son múltiplo escalar equivalente porque ninguna palabra del código de repetición puede ser obtenida del código C mediante la multiplicación de los símbolos en una coordenada fija, o en varias, por un escalar no nulo, es decir, cualquiera de las palabras 000, 111, 222 del código $Rep_3(3)$ es imposible que provenga de alguna de las palabras de C mediante operaciones del tipo (**M**).

Un resultado muy útil a la hora de realizar los cálculos es el siguiente.

Lema 1.1. *Todo $(n, M, d)_q$-código C, sobre un alfabeto $\mathbb{F}_q$ que contiene al 0, es equivalente a un código C' que contiene la palabra nula $\mathbf{0} = \underbrace{0 \ldots 0}_{n-veces}$.*

Demostración. Supongamos que $\mathbf{0} \notin C$, tomando $x \in C$ arbitrario. Si $i_1, i_2, \ldots, i_k$ son las coordenadas distintas de cero de x, se toma la permutación $\pi = (0x_{i_n}) \ldots (0x_{i_2})(0x_{i_1})$ en donde $Biy(\mathcal{A}_q) \simeq \mathbb{S}_q$, por lo tanto, $C' = \pi(C)$ contiene al vector $\mathbf{0}$. Luego, $C \simeq C'$.

(Demostración alternativa). Sea el grupo simétrico $\mathbb{S}_n$, sea $x = x_1 x_2 \ldots x_n$ en donde $x_i \neq 0$, $\forall i \in \{1, 2, \ldots, n\}$, aplicando la matriz de permutación

$$\left(\begin{array}{ccc} 0 & x_i & j \\ x_i & 0 & j \end{array} \right), \forall j \neq 0,\ x_i \neq 0, \forall i \in \{1, 2, \ldots, n\}$$

al símbolo en la posición i, se tiene que $C \simeq C'$.

Recordemos que el grupo simétrico de grado n, denotado por $\mathbb{S}_n$, emplea el símbolo $\sigma = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{smallmatrix}\right) \in \mathbb{S}_n$ para representar $\sigma(1) = i_1,\ \sigma(2) = i_2,\ \ldots,\ \sigma(n) = i_n$.

□

Ejemplo 1.11. Se muestra un ejemplo de lema anterior. Sean C, C' códigos ternarios.

$$C = \left\{ \begin{array}{c} 1\underline{0}1\underline{0}2 \\ 0\underline{1}0\underline{0}1 \\ 2\underline{2}2\underline{1}0 \end{array} \right\} \overset{\mathbf{c}}{\to} \left\{ \begin{array}{c} 10\bar{1}02 \\ 00\bar{0}11 \\ 21\bar{2}20 \end{array} \right\} \overset{\mathbf{s}}{\to} \left\{ \begin{array}{c} 00000 \\ 01101 \\ 21220 \end{array} \right\} = C' \quad \Rightarrow \quad C \simeq C'.$$

Cada código tiene asociado un grupo de automorfismos o autoequivalencias.

Definición 1.13. Sea $\mathbb{F}$ un cuerpo finito y $C \subset \mathbb{F}_q^n$ un código. El grupo de automorfismos de C es

$$\mathrm{Aut}(C) = \{x \in \mathrm{Isom}_n(\mathbb{F}) : Cx \simeq C\}.$$

Presentamos el grupo de los automorfismos que sólo hacen permutar a las coordenadas.

Definición 1.14. Dos códigos lineales C, $C' \subset \mathbb{F}_q^n$, se dicen que son **permutación equivalente** si existe una permutación $\rho \in \mathbb{S}_n$ tal que $C\rho \simeq C'$, en donde, $C\rho = \{y \in C' : y = x\rho, \forall x \in C\}$. Son un caso particular de códigos equivalentes, operación del tipo (**C**) y es la forma más simple de equivalencia.

Ejemplo 1.12. Los códigos $C = \{000, 011, 201, 112\}$, $C' = \{000, 110, 102, 211\}$ en $\mathbb{F}_3^3$ son permutación equivalente. En $\mathbb{S}_3$ hay $3! = 6$ permutaciones, y las matrices de permutación son $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right)$ y $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$. Usando la segunda permutación en C se obtiene C', es decir, $C\rho \simeq C'$.

En códigos binarios, la noción de códigos que son permutación equivalente es la forma más general de equivalencias. Sin embargo, para código sobre otros cuerpos, otras formas de equivalencias son posibles.

Definición 1.15. Sea $\mathbb{F}$ un cuerpo finito y $C \subset \mathbb{F}_q^n$ un código. EL grupo de automorfismos de permutación (Permutation Automorphism) es

$$\mathrm{PAut}(C) = \{x \in \mathbb{S}_n : Cx \simeq C\}.$$

El conjunto de las permutaciones de las coordenadas que se asignan a un código C forman un grupo, es decir, un conjunto con una operación binaria que tiene una identidad y todos los elementos tienen sus inversos, y se llama grupo de automorfismos de permutación de C. Se denota por $\mathrm{PAut}(C)$. Si C es un código de longitud n, entonces $\mathrm{PAut}(C)$ es un subgrupo del grupo simétrico $\mathbb{S}_n$.

Ejemplo 1.13. Dado el código binario de repetición $Rep_2(n)$ con parámetros $[n, 1]_2$ entonces $\mathrm{PAut}(Rep_2(n)) = \mathbb{S}_n$.

Si conocemos el grupo de automorfirmos de un código C, éste nos puede dar información teórica y práctica acerca de C. Mientras que éstos grupos se han determinado para algunos códigos, hay otros que son difíciles de encontrar. El siguiente teorema relaciona el grupo de automorfismos de permutación de un código y su dual.

Teorema 1.2. *Sea C un código sobre $\mathbb{F}_q$, entonces se tiene que* $\mathrm{PAut}(C) = \mathrm{PAut}(C^{\perp})$.

Definición 1.16. Dos códigos C, $C' \subset \mathbb{F}_q^n$, se dicen que son **equivalencia monomial** si existe una matriz $\mu \in M$ tal que $C\mu \simeq C'$. En donde, M es una matriz cuadrada con exactamente una entrada no nula en cada fila y en cada columna, y se conoce como matriz monomial. Generalmente, se escribe de la forma $M = DP$ con D la parte diagonal y P la parte de permutación. En códigos binarios, la equivalencia monomial y la permutación equivalente son las mismas. Un ejemplo de una matriz monomial 3×3 es $M = \begin{pmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{pmatrix}$ con $a, b, c \in \mathbb{F}_q$.

Ejemplo 1.14. Los códigos $C = \{000, 120, 200, 101\}$, $C' = \{000, 011, 020, 110\}$ en $\mathbb{F}_3^3$ son equivalencia monomial, tomando la matriz monomial 3×3, $M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{pmatrix}$ y aplicandola a cada palabra de C, se obtiene C'. Luego, $C\mu \simeq C'$.

Observación 5. Tenemos tres nociones de cuando dos códigos son los "mismos" (isomorfos como espacios vectoriales), permutación equivalente, equivalencia monomial y equivalencia. Las tres son las mismas si el código es binario; la equivalencia y la equivalencia monomial son iguales si el cuerpo considerado tiene un número primo de elementos, es decir, $\mathbb{Z}_p$ con p un número primo.

6. Esferas, la Cota de Hamming y códigos perfectos

Definición 1.17. Sea $x \in \mathcal{A}^n$, con $|\mathcal{A}| = q$, $r \geq 0$, se define la esfera de radio r con centro en la palabra x como

$$S_q(x, r) = \{y \in \mathcal{A}^n : d(x, y) = r\}$$

Definición 1.18. La bola de radio r centrada en x se define como

$$B_q(x, r) = \{y \in \mathcal{A}^n : d(x, y) \leq r\} = \bigcup_{i=0}^{r} S_q(x, i).$$

Definición 1.19. Se define el volumen $V_q(n,r)$ como el cardinal de cualquier bola de radio r en $x \in \mathcal{A}^n$

$$V_q(n,r) = |B_q(x,r)| = \sum_{i=0}^{r} S_q(x,r) = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i.$$

Lema 1.2. *Si C es un código con distancia mínima $d = 2t+1$ ó $d = 2t+2$, entonces*

$$B_q(c,t) \cap B_q(c',t) = \emptyset.$$

El lema anterior dice que las bolas de radio $t = \lfloor \frac{d-1}{2} \rfloor$ centradas en palabras código son disjuntas.

Proposición 1.4. (**La Cota de Hamming**). *Si C es un $(n,M,d)_q$-código con $d = 2t+1$ ó $d = 2t+2$ entonces*

$$M.\sum_{i=0}^{t} \binom{n}{i}(q-1)^i \leq q^n \ \ con \ \ t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Para códigos lineales q-arios con parámetros $[n,k,d]_q$ la cota de Hamming es

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}(q-1)^i \leq q^{n-k},$$

Para códigos lineales binarios se tiene

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} \leq 2^{n-k}.$$

Observación 6. La cota de Hamming da una cota superior para el tamaño M que un código de longitud n con distancia d pudiese tener.

Ejemplo 1.15. Supongamos que existe un código C con parámetros $(9,M,6)_3$ entonces $t = 2$. Usando la cota de Hamming se tiene que

$$M.\sum_{i=0}^{2} \binom{9}{i}2^i \leq 3^9 \qquad \Longleftrightarrow \qquad M = 3^k \leq \frac{3^9}{55} < 547.$$

Luego $k \leq 5$. Por tanto, no existen códigos con parámetros $(9,M,6)_3$ en donde $M = 3^k$, $k \in \{6,7,8,9\}$.

Ejemplo 1.16. Sea C un $[6,k,3]_2$ entonces $t = 1$. Usando la cota de Hamming para códigos lineales binarios se tiene que

$$\sum_{i=0}^{1} \binom{6}{i} \leq 2^{6-k} \qquad \Longleftrightarrow \qquad M = 2^k \leq \frac{2^6}{7} = \frac{64}{1+\binom{6}{1}} < 10.$$

Luego $k \leq 3$, es decir, no existen códigos lineales con parámetros $[6,k,3]_2$ con $k \in \{4,5,6\}$.

Definición 1.20. Un código $C \subset \mathcal{A}^n$ se dice perfecto si existe un $r \geq 1$ tal que las bolas de radio r con centro en las palabras código son todas disjuntas entre sí y cubren todo el espacio, es decir

$$\mathcal{A}^n = \bigcup_{c \in C}^{\bullet} B_q(c, r).$$

Ejemplo 1.17. Consideremos el código de Hamming $\mathcal{H}_q(r)$ q-ario de orden $r \geq 2$, con parámetros $[n, n-r, 3]_q$, en donde la longitud es $n = \frac{q^r-1}{q-1}$. Como $d = 3 = 2.1 + 1$, la bolas de radio $r = 1$, centradas en las palabras código, son todas disjuntas. Ahora

$$M = |\mathcal{H}_q(r)| = q^{n-r},$$

$$|B_q(c,1)| = \sum_{i=0}^{1} \binom{\frac{q^r-1}{q-1}}{i} (q-1)^i = 1 + \frac{(\frac{q^r-1}{q-1})!}{(\frac{q^r-1}{q-1}-1)!}(q-1) = q^r,$$

$$|\mathcal{A}^n| = q^{\frac{q^r-1}{q-1}} = q^n.$$

Como $q^n = q^r q^{n-r}$, deducimos que las bolas $B_q(c, 1)$, con $c \in \mathcal{H}_q(r)$, cubren todo $\mathcal{A}^n$. Luego, el código de Hamming $\mathcal{H}_q(r)$ es un código perfecto.

El tamaño M de un código perfecto está determinado por su longitud n y por su distancia mínima d.

Teorema 1.3. (**Condición de empaquetamiento de esferas**) *Sea C un $(n, M, d)_q$-código. Entonces C es perfecto si, y sólo si $d = 2t + 1$ y*

$$M. \sum_{k=0}^{t} \binom{n}{k} (q-1)^k = q^n.$$

El teorema anterior nos dice que un código es perfecto si, y sólo si la distancia es impar y se alcanza la igualdad en la cota de Hamming.

Observación 7. Es importante notar que la existencia de los números n, M, q, t que satisfagan el teorema anterior no implica la existencia de un código perfecto con parámetros $(n, M, 2t + 1)_q$.

Observación 8. Existen algunas relaciones entre la teoría de códigos y la teoría de diseños en combinatoria. Una de ellas dice que si C es un $(n, M, d)_2$-código binario perfecto entonces los números

$$\lambda_s = \frac{\binom{n-s}{t+1-s}}{\binom{2t+1-s}{t+1-s}}$$

son enteros para todo $s \in \{1, \ldots, t\}$.

En el siguiente ejemplo se ilustran las dos observaciones anteriores.

Ejemplo 1.18. Sean $n = 90, M = 2^{78}, t = 2$ los números que satisfacen la condición de empaquetamiento de esferas para $q = 2$. En efecto,

$$\sum_{k=0}^{2} \binom{90}{k} = 1 + 90 + \binom{90}{2} = 1 + 90 + 45.89 = 4096 = 2^{12}.$$

Entonces se satisface la igualdad, es decir

$$M.\sum_{k=0}^{t} \binom{n}{k} = 2^{78}.2^{12} = 2^{90} = q^n.$$

Usando la observación anterior se tiene que

$$\lambda_1 = \frac{\binom{89}{2}}{\binom{4}{2}} = \frac{3916}{6} \notin \mathbb{Z}, \qquad \lambda_2 = \frac{\binom{88}{1}}{\binom{3}{1}} = \frac{88}{3} \notin \mathbb{Z}.$$

Luego, no existe ningún código perfecto con parámetros $(90, 2^{78}, 5)_2$.

Los códigos perfectos resultan muy interesantes por la gran simetría con que se encuentran distribuídas sus palabras código.

Teorema 1.4. *Sea C un código perfecto no trivial q-ario, donde q es potencia de un primo, es decir, $q = p^n$ para algún número primo p y algún entero positivo n. Entonces, el código C tiene los mismos parámetros de un código de Hamming o de Golay, es decir*

$$\left(\frac{q^r - 1}{q - 1}, q^{n-r}, 3\right)_q, \qquad (23, 2^{11}, 7)_2, \qquad (11, 3^6, 5)_3.$$

Mas aún

(1) *Si C tiene los parámetros de Golay, es equivalente al correspondiente código de Golay.*
(2) *Si C es lineal y tiene los parámetros de Hamming, entonces es equivalente al código de Hamming correspondiente.*

7. Detección y corrección de errores

Al enviar una palabra código se cometerán t errores debido a las interferencias y el ruido en el canal de transmisión, dicho de otra manera, la palabra enviada difiere en exactamente t coordenadas de la palabra recibida y se dirá que se cometió un error de peso igual a t. Supongamos que $C \subset \mathcal{A}^n$

es un código q-ario sobre $\mathcal{A}$ ($\mathcal{A}$ grupo abeliano). Si se transmite la palabra $c \in C$ y se recibe $x \in \mathcal{A}^n$ con $d(x, c) = t$, entonces existe $e \in \mathcal{A}^n$ tal que

$$x = c + e, \qquad w(e) = t$$

en donde $e = x - c$ es conocido como patrón de error.

Definición 1.21. Se dice que un código detecta s errores si cuando en una palabra código se comete un error de peso r, con $1 \leq r \leq s$, la palabra resultante no es una palabra código. Un código es s-detector si detecta s errores pero no detecta $s + 1$ errores, es decir, hay al menos un error de peso $s + 1$ que el codigo no detecta o dicho de otra manera si se cometen $s + 1$, la palabra recibida estará en el código cualquiera sea la palabra código enviada.

Se dice que un código corrige t errores si al decodificar por distancia mínima, se pueden corregir todos los errores de peso t ó menos. Un código es t-corrector si corrige t errores pero no corrige $t + 1$ errores.

Las capacidades detectoras y correctoras de un código están determinadas por su distancia mínima.

Teorema 1.5. *Sea $C \subset \mathcal{A}^n$ un código con distancia mínima d entonces se tiene que*

(1) *El código C es s-detector si, y sólo si $d \geq s + 1$.*
(2) *El código C es t-corrector si, y sólo si $d \geq 2t + 1$.*

Demostración.

(1) ($\Rightarrow$) Supongamos que $d \geq s + 1$ y supongamos que se transmite $c \in C$ y se produce un error en s ó menos coordenadas. Entonces el vector recibido no puede ser una palabra diferente y por lo tanto detecta el error. Luego, $d \geq s + 1$.

($\Leftarrow$) Supongamos que $d \leq s$ entonces el código no detecta s errores. Sean c, c' dos palabras código cuya distancia de Hamming es d. Entonces, $d(c, c') \leq s$ y la palabra código c' se puede obtener modificando a lo sumo s símbolos de la palabra código c y el código c no detecta s errores. Luego C es s-detector.

(2) ($\Rightarrow$) Supongamos que $d \geq 2t + 1$ y supongamos que se envía $c \in C$ y se recibe $x \in \mathcal{A}^n$ con t errores o menos producidos al momento de la transmisión, es decir, $d(c, x) \leq t$. Si $c' \in C$ con $c' \neq c$ entonces $d(c', x) \geq t + 1$. Por otro lado, $d(c', x) \leq t$ implica que

$d(c, c') \leq d(c, x) + d(c', x) \leq 2t$, contradiciendo el hecho que $d \geq 2t + 1$. Así, c es la palabra código más cercana a x, y decodificando por distancia mínima se corrigen los errores. Luego, $d \geq 2t + 1$.

($\Leftarrow$) Supongamos que $d \leq 2t$, entonces existen dos palabras código c, c' tal que la distancia de Hamming es $d(c, c') = d \leq 2t$. Podemos suponer que los d símbolos distintos, son los d primeros, así que $c = (c_1, c_2, \ldots, c_d, c_{d+1}, \ldots, c_n)$, $c' = (c'_1, c'_2, \ldots, c'_d, c_{d+1}, \ldots, c_n)$. Sea r la palabra de longitud n,

$$r = (c'_1, c'_2, \ldots, c'_t, c_{t+1}, c_{t+2}, \ldots, c_d, c_{d+1}, \ldots, c_n)$$

es decir, los primeros t símbolos iguales a los símbolos de la palabra c' y los restantes como los símbolos de la palabra c, que a partir del $(d + 1)$-ésimo símbolo coinciden con los de la palabra c'. De este modo, $d(c, r) = t$ y $d(r, c') = d - t \leq t$ (incluso menor estricto). En esta situación, al transmitir la palabra código c se pueden producir t errores y recibir la palabra r, el proceso de decodificación por distancia mínima no podría asignar la palabra código c a la palabra recibida r, incluso podría asignarle incorrectamente la palabra código c', lo que contradice la hipótesis sobre la capacidad correctora de C.

□

Teorema 1.6. *Sea $C \subset \mathcal{A}^n$ un código con distancia mínima d entonces se tiene*

(1) *El código C es s-detector si, y sólo si $d = s + 1$.*
(2) *El código C es t-corrector si, y sólo si $d = 2t + 1$ ó $d = 2t + 2$.*

Demostración.

(1) ($\Rightarrow$) Supongamos que C es s-detector con $s \geq d$. Sean $c, c' \in C$ tales que $d(c, c') \leq s$, es decir, el error formado por la coordenadas en donde las palabras c, c' difieren tienen peso menor o igual que s no es detectado por C, y esto contradice la hipótesis. Luego, $d \geq s + 1$. Si $d = s + t$ con $t \geq 1$ implica que C es $(s + t - 1)$-corrector y por lo tanto el valor tiene que ser $t = 1$, es decir, $d = s + 1$.

($\Leftarrow$) Supongamos que $c \in C, x \in \mathcal{A}^n$. Si $d(x, y) = s < d$ entonces $x \notin C$ y por lo tanto, C detecta errores de peso menor o igual que $s = d - 1$. Ahora, si $c, c' \in C$ tales que $d(c, c') = d$, el error formado por las coordenadas en que c, c' son distintas tiene peso $d = s + 1$ y no es detectado por el código. Luego, C es s-detector.

(2) ($\Rightarrow$) Supongamos que C es t-corrector entonces $d \geq 2t+1$ por teorema 1.5. Por otra parte, si $d \geq 2t+3 = 2(t+1)+1$ entonces, por la afirmación anterior, C es $(t+1)$-corrector, y esto es una contradicción. Luego, $d = 2t+1$ ó $d = 2t+2$.

($\Leftarrow$) Supongamos que $d = 2t+1$ ó $d = 2t+2$. Por el lema 1.2 se sabe que las bolas de radio t con centro en palabras códigos son disjuntas. Luego, al decodificar por distancia mínima, C corrige errores de peso menor o igual que t. Si $d = 2t+1$, existen $c, c' \in C$ con $d(c, c') = 2t+1$, es decir, c, c' difieren en $2t+1$ coordenadas. Supongamos que se envía c y se recibe x con exactamente $t+1$ errores en la transmisión, y que x coincide con c' en esas $t+1$ coordenadas. Como $d(x, c) = t+1$ y $d(x, c') = 2t+1-(t+1) = t$, al decodificar por distancia mínima, se decodifica de manera incorrecta a x como c'. De donde, C no es $(t+1)$-corrector. Luego C es t-detector. Si $d = 2t+2$ ocurra lo mismo, ya que $d = 2t+2 = 2(t+1)$ entonces C es t-corrector.

□

Proposición 1.5. *Si un código C tiene distancia mínima d, entonces C es un código $(d-1)$-detector y $\lfloor \frac{d-1}{2} \rfloor$-corrector.*

Demostración. Supongamos que C tiene distacia mínima d entonces por el teorema 1.5 se tiene que $d \geq s+1$, de donde, $s \leq d-1$. Luego, el código C es $(d-1)$-detector. Y $d \geq 2t+1$ se tiene que $t \leq \frac{d-1}{2}$. Tomando la función piso en $\lfloor \frac{d-1}{2} \rfloor$ (en donde $\lfloor x \rfloor$ denota el mayor entero igual o menor que x) se tiene que C es $(d-1)$-detector y $\lfloor \frac{d-1}{2} \rfloor$-corrector.

□

Teorema 1.7. *Un código C es simultáneamente $(t+s)$-detector y t-corrector si, y sólo si $d = 2t+s+1$.*

Demostración.

($\Rightarrow$) Supongamos que C es $(t+s)$-detector y t-corrector. Supongamos que $d \leq 2t+s$, sean c, c' dos palabras código tal que distancia de Hamming es $d = d(c, c') \leq 2t+s$. Consideremos la palabra r obtenida cambiando $t+s$ símbolos de la palabra c por $t+s$ símbolos de la palabra c' de entre los d símbolos que son diferentes entre ellas. De esta forma, $d(c, r) = t+s$ y $d(r, c') \leq t+(t+s)-(t+s) = t$, lo que es contradictoria con la hipótesis. Luego $d = 2t+s+1$

($\Leftarrow$) Supongamos que C tiene distancia mínima $d = 2t+s+1$, sea c una palabra código arbitraria, r una palabra tal que distancia de Hamming a la palabra c es menor o igual que $t+s$,

entonces $d(c, r) \leq t + s$. Para cualquier otra palabra código c' distanta de c, se tiene que $d(c, c') \geq d > 2t + s$. Por la desigualdad triangular se sabe que $d(c, c') \leq d(c, r) + d(r, c')$. Despejando se concluye que $d(r, c') \geq d(c, c') - d(c, r) > 2t + s - d(c, r) \geq t$. Por tanto, $d(r, c') > t$. Luego, C es simultáneamente t-corrector y $(t + s)$-detector.

□

El teorema anterior puede ser usado cuando la distancia mínima de C es par, es decir, si $d = 2t + 2$. En este caso, el código C detecta $t + 1$ y corrige t al mismo tiempo.

8. Código extendido, código pinchado y código *MDS*

El código extendido y el código pinchado son métodos usados para crear nuevos códigos a partir de otros ya dados.

Definición 1.22. (**Código extendido**). Es el proceso de agregar una ó más coordenadas a las palabras de un código. La forma de extender un código es agregar un dígito de control de paridad. Si C es un $(n, M, d)_q$-código, el código extendido $\hat{C}$ se define

$$\hat{C} = \{c_1 c_2 \dots c_n c_{n+1} \in \mathbb{F}_q^{n+1} : c_1 c_2 \dots c_n \in C \text{ con } \sum_{k=1}^{n+1} c_k = 0\}$$

con parámetros $(n + 1, M, \hat{d}\,)_2$ en donde $\hat{d} = d$ ó $d + 1$. En el caso binario, $\hat{d} = d + 1$ si d es impar y d en caso contrario. El código extendido no mejora las cualidades correctoras de un código pero si tiene una mejor capacidad para detectar errores.

Si C es lineal entonces $\hat{C}$ también lo es, si C es binario entonces $\hat{C} \subset E(n + 1)$, resultando que $\hat{C}$ tiene todas sus palabras con peso w par.

Sean G, H la matriz generadora y de paridad, respectivamente, de C. Así, la matriz extendida generadora $\hat{G}$ de $\hat{C}$ puede ser obtenida de G agregándole una columna extra, de manera que la suma de las coordenadas de cada fila de G sea 0. La matriz extendida de paridad para $\hat{C}$ es

$$\hat{H} = \left(\begin{array}{ccc|c} 1 & \cdots & 1 & 1 \\ \hline & & & 0 \\ & H & & \vdots \\ & & & 0 \end{array}\right)_{n-k+1 \times n+1}$$

Esta construcción también es conocida como adding an overall parity check.

Definición 1.23. (**Código pinchado**). Es el proceso opuesto al anterior, es decir, en donde una o más coordenadas son quitadas de las palabras código. Si C es un $(n, M, d)_q$-código, con $d \geq 2$, entonces el código que se obtiene al pinchar una de las coordenadas de C, será conocido como C^* y tiene los parámetros $(n-1, M, d^*)_q$ en donde $d^* = d$ ó $d-1$.

Si C es lineal entonces C^* también lo es.

Las construcciones anteriores sirven para probar lo siguiente.

Proposición 1.6. *Existe un código binario C_1 con parámetros $(n, M, 2t+1)_2$ si, y sólo si existe un código binario C_2 con parámetros $(n+1, M, 2t+2)_2$.*

Demostración.

($\Rightarrow$) Supongamos que C_1 tiene parámetros $(n, M, 2t+1)_2$. Como cada palabra en el código extendido $\hat{C}$ tiene peso par, por la relación entre la distancia y el peso, implica que la distancia entre dos palabras código de $\hat{C}$ es par, luego $d(\hat{C}) = 2t+2$. Luego, existe $C_2 = \hat{C}$ con parámetros $(n+1, M, 2t+2)_2$.

($\Leftarrow$) Supongamos que C_2 tiene parámetros $(n+1, M, 2t+2)_2$ y sean $c, c' \in C_2$ tal que $d(c, c') = 2t+2$. Si se pincha el código C_2 en una coordenada en que c, c' son distintas, el código pinchado C^* resultante tiene distancia mínima $d(C^*) = 2t+1$. Luego, existe $C_1 = C^*$ con parámetros $(n, M, 2t+1)_2$

□

Para un $(n, M, d)_2$-código, si se pincha $d-1$ veces consecutivas, se obtiene el siguiente resultado visto anteriormente.

Proposición 1.7. (**La Cota de Singleton**) *Si C es un código con parámetros $(n, M, d)_q$ entonces*

$$M \leq q^{n-d+1} \quad con \quad d \leq n.$$

En particular, si C es un código lineal con parámetros $[n, k, d]_q$ se tiene que

$$k \leq n - d + 1.$$

Demostración. Supongamos que C es un código con parámetros $(n, M, d)_q$. Tomando la aplicación $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-d+1}$ que borra las últimas $d-1$ coordenadas, es decir, $f(C) = C^{*(d-1)}$. En donde $f(C)$ es un código en $\mathbb{F}_q^{n-d+1}$. Como $f_{|C}$ es 1-1. En efecto, si $c, c' \in C$ con $f(c) = f(c')$ entonces

$c = c_1 \dots c_{n-d+1} x_1 \dots x_{d-1}$ y $c' = c_1 \dots c_{n-d+1} y_1 \dots y_{d-1}$ y por lo tanto $d(c, c') \leq d - 1$, lo cual es absurdo. Luego, $M = |C| = |f(C)| \leq q^{n-d+1}$. En particular, si tenemos un $[n, k, d\,]_q$-código con $M = q^k$ se cumple que $q^k \leq q^{n-d+1}$ si, y sólo si $k \leq n - d + 1$.

□

Esta cota dice que los parámetros básicos de un código (lineal o no) son muy rígidos. No es posible tener tamaño y distancia mínima simultáneamente grandes.

Proposición 1.8. *Si C es un $(n, M, d\,)_q$-código. Si* PAut(C) *es transitivo, entonces los n códigos obtenidos al pinchar C en cada coordenada son permutación equivalente. En donde. un subgrupo $H \subseteq \mathbb{S}_n$ es transitivo si para cualquier $1 \leq i,\ j \leq n$, existe $\rho \in H$ tal que $\rho(i) = j$.*

Demostración. Se quiere ver que C_1^* es equivalente a C_j^* con $j \in \{2, 3, \dots, n\}$. Sea $P_j \in \mathrm{PAut}(C)$ tal que lleva la coordenada j a la posición 1, y sea Q_j la matriz obtenida al eliminar la primera fila y la columna j-ésima de P_j^{-1}. Entonces $C_j^* = (CP_j)_1^* Q_j$. Como $P_j \in \mathrm{PAut}(C)$, entonces $CP_j = C$. Se sigue que $C_j^* = C_1^* Q_j$, como se quería ver.

□

Observación 9. Cuando PAut(C) es transitivo, tenemos información acerca de la estructura de los códigos pinchados. Cuando PAut($\hat{C}$) es transitivo, tenemos información acerca del peso mínimo de C.

Si dos códigos son permutación equivalente entonces sus extensiones también lo son. Esto no necesariamente se cumple para los códigos pinchados.

Ejemplo 1.19. Sean $C_1 = \{000, 011, 101, 111\}$, $C_2 = \{000, 110, 101, 111\}$ códigos sobre $\mathbb{F}_2^3$ tal que $C_1\rho \simeq C_2$ con la permutación $\rho = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$. Entonces, el código extendido de C_1 es $\hat{C}_1 = \{0000, 0110, 1010, 1111\}$ y el código extendido de C_2 es $\hat{C}_2 = \{0000, 1100, 1010, 1111\}$ sobre $\mathbb{F}_2^4$ son permutación equivalente, con la permutación $\rho = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{smallmatrix}\right)$.

Ejemplo 1.20. Sea $C = \{00000, 11000, 00111, 11111\}$ un $[5, 2, 2]_2$-código con PAut(C) no transitivo. El $[4, 2, 1]_2$-código pinchado $C_1^* = \{0000, 1000, 0111, 1111\}$ obtenido pinchando la primera coordenada de C, y el $[4, 2, 2]_2$-código pinchando la quinta coordenada de C, $C_5^* = \{0000, 1100, 0011, 1111\}$, no son permutación equivalente, (aunque C es permutación equivalente a sí mismo), ya que sus distancias son distintas.

Definición 1.24. (**Código** *MDS*). Es un código lineal que alzanza la igual en la Cota de Singleton de la proposición 1.7, se conocen como maximun distance separable *MDS* código. Llamado así, porque tiene la mayor distancia mínima posible entre todos los códigos de longitud n y dimensión k fijas. Ningún código con longitud n y distancia mínima d tiene más n-cadenas que un *MDS* código con los mismos parámetros, equivalentemente, no hay códigos con longitud n y M palabras que tenga distancia mínima mayor que un código *MDS* con parámetros $(n, M)_q$. Además, como $k = n - d + 1$, entonces entre todos los códigos de longitud n que son t-correctores, el código *MDS* codifica la mayor cantidad de palabras.

Ejemplo 1.21. Los únicos códigos binarios son los triviales, es decir, $Rep_2(n)$, $E(n)$ y $\mathbb{F}_2^n$ con parámetros $[n, 1, n]_2$, $[n, n-1, 2]_2$ y $[n, n, 1]_2$, respectivamente. Los códigos *MDS* son interesantes para los casos no binarios, como los códigos Reed-Solomon Generalizado.

Para códigos *MDS* lineales se cumple lo siguiente.

Teorema 1.8. *Sea C un $[n, k]_q$-código con $k \geq 1$. Entonces las siguientes afirmaciones son equivalentes*

(1) *El código C es MDS.*

(2) *El código $C^{\perp}$ es MDS.*

Definición 1.25. Diremos que C es un código *MDS* trivial sobre $\mathbb{F}_q$ si, y sólo si $C = \mathbb{F}_q^n$ ó C es equivalencia monomial al código generado por $\mathbf{1}$ ó su dual. Examinando la matriz generadora en forma estándar se verifica el siguiente resultado para códigos lineales.

Teorema 1.9. *Sea C un $[n, k, d\,]_2$-código. Entonces*

(1) *Si C es MDS, entonces C es trivial.*

(2) *Si $3 \leq d$ y $k \geq 5$, entonces $k \leq n - d - 1$.*

Tenemos como ejemplos de códigos *MDS* no triviales los códigos Reed-Solomon sobre $\mathbb{F}_q$ con longitud $n = q - 1$ y sus extensiones con longitudes $n = q \wedge n = q + 1$.

CAPíTULO 2

Códigos lineales

Un código lineal es un subespacio $C \subseteq \mathbb{F}_q^n$, ya que el alfabeto $\mathbb{F}_q$ le da a los códigos lineales estructura de espacio vectorial. Los códigos lineales son los códigos de bloque más sencillos y comunes. Los códigos de Hamming y Reed-Muller son ejemplos de códigos lineales.

1. Matriz generadora

Definición 2.1. Sea C un $[n,k]_q$-código. Una matriz generadora de C es una matriz $G \in \mathbb{F}_q^{k\times n}$ cuyas filas forman una base de C.

Observación 10. La matriz G siempre existe y su rango es k. Además que G genera al código C, es decir

$$C = \{uG : u \in \mathbb{F}_q^k\}.$$

La matriz generadora G suministra una forma fácil para la codificación de palabras en $\mathbb{F}_q^k$. Es decir, cada palabra de $u \in \mathbb{F}_q^k$ será codificada como $uG \in \mathbb{F}_q^n$.

Ejemplo 2.1. Sea $G = \left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right) \in \mathbb{M}_{2\times 3}(\mathbb{Z}_2)$ una matriz generadora con filas linealmente independientes entre si y rango $k = 2$ que genera un código binario C con parámetros $[3,2]_2$. Entonces

$$uG = (x_1,\ x_2)_{1\times 2}\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}_{2\times 3} = (x_1,\ x_1 + x_2,\ x_2)_{1\times 3}$$

Codificando se obtiene

$$00 \longrightarrow 000, \quad 01 \longrightarrow 011, \quad 10 \longrightarrow 110, \quad 11 \longrightarrow 101.$$

Por tanto, el código será

$$C = \{000,\ 011,\ 110,\ 101\} = E(3)$$

con una distancia $d = 2$.

Observación 11. Considerando la transformación lineal $R_G : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$ definida como sigue $u \mapsto uG$. Como R_G es inyectiva 1-1 se tiene que $Im(R_G) = \mathbb{F}_q^k G = C$ con $C \simeq \mathbb{F}_q^k$. Hay k coordenadas que guardan información y $n - k$ que son redundantes (Esta redundancia es utilizada para la detección y corrección de errores y en los algoritmos de decodificación). En el ejemplo anterior, se observó que cualquier par de coordenadas guardan la información de los mensajes originales, y que la coordenada restante es redundante.

Observación 12. La matriz generadora es útil para almacenar el código, es decir, C es un $[n, k]_q$-código con $M = q^k$ palabras código. Luego, se necesitan nq^k dígitos q-arios para almacenar C. Sin embargo, todas estas palabras código se pueden obtener a partir de la matriz generadora $G \in \mathbb{F}_q^{k\times n}$ de C, es decir, con kn dígitos q-arios. Por ejemplo, el código $\mathcal{H}_2(4)$ con parámetros $[15, 11, 3]_2$. Entonces, hacen falta $15 \times 2^{11} = 30.720$ bits para almacenar el código, contra $11 \times 15 = 165$ bits de la matriz generadora.

Observación 13. Si C es un código binario con una matriz generadora cuyas filas tienen todas peso par. Entonces cada palabra código de C tiene peso par.

Definición 2.2. Un $[n, k]_q$-código es sistemático si existen k coordenadas $i_1, \ldots, i_k$ tal que al restringir las palabras código a estas coordenadas se obtienen todas las q^k palabras de longitud k. El código visto en el ejemplo anterior $E(3)$ es sistemático en las coordenadas 1 y 2, más aún, $E(3)$ es sistemático en cualquier par de coordenadas.

Observación 14. Si G es una matriz generadora para el código C entonces toda matriz reducida por filas de G genera el mismo código, ya que sólo cambia la base de C. Pero será más sencillo usar la matriz escalonada reducida G' por filas de G.

Ejemplo 2.2. Sea C el código con matriz generadora $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \in \mathbb{M}_{3\times 4}(\mathbb{Z}_2)$. Entonces genera un $[4, 3]_2$-código dado por la transformación lineal

$$uG = (x_1,\ x_2,\ x_3)_{1\times 3} \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}_{3\times 4} = (x_1 + x_3,\ x_1 + x_2,\ x_2,\ x_1 + x_2 + x_3)_{1\times 4}$$

Pero si se usa la matriz escalonada reducida por filas de G, $G' = \left(\begin{smallmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{smallmatrix}\right) \in \mathbb{M}_{3\times 4}(\mathbb{Z}_2)$.

$$uG' = (x_1,\ x_2,\ x_3)_{1\times 3} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}_{3\times 4} = (x_1,\ x_2,\ x_3,\ x_1 + x_3)_{1\times 4}$$

el código estará dado por una transformación lineal más sencilla que la primera. Resultando el código

$$C = \{0000,\ 0011,\ 0100,\ 0111,\ 1001,\ 1010,\ 1100,\ 1111\}$$

que es sistemático en las primeras tres coordenadas.

Todo $[n, k]_q$-código C es sistemático en k coordenadas ya que si C está generado por G, tomando la escalonada reducida G' por filas de G. De donde $C = \mathbb{F}_q^k G'$ es sistemático en las k coordenadas donde están los 1's líderes de G'.

Definición 2.3. Una matriz generadora se dice en forma estándar si es de la forma $G = (I_k \mid A)$ en donde I_k es la matriz identidad $k \times k$ y A es $k \times n - k$.

Todo $[n, k]_q$-código C con matriz G dada en forma estándar entonces C es sistemático en las primeras k coordenadas ya que $uG = u(I_k \mid A) = (u \mid uA)$. En dicho caso, codificar y decodificar es sencillo usando el esquema

$$u \xrightarrow{cod} uG = (u \mid uA) \xrightarrow{dec} u.$$

Es importante saber que no todo código lineal tiene matriz generadora en forma estándar. Un ejemplo rápido es suponer que el código con parámetros $[3, 2]_2$ está generado por la matriz $G = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in \mathbb{M}_{2\times 3}(\mathbb{Z}_2)$. Sin embargo, se tiene el siguiente resultado.

Proposición 2.1. *Todo código lineal C es equivalente a un código C' con matriz generadora dada forma estándar.*

Corolario 2.1. *Dado un $[n, k]_2$-código C y $1 \leq i_1 \leq \cdots \leq i_k \leq n$, existe un código lineal C' tal que $C \simeq C'$ y sistemático en las $i_1, \ldots, i_k$ coordenadas.*

2. Código dual y matriz de control de paridad

Recordemos que el espacio vectorial $\mathbb{F}_q^n$ posee un producto interno natural definido como

$$x \cdot y = x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

Definición 2.4. Si C es un $[n,k]_q$-código, se define el código dual de C como el conjunto

$$C^\perp = \{x \in \mathbb{F}_q^n : x \cdot c = 0,\ \forall c \in C\}.$$

Teorema 2.1. *Sea C un $[n,k]_q$-código.*

- *Si $G \in \mathbb{F}_q^{k\times n}$ es una matriz generadora de C entonces*

$$C^\perp = \{x \in \mathbb{F}_q^n : Gx^\top = 0\} = \{x \in \mathbb{F}_q^n : xG^\top = 0\}.$$

- *El código dual $C^\perp$ tiene parámetros $[n, n-k]_q$.*
- *Además tenemos que se cumple que $(C^\perp)^\perp = C$.*

Ejemplo 2.3. Los códigos $\{\mathbf{0}\}$, $\mathbb{F}_q^n$, $Rep_q(n)$ y $P_q(n)$ tienen parámetros $[n,0]$, $[n,n]_q$, $[n,1]_q$ y $[n,n-1]_q$ respectivamente. Forman los códigos duales

$$\mathbb{F}_q^n = \{\mathbf{0}\}^\perp, \qquad Rep_q(n) = P_q^\perp(n)$$

en donde $P_q(n) = \{x \in \mathbb{F}_q^n : \sum_{i=1}^{n} x_i = 0\}$ es el código even-like con parámetros $[n, n-1, 2]_q$. Si $q = 2$ se cumple que $P_q(n) = E(n)$, ya que si $x \in \mathbb{F}_2^n$ entonces $\sum_{i=1}^{n} x_i = 0$ si, y sólo si $w(x)$ es par.

Definición 2.5. Un código lineal C es auto-ortogonal cuando $C \subset C^\perp$.

Definición 2.6. Un código lineal C es auto-dual cuando $C = C^\perp$. Un código auto-dual siempre tiene parámetros $[2n,n]_q$ ó $[n, \frac{n}{2}]_q$. Si C es un código auto-dual, entonces toda matriz generadora de C es matriz de paridad y recíprocamente. Luego, si $G = (I_n \mid A)$ es una matriz generadora de C, entonces $H = (-A^\top \mid I_n)$ también lo es.

Ejemplo 2.4. Sea $C = \{\underbrace{0000}_{c_1}, \underbrace{1100}_{c_2}, \underbrace{0011}_{c_3}, \underbrace{1111}_{c_4}\}$ un $[4,2,2]_2$-código. El código dual se define como

$$C^\perp = \{x \in \mathbb{F}_2^4 : x \cdot c = 0,\ \forall c \in C,\ x = x_1x_2x_3x_4\ \}.$$

Para obtener el código $C^{\perp}$ es necesario resolver las siguientes 4 ecuaciones

$$\begin{cases} x \cdot c_1 = 0 & \Rightarrow & x_1 0 + x_2 0 + x_3 0 + x_4 0 = 0 & \Rightarrow & x = 1111. \\ x \cdot c_2 = 0 & \Rightarrow & x_1 1 + x_2 1 + x_3 0 + x_4 0 = 0 & \Rightarrow & x = 0011. \\ x \cdot c_3 = 0 & \Rightarrow & x_1 0 + x_2 0 + x_3 1 + x_4 1 = 0 & \Rightarrow & x = 1100. \\ x \cdot c_4 = 0 & \Rightarrow & x_1 1 + x_2 1 + x_3 1 + x_4 1 = 0 & \Rightarrow & x = 0000. \end{cases}$$

De donde

$$C^{\perp} = \{1111,\ 0011,\ 1100,\ 0000\}.$$

Luego, $C = C^{\perp}$.

Observación 15. En el ejemplo 5.17 se muestra el caso de un código con parámetros $[4, 2, 3]_5$ que no es auto-dual.

Definición 2.7. Sea C un $[n, k]_q$-código. Una matriz H se dice matriz de control de paridad o matriz de paridad de un código C si es una matriz generadora de $C^{\perp}$, es decir,

$$C^{\perp} = \{xH : x \in \mathbb{F}_q^{n-k}\}.$$

Observación 16. La matriz H siempre existe y es una matriz $n - k \times n$, es decir, la matriz $H \in \mathbb{F}_q^{n-k \times n}$.

Proposición 2.2. *Sea $H \in \mathbb{F}_q^{n-k \times n}$ una matriz de paridad de un $[n, k]_q$-código C entonces*

$$C = \{x \in \mathbb{F}_q^n : Hx^{\top} = 0\} = \{x \in \mathbb{F}_q^n : xH^{\top} = 0\}.$$

Demostración. Si $c \in C$ entonces $c = uG \in C$ con $u \in \mathbb{F}_q^k$ y $G \in \mathbb{F}_q^{k \times n}$ es una matriz generadora del código C. Luego, $cH^{\top} = uGH^{\top} = 0$, así $C \subset S_H = \{x \in \mathbb{F}_q^n : Hx^{\top} = 0\}$, en donde S_H es el espacio solución de un sistema lineal homogéneo de $n - k$ ecuaciones con n variables y con rango $n - k$. Como $\dim(S_H) = n - (n - k) = k = \dim(C)$ se tiene que $C = \{x \in \mathbb{F}_q^n : Hx^{\top} = 0\} = \{x \in \mathbb{F}_q^n : (Hx^{\top})^{\top} = (0)^{\top}\} = \{x \in \mathbb{F}_q^n : xH^{\top} = 0\}$.

□

Observación 17. Una manera de hallar la matriz de paridad H de un código C es a partir de la matriz generadora G. Si $G = (I_k \mid A)$ está en forma estándar, entonces $H = (-A^{\top} \mid I_{n-k})$ es la matriz de paridad en forma estándar (aunque no está en forma estándar como matriz generadora de $C^{\perp}$) de C en donde I_k es la matriz identidad $k \times k$ y A es $n - k \times k$. Además, si G y H son las matrices

generadora y de paridad, respectivamente, de C, entonces H y G son las matrices generadora y de paridad, respectivamente, para $C^{\perp}$ y las filas de toda matriz generadora forman una base del código que ésta genera.

3. Distancia de un código lineal y Cota de Singleton

TEOREMA 2.2. *Sea C un $[n, k, d\,]_q$-código y $H \in \mathbb{F}_q^{n-k\times n}$ una matriz de paridad de C. Entonces*

$$d = \min\{r : \text{hay } \ r \ \text{ columnas linealmente dependientes en } \ H\}.$$

O sea, H tiene d columnas linealmente dependientes, pero cualquier conjunto con $d-1$ columnas son linealmente independientes.

DEMOSTRACIÓN. Sean $H_1, H_2, \ldots, H_n$ y $H^1, H^2, \ldots, H^n$ las filas y las columnas, respectivamente, de la matriz de paridad $H \in \mathbb{F}_q^{n-k\times n}$ de un código C. Si $c \in C$ entonces

$$cH^{\top} = 0 \ \Leftrightarrow \ c_1(H^{\top})_1 + c_2(H^{\top})_2 + \cdots + c_n(H^{\top})_n = 0 \Leftrightarrow c_1H^1 + c_1H^2 + \cdots + c_nH^n = 0.$$

Ahora, $w(c) = r, \ c \in C$ si, y sólo si H tiene r columnas linealmente dependientes. Como $r \geq d$, la matriz H no puede tener $d-1$ columnas dependientes o menos.

□

El teorema anterior es usado para construir códigos lineales con distancia d prefijada y tiene como consecuencia la siguiente proposición vista anteriormente.

PROPOSICIÓN 2.3. (**La Cota de Singleton**). *Si C es un $[n, k, d\,]_q$-código entonces se cumple que*

$$d \leq n - k + 1.$$

EJEMPLO 2.5. Un $[31, 26, d\,]_q$-código tendrá como distancia $d \leq n - k + 1 = 31 - 26 + 1 = 3$, es decir, $d \in \{1, 2, 3\}$.

EJEMPLO 2.6. Un $[4, k, 4]_3$-código tendrá como dimensión $k \leq n - d + 1 = 4 - 4 + 1 = 1$, es decir, $k = 1$.

EJEMPLO 2.7. Un $[n, 36, 3]_q$-código tendrá como longitud $n \geq d + k - 1 = 3 + 36 - 1 = 38$, es decir, $n \in \{38, 39, 40, \ldots\}$.

EJEMPLO 2.8. No existen códigos con parámetros $[2n, 2n-1, 3]_q$. Usando la proposición anterior se tiene $d \leq 2n - (2n-1) + 1 = 2$ y esto contradice el hecho que $d = 3$.

4. Decodificación por síndrome

Veamos ahora un método general para decodificar códigos lineales $C \subset \mathbb{F}_q^n$, que saca provecho de la estructura de espacio vectorial del espacio cociente $\mathbb{F}_q^n/C$. Recordemos que $\mathbb{F}_q^n/C = \{x + C : x \in \mathbb{F}_q^n\}$ es el espacio vectorial formado por la coclases $x + C = \{x + c : c \in C\}$, con las operaciones

$$a(x + C) = ax + C, \quad (x + C) + (y + C) = (x + y) + C$$

con $a \in \mathbb{F}_q$, $x, y \in \mathbb{F}_q^n$. El número de coclases es $|\mathbb{F}_q^n/C| = q^{n-k}$.

Definición 2.8. (**Síndrome**). Sea C un $[n, k]_q$ código con matriz de paridad H. Si $x \in \mathbb{F}_q^n$, el síndrome de x se define por

$$s(x) = s_H(x) = xH^\top.$$

Notar que si $x \in C$ si, y sólo si $s(x) = 0$. Las n-cadenas x, y tienen el mismo síndrome si, y sólo si yacen en la misma coclase.

Teorema 2.3. *Sea C un código lineal con matriz de paridad H. Decodificar por distancia mínima es equivalente a decodificar la palabra recibida x como la palabra código $c = x - a$ donde a es una palabra de peso mínimo en la coclase $x + C$, o equivalentemente, donde a es una palabra de peso mínimo con igual síndrome de x.*

Este proceso de decodificación se realiza con el llamado arreglo estándar para C

$$\begin{array}{ccccc} 0 & c_1 & c_2 & \cdots & c_r \\ a_1 & c_1 + a_1 & c_2 + a_1 & \cdots & c_r + a_1 \\ a_2 & c_1 + a_2 & c_2 + a_2 & \cdots & c_r + a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_s & c_1 + a_s & c_2 + a_s & \cdots & c_r + a_s \end{array}$$

donde $r = q^k - 1$ y $s = q^{n-k} - 1$. La primera fila consta del código, es decir, la coclase $0 + C$. Para formar la segunda fila, se toma una palabra de peso mínimo a_1 que no esté en la primera fila. Esto da como resultado la coclase $a_1 + C$. En general, para formar la i-ésima fila, se tomará a_i de peso mínimo que no se encuentre en las primeras $i - 1$ filas. Este proceso terminará cuando se escriban las q^{n-k} filas. Las palabras a_i con $i \in \{1, \ldots, s\}$ serán conocidas como líderes de coclases del arreglo. Así dos palabras tienen igual síndrome si, y sólo si están en la misma fila del arreglo.

Supongamos que se recibe la palabra x que está en la columna j del arreglo, entonces $x = c_j + a_i$ para cierto a_i, en donde a_i es una palabra de peso mínimo en la coclase $x+C$. Luego, se decodificará x como c_j, es decir, como la palabra código de la columna j.

Ejemplo 2.9. Sea $C = \{0000, 0100, 1101, 1001\}$ un $[4, 2]_2$-código binario dado por la matriz generadora

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}_{2\times 4}$$

Las coclases son

$$0000 + C = \{0000,\ 0100,\ 1101,\ 1001\}.$$
$$1000 + C = \{1000,\ 1100,\ 0101,\ 0001\}.$$
$$0010 + C = \{0010,\ 0110,\ 1111,\ 1011\}.$$
$$1010 + C = \{1010,\ 1110,\ 0111,\ 0011\}.$$

Como elegimos los líderes de las coclases de peso mínimo, el arreglo queda

0000	<u>0100</u>	1101	1001
1000	1100	0101	0001
0010	0110	1111	1011
1010	**1110** ↑	0111	0011

Si se recibe la palabra $x = 1110$, se detecta un error ya que x no está en la primera fila del arreglo. Luego, ésta es corregida como la palabra código $c = 0100$, que se encuentra arriba en la misma columna que x.

Pero no será necesario almacenar todo el arreglo. Sólo se necesitará guardar una tabla con los líderes de las coclases con sus correspondientes síndromes, ya que cada fila estará determinada por éstos, es decir, si se recibe la palabra x, se calcula su síndrome $s(x)$ y se busca en la tabla el líder de coclase a_i con igual síndrome que x. Luego, decodificamos x como $c = x - a_i$. Este proceso es conocido como **decodificación por síndrome**.

Ejemplo 2.10. Sea $C = \{0000, 0100, 1101, 1001\}$ el código del ejemplo anterior. Para hallar la matriz de paridad H del código anterior, se hacen operaciones elementales por filas hasta que G esté en su forma estándar, es decir, $G' = \left(\begin{smallmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{smallmatrix}\right)_{2\times 4}$ entonces la matriz de paridad es

$$H = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}_{2\times 4}$$

La tabla de líderes-síndromes queda

Líderes	Síndromes
0000	00
1000	01
0010	10
1010	11

Si se recibe la palabra $x = 1110$, se calcula su síndrome

$$s(x) = 1110.H^{\top} = 11.$$

Luego, se decodificará x como

$$c = 1110 + 1010 = 0100.$$

Observación 18. Si C tiene distancia mínima d, entonces todas las palabras $x \in \mathbb{F}_q^n$ de peso a lo sumo $t = \lfloor \frac{d-1}{2} \rfloor$ son líderes de coclases.

La observación anterior nos permite realizar la siguiente estrategia conocida con el nombre de decodificación incompleta, usada especialmente cuando la distancia es par. Si $d(C) = 2t + 1$ ó $d(C) = 2t + 2$, este método garantiza la corrección de todos los errores de peso a lo sumo t en todas las palabras código y además, en algunos casos, permite detectar errores de peso mayores que t.

El arreglo estándar a continuación estará dividido en dos partes. En la parte superior está el código y todas las coclases con líderes de peso menor o igual que t. En la parte inferior estarán el resto de las coclases, es decir, aquellas con líderes con peso mayor estricto que t. Si la palabra recibida x está en la parte superior del arreglo, se decodificará de manera usual. Si x se encuentra en la parte inferior del arreglo, se detectará que se cometieron al menos $t + 1$ errores y se pedirá la retransmisión del mensaje.

Ejemplo 2.11. Sea C un $[5, 2, 3]_2$-código con $t = 1$ generado por la matriz dada en su forma estándar

$$G = (I_2 \mid A) = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}_{2\times 5}$$

El arreglo es

00000	10110	01011	11101
10000	00110	11011	01101
01000	11110	00011	10101
00100	10010	01111	11001
00010	10100	01001	11111
00001	10111	**01010** ↑	11100
11000	01110	10011	00101
10001	00111	11010	01100

Supongamos que se recibe $x = 01010$, entonces se decodificará como $c = 01011$, pero si se recibe 10011 entonces se pedirá la retransmisión del mensaje.

Al igual que antes, no es necesario almacenar todo el arreglo y se usará la tabla formada por las coclases y sus síndromes. Basta tomar la parte superior del arreglo.

Ejemplo 2.12. La matriz de paridad del código anterior es $H = \begin{pmatrix} 1&0&1&0&0 \\ 1&1&0&1&0 \\ 0&1&0&0&1 \end{pmatrix}_{3\times 5}$ y la tabla de líderes-síndromes queda

Líderes	Síndromes
00000	000
10000	110
01000	011
00100	100
00010	010
00001	001

Si se recibe 11001, se calcula su síndrome $11001.H^\top = 100$ y por lo tanto, se decodificará como 11001 + 00100 = 11101. Pero si se recibe 01110 y se calcula su síndrome $01110.H^\top = 101$ y como no está en la tabla, se pedirá la retransmisión del mensaje.

CAPíTULO 3

Códigos cíclicos

Los códigos cíclicos son códigos lineales, el alfabeto $\mathbb{F}_q$, le da a los códigos cíclicos, estructura de ideal de un anillo cociente, como se verá más adelante. Los códigos *BCH*, Reed-Solomon y algunos códigos de Hamming son ejemplos de códigos cíclicos.

1. Definiciones

Se supone que, en el espacio vectorial $\mathbb{F}_q^n$, los números n, q son primos relativos, es decir, $\text{mcd}(n, q) = 1$, esto con el objetivo de garantizar que, al momento de factorizar la expresión $x^n - 1$, no tenga factores repetidos. Si $q = 2$ entonces n será impar.

Definición 3.1. Un código lineal $C \subset \mathbb{F}_q^n$ es cíclico si

$$c_0c_1 \dots c_{n-2}c_{n-1} \in C \quad \Rightarrow \quad c_{n-1}c_0c_1 \dots c_{n-2} \in C.$$

Si $C \subset \mathbb{F}_q^n$ es un código lineal q-ario, a cada palabra se le asignará un polinomio como sigue

$$\phi : C \longrightarrow \mathbb{F}_q[x], \qquad c_0c_1 \dots c_{n-1} \longmapsto c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$$

en donde $\mathbb{F}_q[x]$ es el anillo con coeficientes en $\mathbb{F}_q$ cuya variable es x.

El mapa ϕ es un isomorfismo de espacio vectorial de C sobre $\phi(C)$. Ya que

$$\begin{aligned} Ker(\phi(C)) &= \{c_0c_1 \dots c_{n-1} \in C : \phi(C) = 0\} \\ &= \{c_0c_1 \dots c_{n-1} \in C : c_0 + c_1x + \cdots + c_{n-1}x^{n-1} = 0\} \\ &= \{c_0c_1 \dots c_{n-1} \in C : c_i = 0,\ 1 \leq i \leq n\}. \end{aligned}$$

Entonces $Ker(\phi) = \{00 \cdots 0\}$, es decir, $\phi(C)$ es inyectiva. Además, $\phi(C)$ es lineal porque

$$\begin{aligned} \phi(\lambda c_0c_1 \dots c_{n-1} + c_0'c_1' \dots c_{n-1}') &= \phi(\lambda c_0 + c_0'\lambda c_1 + c_1' \dots \lambda c_{n-1} + c_{n-1}') \\ &= \lambda c_0 + c_0' + (\lambda c_1 + c_1')x + \cdots + (\lambda c_{n-1} + c_{n-1}')x^{n-1}. \end{aligned}$$

Tenemos que $\phi(C)$ es lineal e inyectiva, luego se tiene un isomorfismo de C sobre $\phi(C)$. En esta sección, las palabras código se escribirán como polinomios. El álgebra de los polinomios con

coeficientes en $\mathbb{F}_q$, grado menor estricto que n, con la suma usual de polinomios y el producto de polinomios seguido de reducción módulo $x^n - 1$ será denotado como el cociente

$$R_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$$

Observación 19. Un código C es cíclico si, y sólo si $\phi(C)$ es un ideal en $\frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle}$. En efecto, si $c_0c_1 \dots c_{n-1} \in C$ entonces

$$\underbrace{x}_{\in \phi(C)} \big(\underbrace{c_0 + c_1x + \cdots + c_{n-1}x^{n-1}}_{\in R_n} \big) = c_0x + c_1x^2 + \cdots + c_{n-1}x^n \ (mod\ x^n - 1)$$

$$= \underbrace{c_{n-1} + c_0x + c_1x^2 \cdots + c_{n-2}x^{n-1}}_{\in \phi(C)}$$

ya que,

$$c_0 + c_1x + \cdots + c_{n-1}x^{n-1} = c_{n-1}(x^n - 1) + c_{n-1} + c_0x + \cdots + c_{n-2}x^{n-1}$$

por el Algoritmo de la División.

Definición 3.2. Si $C \subset \mathbb{F}_q^n$ es un código, entonces el complemento de C, llamado C^{c}, es un código tal que $C + C^{\mathsf{c}} = \mathbb{F}_q^n$ con $C \cap C^{\mathsf{c}} = \{\mathbf{0}\}$. En general, el complemento no es único. Sin embargo, si C es un código cíclico, hay un único complemento de C que también es cíclico. Este código se denomina, complemento cíclico de C.

2. Polinomios ciclotómicos y las clases q-ciclotómicas módulo

A continuación se explican dos maneras para factorizar la expresión $x^n - 1$ en $\mathbb{F}_q[x]$, con el fin de saber todos los códigos cíclicos q-arios con longitud n.

2.1. <u>Primera manera</u>. Usaremos los polinomios ciclotómicos para factorizar $x^n - 1$ en $\mathbb{F}_q[x]$ sobre el cuerpo $\mathbb{F}_q$, en donde n, q no son necesariamente primos relativos.

Definición 3.3. Los polinomios ciclotómicos $\phi_n(x)$ en $\mathbb{F}_q[x]$ sobre el cuerpo $\mathbb{F}_q$ se definen inductivamente (para el caso $q = 2$) mediante:

- Para $n = 1$ se tiene que $\phi_1(x) = x - 1$.
- Para $n = 2$ se tiene que $\phi_2(x) = \frac{x^2-1}{\phi_1(x)} = \frac{x^2-1}{x-1} = x + 1$.

- Para $n = 3$ se tiene que $\phi_3(x) = \frac{x^3-1}{\phi_1(x)} = \frac{x^3-1}{x-1} = x^2 + x + 1$.
- Para $n = 4$ se tiene que $\phi_4(x) = \frac{x^4-1}{\phi_1(x)\phi_2(x)} = \frac{x^4-1}{(x-1)(x+1)}$.
- Para $n = 5$ se tiene que $\phi_5(x) = \frac{x^5-1}{\phi_1(x)} = \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$.
- Para $n = 6$ se tiene que $\phi_6(x) = \frac{x^6-1}{\phi_1(x)\phi_2(x)\phi_3(x)} = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)}$.
- Para $n = 7$ se tiene que $\phi_7(x) = \frac{x^7-1}{\phi_1(x)} = \frac{x^7-1}{x-1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.
- Para $n = 8$ se tiene que $\phi_8(x) = \frac{x^8-1}{\phi_1(x)\phi_2(x)\phi_4(x)}$.
- Para $n = 9$ se tiene que $\phi_9(x) = \frac{x^9-1}{\phi_1(x)\phi_3(x)} = \frac{x^9-1}{(x-1)(x^2+x+1)} = x^6 + x^3 + 1$.
- Para $n = 10$ se tiene que $\phi_{10}(x) = \frac{x^{10}-1}{\phi_1(x)\phi_2(x)\phi_5(x)}$.
- Para $n = 11$ se tiene que $\phi_{11}(x) = \frac{x^{11}-1}{\phi_1(x)} = \frac{x^{11}-1}{x-1} = x^{10} + x^9 + x^8 + \cdots + x^2 + x + 1$.
- Para $n = 12$ se tiene que $\phi_{12}(x) = \frac{x^{12}-1}{\phi_1(x)\phi_2(x)\phi_4(x)\phi_6(x)}$.
- Para $n = 13$ se tiene que $\phi_{13}(x) = \frac{x^{13}-1}{\phi_1(x)} = \frac{x^{13}-1}{x-1} = x^{12} + x^{11} + x^{10} + \cdots + x^2 + x + 1$.

  $\vdots$

- De donde, si $n > 1$, entonces $\phi_n(x) = \frac{x^n-1}{\prod \phi_d(x)}$ donde el producto que aparece en el denominador, el número d recorre todos los divisores de n excepto el mismo n. Estos polinomios se denominan polinomios ciclotómicos y $\phi_n(x)$ es el n-ésimo polinomio ciclotómico. Se usará la siguiente identidad

$$x^n - 1 = \prod_{d|n} \phi_d(x)$$

  donde $\phi_d(x)$ es el d-ésimo polinomio ciclotómico de orden n. Por definición, las raíces de $\phi_d(x)$ son las raíces n-ésimas de la unidad de grado d. Es decir,

$$\phi_d(x) = \prod_{\text{mcd}(k,n)=1} (x - \gamma^k)$$

  donde γ es una raíz primitiva n-ésima de la unidad de orden d.
- Se puede afirmar que si n es un número primo, entonces

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

Ejemplo 3.1. Teniendo en cuenta lo anterior, se tiene que para códigos cíclicos binarios, con longitudes impares $n = 3, 5, 7, 9, 11, 13$, las factorizaciones de $x^n - 1$ sobre $\mathbb{F}_2$, son las siguientes:

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

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1).$$

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

$$x^9 - 1 = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1).$$

$$x^{11} - 1 = (x-1)(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1).$$

$$x^{13} - 1 = (x-1)(x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1).$$

De las expresiones anteriores, se puede afirmar que hay $2^2 = 4$ códigos cíclicos sobre $\mathbb{F}_2$ con longitudes $n = 3, 5, 11, 13$, y que también hay $2^3 = 8$ códigos cíclicos con longitudes $n = 7$ y $n = 9$ sobre $\mathbb{F}_2$. Notemos que en la definición 3.3, si n es par, se tienen factores repetidos en el denominador, de allí el hecho de suponer que $\text{mcd}(n, q) = 1$.

Observación 20. Es importante poder factorizar $x^n - 1$ sobre cuerpos finitos, ya que si la expresión $x^n - 1$ se puede factorizar completamente sobre $\mathbb{F}_q$, entonces se puede saber cuáles son todos los códigos cíclicos q-arios con longitud n. Sin embargo, puede suceder que algunos sean equivalentes entre sí, como se verá en el ejemplo 3.9.

2.2. Segunda manera. Usaremos las clases q-ciclotómicas módulo n y los polinomios minimales para factorizar $x^n - 1$ en $\mathbb{F}_q[x]$, sobre el cuerpo $\mathbb{F}_q$, para n, q coprimos. A continuación se enuncian tres teoremas usados para realizar las cuentas.

Teorema 3.1. (**Elemento primitivo**). *Sea $\mathbb{F}_q^*$ el grupo de todos los elementos no nulos de $\mathbb{F}_q$ entonces se tiene*

(1) *El grupo $\mathbb{F}_q^*$ es cíclico con $q-1$ elementos bajo la multiplicación en $\mathbb{F}_q$.*
(2) *Si γ es un elemento generador de este grupo cíclico entonces*

$$\mathbb{F}_q = \{0, 1 = \gamma^0, \gamma, \gamma^2, \ldots, \gamma^{q-2}\} \text{ con } \gamma^i = 1 \text{ si, y solo si } q - 1 \mid i.$$

Cada generador $\gamma \in \mathbb{F}_q^*$ es llamado elemento primitivo de $\mathbb{F}_q$. Cuando los elementos no nulos de un cuerpo finito son expresados en potencias de γ, la multiplicación en el cuerpo se lleva a cabo mediante la regla $\gamma^i\gamma^j = \gamma^{i+j} = \gamma^s$ con $0 \leq s \leq q-2$ y $i + j \equiv s \,(mod\ q-1)$

Sea γ un elemento primitivo de $\mathbb{F}_q$ entonces $\gamma^{q-1} = 1$. Por tanto $(\gamma^i)^{q-1} = 1$ con $0 \leq i \leq q-2$ mostrando que los elementos de $\mathbb{F}_q^*$ son raíces de $x^{q-1} - 1 \in \mathbb{F}_p[x]$ y por tanto serán raíces de $x^q - x$. Como 0 es raíz de $x^q - x$ se tiene que los elementos de $\mathbb{F}_q$ son las raíces de $x^q - x$, dando este importante teorema

Teorema 3.2. *Las raíces de $x^q - x$ son exactamente los elementos de $\mathbb{F}_q$.*

Analizando la estructura de cuerpo, será útil saber el número de elementos primitivos en $\mathbb{F}_q$ y cómo encontrar a todos ellos una vez que un elemento primitivo ha sido encontrado. Ya que $\mathbb{F}_q^*$ es un grupo cíclico, recordamos varios hechos acerca de los grupos cíclicos finitos. En un grupo cíclico G de orden n con generador g, los generadores de G son precisamente los elementos g^i con $\text{mcd}(i, n) = 1$. Sea $\Phi(n)$ el número de enteros i donde $1 \leq i \leq n$ tal que $\text{mcd}(i, n) = 1$, es la llamada **Φ-función de Euler**. Por lo que hay $\Phi(n)$ generadores de G. El orden de un elemento $\alpha \in$ G es el entero positivo más pequeño i tal que $\alpha^i = 1$. Un elemento de G tiene orden d si, y sólo si $d \mid n$. Además, g^i tiene orden $d = \frac{n}{\text{mcd}(i,n)}$ y por lo que hay $\Phi(d)$ elementos de orden d. Cuando se habla de los elementos $\alpha \in \mathbb{F}_q^*$, 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 de orden $q-1$. El siguiente teorema sigue de la discusión anterior.

Teorema 3.3. *Sea $\gamma \in \mathbb{F}_q$ un elemento primitivo.*

- *Hay $\Phi(q-1)$ elementos primitivos en $\mathbb{F}_q$, estos son los elementos γ^i con* $\text{mcd}(i, q-1) = 1$.
- *Para cualquier d donde $d \mid (q-1)$, hay $\Phi(d)$ elementos en $\mathbb{F}_q$ de orden d, estos son los elementos $\gamma^{\frac{i(q-1)}{d}}$ con* $\text{mcd}(i, d) = 1$.

Un elemento $\xi \in \mathbb{F}_q$ es una raíz n-ésima de la unidad si $\xi^n = 1$, y es una raíz primitiva n-ésima de la unidad si $\xi^s \neq 1$ para $0 < s < n$. Un elemento primitivo $\gamma \in \mathbb{F}_q$ es por lo tanto una raíz primitiva $(q-1)$-ésima de la unidad. Del teorema 3.1 se sigue que el cuerpo $\mathbb{F}_q$ contiene una raíz primitiva n-ésima de la unidad si, y sólo si $n \mid (q-1)$, en cuyo caso $\gamma^{\frac{q-1}{n}}$ es una raíz primitiva n-ésima de la unidad.

Ejemplo 3.2. El elemento generador $\alpha = 2 \in \mathbb{F}_{13}$ es un elemento primitivo de $\mathbb{F}_{13}$, ya que 2 es un elemento generador del grupo cíclico $\mathbb{F}_{13}^*$ con 12 elementos no nulos bajo la multiplicación en $\mathbb{F}_{13}$, entonces por teorema 3.1 se tiene que $\mathbb{F}_{13} = \{0;\ 1 = \alpha^0;\ 2 = \alpha;\ 4 = \alpha^2;\ 8 = \alpha^3;\ 3 = 16 = \alpha^4;\ 6 = 32 = \alpha^5;\ 12 = 64 = \alpha^6;\ 11 = 128 = \alpha^7;\ 9 = 256 = \alpha^8;\ 5 = 512 = \alpha^9;\ 10 = 1024 = \alpha^{10};\ 7 =$

$2048 = \alpha^{11}\} = \{0, 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$ con $\alpha^i = 1$ si, y sólo si $12 \mid i$. Por el teorema 3.3 hay $\Phi(12) = 4$ elementos primitivos en $\mathbb{F}_{13}$, los cuales son $\alpha = 2$, $\alpha^5 = 6$, $\alpha^7 = 11$, $\alpha^{11} = 7$.

Observación 21. Resumiendo la información anterior, para factorizar $x^n - 1$ sobre $\mathbb{F}_q$, es útil encontrar una extensión $\mathbb{F}_{q^t}$ de $\mathbb{F}_q$ que contenga todas sus raíces. En otras palabras, $\mathbb{F}_{q^t}$ debe contener una raíz primitiva n-ésima de la unidad, que ocurre cuando $n \mid (q^t - 1)$ por el teorema 3.3. El orden $\boldsymbol{ord_n(q)}$ de q módulo n es el entero positivo más pequeño a que satisface $q^a \equiv 1 \ (mod\ n)$. Note que si $\boldsymbol{t = ord_n(q)}$, entonces $\mathbb{F}_{q^t}$ contiene una raíz primitiva n-ésima de la unidad α, pero no hay cuerpo de extensión más pequeño de $\mathbb{F}_q$ que contenga una raíz primitiva. Como α^i son distintos para $0 \leq i < n$ y $(\alpha^i)^n = 1$, $\mathbb{F}_{q^t}$ contiene todas las raíces de $x^n - 1$. Consecuentemente, $\mathbb{F}_{q^t}$ es llamado cuerpo de descomposición de $x^n - 1$ sobre $\mathbb{F}_q$. por lo que los factores irreducibles de $x^n - 1$ sobre $\mathbb{F}_q$ debe ser el producto de los distintos polinomios mínimales de las n-ésimas raíces de la unidad en $\mathbb{F}_{q^t}$. Supongamos que γ es un elemento primitivo de $\mathbb{F}_{q^t}$. Entonces, $\alpha = \gamma^d$ es una raíz primitiva n-ésima de la unidad cuando $d = \frac{q^t-1}{n}$. Las raíces de $M_s(x)$ son $\{\gamma^{ds}, \gamma^{dsq}, \gamma^{dsq^2}, \ldots, \gamma^{dsq^{r-1}}\} = \{\alpha^s, \alpha^{sq}, \alpha^{sq^2}, \ldots, \alpha^{sq^{r-1}}\}$, donde r es el menor entero positivo tal que $dsq^r \equiv ds \ (mod\ \ q^t - 1)$. Pero, $dsq^r \equiv ds \ (mod\ \ q^t - 1)$ si, y sólo si $sq^r \equiv s \ (mod\ n)$.

Definición 3.4. (**Clases q-ciclotómicas módulo n**). Sea $s \in \mathbb{Z}$ tal que $0 \leq s < n$. El conjunto que se define por

$$C_s = \{s, sq, \ldots, sq^{r-1}\} \ (mod\ n)$$

en donde r es el entero positivo más pequeño tomado de tal manera que se cumpla

$$sq^r \equiv s \ (mod\ n) \quad \Longleftrightarrow \quad n \mid sq^r - s$$

son conocidas como las clases q-ciclotómicas módulo n. Los conjuntos C_s, son particiones del conjunto $\{0, 1, 2, \ldots, n-1\}$ de los enteros en conjuntos disjuntos.

Ejemplo 3.3. A continuación, se calcula el conjunto de todos los representantes de las clases 2-ciclotómicas módulo 7 son

$$\begin{cases} C_0 = \{0\}. \\ C_1 = \{1, 2, 4\}, \text{ con } r = 3. \\ C_2 = \{2, 4, 8\} = \{2, 4, 1\} = C_1 \text{ con } r = 3. \\ C_3 = \{3, 6, 12\} = \{3, 6, 5\} \text{ con } r = 3. \\ C_4 = \{4, 8, 16\} = \{4, 1, 2\} = C_2 = C_1 \text{ con } r = 3. \\ C_5 = \{5, 10, 20\} = \{5, 3, 6\} = C_3 \text{ con } r = 3. \\ C_6 = \{6, 12, 24\} = \{6, 5, 3\} \text{ con } r = 3. \\ C_7 = \{7\} = \{0\} \text{ con } r = 1. \end{cases}$$

Descartando los conjuntos que tienen representantes de clases repetidas, se tienen tres clases 2-ciclotómicas módulo 7, las cuales son

$$\begin{cases} C_0 = \{0\}, \text{ con } s = 0. \\ C_1 = \{1, 2, 4\}, \text{ con } r = 3, \ s = 1. \\ C_3 = \{3, 5, 6\}, \text{ con } r = 3, \ s = 3. \end{cases}$$

Notemos que $C_0 \cap C_1 \cap C_3 = \emptyset$, con $t = ord_7(2) = 3$ el tamaño de C_1.

Todo lo discutido anteriormente nos da el siguiente teorema.

Teorema 3.4. *Sea n un entero positivo tal que* $\text{mcd}(q, n) = 1$. *Sea $\boldsymbol{t = ord_n(q)}$ el tamaño de la clase q-ciclotómica módulo n de C_1. Sea α una raíz primitiva n-ésima de la unidad en el cuerpo $\mathbb{F}_{q^t}$.*

(1) *Para cada entero s con $0 \leq s \leq n$, el polinomio minimal de α^s sobre $\mathbb{F}_q$ es*

$$M_{\alpha^s}(x) = \prod_{i \in C_s} (x - \alpha^i)$$

donde C_s es la clase q-ciclotómica módulo n.

(2) *Los conjugados de α^s son los elementos α^i con $i \in C_s$.*

(3) *Además,*

$$x^n - 1 = \prod_s M_{\alpha^s}(x)$$

es la factorización de $x^n - 1$ en factores irreducibles sobre $\mathbb{F}_q$, en donde s recorre los subíndices de todos los conjuntos de las clases q-ciclotómicas módulo n.

Ejemplo 3.4. Vamos a factorizar la expresión $x^7 - 1$ sobre $\mathbb{F}_2$. Las clases 2-ciclotómicas módulo 7 son $C_0 = \{0\}$, $C_1 = \{1, 2, 4\}$ y $C_3 = \{3, 5, 6\}$ con $ord_7(2) = 3$ y las raíces primitivas 7-ésima de la unidad están en $\mathbb{F}_{2^3}$ pero no están en una extensión menor de $\mathbb{F}_2$. Los factores irreducibles de $x^7 - 1$ sobre $\mathbb{F}_2$ tienen grados 1, 3 y 3 que son las cantidades de elementos que están en C_0, C_1 y C_3 respectivamente. Dado el polinomio irreducible, $f(x) = x^3 + x + 1$ sobre $\mathbb{F}_2$. Como $ord_7(2) = 3$, entonces el factor $x^7 - 1$ tiene raíz en $\mathbb{F}_{2^3} = \mathbb{F}_8$. Sea α un elemento primitivo en $\mathbb{F}_{2^3}$, entonces $f(\alpha) = \alpha^3 + \alpha + 1 = 0$, por que α es una raíz. Primero se calculan las potencias de α, para ello se usa el hecho que $f(\alpha) = \alpha^3 + \alpha + 1 = 0$, luego se usan en el cálculo para encontrar los polinomios minimales.

$$\begin{cases} \alpha^3 = \alpha + 1. \\ \alpha^4 = \alpha^3\alpha = (\alpha + 1)\alpha = \alpha^2 + \alpha. \\ \alpha^5 = \alpha^4\alpha = (\alpha^2 + \alpha)\alpha = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1. \\ \alpha^6 = \alpha^5\alpha = (\alpha^2 + \alpha + 1)\alpha = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1. \\ \alpha^7 = \alpha^6\alpha = (\alpha^2 + 1)\alpha = \alpha^3 + \alpha = 1. \\ \alpha^8 = \alpha^7\alpha = \alpha. \\ \alpha^9 = \alpha^8\alpha = \alpha^2. \\ \alpha^{10} = \alpha^9\alpha = \alpha^3 = \alpha + 1. \\ \alpha^{11} = \alpha^{10}\alpha = (\alpha + 1)\alpha = \alpha^2 + \alpha. \\ \alpha^{12} = \alpha^{11}\alpha = (\alpha^2 + \alpha)\alpha = \alpha^2 + \alpha + 1. \\ \alpha^{13} = \alpha^{12}\alpha = (\alpha^2 + \alpha + 1)\alpha = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1. \\ \alpha^{14} = \alpha^{13}\alpha = (\alpha^2 + 1)\alpha = \alpha^3 + \alpha = 1. \end{cases}$$

Usando la primera parte del teorema 3.4 con las potencias de α, tenemos que los polinomios minimales son

Para $s = 0$ se tiene que el polinomio irreducible asociado a $C_0 = \{0\}$ es,

$$M_{\alpha^0}(x) = \prod_{i \in C_0} (x - \alpha^i) = x - \alpha^0 = x - 1 = x + 1.$$

Para $s = 1$ se tiene que el polinomio irreducible asociado a $C_1 = \{1, 2, 4\}$ es,

$$\begin{aligned} M_{\alpha^1}(x) &= \prod_{i \in C_1} (x - \alpha^i) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4) \\ &= (x^2 - \alpha^2 x - \alpha x + \alpha^3)(x - \alpha^4) \\ &= x^3 - \alpha^4 x^2 - \alpha^2 x^2 + \alpha^6 x - \alpha x^2 + \alpha^5 x + \alpha^3 x - \alpha^7 \\ &= x^3 - (\alpha^4 + \alpha^2 + \alpha)x^2 + (\alpha^6 + \alpha^5 + \alpha^3)x - \alpha^7 \\ &= x^3 - (\alpha^2 + \alpha + \alpha^2 + \alpha)x^2 + (\alpha^2 + 1 + \alpha^2 + \alpha + 1 + \alpha + 1)x + 1 \\ &= x^3 + x + 1. \end{aligned}$$

Para $s = 3$ se tiene que el polinomio irreducible asociado a $C_3 = \{3, 5, 6\}$ es,

$$\begin{aligned} M_{\alpha^3}(x) &= \prod_{i \in C_3} (x - \alpha^i) = (x - \alpha^3)(x - \alpha^5)(x - \alpha^6) \\ &= (x^2 - \alpha^5 x - \alpha^3 x + \alpha^8)(x - \alpha^6) \\ &= x^3 - \alpha^6 x^2 - \alpha^5 x^2 + \alpha^{11} x - \alpha^3 x^2 + \alpha^9 x + \alpha^8 x - \alpha^{14} \\ &= x^3 - (\alpha^6 + \alpha^5 + \alpha^3)x^2 + (\alpha^{11} + \alpha^9 + \alpha^8)x + 1 \\ &= x^3 - (\alpha^2 + 1 + \alpha^2 + \alpha + 1 + \alpha + 1)x^2 + (\alpha^2 + \alpha + \alpha^2 + \alpha)x + 1 \\ &= x^3 + x^2 + 1. \end{aligned}$$

Usando la tercera parte del teorema anterior 3.4, se tiene que,

$$x^7 - 1 = \prod_{s \in \{0,1,3\}} M_{\alpha^s}(x) = M_{\alpha^0}(x) M_{\alpha^1}(x) M_{\alpha^3}(x) = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Observación 22. La cuenta del ejercicio anterior 3.4 se puede evitar sabiendo que los únicos polinomios irreducibles sobre $\mathbb{F}_2$ con grado 3 son $x^3 + x + 1 \wedge x^3 + x^2 + 1$.

Ejemplo 3.5. Vamos a factorizar la expresión $x^9 - 1$ sobre $\mathbb{F}_2$. Las clases 2-ciclotómicas módulo 9 son $C_0 = \{0\}$, $C_1 = \{1, 2, 4, 5, 7, 8\}$ y $C_3 = \{3, 6\}$ con $ord_9(2) = 6$ y las raíces primitivas 9 -ésimas de la unidad están en $\mathbb{F}_{2^6} = \mathbb{F}_{64}$ pero no están en una extensión menor de $\mathbb{F}_2$. Los factores irreducibles de la expresión $x^9 - 1$ sobre $\mathbb{F}_2$ tienen grados 1, 6 y 2. Estos polinomios son $M_{\alpha^0}(x) = M_1(x) = x + 1$, $M_{\alpha^1}(x) = M_\alpha(x)$ y $M_{\alpha^3}(x)$, en donde α es una raíz primitiva 9-ésima de la unidad

en $\mathbb{F}_{64}$. El único polinomio irreducible de grado 2 sobre $\mathbb{F}_2$ es $x^2 + x + 1$, que por lo tanto debe ser $M_{\alpha^3}(x)$ y $M_\alpha(x) = x^6 + x^3 + 1$. Por tanto, la factorización de $x^9 - 1 = (x+1)(x^2+x+1)(x^6+x^3+1)$.

Observación 23. Las factorizaciones en el ejemplo 3.4 y 3.5 coinciden con las factorizaciones del ejemplo 3.1 con $n = 7$ y $n = 9$.

Ejemplo 3.6. Vamos a factorizar la expresión $x^{13}-1$ sobre $\mathbb{F}_3$. Las clases 3-ciclotómicas módulo 13 son $C_0 = \{0\}$, $C_1 = \{1, 3, 9\}$, $C_2 = \{2, 5, 6\}$, $C_4 = \{4, 10, 12\}$ y $C_7 = \{7, 8, 11\}$ con $ord_{13}(3) = 3$ y las raíces primitivas 13 -ésimas de la unidad están en $\mathbb{F}_{3^3} = \mathbb{F}_{27}$ pero no están en una extensión menor de $\mathbb{F}_3$. Los factores irreducibles de la expresión $x^{13} - 1$ sobre $\mathbb{F}_3$ tienen grados 1, 3, 3, 3 y 3. Estos polinomios son, $M_1(x) = x - 1$, $M_\alpha(x) = x^3 + 2x + 2$, $M_{\alpha^2}(x) = x^3 + x^2 + x + 2$, $M_{\alpha^4}(x) = x^3 + x^2 + 2$, $M_{\alpha^7}(x) = x^3 + 2x^2 + 2x + 2$. Por tanto, la factorización de $x^{13} - 1 = (x - 1)(x^3 + 2x + 2)(x^3 + x^2 + x + 2)(x^3 + x^2 + 2)(x^3 + 2x^2 + 2x + 2)$.

3. Polinomio generador

El siguiente resultado reune algunos hechos básicos de los códigos cíclicos.

Teorema 3.5. *Sea C un ideal distinto de cero en R_n, es decir, un código cíclico no nulo con longitud n. Entonces se cumplen*

(1) *Existe un único polinomio mónico $g(x)$ de grado mínimo en C. Además, este polinomio es el polinomio generador de un código C, es decir, $C = \langle g(x) \rangle$.*
(2) *Para $g(x) \in C$ se cumple que $g(x) \mid x^n - 1$.*
(3) *Si $gr(g(x)) = r$, entonces C tiene dimensión $n - r$. Mas aún,*

$$C = \langle g(x) \rangle = \{r(x)g(x) : gr(r(x)) < n - r\}.$$

(4) *Si $g(x) = g_0 + g_1 x + \cdots + g_r x^r$, entonces $g_0 \neq 0$ y C tiene matriz generadora*

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r \end{pmatrix}_{n-r \times n}$$

donde cada fila de G es un desplazamiento cíclico de la fila previa.

(5) *Si α es una raíz primitiva n-ésima de la unidad para alguna extensión del cuerpo $\mathbb{F}_q$, entonces*

$$g_z(x) = \prod_s M_{\alpha^s}(x)$$

en donde $M_{\alpha^s}(x)$ es el producto de los polinomios minimales sobre $\mathbb{F}_q$ del teorema 3.4*, con $0 \leq s \leq n$ el subíndice de cada conjunto de las clases q-ciclotómicas módulo n y en donde z indica las combinaciones posibles de estos subíndices.*

Demostración.

(1) Sea $g(x)$ un único polinomio mónico de grado mínimo en C. Ya que C no es cero, tal polinomio existe. Si $c(x) \in C$ entonces por el Algoritmo de la División, $c(x) = g(x)h(x) + r(x)$ con $c(x), g(x), h(x), r(x) \in \mathbb{F}_q[x]$ en donde $r(x) = 0$ ó $gr(r(x)) < gr(g(x))$. Como C es un ideal R_n, $r(x) \in C$ y $g(x)$ es de grado mínimo se tiene que $r(x) = 0$. De donde, $g(x)$ es mónico de grado mínimo en C y $C = \langle g(x) \rangle$.

(2) $g(x) \in C$. Por el Algoritmo de la División, se tiene que $x^n - 1 = g(x)h(x) + r(x)$ en donde, nuevamente $r(x) = 0$ ó $gr(r(x)) < gr(g(x))$ con $g(x), h(x), r(x) \in \mathbb{F}_q[x]$. Como $x^n - 1$ corresponde al vector $\mathbf{0} \in C$ y C es un ideal en R_n, $r(x) \in C$, una contradicción a menos que $r(x) = 0$. De donde, $g(x) \mid x^n - 1$.

(3) El ideal generado por $g(x)$ es $\langle g(x) \rangle = \{f(x)g(x) : f(x) \in R_n\}$. Basta ver que al restringir $f(x)$ a polinomios de grado menor estricto a $n - r$. Se sabe que $x^n - 1 = h(x)g(x)$ para algún polinomio $h(x)$ con grado $n - r$. Al dividir se tiene, $f(x) = q(x)h(x) + r(x)$ con $gr(r(x)) < n - r$. Entonces

$$f(x)g(x) = q(x)h(x)g(x) + r(x)g(x) = q(x)(x^n - 1) + r(x)g(x)$$

y así $f(x)g(x) = r(x)g(x)$ en R_n, que es lo que se quería ver. Esto también nos muestra que el conjunto

$$\{g(x), xg(x), \ldots, x^{n-r+1}g(x)\}$$

genera al código C y como es linealmente independiente, forma una base para C. Luego $\dim(C) = n - r$.

(4) Si $g_0 = 0$ entonces $g(x) = xg_1(x)$ con $gr(g_1(x)) < r$. Pero entonces se tiene que

$$g_1(x) = 1.g_1(x) \equiv x^n g_1(x) = x^{n-1}g(x) \in C$$

lo cual es absurdo ya que $g_1 \neq 0$ tiene grado menor que $g(x)$. Por lo tanto $g_0 = 0$. Por último, G es la matriz generadora de un código C, pues $\{g(x), xg(x), \ldots, x^{n-r+1}g(x)\}$ es una base de C.

(5) Se cumple usando la última parte del teorema 3.4 con $\text{mcd}(q, n) = 1$.

□

En el siguiente ejemplo se verá que un codigo cíclico C puede ser generado por otros polinomios generadores además de su polinomio generador.

Ejemplo 3.7. Como $1+x$ divide a x^3-1 entonces el código $C = \langle 1+x \rangle$ es cíclico en $R_3 = \frac{\mathbb{F}_2[x]}{\langle x^3-1 \rangle}$. Por el tercer apartado del teorema anterior, se tiene que $\dim(C) = 3 - 1 = 2$ y C está formado por los múltiplos de $1 + x$, es decir,

$$\underbrace{0}_{00}(1+x), \quad \underbrace{1}_{10}(1+x), \quad \underbrace{x}_{01}(1+x), \quad \underbrace{(1+x)}_{11}(1+x).$$

De donde, el código es

$$C = \{0,\ 1+x,\ 1+x^2,\ x+x^2\} = \{000,\ 110,\ 101,\ 011\} = E(3).$$

Notemos que

$$\langle 1+x^2 \rangle = \{0,\ 1+x^2,\ x(1+x^2),\ (1+x)(1+x^2)\} = \{0,\ 1+x^2,\ 1+x,\ x+x^2\} = C$$

es decir, el código C también está generado por $1 + x^2$ pero, $1 + x^2$ no divide a $x^3 - 1$.

En el ejemplo anterior vimos que el código C está generado por dos polinomios generadores distintos, es decir, $C = \langle 1 + x \rangle = \langle 1 + x^2 \rangle$. Para diferenciarlos, se utiliza la notación $C = \langle\langle p(x) \rangle\rangle$ para indicar que C es el ideal generado por $p(x)$ y que $p(x)$ es el polinomio generador C.

Corolario 3.1. *Si C un código cíclico en R_n. Se tiene que las siguientes afirmaciones son equivalentes:*

- *$g(x)$ es un polinomio mónico con grado mínimo en C.*
- *$C = \langle g(x) \rangle$ con $g(x)$ mónico, y $g(x) \mid x^n - 1$.*

Las siguientes proposiciones se desprenden del teorema 3.5 y sirven para relacionar los códigos cíclicos dados sus polinomios generadores.

Proposición 3.1. *Sean $C_1 = \langle\langle g(x) \rangle\rangle$ y $C_2 = \langle\langle f(x) \rangle\rangle$ códigos cíclicos en R_n. Entonces*

- $C_1 \subset C_2$ *si, y sólo si* $f(x) \mid g(x)$.
- *El polinomio generador de la intersección es* $C_1 \cap C_2 = \langle\langle \text{mcm}\{g(x),\ f(x)\}\rangle\rangle$.
- *El polinomio generador de la suma es* $C_1 + C_2 = \langle\langle \text{mcd}\{g(x),\ f(x)\}\rangle\rangle$.

En donde, la suma se define como $C_1 + C_2 = \{c_1 + c_2 \in C_1 + C_2 : c_1 \in C_1,\ c_2 \in C_2\}$ *y es el menor código cíclico que contiene a* C_1 *y a* C_2.

Observación 24. La intersección y la suma de dos códigos cíclicos también resultan ser códigos cíclicos.

Proposición 3.2. *Sea* $E(n) = \{x \in \mathbb{F}_2^n : w(x) \equiv 0\ (mod\ 2)\}$ *el código que consta de todas las palabras de peso par en* $\mathbb{F}_2^n$*, y sea C un código cíclico binario de longitud n. Entonces*

- $E(n) = \langle\langle x - 1\rangle\rangle$.
- $C = \langle\langle g(x)\rangle\rangle \subset E(n)$ *si, y sólo si* $x - 1 \mid g(x)$.

4. Polinomio de control

Dado que el polinomio generador $g(x)$ con $gr(g(x)) = r$ de un $[n, n-r]_q$-código cíclico C en R_n divide a $x^n - 1$, entonces se tiene que

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

en donde $h(x)$ es un polinomio de grado $n - r$ y será conocido como el polinomio de control o chequeo de C.

Teorema 3.6. *Sea* $h(x)$ *el polinomio de control de un código cíclico C de* R_n*. Entonces:*

(1) *El código cíclico C puede escribirse también como*

$$C = \{p(x) \in R_n : p(x)h(x) \equiv 0\ (mod\ x^n - 1)\}.$$

(2) *Si* $h(x) = h_0 + h_1 x + \cdots + h_{n-r}x^{n-r}$*, entonces la matriz de control de paridad de está dada por:*

$$H = \begin{pmatrix} h_{n-r} & \cdots & \cdots & h_1 & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_{n-r} & \cdots & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_{n-r} & \cdots & \cdots & h_1 & h_0 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & h_{n-r} & \cdots & \cdots & h_1 & h_0 \end{pmatrix}_{r \times n}$$

(3) *El código dual $C^\perp$ es un código cíclico de dimensión r con polinomio generador*

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

Ejemplo 3.8. El código $C = \langle x^3 + x + 1\rangle = \mathcal{H}_2(3)$ del ejemplo 4.1 tiene polinomio de control o chequeo

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

y como

$$h^\perp(x) = x^4 h(x^{-1}) = x^4(x^{-4} + x^{-2} + x^{-1} + x + 1) = 1 + x^2 + x^3 + x^4$$

el código C tiene matriz de paridad

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}_{3\times 7}$$

Observación 25. El código dual $C^\perp$ de un código cíclico C es cíclico. Ejemplos: los códigos cíclicos $\mathbb{F}_q^n$ y $\{\mathbf{0}\}$ son duales el uno del otro; el código de repetición $Rep_q(n)$ es un código cíclico cuyo dual es el código cíclico de los vectores even-like en $\mathbb{F}_q^n$. Además, el subcódigo de un código cíclico también es dual.

5. Polinomio recíproco

Si $f(x) = f_0 + f_1 x + \cdots + f_{a-1}x^{a-1} + f_a x^a$ es un polinomio de grado a sobre $\mathbb{F}_q$. El polinomio recíproco de $f(x)$ es

$$f^*(x) = x^a f(x^{-1}) = f_a + f_{a-1}x + \cdots + f_1 x^{a-1} + f_0 x^a.$$

en donde sus coeficientes son los de $f(x)$ pero en orden inverso.

Proposición 3.3. *Si $C_1 = \langle\langle f(x)\rangle\rangle$ y $C_2 = \langle\langle f^*(x)\rangle\rangle$ con $f(x)$ y $f^*(x)$ polinomios recíprocos el uno del otro entonces $C_1 \simeq C_2$.*

6. Códigos cíclicos en $R_7 = \frac{\mathbb{F}_2[x]}{x^7-1}$

Ejemplo 3.9. Se estudiarán los códigos cíclicos binarios con longitud 7. Usando los polinomios ciclotómicos para factorizar $x^7 - 1$ se obtiene $\phi_7(x) = \frac{x^7-1}{\phi_1(x)}$ en donde

$$\phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x + 1)(x^3 + x^2 + 1).$$

Por tanto, la factorización es

$$x^7 - 1 = \phi_1(x)\phi_7(x) = (x-1)(x^3+x+1)(x^3+x^2+1)$$

en donde $g_0(x) = x-1$, $g_1(x) = x^3+x+1$, $g_3(x) = x^3+x^2+1$ son irreducibles sobre $\mathbb{F}_2$, con las clases 2-ciclotómicas C_0, C_1, C_3, respectivamente, del ejemplo 3.3. Como R_7 se parte como el producto de 3 polinomios sobre $\mathbb{F}_2$ entonces hay $2^3 = 8$ códigos cíclicos. Estos son los siguientes:

(1) $C_1(7) = \langle x^7-1\rangle = \langle x^7+1\rangle = \langle 0\rangle = \{0000000\} = \{\mathbf{0}\}$ con parámetros $[7, 0, -]$.

(2) $C_2(7) = \langle g_{1,3}(x)\rangle = \langle g_1(x)g_3(x)\rangle$

$$= \langle (x^3+x+1)(x^3+x^2+1)\rangle = \langle x^6+x^5+x^4+x^3+x^2+x+1\rangle.$$

Usando el teorema 3.5, se obtiene la matriz generadora $G_2(7) = (1\ 1\ 1\ 1\ 1\ 1\ 1)_{1\times 7}$ con polinomio generador $g(x) = x^6+x^5+x^4+x^3+x^2+x+1$. De esta manera se genera el código

$$C_2(7) = \{uG_2(7) : u \in \mathbb{F}_2\} = (u)_{1\times 1}(1\ 1\ 1\ 1\ 1\ 1\ 1)_{1\times 7} = (u\ u\ u\ u\ u\ u\ u)_{1\times 7}$$

como $u \in \mathbb{F}_2 = \mathbb{Z}_2$ se tiene

$$C_2(7) = \{0000000,\ 1111111\} = Rep_2(7).$$

con parámetros $[7, 1, 7]_2$.

(3) $C_3(7) = \langle g_{0,1}(x)\rangle = \langle g_0(x)g_1(x)\rangle = \langle (x-1)(x^3+x+1)\rangle = \langle x^4+x^3+x^2+1\rangle$. Usando la proposición 3.2 se tiene $C_3(7) \subset E(7)$, ya que $x-1 \mid g_{0,1}(x)$. Este código tiene los parámetros $[7, 3, 2]_2$ y su matriz generadora es

$$G_3(7) = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}_{3\times 7}$$

(4) $C_4(7) = \langle g_{0,3}(x)\rangle = \langle g_0(x)g_3(x)\rangle = \langle (x-1)(x^3+x^2+1)\rangle = \langle x^4+x^2+x+1\rangle$, este código tiene polinomio generador $g_{0,3}(x) = x^4+x^2+x+1$ y el recíproco es $g^*_{0,3}(x) = x^4+x^3+x^2+1$ coincidiendo con el polinomio generador de $C_3(7)$. De esta manera se cumple que $C_4(7) \simeq C_3(7)$ y tiene los mismos parámetros $[7, 3, 2]_2$ del código $C_3(7)$.

(5) $C_5(7) = \langle g_1(x)\rangle = \langle x^3+x+1\rangle$ con parámetros $[7, 4, 3]_2$, para construir este código se construyó la siguiente tabla, donde en la primera columna se colocan los factores $p(x)$ y en la segunda columna los múltiplos $p(x)(x^3+x+1)$ del polinomio generador. Como

multiplicar por x es hacer un desplazamiento cíclico en las palabras de $\mathbb{F}_2^7$, las palabras código se obtienen haciendo los desplazamientos del polinomio generador por $1, x, x^2, x^3$, y luego haciendo todas las sumas posibles de estas 4 palabras código

$p(x)$	$p(x).(x^3 + x + 1)$	Palabras código
0	0	0000000
1	$x^3 + x + 1$	1101000
x	$x^4 + x^2 + x$	0110100
x^2	$x^5 + x^3 + x^2$	0011010
x^3	$x^6 + x^4 + x^3$	0001101

Resultando el código que tiene $M = 2^4 = 16$ palabras, las cuales son

$$C_5(7) = \left\{ \begin{array}{cccc} 0000000, & 1101000, & 0110100, & 0011010 \\ 0001101, & 1011100, & 1001011, & 1110010 \\ 1100101, & 0101110, & 0111001, & 0010111 \\ 1000110, & 1010001, & 1111111, & 0100011 \end{array} \right\}$$

Este código es equivalente al código de Hamming binario $\mathcal{H}_2(r)$ del ejemplo 4.1 con $r = 3$, ya que es lineal y tiene los parámetros $[7, 4, 3]_2$.

(6) $C_6(7) = \langle g_3(x) \rangle = \langle x^3 + x^2 + 1 \rangle$, este es un código cuyo polinomio generador $g_3(x) = x^3 + x^2 + 1$ y su recíproco es $g_3^*(x) = x^3 + x + 1$ coincidiendo con el polinomio generador de $C_5(7)$. De esta manera, se tiene que $C_6(7) \simeq C_5(7)$ por proposición 3.3, entonces tiene los mismos parámetros $[7, 4, 3]_2$ del código $C_5(7)$.

(7) $C_7(7) = \langle g_0(x) \rangle = \langle x - 1 \rangle = \langle x + 1 \rangle = E(7)$ por la proposición 3.2, y este código tiene parámetros $[7, 6, 2]_2$.

(8) $C_8(7) = \langle 1 \rangle = \mathbb{F}_2^7$. Como el polinomio generador es $\langle 1 \rangle$, entonces por el cuarto apartado del teorema 3.5, la matriz generadora es $G_8(7) = I_7$, en donde I es la identidad 7×7, por lo tanto

$$C_8(7) = \{uG_8(7) : u \in \mathbb{F}_2^7\} = \mathbb{F}_2^7 = \mathbb{Z}_2^7$$

con parámetros $[7, 7, 1]_2$.

Resumiendo la información de los códigos cíclicos en R_7, estudiados en esta parte en el recuadro a continuación. En donde z nos indica la clase q-ciclotómica (mod n) usada, es decir, si $z = 0, 1, 3$ involucra las clases ciclotómicas $C_0 \cup C_1 \cup C_3$. El número k es la dimensión del código

cíclico en R_7. El polinomio generador $g_z(x)$ del código cíclico asociado a la clase ciclotómica. El símbolo $\simeq$ indica que dos códigos son equivalentes.

z	k	$g_z(x)$	Códigos
$0,1,3$	0	$g_{0,1,3}(x) = x^7 - 1$	$C_1(7) = \{\mathbf{0}\}$
$1,3$	1	$g_{1,3}(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	$C_2(7) = Rep_2(7)$
$0,1$	3	$g_{0,1}(x) = x^4 + x^3 + x^2 + 1$	$C_3(7) \subset E(7)$
$0,3$	3	$g_{0,3}(x) = x^4 + x^2 + x + 1$	$C_4(7) \simeq C_3(7)$
1	4	$g_1(x) = x^3 + x + 1$	$C_5(7) \simeq \mathcal{H}_2(3)$
3	4	$g_3(x) = x^3 + x^2 + 1$	$C_6(7) \simeq C_5(7)$
0	6	$g_0(x) = x - 1$	$C_7(7) = E(7)$
	7	1	$C_8(7) = \mathbb{Z}_2^7$

7. Códigos cíclicos en $R_9 = \frac{\mathbb{F}_2[x]}{x^9-1}$

Ejemplo 3.10. Se estudiarán los códigos cíclicos binarios de longitud 9. Del ejemplo 3.5 se tiene que las clases 2-ciclotómicas módulo 9 son $C_0 = \{0\}$, $C_1 = \{1,2,4,5,7,8\}$ y $C_3 = \{3,6\}$, con los polinomios minimales, $M_1(x) = x + 1$, $M_\alpha(x) = x^6 + x^3 + 1$ y $M_{\alpha^3}(x) = x^2 + x + 1$ respectivamente. Usando el teorema 3.5, último apartado, se tienen los polinomios generadores $g_0(x) = x + 1$, $g_1(x) = x^6 + x^3 + 1$ y $g_3(x) = x^2 + x + 1$. Tenemos $2^3 = 8$ códigos cíclicos. Resumiendo los datos en el siguiente cuadro:

z	k	$g_z(x)$	Códigos
$0,1,3$	0	$g_{0,1,3}(x) = x^9 - 1$	$C_1(9) = \{\mathbf{0}\}$
$1,3$	1	$g_{1,3}(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	$C_2(9) = Rep_2(9)$
$0,1$	2	$g_{0,1}(x) = x^7 + x^6 + x^4 + x^3 + x + 1$	$C_3(9) \subset E(9)$
1	3	$g_1(x) = x^6 + x^3 + 1$	$C_4(9) \supset C_3(9)$
$0,3$	6	$g_{0,3}(x) = x^3 + 1$	$C_5(9) \subset E(9)$
3	7	$g_3(x) = x^2 + x + 1$	$C_6(9) \supset C_5(9)$
0	8	$g_0(x) = x + 1$	$C_7(9) = E(9)$
	9	1	$C_8(9) = \mathbb{Z}_2^9$

8. Códigos cíclicos en $R_{13} = \dfrac{\mathbb{F}_3[x]}{x^{13}-1}$

Ejemplo 3.11. Se estudiarán los códigos cíclicos ternarios con longitud 13. Teniendo en cuenta las 3-clases ciclotómicas módulo 13 y los polinomios minimales del ejemplo 3.6, y usando la última parte del teorema 3.5 para obtener los polinomios generadores. Los cuales son $g_0(x) = x-1$, $g_1(x) = x^3 + 2x + 2$, $g_2(x) = x^3 + x^2 + x + 2$, $g_4(x) = x^3 + x^2 + 2$ y $g_7(x) = x^3 + 2x^2 + 2x + 2$ con $C_0 = \{0\}$, $C_1 = \{1, 3, 9\}$, $C_2 = \{2, 5, 6\}$, $C_4 = \{4, 10, 12\}$ y $C_7 = \{7, 8, 11\}$, respectivamente. Como la expresión $x^{13} - 1$ se parte en el producto de 5 polinomios irreducible sobre $\mathbb{F}_3$, entonces hay $2^5 = 32$ códigos cíclicos sobre $\mathbb{F}_3$ con longitud $n = 13$. Resumiendo la información en el siguiente recuadro:

z	k	$g_z(x)$	Códigos
$0, 1, 2, 4, 7$	0	$g_{0,1,2,4,7}(x) = x^{13} - 1$	$C_1(13) = \{\mathbf{0}\}$
$1, 2, 4, 7$	1	$g_{1,2,4,7}(x) = x^{12} + x^{11} + x^{10} + x^9 + \cdots + x^3 + x^2 + x + 1$	$C_2(13) = Rep_3(13)$
$0, 1, 2, 4$	3	$g_{0,1,2,4}(x) = x^{10} + x^9 + 2x^8 + x^7 + x^6 + x^5 + 2x^3 + 2x + 1$	$C_3(13) \subset P_3(13)$
$0, 1, 2, 7$	3	$g_{0,1,2,7}(x) = x^{10} + 2x^9 + x^8 + 2x^6 + 2x^5 + x^4 + x^3 + x^2 + x + 1$	$C_4(13) \subset P_3(13)$
$0, 1, 4, 7$	3	$g_{0,1,4,7}(x) = x^{10} + 2x^9 + 2x^7 + x^5 + x^3 + 2x + 1$	$C_5(13) \subset P_3(13)$
$0, 2, 4, 7$	3	$g_{0,2,4,7}(x) = x^{10} + 2x^9 + 2x^7 + x^6 + x^5 + 2x^4 + x^3 + 2x^2 + 2x + 2$	$C_6(13) \subset P_3(13)$
$1, 2, 4$	4	$g_{1,2,4}(x) = x^9 + 2x^8 + x^7 + 2x^6 + x^4 + x^3 + 2$	$C_7(13) \subset \mathcal{H}_3(3)$
$1, 2, 7$	4	$g_{1,2,7}(x) = x^9 + x^7 + x^6 + 2x^4 + x^2 + 2x + 2$	$C_8(13) \subset \mathcal{H}_3(3)$
$2, 4, 7$	4	$g_{2,4,7}(x) = x^9 + x^8 + 2x^7 + x^5 + 2x^3 + 2x^2 + 2$	$C_9(13) \subset \mathcal{H}_3(3)$
$1, 4, 7$	4	$g_{1,4,7}(x) = x^9 + 2x^6 + 2x^5 + x^3 + 2x^2 + x + 2$	$C_{10}(13) \subset \mathcal{H}_3(3)$
$0, 1, 2$	6	$g_{0,1,2}(x) = x^7 + 2x^5 + x^3 + 2x^2 + x + 2$	$C_{11}(13) \subset P_3(13)$
$0, 1, 4$	6	$g_{0,1,4}(x) = x^7 + x^5 + x^4 + 2x^3 + 2x^2 + 2$	$C_{12}(13) \subset P_3(13)$
$0, 1, 7$	6	$g_{0,1,7}(x) = x^7 + x^6 + 2x^5 + x^4 + 2x^3 + 2x + 2$	$C_{13}(13) \subset P_3(13)$
$0, 2, 4$	6	$g_{0,2,4}(x) = x^7 + x^5 + x^4 + 1$	$C_{14}(13) \subset P_3(13)$
$0, 2, 7$	6	$g_{0,2,7}(x) = x^7 + 2x^6 + 2x^5 + x^2 + x + 2$	$C_{15}(13) \subset P_3(13)$
$0, 4, 7$	6	$g_{0,4,7}(x) = x^7 + x^6 + x^5 + 2x^4 + x^2 + 2x + 2$	$C_{16}(13) \subset P_3(13)$
$1, 2$	7	$g_{1,2}(x) = x^6 + x^5 + x^2 + 2x + 1$	$C_{17}(13) \subset \mathcal{H}_3(3)$
$1, 4$	7	$g_{1,4}(x) = x^6 + x^5 + 2x^4 + 2x^2 + 2x + 1$	$C_{18}(13) \subset \mathcal{H}_3(3)$
$1, 7$	7	$g_{1,7}(x) = x^6 + 2x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1$	$C_{19}(13) \subset \mathcal{H}_3(3)$
$2, 4$	7	$g_{2,4}(x) = x^6 + 2x^5 + 2x^4 + 2x^3 + x^2 + 2x + 1$	$C_{20}(13) \subset \mathcal{H}_3(3)$
$2, 7$	7	$g_{2,7}(x) = x^6 + 2x^4 + 2x^3 + 2x^2 + 1$	$C_{21}(13) \subset \mathcal{H}_3(3)$

$4,7$	7	$g_{4,7}(x) = x^6 + 2x^5 + 2x^4 + x^3 + x^2 + 2x + 1$	$C_{22}(13) \subset \mathcal{H}_3(3)$
$0,1$	9	$g_{0,1}(x) = x^4 + 2x^3 + 2x^2 + 1$	$C_{23}(13) \subset P_3(13)$
$0,2$	9	$g_{0,2}(x) = x^4 + x + 1$	$C_{24}(13) \subset P_3(13)$
$0,4$	9	$g_{0,4}(x) = x^4 + 2x^2 + 2x + 1$	$C_{25}(13) \subset \mathcal{H}_3(3)$
$0,7$	9	$g_{0,7}(x) = x^4 + x^3 + x$	$C_{26}(13) \subset P_3(13)$
1	10	$g_1(x) = x^3 + 2x + 2$	$C_{27}(13) \simeq \mathcal{H}_3(3)$
2	10	$g_2(x) = x^3 + x^2 + x + 2$	$C_{28}(13) \simeq \mathcal{H}_3(3)$
4	10	$g_4(x) = x^3 + x^2 + 2$	$C_{29}(13) \simeq \mathcal{H}_3(3)$
7	10	$g_7(x) = x^3 + 2x^2 + 2x + 2$	$C_{30}(13) \simeq \mathcal{H}_3(3)$
0	12	$g_0(x) = x - 1$	$C_{31}(13) = P_3(13)$
	13	1	$C_{32}(13) = \mathbb{F}_3^{13}$

9. Codificación y decodificación de códigos cíclicos

Existen dos manera directas de codificar mensajes usando códigos cíclicos, una llamada Codificación No Sistemática y otra conocida como Codificación Sistemática.

Sea $C = \langle\langle g(x)\rangle\rangle$ un $[n, n-k]_q$-código cíclico, con $gr(g(x)) = r$. Entonces, C puede codificar mensajes q-arios de longitud $n - r$ y requiere r símbolos de redundancia.

Definición 3.5. (**Codificación No Sistemática**). Dado un mensaje $a_0, a_1, \ldots, a_{n-r-1}$ en $\mathbb{F}_q^{n-r}$, se forma el polinomio mensaje

$$a(x) = a_0 + a_1 x + \cdots + a_{n-r-1} x^{n-r-1}.$$

Este polinomio se codificará como el producto $c(x) = a(x)g(x) \in C$, es decir

$$a(x) \rightsquigarrow a(x)g(x).$$

Ejemplo 3.12. Consideremos el $[7, 4, 3]_2$-código de Hamming $\mathcal{H}_2(3)$ del ejemplo 4.1 como código cíclico generado por $g(x) = \boldsymbol{x^3 + x + 1}$. Consideremos el mensaje 1010. Usando la codificación no sistemática se formará el polinomio $a(x) = 1 + x^2$ y se codificará como

$$c(x) = a(x)g(x) = (x^2 + 1)(x^3 + x + 1) = x^5 + x^2 + x + 1 \in \mathcal{H}_2(3)$$

es decir,

$$1010 \rightsquigarrow 1110010.$$

Definición 3.6. (**Codificación Sistemática**). Para obtener una codificación sistemática, se formará el polinomio mensaje

$$\overline{a}(x) = a_0 x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-r-1} x^r.$$

Notar que $\overline{a}(x)$ no tiene términos de grado menores que r. Ahora, dividimos $\overline{a}(x)$ por $g(x)$ obteniendo que

$$\overline{a}(x) = q(x)g(x) + r(x), \qquad gr(r(x)) < r$$

y mandamos el código

$$c(x) = \overline{a}(x) - r(x) = q(x)g(x) \in C$$

es decir, se codificará

$$\overline{a}(x) \rightsquigarrow q(x)g(x).$$

Ejemplo 3.13. Consideremos el $[7, 4, 3]_2$-código de Hamming $\mathcal{H}_2(3)$ como un código cíclico generado por $g(x) = \boldsymbol{x^3 + x + 1}$. Consideremos el mensaje 1010. Usando la codificación sistemática, se formará el polinomio

$$\overline{a}(x) = x^6 + x^4$$

y dividimos

$$\overline{a}(x) = (x^3 - 1)(x^3 + x + 1) + (x + 1).$$

Luego, se codificará como

$$c(x) = \overline{a}(x) - r(x) = x^6 + x^4 + x + 1 \in \mathcal{H}_2(3),$$

es decir

$$1010 \rightsquigarrow 1100\underleftarrow{101}.$$

Leyendo esta palabra código 1100101 de atrás para adelante, las primeras 4 coordenadas dan la palabra 1010.

Definición 3.7. (**Decodificación**). Como todo código cíclico es lineal, se podrá decodificar usando decodificación por síndrome pero en su forma polinómica, Si $c(x) \in C$ es el código enviado y $u(x)$ es el polinomio recibido entonces $e(x) = u(x) - c(x)$ se conoce como el polinomio error. El peso de un polinomio es el número de coeficientes no nulos.

Definición 3.8. Sea $C = \langle\langle g(x)\rangle\rangle$ un $[n, n-k]_q$-código cíclico. El síndrome de un polinomio $u(x)$ es el resto de la división $u(x)$ por $g(x)$, es decir

$$u(x) = q(x)g(x) + syn(u(x)), \qquad gr(syn(u(x))) < r$$

en donde $syn(u(x))$ es el síndrome del polinomio $u(x)$.

Un polinomio recibido $u(x)$ es una palabra código si, y sólo si su síndrome es el polinomio nulo. Además, dos polinomios tienen el mismo síndrome si, y sólo si están en la misma coclase de C. Luego, la forma polinómica de decodificación por síndrome es análoga a la forma vectorial.

Ejemplo 3.14. Como el $[7, 4, 3]_2$-código de Hamming $\mathcal{H}_2(3)$ es 1-corrector, entonces es capaz de corregir todos los polinomios error de peso a lo sumo de 1. Luego, los líderes de coclase (potencias de x) y sus síndromes son

Líderes	Síndromes
0	0
1	1
x	x
x^2	x^2
$\boldsymbol{x^3}$	$\boldsymbol{x+1}$
x^4	$x^2 + x$
x^5	$x^2 + x + 1$
x^6	$x^2 + 1$

Si se recibe el polinomio $u(x) = x^6 + x + 1$, calculamos su síndrome

$$x^6 + x + 1 = (x^3 + x + 1)(x^3 + x + 1) + (x^2 + x).$$

Como $syn(u(x)) = x^2 + x$, por la tabla líderes-síndromes anterior vemos que el líder de coclase es $a(x) = x^4$, por lo tanto, se decodifica $u(x)$ como

$$c(x) = u(x) - a(x) = x^6 + x^4 + x + 1 = 1100101 \in \mathcal{H}_2(3).$$

Hasta ahora hemos usado que C es lineal pero no que es cíclico. Vamos a sacar provecho para mejorar el proceso de decodificación. Supongamos que para decodificar, el coeficiente principal de $u(x)$ es x^{n-1}, sin importar si es nulo. Luego, se puede decodificar el coeficiente principal de $u(x)$, realizando un desplazamiento cíclico módulo $x^n - 1$ y después decodificando el nuevo coeficiente

principal de $u(x)$, que será x^{n-2}. Repitiendo este proceso se decodifican todas las palabras código. Este método ahorra tiempo, ya que sólo se necesitan las filas de la tabla con los líderes y los síndromes que contienen los líderes de grado igual que $n-1$.

Ejemplo 3.15. Teniendo en cuenta en ejemplo anterior, como el único líder de peso 1 y grado $n-1=6$ es la palabra x^6, sólo necesitamos la siguiente tabla

Líder	Síndrome
x^6	x^2+1

Si se recibe, al igual que antes, el polinomio $u(x)=x^6+x+1$ y como $syn(u(x))=x^2+x$ no está en la tabla, se asume que el coeficiente de $u(x)$ es correcto. Se realiza un desplazamiento a $u(x)$

$$x(x^6+x+1)\,(mod\ x^7-1)=x^2+x+1$$

y se calcula su síndrome, que es x^2+x+1. Como no está en la tabla se asume que el coeficiente x^5 es correcto. Se realiza, una vez más, un desplazamiento y se calcula su síndrome

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

Obteniendo que el síndrome x^2+1 está en la tabla, por tanto se deduce que el coeficiente de x^4 en $u(x)$ es incorrecto. Continuando este procedimiento, se decodifica $u(x)$ como

$$c(x)=x^6+x^4+x+1\in\mathcal{H}_2(3).$$

Definición 3.9. (**Ceros**). Se conoce como ceros del código a las raíces de polinomio generador de un código cíclico. Sea $T=\bigcup_s C_s$, en donde C_s son las clases q-ciclotómicas módulo n. Las raíces de la unidad $\{\alpha^i : i\in T\}$ son denominadas ceros de un código cíclico C. El conjunto T es llamado conjunto definido de C. Tengamos en cuenta que si se cambia la raíz n-ésima de la unidad, cambia T, por lo que T se calcula en relación con una raíz primitiva fija. La descripción de códigos cíclicos a través de sus ceros permite definir muchas familias de códigos cíclicos importantes, como los códigos BCH y los códigos Reed-Solomon que más adelante se verán.

Ejemplo 3.16. De los ejemplos 3.3 y 3.4 se tiene que las clases 2-ciclotómicas módulo 7 son $C_0=\{0\}$, $C_1=\{1,2,4\}$ y $C_3=\{3,5,6\}$ entonces los ceros del código cíclico binario de longitud $n=7$ son $\{\alpha^i : i\in T=C_0=\{0\}\}=\{1\}$ para el polinomio minimal $M_{\alpha^0}(x)=x+1$; $\{\alpha^i : i\in T=C_1=\{1,2,4\}\}=\{\alpha,\alpha^2,\alpha^4\}$ para el polinomio minimal $M_{\alpha^1}(x)=x^3+x+1$; $\{\alpha^i : i\in T=C_3=\{3,5,6\}\}=\{\alpha^3,\alpha^5,\alpha^6\}$ para el polinomio minimal $M_{\alpha^3}(x)=x^3+x^2+1$; $\{\alpha^i : i\in T=$

$C_1 \cup C_3 = \{1, 2, 4\} \cup \{3, 5, 6\}\} = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ para el polinomio minimal $M_{\alpha^1}(x)M_{\alpha^3}(x) = x^6 + x^5 + x^4 + x^3 + x^2 + 1$.

CAPíTULO 4

Códigos de Hamming y Reed-Muller

1. Códigos de Hamming

DEFINICIÓN 4.1. (**CÓDIGOS DE HAMMING**). Los códigos de Hamming $\mathcal{H}_q(r)$ fueron descubiertos independientemente por Marcel Golay en el año 1949 y por el profesor Richard Wesley Hamming en 1950. Sus parámetros satisfacen la cota de Hamming, por lo tanto los códigos de Hamming $\mathcal{H}_q(r)$ son perfectos y además corrigen 1 error al momento de la transmisión del mensaje. Actualmente, los códigos de Hamming son fundamentales en la teoría de codigos y tienen una gran cantidad de aplicaciones prácticas. En concreto, los códigos correctores de errores tienen un papel esencial en la vida cotidiana y son usados por modems, memorias e incluso en comunicaciones vía satélite.

Presentamos a continuación el caso binario con un ejemplo.

EJEMPLO 4.1. Consideremos el código lineal C con parámetros $[7, 4, d\,]_2$ y la matriz de paridad

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \in \mathbb{M}_{3\times 7}(\mathbb{Z}_2)$$

cuyas columnas son las $2^3 - 1 = 7$ palabras no nulas de $\mathbb{F}_2^3$, escritas en forma ascendente. Podemos calcular su distancia mínima usando el teorema 2.2. Como H tiene 3 columnas linealmente dependientes, entonces su distancia mínima es $d = 3$. Para saber cuales son las $M = 16$ palabras de C, es necesario resolver las ecuaciones de control de paridad determinadas por H. Estas ecuaciones son las siguientes:

$$\begin{cases} x_4 + x_5 + x_6 + x_7 = 0. \\ x_2 + x_3 + x_6 + x_7 = 0. \\ x_1 + x_3 + x_5 + x_7 = 0. \end{cases}$$

Los líderes son $x_1,\ x_2,\ x_4$ y las variables libres son $x_3 = a,\ x_5 = b,\ x_6 = c,\ x_7 = d$ con $a,\ b,\ c,\ d \in \mathbb{Z}_2 = \mathbb{F}_2$. Entonces

$$\begin{cases} x_4 = x_5 + x_6 + x_7 = b + c + d. \\ x_2 = x_3 + x_6 + x_7 = a + c + d. \\ x_1 = x_3 + x_5 + x_7 = a + b + d. \end{cases}$$

De donde,

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix}_{7\times 1} = \begin{pmatrix} a+b+d \\ a+c+d \\ a \\ b+c+d \\ b \\ c \\ d \end{pmatrix}_{7\times 1}$$

Asignandoles valores a las variables libres de la siguiente manera

$$\begin{cases} a = 1,\ b = c = d = 0. \\ b = 1,\ a = c = d = 0. \\ c = 1,\ a = b = d = 0. \\ d = 1,\ a = b = c = 0. \end{cases}$$

Se obtienen las palabras código

$$\begin{cases} c_1 = 1110000. \\ c_2 = 1001100. \\ c_3 = 0101010. \\ c_4 = 1101001. \end{cases}$$

Para finalizar, se harán todas las sumas posibles entre las palabras $c_1,\ c_2,\ c_3,\ c_4$. Resultando

$$\mathcal{H}_2(3) = \begin{Bmatrix} 0111100, & 1011010, & 0011001, & 1100110 \\ 0100101, & 1001011, & 0000000, & 1110000 \\ 1001100, & 0101010, & 1101001, & 1111111 \\ 0010110, & 1010101, & 0110011, & 0001111 \end{Bmatrix}$$

Este es el código de Hamming binario de longitud $n = 7,\ r = 3$ y se denota $\mathcal{H}_2(3)$.

Definición 4.2. La construcción anterior se puede hacer para cualquier $r \geq 2$, es decir, si se forma la matriz H cuyas columnas son las $2^r - 1$ palabras no nulas de $\mathbb{F}_2^r$, se tendrá una matriz $r \times n$ con $n = 2^r - 1$, en donde cualquier par de columnas son linealmente independientes, pero hay 3 columnas linealmente dependientes. Así, H será la matriz de paridad de un código lineal denotado por $\boldsymbol{\mathcal{H}_2(r)}$ con parámetros

$$n = 2^r - 1, \quad k = n - r = 2^r - r - 1, \quad d = 3.$$

es el llamado código de Hamming binario de orden r. De esta manera, se tiene

$$\mathcal{H}_2(r) = \{x \in \mathbb{F}_2^n : xH^\top = 0\}.$$

Ejemplo 4.2. El código de Hamming $\mathcal{H}_2(5)$ tiene parámetros $[31, 26, 3]_2$, luego codificará $M = 2^{26} = 67.108.864$ mensajes y corregirá 1 error.

Teorema 4.1. *Cualquier código binario con los parámetros* $[2^r - 1, 2^r - r - 1, 3]_2$ *es equivalente al código de Hamming* $\mathcal{H}_2(r)$.

Definición 4.3. La matriz $H_{q,r} \in M_{r \times n}(\mathbb{F}_q)$ con $n = \frac{q^r - 1}{q - 1}$ es la matriz de Hamming de orden r y es la matriz de paridad de un código lineal q-ario con parámetros

$$n = \frac{q^r - 1}{q - 1}, \quad k = n - r, \quad d = 3$$

y se conoce como código de Hamming q-ario de orden r, se denota por $\boldsymbol{\mathcal{H}_q(r)}$. Por lo tanto

$$\mathcal{H}_q(r) = \{x \in \mathbb{F}_q^n : xH_{q,r}^\top = 0\}.$$

Observación 26. Los códigos de Hamming $\mathcal{H}_q(r)$ son códigos perfectos, y además son 1-correctores.

Una forma fácil para la construcción de una matriz $H_{q,r}$ es tomando todos los vectores en $\mathbb{F}_q^r$ cuya primera coordenada no nula es 1 (notar que en el caso binario es equivalente a tomar todas las palabras en orden ascendente). En efecto, hay $q^r - 1$ vectores no nulos y el primer elemento no nulo puede ser $1, 2, \ldots, q - 1$. Luego, hay $\frac{q^r - 1}{q - 1}$ vectores cuya primera coordenada no nula comienza con 1.

Ejemplo 4.3. El código $\mathcal{H}_3(2)$ con parámetros $[4, 2, 3]_3$ es auto-dual y tiene matriz de paridad

$$H_{3,2} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}_{2\times 4}$$

Este código también se conoce como tetracódigo y es 1-corrector. Tiene $M = 3^2 = 9$ palabras código, las cuales son

$$\mathcal{H}_3(2) = \{2210,\ 1120,\ 0111,\ 2102,\ 1012,\ 0222,\ 2021,\ 1201,\ 0000\}.$$

Ejemplo 4.4. El código $\mathcal{H}_3(3)$ tiene parámetros $[13, 10, 3]_3$ con matriz de paridad

$$H_{3,3} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}_{3\times 13}$$

Ejemplo 4.5. El código $\mathcal{H}_5(3)$ con parámetros $[31, 28, 3]_5$ con matriz de paridad

$$H_{5,3} = \begin{pmatrix} 0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&1&1&1&1&1&0&0&0&0&0&1&1&1&1&1&2&2&2&2&2&3&3&3&3&3&4&4&4&4&4 \\ 1&0&1&2&3&4&0&1&2&3&4&0&1&2&3&4&0&1&2&3&4&0&1&2&3&4&0&1&2&3&4 \end{pmatrix}_{3\times 31}$$

Observación 27. La elección de las columnas en la construcción previa no es única y por lo tanto habrán muchos códigos de Hamming con los mismos parámetros, Sin embargo, todos los códigos de Hamming de igual tamaño son múltiplo escalar equivalente. Mas aún, todo código que es lineal con parámetros de Hamming será múltiplo escalar equivalente a un código de Hamming.

Teorema 4.2. *Cualquier código C con parámetros $\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3\right]_q$ es equivalente monomial al código de Hamming $\mathcal{H}_q(r)$.*

Observación 28. Hay códigos no lineales con los parámetros de Hamming. Luego, hay códigos perfectos que no son lineales.

La decodificación por síndrome con algunas matrices de Hamming es mejor que con otras. Las matrices descriptas anteriormente, en donde la primera coordenada no nula es igual a 1, son un ejemplo de esto.

VAMOS A DECODIFICAR CÓDIGOS DE HAMMING $\mathcal{H}_q(r)$ CON PARÁMETROS $\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3\right]_q$.

Para el caso binario $\mathcal{H}_2(r)$. Si se comete un error en la transmisión en la i-ésima coordenada, el vector que resulta es e_i. Luego, el síndrome de la palabra recibida es

$$s(e_i) = e_i H^\top.$$

Más aún, el número binario que representa este vector coincide con la posición del error, es decir, i.

Ejemplo 4.6. Sea $\mathcal{H}_2(3)$ el código de Hamming con parámetros $[7, 4, 3]_2$ definido por la matriz H del ejemplo 4.1. Supongamos que se comete un error en la tercera coordenada, es decir, el patrón de error es $e_3 = 0010000$. Luego se halla

$$s(e_3) = e_3 H^\top = (0010000)H^\top = (H_3)^\top = 011.$$

Es decir, el síndrome determinará la coordenada errónea.

Ejemplo 4.7. Sea $\mathcal{H}_2(3)$ el código de Hamming definido por la matriz H del ejemplo 4.1. Si se recibe la palabra $x = 1101011$, se calcula su síndrome, entonces si, $s(x) = \mathbf{0}$ se asume que x fue la palabra enviada, pero ya que $s(x) = 110 \neq \mathbf{0}$, lo que indica que hay un error en la sexta posición, por lo que la decodificación es $c = 1101001 \in \mathcal{H}_2(3)$.

Para el caso general $\mathcal{H}_q(r)$ es muy similar al caso binario. Si se comete un error en la coordenada i, el vector error es de la forma αe_i con $\alpha \in \mathbb{F}_q^*$. Luego, el síndrome es

$$s(e_i) = \alpha e_i H_{q,r}^\top.$$

Ejemplo 4.8. Sea $\mathcal{H}_3(2)$ el código de Hamming con parámetros $[4, 2, 3]_3$ definido por la matriz de paridad $H = H_{3,2}$ del ejemplo 4.3. Si recibimos la palabra $x = 0221$, su síndrome es

$$s(x) = xH^\top = 21 = 2.(12) = 2 \times (\text{columna } 4 \text{ de } H).$$

Por lo tanto, se detecta un error de magnitud 2 en la coordenada 4 de la palabra recibida x. Luego, la palabra x se decodifica como la palabra en el tetracódigo

$$c = x - 2e_4 = 0221 - 0002 = 0222 \in \mathcal{H}_3(2).$$

Ejemplo 4.9. Sea $\mathcal{H}_3(3)$ el código de Hamming con parámetros $[13, 10, 3]_3$ definido por la matriz de paridad $H = H_{3,3}$ del ejemplo 4.4. Si se recibe la palabra $x = 1101112211201$, su síndrome será

$$s(x) = xH^\top = 201 = 2.(102) = 2 \times (\text{columna } 7 \text{ de } H).$$

Por lo tanto, se detecta un error de magnitud 2 en la coordenada 7 de la palabra recibida x. Luego, la palabra x se decodifica como

$$c = x - 2e_7 = 1101112211201 - 0000002000000 = 1101110211201 \in \mathcal{H}_3(3).$$

Teorema 4.3. *Los códigos de Hamming $\mathcal{H}_2(r)$ son equivalentes a códigos cíclicos. En el caso general, el código de Hamming $\mathcal{H}_q(r)$ con parámetros $[n, n-r, 3]_q$ con $n = \frac{q^r-1}{q-1}$ es equivalente a un código cíclico si, y sólo si* $\text{mcd}(n, q-1) = 1$.

Demostración. Para el caso general, sea $\mathcal{H}_q(r)$ equivalente a un código cíclico, si $\gamma \in \mathbb{F}_q$ es una raíz primitiva n-ésima de la unidad y $L = (1^0 \quad \gamma^1 \quad \dots \quad \gamma^{n-1})_{1\times n}$ una matriz, expresando esos elementos como se hizo en la definición 3.9 de los ceros como coordenadas de $\mathbb{F}_{q^r}$ visto como espacio vectorial sobre $\mathbb{F}_q$, $H = (\overline{1^0} \ \overline{\gamma^1} \ \dots \ \overline{\gamma^{n-1}})_{r\times n}$. Note que $\mathbb{F}_q^r$ tiene exactamente n subespacios con dimensión 1, y como ése es precisamente el número de columnas de H, basta ver que tomando dos columnas cualesquiera, éstas son linealmente independiente. Luego, H es matriz de paridad del código de Hamming $\mathcal{H}_q(r)$. Supongamos que $\text{mcd}(n, q-1) = 1 \wedge a\gamma^i = \gamma^j$, con $0 \le i, j < n$. Entonces, $a\gamma^{i-j} = 1$, así que $(a\gamma^{i-j})^{q-1} = 1$. Pero $a \in \mathbb{F}_q$, luego $a^{q-1} = 1$, por lo que $\gamma^{(i-j)(q-1)} = 1$, de donde $n \mid (i-j)(q-1)$, pero $\text{mcd}(n, q-1) = 1$, luego $i = j$.

□

Ejemplo 4.10. Sean $\mathcal{H}_3(2m+1)$, $\mathcal{H}_3(2m)$ códigos ternarios de Hamming con $m \ge 1$, entonces se tiene que

- Los códigos de Hamming $\mathcal{H}_3(2m+1)$ son equivalentes a códigos cíclicos ya que $\text{mcd}(n, q-1) = \text{mcd}(\frac{3^{2m+1}-1}{2}, 2) = 1$.
- Para $\mathcal{H}_3(2m)$ se tiene que $\text{mcd}(n, q-1) = \text{mcd}(\frac{3^{2m}-1}{2}, 2) = 2$, y por lo tanto, no se puede asegurar que sea equivalente a un código cíclico.

Ejemplo 4.11. El código de Hammng $\mathcal{H}_3(2)$ con parámetros $[4, 2, 3]_3$ no es equivalente a ningún código cíclico. Supongamos que $C \subset \mathbb{F}_3^4$, es decir, que C es un ideal de $\frac{\mathbb{F}_3[x]}{x^4-1}$. Sobre $\mathbb{F}_3$ se tiene la

factorización en factores irreducibles

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

Por tanto, se tienen $2^3 = 8$ códigos cíclicos ternarios con longitud $n = 4$ pero sólo hay dos códigos con $k = 2$, estos son

$$C_1 = \langle x^2+1\rangle, \quad C_2 = \langle (x-1)(x+1)\rangle = \langle x^2-1\rangle = \langle x^2+2\rangle.$$

Como $w(x^2+1) = w(1010) = 2$ y $w(x^2+2) = w(2010) = 2$, se tiene que $w(C) \leq 2$, de esta manera se obtiene $w(C) \neq w(\mathcal{H}_3(2))$. Luego, $\mathcal{H}_3(2)$ no será equivalente a un código cíclico, ya que el código de Hamming siempre tiene distancia $d = 3$.

2. Códigos Reed-Muller

Definición 4.4. **Suma directa**. Si C_i con $i \in \{1,2\}$ son códigos con parámetros $(n_i, M_i, d_i)_q$ con $i \in \{1,2\}$, respectivamente. Se define el código

$$C_1C_2 = \{c_1c_2 : c_1 \in C_1, c_2 \in C_2\}$$

con parámetros $(n_1+n_2, M_1M_2, \min\{d_1,d_2\})_q$.

Definición 4.5. Si C_i con $i \in \{1,2\}$ son códigos y tienen matrices generadoras G_i con $i \in \{1,2\}$ y matrices de control de paridad H_i con $i \in \{1,2\}$, respectivamente. Entonces

$$G_1G_2 = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}, \qquad H_1H_2 = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}$$

son las matrices generadoras y de control de paridad de un C_1C_2, respectivamente.

Ejemplo 4.12. Dados los códigos $C_1 = \{00, 10, 01\}$ y $C_2 = \{000, 011, 101, 110\}$ con parámetros $(2,3,1)_2$ y $[3,2,2]_2$, respectivamente, entonces la suma directa es

$$C_1C_2 = \begin{Bmatrix} 00000, & 00011, & 00101, & 00110, & 10000, & 10011, \\ 10101, & 10110, & 01000, & 01011, & 01101, & 01110. \end{Bmatrix}$$

con parámetros $(5, 12, d)_2$ en donde $d = \min\{d_1, d_2\} = 1$. Por tanto, la suma directa se puede interpretar como la yuxtaposición de las palabras código.

Definición 4.6. **La construcción de Plotkin $(u, u+v)$**. Esta es una construcción muy útil y sólo puede realizarse en códigos con la misma longitud y sobre el mismo alfabeto $\mathbb{F}_q$. Si C_i con

$i \in \{1,2\}$ son códigos con parámetros $(n, M_i, d_i)_q$ con $i \in \{1,2\}$, respectivamente. Se define el código

$$C_1 \oplus C_2 = \{c(c+d) : c \in C_1,\ d \in C_2\}$$

con parámetros $(2n, M_1 M_2, \min\{2d_1, d_2\})_q$.

Para códigos lineales, se tienen que dados C_i con $i \in \{1,2\}$ códigos con parámetros $[n, k_i, d_i]_q$ con $i \in \{1,2\}$, respectivamente, entonces la contrucción de Plotkin $C_1 \oplus C_2$ tiene parámetros $[2n, k_1 + k_2, \min\{2d_1, d_2\}]_q$.

Definición 4.7. Si C_i con $i \in \{1,2\}$ tienen matrices generadoras G_i con $i \in \{1,2\}$ y matrices de control de paridad H_i con $i \in \{1,2\}$, respectivamente. Entonces las matrices generadoras y de control de paridad de un $C_1 \oplus C_2$ son, respectivamente

$$G_1 \oplus G_2 = \begin{pmatrix} G_1 & G_1 \\ 0 & G_2 \end{pmatrix}, \qquad H_1 \oplus H_2 = \begin{pmatrix} H_1 & 0 \\ -H_2 & H_2 \end{pmatrix}$$

Ejemplo 4.13. Dados dos códigos con la misma longitud y sobre el mismo alfabeto $C_1 = \{011, 001, 111\}$ con parámetros $(3,3,1)_2$ y $C_2 = \{000, 101\}$ con parámetros $(3,2,2)_2$. El código $(u, u+v)$ es

$$C_1 \oplus C_2 = \{c(c+d) : c \in C_1,\ d \in C_2\}$$

entonces

$$\begin{aligned}
\underbrace{011}_{\in C_1}\left(\underbrace{011}_{\in C_1} + \underbrace{000}_{\in C_2}\right) &= \underbrace{011011}_{\in C_1 \oplus C_2} \\
\underbrace{011}_{\in C_1}\left(\underbrace{011}_{\in C_1} + \underbrace{101}_{\in C_2}\right) &= \underbrace{011110}_{\in C_1 \oplus C_2} \\
\underbrace{001}_{\in C_1}\left(\underbrace{001}_{\in C_1} + \underbrace{101}_{\in C_2}\right) &= \underbrace{001001}_{\in C_1 \oplus C_2} \\
\underbrace{001}_{\in C_1}\left(\underbrace{001}_{\in C_1} + \underbrace{101}_{\in C_2}\right) &= \underbrace{001100}_{\in C_1 \oplus C_2} \\
\underbrace{111}_{\in C_1}\left(\underbrace{111}_{\in C_1} + \underbrace{000}_{\in C_2}\right) &= \underbrace{111111}_{\in C_1 \oplus C_2} \\
\underbrace{111}_{\in C_1}\left(\underbrace{111}_{\in C_1} + \underbrace{101}_{\in C_2}\right) &= \underbrace{111010}_{\in C_1 \oplus C_2}
\end{aligned}$$

Así, la construcción de Plotkin es

$$C_1 \oplus C_2 = \{011011,\ 011110,\ 001001,\ 001100,\ 111111,\ 111010\}$$

con parámetros $(6,6,2)_2$.

Definición 4.8. (**CÓDIGOS REED-MULLER**). Es la familia de los códigos binarios $\mathcal{R}(r,m)$ lineales más usados en la práctica, a pesar de ser uno de los más viejos, conocidos como Reed-Muller, se deben a I. S. Reed y D. E. Muller, el primero en construirlos y explorarlos fue Muller en el año 1954 y en ese mismo año, Reed construyó un algoritmo lógico para su decodificación, (los códigos Reed-Muller no binarios fueron descubiertos independientemente por varias personas como P. Delsarte, J. L Massey, D. J Costello y J. Justensen, entre otros). Aunque su distancia mínima es relativamente pequeña, son de gran importancia práctica debido a la facilidad con las que pueden ser implementados y decodificados. Una de las maneras para construirlo es basada en la construcción de Plotkin.

Para el caso binario, sea m un número entero positivo y r un entero no negativo con $0 \leq r \leq m$. Este es un código binario de longitud 2^m. Para cada longitud m se definen $m+1$ códigos lineales que serán denotados por

$$\mathcal{R}(0,m),\ \mathcal{R}(1,m),\ldots,\ \mathcal{R}(m,m).$$

Estos son los llamados códigos Reed-Muller $\mathcal{R}(r,m)$ de orden r y longitud 2^m.

El código $\mathcal{R}(0,m)$ es el código binario de repetición $Rep_2(2^m) = \{\mathbf{0},\mathbf{1}\}$ y el código $\mathcal{R}(m,m)$ es el espacio vectorial $\mathbb{F}_2^{2^m}$. Para $1 \leq r < m$ definimos

$$\begin{aligned}\mathcal{R}(r,m) &= \{(u,u+v) \in \mathbb{F}_2^{2^m} : u \in \mathcal{R}(r,m-1),\ v \in \mathcal{R}(r-1,m-1)\}\\ &= \mathcal{R}(r,m-1) \oplus \mathcal{R}(r-1,m-1).\end{aligned}$$

Sean $G(0,m) = \{11\ldots1\}$, $G(m,m) = I_{2^m}$. A partir de la descripción anterior, estas son las matrices generadoras para $\mathcal{R}(0,m) = Rep_2(2^m) = \{\mathbf{0},\mathbf{1}\}$ y $\mathcal{R}(m,m) = \mathbb{F}_2^{2^m}$, respectivamente. Para $1 \leq r < m$ usando la definición 4.7, la matriz generadora $G(r,m)$ para el código Reed-Muller $\mathcal{R}(r,m)$ es

$$G(r,m) = G(r,m-1) \oplus G(r-1,m-1) = \begin{pmatrix} G(r,m-1) & G(r,m-1) \\ 0 & G(r-1,m-1) \end{pmatrix}_{k \times 2^n}$$

Ejemplo 4.14. Las matrices generadoras para $\mathcal{R}(r,m)$ con $1 \leq r < m \leq 3$ son

$$G(1,2) = G(1,1) \oplus G(0,1) = \begin{pmatrix} G(1,1) & G(1,1) \\ 0 & G(0,1) \end{pmatrix} = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 \end{array}\right)_{3\times 4}$$

$$G(1,3) = G(1,2) \oplus G(0,2) = \begin{pmatrix} G(1,2) & G(1,2) \\ 0 & G(0,2) \end{pmatrix} = \left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)_{4\times 8}$$

$$G(2,3) = G(2,2) \oplus G(1,2) = \begin{pmatrix} G(2,2) & G(2,2) \\ 0 & G(1,2) \end{pmatrix} = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right)_{7\times 8}$$

A partir de estas matrices se tiene que $\mathcal{R}(1,2)$ y $\mathcal{R}(2,3)$ son el conjuntos de todas las palabras código de peso par en $\mathbb{F}_2^4$ y $\mathbb{F}_2^8$, respectivamente. Además, el código $\mathcal{R}(1,3)$ con parámetros $[8,4,4]_2$ es auto-dual, y coincide con $\hat{\mathcal{H}}_2(3)$. Cabe destacar que las matrices generadoras dadas en el ejemplo 4.14 no son únicas.

Ejemplo 4.15. Veamos los códigos Reed-Muller, $\mathcal{R}(r,m)$ para $m \leq 3$. Los primeros son casos triviales. En efecto, $\mathcal{R}(0,0) = \{\mathbf{0}, \mathbf{1}\}$, $\mathcal{R}(0,1) = \{00, 11\}$ y $\mathcal{R}(1,1) = \{00, 01, 10, 11\}$. Además, se tienen $\mathcal{R}(0,2) = \{0000, 1111\}$ y $\mathcal{R}(2,2) = \mathbb{F}_2^4$. Para el primer caso no trivial se tiene el código Reed-Muller $\mathcal{R}(r,m)$ con $r = 1, m = 2$. Por la definición 4.6 se tiene

$$\mathcal{R}(1,2) = \{(u, u+v) \in \mathbb{F}_2^4 : u \in \mathcal{R}(1,1),\ v \in \mathcal{R}(0,1)\} = \mathcal{R}(1,1) \oplus \mathcal{R}(0,1).$$

Obteniendo las palabras código

$$(00, 00+00),\ \ (01, 01+00),\ \ (10, 10+00),\ \ (11, 11+00)$$

$$(00, 00+11),\ \ (01, 01+11),\ \ (10, 10+11),\ \ (11, 11+11)$$

y por tanto se tiene

$$\mathcal{R}(1,2) = \{0000,\ 0011,\ 0101,\ 0110,\ 1010,\ 1001,\ 1111,\ 1100\} = E(4).$$

Para el caso con $m = 3$, además de los triviales $\mathcal{R}(0,3) = Rep_2(8)$, $\mathcal{R}(3,3) = \mathbb{F}_2^8$ se tienen

$$\mathcal{R}(1,3) = \mathcal{R}(1,2) \oplus \mathcal{R}(0,2).$$

$$\mathcal{R}(2,3) = \mathcal{R}(2,2) \oplus \mathcal{R}(1,2).$$

Observación 29. El código $\mathcal{R}(1,3)$ se construye usando la construcción de Plotkin y aparece reseñado en la observación 30, la parte (4a). Cabe resaltar que si se hubiesen usado sus matrices generadoras para construirlos, estos códigos hubiesen sido equivalentes.

Una de las mayores ventajas de estos códigos es que sus parámetros (longitud, dimensión, peso) y sus códigos duales se calculan mediante fórmulas.

Teorema 4.4. *Sea r un entero tal que $0 \leq r \leq m$. Entonces*

(1) *Si $0 \leq i \leq j \leq m$ entonces $\mathcal{R}(i,m) \subseteq \mathcal{R}(j,m)$, es decir,*

$$\mathcal{R}(0,m) \subset \mathcal{R}(1,m) \subset \cdots \subset \mathcal{R}(r-1,m) \subset \mathcal{R}(r,m).$$

(2) *El código $\mathcal{R}(r,m)$ es binario con longitud $n = 2^m$.*

(3) *La dimensión de $\mathcal{R}(r,m)$ es*

$$\sum_{i=0}^{r} \binom{m}{i} = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r}.$$

(4) *El peso mínimo $w(\mathcal{R}(r,m))$ es 2^{m-r}.*

(5) *$\mathcal{R}(m-1,m) = E(2^m)$. Luego, si $r < m$ se tiene que $\mathcal{R}(r,m)$ contiene sólo las palabras código de peso par.*

(6) *Todas las palabras código en $\mathcal{R}(1,m)$ tienen peso 2^{m-1} salvo $\mathbf{0}$ y $\mathbf{1}$.*

(7) *$\mathcal{R}^{\perp}(m,m) = \{\mathbf{0}\}$ y si $0 \leq r < m$ entonces $\mathcal{R}^{\perp}(r,m) = \mathcal{R}(m-r-1,m)$.*

Demostración.

(1) Se cumple para $m = 1$ ya que $\mathcal{R}(0,1) = \{00, 11\} \subset \{00, 01, 10, 11\} = \mathcal{R}(1,1)$ y si $j = m$ entonces $\mathcal{R}(m,m) = \mathbb{F}_2^{2^m}$. Se asume inductivamente que los códigos $\mathcal{R}(k, m-1) \subseteq \mathcal{R}(l, m-1)$ con $0 \leq k \leq l < m$. Sea $0 < i \leq j < m$. Entonces

$$\begin{aligned}
\mathcal{R}(i,m) &= \{(u, u+v) \in \mathbb{F}_2^{2^m} : u \in \mathcal{R}(i, m-1),\ v \in \mathcal{R}(i-1, m-1)\} \\
&\subseteq \{(u, u+v) \in \mathbb{F}_2^{2^m} : u \in \mathcal{R}(j, m-1),\ v \in \mathcal{R}(j-1, m-1)\} \\
&= \mathcal{R}(j,m).
\end{aligned}$$

Así, (1) sigue por inducción cuando $i > 0$. Si $i = 1$, sólo necesitamos ver que todo vector $\mathbf{1}$ de longitud 2^m está en $\mathcal{R}(j, m)$ con $j < m$. Por inducción, se asume que toda palabra $\mathbf{1}$ de longitud 2^{m-1} está en $\mathcal{R}(j, m-1)$. Entonces, por la definición de códigos Reed-Muller, vemos que toda $\mathbf{1} \in \mathbb{F}^{2^m}$ está en $\mathcal{R}(j, m)$ donde una opción para $\mathbf{u}$ es $\mathbf{1}$ y una opción para $\mathbf{v}$ es $\mathbf{0}$.

(2) La suma de los m números combinatorios es 2^m, es decir, $\sum_{i=0}^{m} \binom{m}{i} = 2^m$.

(3) Se cumple para $r = m$, ya que $\mathcal{R}(m, m) = \mathbb{F}_2^{2^m}$ y

$$\sum_{i=0}^{m} \binom{m}{i} = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{m} = 2^m.$$

También se cumple para $m = 1, r \neq 0$ ya que $\mathcal{R}(1, 1) = \mathbb{F}_2^2 = \{00, 01, 10, 11\}$ y

$$\sum_{i=0}^{1} \binom{1}{i} = \binom{1}{0} + \binom{1}{1} = 2.$$

Ahora se asume que $\mathcal{R}(i, m-1)$ tiene dimensión

$$\sum_{j=0}^{i} \binom{m-1}{j} = \binom{m-1}{0} + \binom{m-1}{1} + \cdots + \binom{m-1}{i}, \ \forall\, i \in \{0, 1, \ldots, m\}.$$

Por la construcción de Plotkin para códigos lineales se tiene que la dimensión de $\mathcal{R}(r, m) = \mathcal{R}(r, m-1) \oplus \mathcal{R}(r-1, m-1)$ es la suma de las dimensiones de $\mathcal{R}(r, m-1)$ y $\mathcal{R}(r-1, m-1)$, es decir, $\sum_{i=0}^{r} \binom{m-1}{i} + \sum_{i=0}^{r-1} \binom{m-1}{i}$

$$= \binom{m-1}{0} + \binom{m-1}{1} + \cdots + \binom{m-1}{r} + \binom{m-1}{0} + \binom{m-1}{1} + \cdots + \binom{m-1}{r-1}.$$

Usando las propiedades de la combinatoria $\binom{m-1}{0} = \binom{m}{0}$, $\binom{m-1}{i-1} + \binom{m-1}{i} = \binom{m}{i}$ se tiene

$$\sum_{i=0}^{r} \binom{m-1}{i} + \sum_{i=0}^{r-1} \binom{m-1}{i} = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r} = \sum_{i=0}^{r} \binom{m}{i}.$$

(4) Se cumple para $m = 1, \ r \neq 0$, ya que $\mathcal{R}(1, 1) = \{00, 01, 10, 11\}$ y

$$w(\mathcal{R}(1, 1)) = 2^{1-1} = 1$$

también para $r = 0$ se tiene que $w(\mathcal{R}(0, m)) = w(Rep_q(2^m)) = 2^m$ y de igual modo para $r = m$ se tiene $w(\mathcal{R}(m, m)) = w(\mathbb{F}_2^{2^m}) = 1$. Se asume que $\mathcal{R}(i, m-1)$ tiene peso mínimo $2^{m-1-i}, \forall i \in \{1, 2, \ldots, m\}$. Si $0 < r < m$ y por la construcción de Plotkin para códigos lineales se tiene que el peso de $\mathcal{R}(r, m) = \mathcal{R}(r, m-1) \oplus \mathcal{R}(r-1, m-1)$ es igual al $\min\{2.2^{m-1-r}, 2^{m-1-(r-1)}\} = 2^{m-r}$.

(5) Ya que cada monomio de grado menor a m tiene peso par y ya que ellos abarcan $\mathcal{R}(m-1,m)$, sigue que todas las palabras en $\mathcal{R}(m-1,m)$ tienen peso par. La dimensión es $\sum_{i=0}^{m-1}\binom{m}{i} = 2^m - 1 = n-1$. Se concluye que $\mathcal{R}(m-1,m) = E(2^m)$.

(6) Tomando $r = 1$ en el apartado (4) se tiene que $w(\mathcal{R}(1,m)) = 2^{m-1}$. Las palabras $\mathbf{0}$ y $\mathbf{1}$ tienen peso 0 y 2^m respectivamente.

(7) Se tiene que $\mathcal{R}^{\perp}(m,m)$ es $\{\mathbf{0}\}$, ya que $\mathcal{R}(m,m) = \mathbb{F}_2^{2^m}$. Si definimos $\mathcal{R}(-1,m) = \{\mathbf{0}\}$ entonces $\mathcal{R}^{\perp}(-1,m) = \mathcal{R}(m-(-1)-1,m), \forall m > 0$. Por cálculo directo, $\mathcal{R}^{\perp}(r,m) = \mathcal{R}(m-r-1,m), \forall r$ con $-1 \leq r \leq m = 1$. Se asume por inducción que si $-1 \leq i \leq m-1$, entonces $\mathcal{R}^{\perp}(i,m-1) = \mathcal{R}((m-1)-i-1,m-1)$. Sea $0 \leq r < m$. Para probar que $\mathcal{R}^{\perp}(r,m) = \mathcal{R}(m-r-1,m)$ es suficiente ver que $\mathcal{R}(m-r-1,m) \subseteq \mathcal{R}^{\perp}(r,m)$ ya que $\dim(\mathcal{R}(r,m)) + \dim(\mathcal{R}(m-r-1,m)) = 2^m$ por la parte (3). Note que con la definición de $\mathcal{R}(-1,m)$, se extiende al caso $r = 0$. Sea $x = (a, a+b) \in \mathcal{R}(m-r-1,m)$ donde $a \in \mathcal{R}(m-r-1,m-1)$ y $b \in \mathcal{R}(m-r-2,m-1)$ y sea $y = (u, u+v) \in \mathcal{R}(r,m)$ donde $u \in \mathcal{R}(r,m-1)$ y $v \in \mathcal{R}(r-1,m-1)$. Entonces $x \cdot y = 2a \cdot u + a \cdot v + b \cdot u + b \cdot v = a \cdot v + b \cdot u + b \cdot v$. Cada término es 0, ya que $a \in \mathcal{R}(m-r-1,m-1) = \mathcal{R}^{\perp}(r-1,m-1)$, $a \cdot v = 0$ y $b \in \mathcal{R}(m-r-2,m-1) = \mathcal{R}^{\perp}(r,m-1)$, $b \cdot u = 0$ y $b \cdot v = 0$ usando la parte (1) se tiene $\mathcal{R}(r-1,m-1) \subseteq \mathcal{R}(r,m-1)$. Concluyendo que $\mathcal{R}(m-r-1,m) \subseteq \mathcal{R}^{\perp}(r,m)$ se completa (7).

□

VAMOS A DECODIFICAR EL CÓDIGO REED-MULLER $\mathcal{R}(1,3)$ CON PARÁMETROS $[8,4,4]_2$.

El código $\mathcal{R}(1,3)$ es 1-corrector con parámetros $[8,4,4]_2$ es auto-dual, por lo que la matriz generadora dada en el ejemplo 4.14 es su matriz de paridad, entonces

$$G(1,3) = H(1,3) = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}_{4\times 8}$$

Supongamos que se recibe la palabra $x = 00110001$, se calcula su síndrome $s(x) = 1011$. Por lo tanto, se detecta que hay un error en la séptima coordenada de la palabra recibida x. Luego, la palabra x es decodificada como $c = 00110011$.

3. Estudio comparativo

Observación 30.

ANALIZANDO VARIOS CÓDIGOS REED-MULLER Y HAMMING.

En los códigos Reed-Muller $\mathcal{R}(r, m)$ binarios se cumple que

(1) Para $r = 0$, $m = 0, 1, 2, 3, \ldots$ se tienen
   (a) $\mathcal{R}(0, 0) = \{0, 1\} = Rep_2(1) = \mathbb{Z}_2$ con parámetros $[1, 1, 1]_2$, $M = 2$.
   (b) $\mathcal{R}(0, 1) = \{00, 11\} = Rep_2(2)$ con parámetros $[2, 1, 2]_2$, $M = 2$.
   (c) $\mathcal{R}(0, 2) = \{0000, 1111\} = Rep_2(4)$ con parámetros $[4, 1, 4]_2$, $M = 2$.
   (d) $\mathcal{R}(0, 3) = \{00000000, 11111111\} = Rep_2(8)$ con parámetros $[8, 1, 8]_2$, $M = 2$.
   $\vdots$
   (e) $\mathcal{R}(0, m) = \{00\ldots0, 11\ldots1\} = Rep_2(2^m)$ con parámetros $[2^m, 1, 2^m]_2$, $M = 2$.

(2) Para $r = m = 1, 2, 3, \ldots$ se tienen
   (a) $\mathcal{R}(1, 1) = \{00, 01, 10, 11\} = \mathbb{Z}_2^2$ con parámetros $[2, 2, 1]_2$, $M = 4$.
   (b) $\mathcal{R}(2, 2) = \mathbb{Z}_2^4$ con parámetros $[4, 4, 1]_2$, $M = 16$.
   (c) $\mathcal{R}(3, 3) = \mathbb{Z}_2^8$ con parámetros $[8, 8, 1]_2$, $M = 256$.
   $\vdots$
   (d) $\mathcal{R}(m, m) = \mathbb{Z}_2^{2^m}$ con parámetros $[2^m, 2^m, 1]_2$, $M = 2^{2^m}$.

(3) Para $r = 1$, $m = 2$ se tiene
   (a) $\mathcal{R}(1, 2) = E(2^2) = E(4)$ con parámetros $[4, 3, 2]_2$, $M = 8$.

(4) Para $r = 1$, $m = 3$ se tiene
   (a) $\mathcal{R}(1, 3) = \mathcal{R}(1, 2) \oplus \mathcal{R}(0, 2) = E(4) \oplus Rep_2(4)$ con parámetros $[8, 4, 4]_2$, $M = 16$. Por la construcción de Plotkin se tiene

$$\mathcal{R}(1,3) = \left\{ \begin{array}{cccc} 00000000, & 00001111, & 11001100, & 11000011 \\ 00110011, & 00111100, & 01100110, & 01101001 \\ 10101010, & 10100101, & 01010101, & 01011010 \\ 10011001, & 10010110, & 11111111, & 11110000 \end{array} \right\}$$

   en donde, este código sólo contiene palabras de peso par.

(5) Para $r = 2$, $m = 3$ se tiene
   (a) $\mathcal{R}(2, 3) = \mathcal{R}(2, 2) \oplus \mathcal{R}(1, 2) = \mathbb{Z}_2^4 \oplus E(4)$ con parámetros $[8, 7, 2]_2$, $M = 128$.

De lo anterior se puede concluir que

- $\mathcal{R}(0,1) = Rep_2(2) = \{00, 11\} \subset \{00, 01, 10, 11\} = \mathbb{Z}_2^2 = \mathcal{R}(1,1)$.
- $\mathcal{R}(0,2) = Rep_2(4) \subset \mathcal{R}(1,2) = E(4) \subset \mathbb{Z}_2^4 = \mathcal{R}(2,2)$.
- $\mathcal{R}(0,3) = Rep_2(8) \subset \mathcal{R}(1,3) \subset \mathcal{R}(2,3) = E(8) \subset \mathbb{Z}_2^8 = \mathcal{R}(3,3)$.

En los códigos cíclicos de Hamming binarios $\mathcal{H}_2(r)$ se tienen

(1) Para $r = 2$ se tiene $\mathcal{H}_2(2)$ con parámetros $[3, 1, 3]_2$ con $M = 2$ y tiene polinomio generador $g(x) = x^2 + x + 1$.
(2) Para $r = 3$ se tiene $\mathcal{H}_2(3)$ con parámetros $[7, 4, 3]_2$ con $M = 16$, tiene polinomio generador $g(x) = x^3 + x + 1$.
(3) Para $r = 4$ se tiene $\mathcal{H}_2(4)$ con parámetros $[15, 11, 3]_2$ con $M = 2.048$ y tiene polinomio generador $g(x) = x^4 + x + 1$.
(4) Para $r = 5$ se tiene $\mathcal{H}_2(5)$ con parámetros $[31, 26, 3]_2$ con $M = 67.108.864$ y tiene polinomio generador $g(x) = x^5 + x^2 + 1$.
(5) Para $r = 6$ se tiene $\mathcal{H}_2(6)$ con parámetros $[63, 57, 3]_2$ con $M = 2^{57}$ y tiene polinomio generador $g(x) = x^6 + x + 1$.

En los códigos de Hamming $\mathcal{H}_q(r)$ se tienen

(1) Para $q = 3$, $r = 2$ se tiene $\mathcal{H}_3(2)$ con parámetros $[4, 2, 3]_3$ con $M = 9$, no es cíclico.
(2) Para $q = 3$, $r = 3$ se tiene $\mathcal{H}_3(3)$ con parámetros $[13, 10, 3]_3$ con $M = 59.049$, si es cíclico y tiene polinomio generador $g(x) = x^3 + x^2 + 2$.
(3) Para $q = 3$, $r = 4$ se tiene $\mathcal{H}_3(4)$ con parámetros $[40, 36, 3]_3$ con $M = 3^{36}$, no es cíclico.
(4) Para $q = 4$, $r = 2$ se tiene $\mathcal{H}_4(2)$ con parámetros $[5, 3, 3]_4$ con $M = 64$, si es cíclico.
(5) Para $q = 4$, $r = 3$ se tiene $\mathcal{H}_4(3)$ con parámetros $[21, 18, 3]_4$ con $M = 4^{18}$, no es cíclico.
(6) Para $q = 5$, $r = 2$ se tiene $\mathcal{H}_5(2)$ con parámetros $[6, 4, 3]_5$ con $M = 625$, no es cíclico.
(7) Para $q = 5$, $r = 3$ se tiene $\mathcal{H}_5(3)$ con parámetros $[31, 28, 3]_5$ con $M = 5^{28}$, si es cíclico.
(8) Para $q = 6$, $r = 2$ se tiene $\mathcal{H}_6(2)$ con parámetros $[7, 5, 3]_6$ con $M = 7.776$, si es cíclico.
(9) Para $q = 6$, $r = 3$ se tiene $\mathcal{H}_6(3)$ con parámetros $[43, 40, 3]_6$ con $M = 6^{40}$, si es cíclico.

Si tenemos el polinomio generador $g(x)$, se tiene la matriz generadora G. Si G es equivalente por filas a la matriz estándar G' entonces se puede encontrar la matriz de paridad H, sino, se encuentra el polinomio de chequeo $h(x)$, usando el polinomio generador $g(x)$. Si tenemos el polinomio de chequeo $h(x)$, se puede hallar la matriz de paridad. Con

el polinomio generador $g(x)$ y su recíproco $g^*(x)$ se pueden estudiar las equivalencias entre códigos.

De todo lo visto se tiene

- Ya que $\mathcal{R}(0,m)$ es el código binario de repetición con longitud 2^m, entonces el código $\mathcal{R}(m-1,m) = \mathcal{R}^{\perp}(0,m)$ es el código de todos los vectores de peso par en $\mathbb{F}_2^{2^m}$. Los códigos $\mathcal{R}(1,2)$ y $\mathcal{R}(2,3)$ son ejemplos de esto.
- Si $m = 2r+1$, usando los apartados (4) y (7) del teorema anterior se obtiene que $\mathcal{R}(r,m) = \mathcal{R}(\frac{m-1}{2},m)$ es auto-dual con peso mínimo $2^{\frac{m-1}{2}}$. El código $\mathcal{R}(1,3)$ con parámetros $[8,4,4]_2$, que aparece reseñado en la parte (4a) es auto-dual.
- Pinchando el código $\mathcal{R}(1,m)$ con longitud 2^m y luego tomando el subcódigo de todas las palabras de peso par, se produce el llamado código Simplex $\boldsymbol{\mathcal{S}_m}$ con longitud $2^m - 1$. En general, el código simplex, es el dual de $\mathcal{H}_q(r)$, $r \geq 2$ y tiene parámetros $[\frac{q^r-1}{q-1}, r, q^{r-1}]_q$. El código Simplex $\mathcal{H}_2^{\perp}(3)$ con parámetros $[7,3,4]_2$ tiene sólo palabras de peso constante $w = 4$. Ya que el tetracódigo $\mathcal{H}_3(2)$ con parámetros $[4,2,3]_3$ es auto-dual, también es un código Simplex y sus palabras no nulas tienen todas peso constante $w = 3$.
- Dado el código $\mathcal{R}(r,m)$ con $0 \leq r < m$, el código pinchado $\mathcal{R}^*(r,m)$ es el código obtenido de $\mathcal{R}(r,m)$ suprimiendo la posición coordenada que corresponde al 0. Dado el código auto-dual $\mathcal{R}(1,3)$ con parámetros $[8,4,4]_2$, el código pinchado $\mathcal{R}^*(1,3)$ tiene los parámetros $[7,4,3]_2$ y es lineal, además de tener los mismos parámetros del código de Hamming $\mathcal{H}_2(3)$. Luego, $\mathcal{R}^*(1,3) \simeq \mathcal{H}_2(3)$ por el teorema 4.1.
- Dado el código de Hamming $\mathcal{H}_2(3)$, el código de Hamming extendido $\hat{\mathcal{H}}_2(3)$ es equivalente a $\mathcal{R}(1,3)$ y tiene matriz extendida de paridad dada en la definición 1.22, es decir

$$\hat{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}_{4\times 8}$$

- Dado el código de Hamming $\mathcal{H}_2(m)$, el código de Hamming extendido $\hat{\mathcal{H}}_2(m)$, (usando la definición 1.11) es equivalente a $\mathcal{R}(m-2,m)$ con matriz extendida de paridad dada en la definición 1.22 de código extendido.

4. Algunas aplicaciones importantes

Observación 31.

- Los códigos de Hamming son utilizados para corregir errores en los bits almacenados en las memorias RAM (Random-Access Memory) dinámicas insertadas dentro de circuitos integrados y en comunicaciones en las redes de Wifi.
- Entre los años 1969 y 1972, las sondas Mariner 6, 7 y 9 enviaron fotografías del planeta Marte. En enero de 1972, la sonda Mariner 9 tomó fotografías en blanco y negro de Marte, esta vez de $600 \times 600 = 360.000$ pixeles. Se utilizó el código binario Reed-Muller $\mathcal{R}(1,5)$ con parámetros $[32,6,16]_2$ con $M = 2^6 = 64$ palabras código. Este es un código tiene distancia $d = 2t + s + 1 = 2.7 + 1 + 1$ entonces por el teorema 1.7 se tiene que $\mathcal{R}(1,5)$ es simultáneamente 8-detector y 7-corrector, con una tasa de información $Tasa(\mathcal{R}(1,5)) = \frac{3}{16}$. A cada pixel se le asignó una 6-cadena representando el brillo. Ahora, cada pixel fue codificado como una palabra con longitud $n = 32$ con $n - k = 32 - 6 = 26$ bits de redundancia. La tasa de transmisión fue aumentada de $8\frac{1}{3}$ a 16.200 bits por segundo. Sin embargo, las cámaras tomaban imágenes a razón de más de 100.000 bits por segundo, por lo que los datos debieron ser almacenados en cintas magnéticas antes de la transmisión. Recordemos que un bit es una señal electrónica que puede estar encendida (1) o apagada (0), es la unidad más pequeña de información que utiliza un ordenador. Son necesarios 8 bits para crear un byte. La mayoría de las veces los bits se utilizan para describir velocidades de transmisión, mientras que los bytes se usan para describir capacidad de almacenamiento o memoria. El término bit proviene de la frase en inglés binary digit.

CAPíTULO 5

Códigos *BCH* y Reed-Solomon

Anteriormente se vió que los códigos de Hamming son 1-correctores. Existen códigos que en cierta manera son generalizaciones de éstos y que corrigen t errores durante el transcurso de la transmisión, para un entero t dado. Estos son conocidos como códigos BCH, en el caso binario los descubrió A. Hocquenghem en 1959 y luego fueron descubiertos independientemente del primero por R. C. Bose y D. K. Ray-Chaudhuri en 1960. La generalización para un código q-ario fue realizada por D. C. Gorenstein y N. Zierler. Los códigos Reed-Solomon son un caso particular de los BCH y fueron descubiertos por I. S. Reed y G. Solomon y son usados para mejorar la seguridad en los discos compactos, cintas de audio digitales y otros sistemas para el almacenamiento de datos.

1. Códigos *BCH*

Definición 5.1. Los códigos BCH son códigos cíclicos diseñados para aprovechar la Cota de BCH. Construiremos un código cíclico con un peso mínimo w y dimensión k simultáneamente grandes. Un gran peso mínimo, que puede lograrse (por la Cota de BCH) mediante la selección del conjunto definido T de C con un gran número de elementos consecutivos. La dimensión de C es $n - |T|$, se quiere que $|T|$ sea lo más pequeño posible. Por lo que si queremos que C tenga distancia mínima mayor o igual que δ, se selecciona el conjunto definido T lo más pequeño posible que es una unión de las clases q-ciclotómicas con $\delta - 1$ elementos consecutivos.

Sea δ un número entero tal que $2 \leq \delta \leq n$. Un código BCH, $C \subset \mathbb{F}_q^n$ con longitud n y distancia diseñada δ es un código cíclico con el conjunto definido

$$T = C_b \cup C_{b+1} \cup \cdots \cup C_{b+\delta-2}$$

en donde cada C_i es la clase q-ciclotómica módulo n que contiene i. Por la cota de BCH este código tiene distancia mínima de por lo menos δ, es decir, $d \geq \delta$.

Teorema 5.1. (**La Cota de** BCH) *Si C es un código cíclico de longitud n y con distancia mínima d sobre $\mathbb{F}_q$ con el conjunto definido T. Suponemos que T contiene $\delta - 1$ elementos consecutivos para algún entero δ. Entonces $d \geq \delta$.*

Teorema 5.2. *Los códigos BCH con distancia diseñada δ tienen peso mínimo de por lo menos δ, es decir, $w(C) \geq \delta$.*

Cuando el valor de b varia, se producen códigos con posibilidades distintas de distancias mínimas y dimensiones. Para el caso $b = 1$ se tiene el código *BCH* narrow-sense. Si $n = q^t - 1$ se tiene el código *BCH* primitivo. Si $t = 1$ en el caso de *BCH* primitivo se tiene el código Reed-Solomon.

Teorema 5.3. *Para $i \in \{1, 2\}$, sean C_i códigos BCH sobre $\mathbb{F}_q$ con el conjunto definido $T_i = C_b \cup C_{b+1} \cup \cdots \cup C_{b+\delta_i-2}$ con $\delta_1 < \delta_2$. Entonces $C_2 \subseteq C_1$.*

A continuación, se construyen varios códigos *BCH* sobre $\mathbb{F}_3$ de longitud $n = 13$.

Ejemplo 5.1. Las clases 3-ciclotómicas (*mod* 13) son

$$C_0 = \{0\},\ C_1 = \{1, 3, 9\},\ C_2 = \{2, 5, 6\},\ C_4 = \{4, 10, 12\},\ C_7 = \{7, 8, 11\}.$$

Como $ord_{13}(3) = 3$ entonces el factor $x^{13} - 1$ tiene raíces en $\mathbb{F}_{3^3}$. Sea $\alpha \in \mathbb{F}_{3^3}$ un elemento primitivo que satisface $\alpha^3 + 2\alpha + 2 = 0$. Entonces, por observación 21, se tiene que $\beta = \alpha^{\frac{3^3-1}{13}} = \alpha^2$ es una raíz primitiva 13-ésima de la unidad en $\mathbb{F}_{3^3}$. Usando β, se tiene el código *BCH* narrow-sense C_1 de distancia diseñada $\delta = 2$ que tiene conjunto definido $T = C_1 = \{1, 3, 9\}$ con $\delta - 1 = 1$ elemento y polinomio generador $g_1(x) = x^3+x^2+x+2$. Por el teorema 5.2, la distancia mínima es igual o mayor que $\delta = 2$. Sin embargo, $C_1\mu_2$, que es equivalente a C_1, es un código *BCH* (non-narrow-sense) con conjunto definido $2^{-1}C_1 = C_7 = C_8$. Este código tiene distancia diseñada 3 y polinomio generador $g_7(x) = x^3 + 2x + 2$. Así, C_1 es un código *BCH* con parámetros $[13, 10, 3]_3$. El subcódigo even-like $C_{1,e} \subset C_1$ es *BCH*, tiene el conjunto definido $C_0 \cup C_1$ con $\delta - 1 = 2$ elementos consecutivos con distancia diseñada $\delta = 3$ y distancia mínima $d = 3$ ya que $(x-1)g_1(x) = x^4 + x + 1$ es even-like con peso 3. El subcódigo $C_{1,e}$ tiene polinomio generador $g_{1,e}(x) = x^4 + 2x^3 + 2x^2 + 1$, entonces $C_{1,e}$ es un $[13, 9, 3]_3$-código. Note que el subcódigo even-like de $C_1\mu_2$ es equivalente a $C_{1,e}$ pero no es *BCH*. (La función μ_a con $a \in \mathbb{Z}^+$ tal que $\text{mcd}(a, n) = 1$ definida en $\{0, 1, \ldots, n-1\}$ por $i\mu_a \equiv ia(mod\ n)$ es una permutación de las posiciones $\{0, 1, \ldots, n-1\}$ en las coordenadas de un código cíclico con longitud n).

Ejemplo 5.2. El código *BCH* narrow-sense C_2 con distancia diseñada $\delta = 3$ tiene conjunto definido $C_1 \cup C_2$ con $\delta - 1 = 2$ elementos consecutivos, (como el conjunto definido también es igual

a $C_1 \cup C_2 \cup C_3$ con $\delta - 1 = 3$ elementos consecutivos, entonces, el código C_2 también tiene distancia diseñada $\delta = 4$), el código C_2 tiene polinomio generador $g_{1,2}(x) = x^6 + 2x^5 + 2x^4 + 2x^3 + x^2 + 2x + 1$ y $(x+1)g_{1,2}(x) = x^7 + x^5 + x^4 + 1$ tiene peso 4. Así, el código *BCH* narrow-sense C_2 tiene parámetros $[13, 7, 4]_3$.

Ejemplo 5.3. Finalmente, el código *BCH* narrow-sense C_3 con distancia diseñada $\delta = 5$ tiene conjunto definido $C_1 \cup C_2 \cup C_3 \cup C_4$ con $\delta - 1 = 4$ elementos consecutivos, (este código también es un código *BCH* narrow-sense con distancia diseñada $\delta = 7$ que tiene el conjunto definido $C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6$ con $\delta - 1 = 6$ elementos consecutivos), el código C_3 tiene polinomio generador $g_{1,2,4}(x) = x^9 + x^8 + 2x^7 + x^5 + 2x^3 + 2x^2 + 2$ y peso 7, por lo tanto C_3 es un código *BCH* con parámetros $[13, 4, 7]_3$.

Observación 32. En los códigos *BCH* vistos en los tres ejemplos anteriores se cumple que los códigos $C_3 \subset C_2 \subset C_1$, por el teorema 5.3.

A continuación, se construyen varios códigos *BCH* sobre $\mathbb{F}_2$ con longitud $n = 31$ mediante sus ceros.

Ejemplo 5.4. Como $n = 2^5 - 1 = 31$, entonces todos los códigos descriptos en este ejemplo son *BCH* primitivos. Se escriben las clases 2-ciclotómicas módulo 31 con sus polinomios minimales asociados en el siguiente cuadro:

s	C_s	$M_{\alpha^s}(x)$
0	$\{0\}$	$x + 1$
1	$\{1, 2, 4, 8, 16\}$	$x^5 + x^2 + 1$
3	$\{3, 6, 12, 17, 24\}$	$x^5 + x^4 + x^3 + x^2 + 1$
5	$\{5, 9, 10, 18, 20\}$	$x^5 + x^4 + x^2 + x + 1$
7	$\{7, 14, 19, 25, 28\}$	$x^5 + x^3 + x^2 + x + 1$
11	$\{11, 13, 21, 22, 26\}$	$x^5 + x^4 + x^3 + x^2 + x + 1$
15	$\{15, 23, 27, 29, 30\}$	$x^5 + x^3 + 1$

El polinomio generador $M_\alpha(x)M_{\alpha^3}(x)$, con ceros en $\{\alpha^i : i \in C_1 \cup C_3\}$, genera el código *BCH* con parámetros $[31, 21, 5]_2$ y distancia diseñada $\delta = 5$. Si se toma el polinomio $M_\alpha(x)M_{\alpha^3}(x)M_{\alpha^5}(x)$, con ceros en $\{\alpha^i : i \in C_1 \cup C_3 \cup C_5\}$ se genera un código *BCH* con parámetros $[31, 16, 7]_2$ y distancia diseñada $\delta = 7$. Si el polinomio generador es $M_\alpha(x)M_{\alpha^3}(x)M_{\alpha^5}(x)M_{\alpha^7}(x)$ con ceros en

$\{\alpha^i : i \in C_1 \cup C_3 \cup C_5 \cup C_7\}$, entonces genera un código *BCH* con parámetros $[31, 11, 11]_2$ y distancia diseñada $\delta = 9$ ó 11. Si el polinomio generador es $M_\alpha(x)M_{\alpha^3}(x)M_{\alpha^5}(x)M_{\alpha^7}(x)M_{\alpha^{11}}(x)$ con ceros en $\{\alpha^i : i \in C_1 \cup C_3 \cup C_5 \cup C_7 \cup C_{11}\}$, entonces se genera un código *BCH* con parámetros $[31, 5, 15]_2$ y distancia diseñada $\delta = 13$ ó 15. Tomando el polinomio generador $M_\alpha(x)M_{\alpha^3}(x)M_{\alpha^5}(x)M_{\alpha^7}(x)M_{\alpha^{11}}(x)M_{\alpha^{15}}(x)$ con ceros en $\{\alpha^i : i \in C_1 \cup C_3 \cup C_5 \cup C_7 \cup C_{11} \cup C_{15}\}$, se genera el código *BCH* con parámetros $[31, 1, 31]_2$ con distancia diseñada igual a cualquiera de estos valores $\delta \in \{17, 19, 21, 23, 25, 27, 29, 31\}$, que es equivalente al código $Rep_2(31)$. Notemos que la distancia diseñada fue tomada impar, como se enuncia en el teorema 5.5 más adelante.

El siguiente teorema mostrará que muchos códigos de Hamming son códigos BCH narrow-sense.

Teorema 5.4. *Sea* $n = \frac{q^r-1}{q-1}$ *tal que* $\text{mcd}(r, q-1) = 1$. *Sea C el código BCH narrow-sense con conjunto definido* $T = C_1$. *Entonces C es equivalente a un código de Hamming* $\mathcal{H}_q(r)$.

Ejemplo 5.5. Usando las clases 2-ciclotómica módulo 31, con el conjunto definido $T = C_1 = \{1, 2, 4, 8, 16\}$ que tiene el polinomio minimal $M_\alpha(x) = x^5 + x^2 + 1$ obtenidos en el ejemplo 5.4, genera un código C que es *BCH* y tiene parámetros $[31, 26, 3]_2$ con distancia diseñada $\delta = 2$, entonces por el teorema anterior, C es equivalente al código de Hamming $\mathcal{H}_2(5)$.

Corolario 5.1. *Todo código binario de Hamming es un código BCH narrow-sense primitivo pero no todo código de Hamming es equivalente a un código BCH. De hecho, algunos códigos de Hamming no son equivalentes a ningún código cíclico, como se vio en el ejemplo* 4.11.

Los códigos de Hamming del teorema anterior tienen distancia diseñada $\delta = 2$, sin embargo, la distancia mínima es $d = 3$. En el caso binario se puede explicar de la siguiente manera. Estos códigos de Hamming son códigos *BCH* narrow-sense con distancia diseñada $\delta = 2$ y conjunto definido $T = C_1$ con $\delta - 1 = 1$ elemento. Pero en el caso binario, $C_1 = C_2$ y así, $T = C_1 \cup C_2$ también es un conjunto definido con $\delta - 1 = 2$ elementos consecutivos para el código *BCH* narrow-sense con distancia diseñada $\delta = 3$. Este mismo argumento puede ser usado con cada código binario *BCH* narrow-sense, en tal caso la distancia diseñada siempre se puede asumir impar. En el próximo teorema se da una cota inferior a la dimensión de un código *BCH* en términos de δ y $ord_n(q)$. Por supuesto, la dimensión exacta esta determinada por el tamaño del conjunto definido.

Teorema 5.5. *Sea C un* $[n, k]_q$*-código con distancia diseñada* δ. *Entonces*

- *Se cumple que* $k \geq n - ord_n(q)(\delta - 1)$*, en donde* $ord_n(q)$ *es el tamaño de la clase q-ciclotómicas módulo n de* C_1.
- *Si* $q = 2$ *y C es un código BCH narrow-sense entonces* δ *puede suponerse como un número impar, además si* $\delta = 2w + 1$*, entonces se cumple que* $k \geq n - ord_n(q)w$.

Observación 33. Es posible que más de un valor para la distancia diseñada δ sea usado para construir el mismo código *BCH* como se vió en el ejemplo 5.4.

2. Códigos Reed-Solomon

Definición 5.2. (**CÓDIGOS REED-SOLOMON**). Son un caso particular de códigos *BCH*, es decir, que son una subfamilia de los códigos *BCH*. Un código Reed-Solomon es un código *BCH* sobre $\mathbb{F}_q$ con longitud $n = q - 1$. Así, $ord_n(q) = 1$ implicando que todos los factores irreducibles de $x^n - 1$ tienen grado 1 y todas las clases q-ciclotómicas módulo n tienen tamaño igual a 1. De hecho, las raices de $x^n - 1$ son exactamente los elementos distintos de cero en $\mathbb{F}_q$ y una n-ésima raíz primitiva de la unidad es un elemento primitivo de $\mathbb{F}_q$. Por lo que que si C tiene distancia diseñada δ, el conjunto definido T de C tiene $\delta - 1$ elementos consecutivos y es $T = \{b, b + 1, \ldots, b + \delta - 2\}$ para algún entero b. Por el teorema 5.2 y usando la Cota de Singleton, se tiene que la dimensión k y la distancia mínima d del código C satisfacen $k = n - \delta + 1 \geq n - d + 1 \geq k$. Luego, $k = n - d + 1$ y $d = \delta$. En particular, C es un código *MDS*. Se resume la información en el siguiente teorema.

Teorema 5.6. *Si C es un código Reed-Solomon con longitud* $n = q - 1$ *sobre el espacio* $\mathbb{F}_q$ *con distancia diseñada* δ*. Entonces*

- *El código C tiene como conjunto definido* $T = \{b, b + 1, \ldots, b + \delta - 2\}$ *para algún entero b.*
- *El código C tiene distancia mínima* $d = \delta$ *y dimensión* $k = n - d + 1$.
- *El código C es MDS*.
- *El código C tiene parámetros* $[q - 1, q - d, d\,]_q$ *en donde* $d = \delta$ *es la distancia diseñada.*

En general, el dual y el complemento cíclico de un código *BCH* no es un código *BCH*, este no es el caso en los códigos Reed-Solomon.

Ejemplo 5.6. Sea 2 un elemento primitivo de $\mathbb{F}_{13}$. Sea C el código Reed-Solomon narrow-sense con distancia diseñada $\delta = 5$ sobre $\mathbb{F}_{13}$. Este código tiene longitud $n = 12$, conjunto definido

$T = \{1, 2, 3, 4\}$ con $\delta - 1 = 4$ elementos consecutivos y polinomio generador

$$g(x) = (x-2)(x-2^2)(x-2^3)(x-2^4) = x^4 + 9x^3 + 7x^2 + 2x + 10.$$

Por el teorema 5.6, este código tiene distancia mínima $d = 5$ y C es un código MDS con parámetros $[12, 8, 5]_{13}$. La matriz generadora de C, usando el teorema 3.5 es

$$G = \begin{pmatrix} 10 & 2 & 7 & 9 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 10 & 2 & 7 & 9 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 10 & 2 & 7 & 9 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 10 & 2 & 7 & 9 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 10 & 2 & 7 & 9 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 10 & 2 & 7 & 9 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 10 & 2 & 7 & 9 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 10 & 2 & 7 & 9 & 1 \end{pmatrix}_{8\times 12}$$

Ejemplo 5.7. Sea C el código anterior. El complemento cíclico C^{c} de C, es un $[12, 4, 9]_{13}$-código Reed-Solomon (non-narrow-sense), tiene conjunto definido $T = \{0, 5, 6, 7, 8, 9, 10, 11\}$ con $\delta - 1 = 8$ elementos consecutivos y polinomio generador

$$\begin{aligned} g^{\mathsf{c}}(x) &= (x-2^0)(x-2^5)(x-2^6)(x-2^7)(x-2^8)(x-2^9)(x-2^{10})(x-2^{11}) \\ &= x^8 + 4x^7 + 9x^6 + 6x^5 + 8x^4 + 10x^3 + 12x^2 + 6x + 9. \end{aligned}$$

Ejemplo 5.8. Si C es el código del ejemplo 5.6. El código dual $C^{\perp}$ con parámetros $[12, 4, 9]_{13}$ es un código Reed-Solomon (non-narrow-sense), tiene conjunto definido $T' = \{0, 1, 2, 3, 4, 5, 6, 7\}$ con $\delta - 1 = 8$ elementos consecutivos y polinomio generador

$$\begin{aligned} g'(x) &= (x-2^0)(x-2)(x-2^2)(x-2^3)(x-2^4)(x-2^5)(x-2^6)(x-2^7) \\ &= x^8 + 5x^7 + 10x^6 + 4x^5 + 11x^4 + 5x^3 + x^2 + 12x + 3. \end{aligned}$$

La matriz generadora del código dual $C^{\perp}$ usando el teorema 3.5 es

$$G' = \begin{pmatrix} 3 & 12 & 1 & 5 & 11 & 4 & 10 & 5 & 1 & 0 & 0 & 0 \\ 0 & 3 & 12 & 1 & 5 & 11 & 4 & 10 & 5 & 1 & 0 & 0 \\ 0 & 0 & 3 & 12 & 1 & 5 & 11 & 4 & 10 & 5 & 1 & 0 \\ 0 & 0 & 0 & 3 & 12 & 1 & 5 & 11 & 4 & 10 & 5 & 1 \end{pmatrix}_{4\times 12}$$

La matriz estándar de G' es

$$G'' = (I_4 \mid A) = \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 12 & 1 & 5 & 11 & 4 & 10 & 5 \\ 0 & 1 & 0 & 0 & 11 & 8 & 7 & 2 & 2 & 4 & 6 & 11 \\ 0 & 0 & 1 & 0 & 6 & 9 & 10 & 4 & 11 & 10 & 11 & 3 \\ 0 & 0 & 0 & 1 & 4 & 9 & 6 & 8 & 10 & 12 & 6 & 9 \end{pmatrix}_{4\times 12}$$

La matriz de paridad H de $C^{\perp}$ usando la matriz estándar G'' es

$$H = (-A^{\top} \mid I_8) = \begin{pmatrix} 10 & 2 & 7 & 9 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 5 & 4 & 4 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 12 & 6 & 3 & 7 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 8 & 11 & 9 & 5 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 2 & 11 & 2 & 3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 9 & 9 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 7 & 2 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 8 & 2 & 10 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}_{8\times 12}$$

Ejemplo 5.9. Si queremos decodificar el $[12, 4, 9]_{13}$-código dual $C^{\perp}$ del ejemplo 5.8, que es 4-corrector, usamos la matriz de paridad H. Supongamos que se quiere enviar la palabra código $c_1 = (3, 12, 1, 5, 11, 4, 10, 5, 1, 0, 0, 0)$, pero se recibe $x_1 = (\underline{4}, 12, 1, 5, \underline{9}, 4, 10, 5, 1, 0, 0, 0)$, se detectan 2 errores. Su síndrome es

$$s(x_1) = (8, 1, 12, 8, 2, 9, 3, 8) = 1 \times (\text{columna } 1 \text{ de } H) + 11 \times (\text{columna } 5 \text{ de } H).$$

Decodificando, se tiene

$$\begin{aligned} c_1 &= x_1 - 1e_1 - 11e_5 \\ &= (4, 12, 1, 5, 9, 4, 10, 5, 1, 0, 0, 0) - (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \\ &\qquad - (0, 0, 0, 0, 11, 0, 0, 0, 0, 0, 0, 0) \\ &= (3, 12, 1, 5, 11, 4, 10, 5, 1, 0, 0, 0) \in C^{\perp}. \end{aligned}$$

Supongamos ahora, que se envia la palabra código $c_2 = (1,0,0,0,3,12,1,5,11,4,10,5)$, pero recibimos $x_2 = (1,0,\underline{7},0,3,\underline{2},\underline{9},5,11,4,10,\underline{12})$, se detectan 4 errores. Hallamos el síndrome,

$$\begin{aligned} s(x_2) &= (10,5,3,11,1,8,1,12) \\ &= 7 \times (\text{columna } 3 \text{ de } H) + 3 \times (\text{columna } 6 \text{ de } H) \\ &\quad + 8 \times (\text{columna } 7 \text{ de } H) + 7 \times (\text{columna } 12 \text{ de } H). \end{aligned}$$

Por lo tanto, decodificando tenemos

$$c_2 = x_2 - 7e_3 - 3e_6 - 8e_7 - 7e_{12} = (1,0,0,0,3,12,1,5,11,4,10,5) \in C^{\perp}.$$

A continuación se dará una definición alternativa para los códigos Reed-Solomon narrow-sense con un teorema importante que nos permite generalizar estos importantes códigos.

Teorema 5.7. *Sea $\mathcal{P}_k$ el conjunto de todos los polinomios en $\mathbb{F}_q[x]$ de grado menor estricto que k, incluyendo el polinomio nulo $\mathcal{P}_0$ en $\mathbb{F}_q[x]$, sea α un elemento primitivo en $\mathbb{F}_q$ y k un entero tal que $0 \leq k \leq n = q-1$. Entonces*

$$C = \{(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{q-2})) : f \in \mathcal{P}_k\}$$

es un código Reed-Solomon narrow-sense con parámetros $[n, k, n-k+1]_q$.

Definición 5.3. Sea $MP : \mathcal{P}_k \longrightarrow \mathbb{F}_q^n$ dado por

$$MP(f) = (f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{q-2}))$$

en donde α es elemento primitivo de $\mathbb{F}_q$ con $n = q-1$. El mapa MP es una transformación lineal no singular, es decir, una transformación lineal invertible.

Notar que el código Reed-Solomon narrow-sense con $k = 0$ es el código cero.

Esta formulación alternativa de códigos Reed-Solomon narrow-sense nos da un esquema de codificación alternativo. Supongamos que $f_0, f_1, \ldots, f_{k-1}$ con k símbolos de información y $f(x) = f_0 + f_1 x + \cdots + f_{k-1}x^{k-1}$ entonces

$$(f_0, f_1, \ldots, f_{k-1}) \xrightarrow{cod} (f(1), f(\alpha), \ldots, f(\alpha^{q-2})).$$

Esta manera de codificar no es sistemática. Hay un esquema para decodificar códigos Reed-Solomon que no es usual en el sentido que se encuentran directamente en los símbolos de información, usando la codificación anterior. No es decodificación por síndrome pero es un ejemplo de un esquema de decodificación basado mayoritariamente en la lógica y desarrollado originalmente por Reed y Solomon.

3. Códigos Reed-Solomon Generalizado

DEFINICIÓN 5.4. La construcción del código Reed-Solomon narrow-sense en el teorema anterior se puede generalizar para código posiblemente no cíclicos. Sea n un entero tal que $1 \leq n \leq q$. Tomando $\gamma = \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\}$ una n-tupla de elementos diferentes en $\mathbb{F}_q$ y $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ una n-tupla no nula, pero no necesariamente elementos distintos de $\mathbb{F}_q$. Sea k un entero tal que $1 \leq k \leq n$. Entonces el código

$$RSG_k(\gamma, \mathbf{v}) = \{(v_0 f(\gamma_0), v_1 f(\gamma_1), \ldots, v_{n-1} f(\gamma_{n-1})) : f \in \mathcal{P}_k,\ gr(f) < k\}$$

es el código Reed-Solomon Generalizado. Porque ningún v_i es 0. El código $RSG_k(\gamma, \mathbf{v})$ es k-dimensional. Porque el polinomio no nulo $f \in \mathcal{P}_k$ tiene como máximo $k-1$ ceros, $RSG_k(\gamma, \mathbf{v})$ tiene distancia mínima de por lo menos $n-(k-1) = n-k+1$. Por la Cota de Singleton, tiene distancia mínima de a lo sumo $n-k+1$, por lo tanto, $RSG_k(\gamma, \mathbf{v})$ tiene distancia mínima $d = n-k+1$. Así, RSG también es MDS, al igual que los códigos Reed-Solomon. Si $\mathbf{w}$ es otra n-tupla no nula de elementos en $\mathbb{F}_q$ entonces $RSG_k(\gamma, \mathbf{v})$ es equivalencia monomial a $RSG_k(\gamma, \mathbf{w})$. El código Reed-Solomon narrow-sense es un código RSG con parámetros $n = q-1$, $\gamma_i = \alpha^i$ con α una raíz primitiva n-ésima de la unidad y $v_i = 1$ con $i \in \{0, \ldots, n-1\}$. Se resume la información en el siguiente teorema.

TEOREMA 5.8. *Para los códigos Reed-Solomon Generalizado se tiene*

- *El código* $RSG_k(\gamma, \mathbf{v})$ *es un código MDS con parámetros* $[n, k, n-k+1]_q$.
- *El código* $RSG_k(\gamma, \mathbf{v})$ *es equivalente monomial al código* $RSG_k(\gamma, \mathbf{w})$.
- *El código Reed-Solomon narrow-sense es RSG con parámetros* $n = q-1$, $\gamma_i = \alpha^i$ *y* $v_i = 1$ *para* $i \in \{0, 1, \ldots, n-1\}$.

Los códigos Reed-Solomon narrow-sense con parámetros $[q-1, k, q-k]_q$ puede ser extendidos a códigos MDS de la siguiente manera. Definimos dicho código, sea el código $C =$

$\{(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{q-2})) : f \in \mathcal{P}_k\}$. Así,

$$\widehat{C} = \{(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{q-2}), f(0)) : f \in \mathcal{P}_k\}$$

es la extensión del código C. Notar que $\widehat{C}$ también es un código RSG con parámetros $n = q$, $\gamma_i = \alpha^i$ con $i \in \{0, 1, \ldots, n-2\}$, $\gamma_{n-1} = 0$, $v_i = 1$ con $i \in \{0, 1, \ldots, n-2\}$. Por lo tanto $\widehat{C}$ es un $[q, k, q-k+1]_q$-código MDS. En otras palabras, cuando se extiende un código Reed-Solomon narrow-sense mediante adding an overall parity check (definición 1.22), el peso mínimo aumenta. En general, se cumple para códigos sobre cuerpos arbitrarios si las palabras código con peso mínimo son todas odd-like. Esto resulta en el siguiente teorema.

Teorema 5.9. *El código con parámetros $[q, k, q-k+1]_q$ narrow-sense Reed-Solomon extendido es RSG y MDS.*

Observación 34. Si $f \in \mathcal{P}_k$ con $k < q$ entonces $\sum_{\beta \in \mathbb{F}_q} f(\beta) = 0$.

Ahora se verá que el dual de un código RSG es también RSG.

Teorema 5.10. *Sea $\gamma = \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\}$ una n-tupla de elementos distintos en $\mathbb{F}_q$ y sea $\mathbf{v} = (v_0, \ldots, v_{n-1})$ una n-tupla de elementos no nulos en $\mathbb{F}_q$. Entonces existe una n-tupla $\mathbf{w} = (w_0, \ldots, w_{n-1})$ de elementos no nulos en $\mathbb{F}_q$ tal que $RSG_k^{\perp}(\gamma, \mathbf{v}) = RSG_{n-k}(\gamma, \mathbf{w})$ para todo k con $k \in \{0, \ldots, n-1\}$. Además, el vector $\mathbf{w}$ es cualquier palabra código no nula en el código 1-dimensional $RSG_{n-1}^{\perp}(\gamma, \mathbf{v}) = RSG_1(\gamma, \mathbf{w})$ y satisface*

$$\sum_{i=0}^{n-1} w_i v_i h(\gamma_i) = 0 \tag{5.1}$$

para cualquier polinomio $h \in \mathcal{P}_{n-1}$.

Definición 5.5. (**Matriz generadora y de paridad**). La matriz generadora para el código $RSG_k(\gamma, \mathbf{v})$ con parámetros $[n, k, n-k+1]_q$ es

$$G = \begin{pmatrix} v_0 & v_1 & \cdots & v_{n-1} \\ v_0\gamma_0 & v_1\gamma_1 & \cdots & v_{n-1}\gamma_{n-1} \\ v_0\gamma_0^2 & v_1\gamma_1^2 & \cdots & v_{n-1}\gamma_{n-1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ v_0\gamma_0^{k-1} & v_1\gamma_1^{k-1} & \cdots & v_{n-1}\gamma_{n-1}^{k-1} \end{pmatrix}_{k \times n}$$

Por el teorema 5.10, la matriz de paridad de $RSG_k(\gamma, \mathbf{v})$, es la matriz generadora del código $RSG_{n-k}(\gamma, \mathbf{w})$ en donde $\mathbf{w} = (w_0, \ldots, w_{n-1})$ está dado en el teorema 5.10. Por lo tanto la matriz de paridad del código $RSG_k(\gamma, \mathbf{v})$ con parámetros $[n, k, n-k+1]_q$ es

$$H = \begin{pmatrix} w_0 & w_1 & \cdots & w_{n-1} \\ w_0\gamma_0 & w_1\gamma_1 & \cdots & w_{n-1}\gamma_{n-1} \\ w_0\gamma_0^2 & w_1\gamma_1^2 & \cdots & w_{n-1}\gamma_{n-1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ w_0\gamma_0^{n-k-1} & w_1\gamma_1^{n-k-1} & \cdots & w_{n-1}\gamma_{n-1}^{n-k-1} \end{pmatrix}_{n-k \times n}$$

Definición 5.6. (**Extensión $\ddot{C}$**). Sabemos por el teorema 5.8 que $C = RSG_k(\gamma, \mathbf{v})$ es MDS. Queremos describir una extensión de C, denotada por $\ddot{C}$, que también es MDS. Sea $v \in \mathbb{F}_q$ un elemento distinto de cero. La matriz generadora extendida de $\ddot{C}$ es $\ddot{G} = (G\mathbf{u}^\top) \in \mathbb{F}_q^{k \times n+1}$, en donde $\mathbf{u} = (0, 0, \ldots, 0, v) \in \mathbb{F}_q^{1 \times k}$. Este código extendido generalmente no será even-like. Tomando $w \in \mathbb{F}_q$ tal que

$$\sum_{i=0}^{n-1} v_i w_i \gamma_i^{n-1} + vw = 0. \tag{5.2}$$

Dicho w existe ya que $v \neq 0$. Usando la ecuación (5.1) y la definición de $w \in \mathbb{F}_q$, se tiene que el código $\ddot{C}$ tiene matriz de paridad extendida

$$\ddot{H} = \begin{pmatrix} w_0 & w_1 & \cdots & w_{n-1} & 0 \\ w_0\gamma_0 & w_1\gamma_1 & \cdots & w_{n-1}\gamma_{n-1} & 0 \\ w_0\gamma_0^2 & w_1\gamma_1^2 & \cdots & w_{n-1}\gamma_{n-1}^2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ w_0\gamma_0^{n-k} & w_1\gamma_1^{n-k} & \cdots & w_{n-1}\gamma_{n-1}^{n-k} & w \end{pmatrix}_{n-k+1 \times n+1}$$

Notemos que si $w = 0$; $\sum_{i=0}^{n-1} w_i v_i h(\gamma_i) = 0,\ \forall h \in \mathcal{P}_n$ implicando que $\mathbf{v} \in \mathbb{F}_q^n$ es un vector distinto de cero que es ortogonal a todos los vectores en $\mathbb{F}_q^n$ que es una contradicción. De donde, $w \neq 0$.

Tenemos el siguiente teorema.

Teorema 5.11. *Para $1 \leq k \leq n \leq q$, el código $RSG_k(\gamma, \mathbf{v})$ es un MDS, y puede ser extendido a un código MDS con longitud $n+1$.*

Sabemos que el códigos con parámetros $[q-1, k, q-k]_q$ narrow-sense Reed-Solomon puede ser extendido mediante el proceso de adding an overall parity check, resultando que el código $[q, k, q-k+1]_q$ es RSG y MDS por el teorema 5.9. Este código en sí, puede extenderse a un MDS por el teorema anterior. Así, el código Reed-Solomon narrow-sense con longitud $n = q-1$ puede ser extendido dos veces a un código MDS con longitud $n = q+1$.

En general, los códigos Reed-Solomon Generalizado C y sus extensiones $\ddot{C}$ son códigos MDS. Hay códigos MDS que no son equivalentes a dichos códigos. Sin embargo, no hay códigos MDS con parámetros distintos a los derivados de los códigos RSG o sus extensiones conocidas.

4. El Algoritmo de Decodificación Sudan-Guruswami

En el año 1997 Madhu Sudan desarrolló un procedimiento para decodificar códigos con los parámetros $[n, k, d]_q$ capaz de corregir algunos errores e cuando $e > \lfloor \frac{d-1}{2} \rfloor$. Este método fue extendido por Sudan y Guruswami para eliminar ciertas restricciones en el Algoritmo de Sudan original. Para ser capaz de corregir e errores cuando $e > \lfloor \frac{d-1}{2} \rfloor$, el algoritmo produce una lista de todas las posibles n-cadenas con distancia de Hamming e y cualquier vector recibido, tal algoritmo es llamado Algoritmo List-Decoding. El Algoritmo Sudan-Guruswami se aplica para los códigos RSG y algunos códigos BCH.

Definición 5.7. Sean x, y indeterminados independientemente y

$$p(x, y) = \sum_i \sum_j p_{i,j} x^i y^j$$

un polinomio en $\mathbb{F}_q[x, y]$, en donde $\mathbb{F}_q[x, y]$ es el anillo de todos los polinomios en dos variables.

Definición 5.8. Sean x, y indeterminados independientemente. EL grado del polinomio en dos variables $p(x, y)$ es el valor más grande de la suma de los exponentes de variables en cada término, es decir, si $p(x, y) = x^7 + x^3y^5 + 1$ entonces $gr(p(x, y)) = 3 + 5 = 8$.

Definición 5.9. Sean w_x, w_y números reales no negativos. El **grado-(w_x, w_y)** de $p(x, y)$ es definido como

$$\max\{w_x i + w_y j : p_{i,j} \neq 0\}.$$

El **grado-$(1, 1)$** de $p(x, y)$ es el grado de $p(x, y)$.

Definición 5.10. Para un entero positivo s y δ, se denota $\mathcal{N}_s(\delta)$ como el número de monomios $x^i y^j$ cuyo grado-$(1, s)$ es menor o igual que δ. Si $(\alpha, \beta) \in \mathbb{F}_q^2$ es raíz del polinomio $p(x, y)$ entonces se cumple que $p(\alpha, \beta) = 0$. Si $f(x) \in \mathbb{F}_q[x]$ y α una raíz de $f(x)$ entonces su multiplicidad como raíz es el número m tal que $f(x) = (x-\alpha)^m g(x)$ para algún polinomio $g(x) \in \mathbb{F}_q[x]$ con $g(\alpha) \neq 0$. Cuando se trabaja en dos variables no se puede generalizar esta noción de manera directa. Sin embargo, se tiene $f(x + \alpha) = x^m h(x)$ con $h(x) = g(x + \alpha)$ y $h(0) \neq 0$. En particular, $f(x + \alpha)$ contiene los monomios de grado m pero ninguno de menor grado. Este concepto se puede generalizar. La raíz (α, β) del polinomio $p(x, y)$ tiene multiplicidad m cuando el polinomio $p(x + \alpha, y + \beta)$ contiene los monomios de grado m pero no a los monomios de menor grado.

Recordemos que $[n, k]_q$-código Reed-Solomon Generalizado se define como

$$RSG_k(\gamma, \mathbf{v}) = \{(v_0 f(\gamma_0), v_1 f(\gamma_1), \ldots, v_{n-1} f(\gamma_{n-1})) : f \in \mathcal{P}_k,\ gr(f) < k\}$$

donde $\gamma = \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\}$ es una n-tupla de elementos distintos en $\mathbb{F}_q$, $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ una n-tupla de elementos no nulos en $\mathbb{F}_q$ y $\mathcal{P}_k$ el conjunto de polinomios en $\mathbb{F}_q[x]$ sobre $\mathbb{F}_q$ con grado menor o igual que $k - 1$ incluyendo en polinomio cero. Supongamos que se transmite la palabra $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in RSG_k(\gamma, \mathbf{v})$ y se recibe $\mathbf{y}' = (y'_0, y'_1, \ldots, y'_{n-1}) = \mathbf{c} + \mathbf{e}$. Entonces hay un único polinomio $f \in \mathcal{P}_k$ tal que $c_i = v_i f(\gamma_i), \forall i \in \{0, 1, \ldots, n - 1\}$. Podemos encontrar $\mathbf{c}$ si se determina el polinomio f. Sea $\mathcal{A} = \{(\gamma_0, y_0), (\gamma_1, y_1), \ldots, (\gamma_{n-1}, y_{n-1})\}$ con $y_i = \dfrac{y'_i}{v_i}, \forall i \in \{0, 1, \ldots, n - 1\}$. Supongamos por un momento que no se han producido errores al momento de transmitir la palabra $\mathbf{c}$. Entonces $y_i = \dfrac{c_i}{v_i} = f(\gamma_0), \forall i \in \{0, 1, \ldots, n - 1\}$. En particular, todos los puntos de $\mathcal{A}$ están en el polinomio $p(x, y) = y - f(x)$. Supongamos ahora que si ocurren errores. Se define el polinomio localizador del error $\Lambda(x, y)$ como cualquier polinomio en $\mathbb{F}_q[x, y]$ tal que $\Lambda(\gamma_i, y_i) = 0, \forall i \in \{0, 1, \ldots, n-1\}$ con $y_i = \dfrac{c_i}{v_i}$. Ya que $y_i - f(\gamma_i) = 0$ si $y_i = \dfrac{c_i}{v_i}$, todos los puntos de $\mathcal{A}$ están en el polinomio $p(x, y) = \Lambda(x, y)(y - f(x))$. La idea básica del Algoritmo de Decodificación Sudan-Guruswami es encontrar un polinomio $p(x, y) \in \mathbb{F}_q[x, y]$ donde cada elemento de $\mathcal{A}$ es una raíz con cierta multiplicidad y luego buscar los factores de ese polinomio de la forma $y - f(x)$. Se imponen más restricciones $p(x, y)$ para garantizar la capacidad de corrección de errores en el algoritmo.

Definición 5.11. El Algoritmo de Decodificación Sudan-Guruswami para el código Reed-Solomon Generalizado $RSG_k(\gamma, \mathbf{v})$ con parámetros $[n, k, n - k + 1]_q$ es el siguiente:

- Paso 1. Se fija un entero positivo m. Se escoge δ como el entero positivo que satisfaga la desigualdad
$$\frac{nm(m+1)}{2} < \mathcal{N}_{k-1}(\delta).$$
- Paso 2. Se construye un polinomio no nulo $p(x,y) \in \mathbb{F}_q[x,y]$ tal que cada elemento de $\mathcal{A}$ es raíz de $p(x,y)$ con multiplicidad mayor o igual que m, y $p(x,y)$ tiene grado-$(1,k-1)$ menor o igual que δ.
- Paso 3. Se hallan todos los factores de $p(x,y)$ de la forma $y - f(x)$ con $f(x) \in \mathcal{P}_k$ y $f(\gamma_i) = y_i$, para al menos t γ_i's con $t = \lfloor \frac{\delta}{m} \rfloor + 1$. Para cada f tal que produce la palabra código correspondiente $RSG_k(\gamma, \mathbf{v})$.

Debemos verificar que este algoritmo funciona y dar una cota para el número de errores que se corregirán. Para eso se necesitan los tres siguientes lemas.

LEMA 5.1. *Sea $(\alpha,\beta) \in \mathbb{F}_q^2$ una raíz en $p(x,y) \in \mathbb{F}_q[x,y]$ con multiplicidad m ó más. Si $f(x)$ es un polinomio sobre $\mathbb{F}_q$ tal que $f(\alpha) = \beta$, entonces $g(x) = p(x, f(x)) \in \mathbb{F}_q[x]$ es divisible por $(x-\alpha)^m$.*

LEMA 5.2. *Se fijan los enteros positivos m, t, δ tal que $mt > \delta$ en donde $t = \lfloor \frac{\delta}{m} \rfloor + 1$. Sea $p(x,y) \in \mathbb{F}_q[x,y]$ un polinomio tal que (γ_i, y_i) es raíz de $p(x,y)$ con multiplicidad de al menos m para $i \in \{0,1,\ldots,n-1\}$. Además, asumiendo que $p(x,y)$ tiene grado-$(1,k-1)$ a lo sumo δ. Sea $f(x) \in \mathcal{P}_k$ con $y_i = f(\gamma_i)$ para al menos t valores de i en donde $0 \le i \le n-1$. Entonces $y - f(x)$ divide a $p(x,y)$.*

LEMA 5.3. *Sea $p(x,y) = \sum_j \sum_l p_{j,l} x^j y^l \in \mathbb{F}_q[x,y]$. Suponemos que*
$$p'(x,y) = \sum_a \sum_b p'_{a,b} x^a y^b = p(x+\alpha, y+\beta), \quad \forall \ (\alpha,\beta) \in \mathbb{F}_q^2.$$
Entonces
$$p'_{a,b} = \sum_{j \ge a} \sum_{l \ge b} \binom{j}{a} \binom{l}{b} \alpha^{j-a} \beta^{l-b} p_{j,l}.$$

Ahora estamos en condiciones de verificar el Algoritmo Sudan-Guruswami y de dar la cota del error para que el algoritmo sea válido.

TEOREMA 5.12. *El Algoritmo de Decodificación Sudan-Guruswami aplicado a $RSG_k(\gamma, \mathbf{v})$ con parámetros $[n, k, n-k+1]_q$ producirá todas las n-cadenas tal que la distancia de Hamming entre los vectores recibidos es menor o igual que e, en donde, $e = n - \lfloor \frac{\delta}{m} \rfloor - 1$.*

Como el paso uno requiere calcular $\boldsymbol{N_{k-1}(\delta)}$, el siguiente lema resulta útil.

LEMA 5.4. *Sean s, δ enteros positivos. Entonces*

$$\boldsymbol{N_s(\delta)} = \left(\delta + 1 - \frac{s}{2}\left\lfloor \frac{\delta}{s} \right\rfloor\right)\left(\left\lfloor \frac{\delta}{s} \right\rfloor + 1\right) > \frac{\delta(\delta+2)}{2s}.$$

EJEMPLO 5.10. Sea C_1 un código Reed-Solomon con parámetros $[15, 6, 10]_{16}$. Tomando $m = 2$ en el Algoritmo de Decodificación Sudan-Guruswami, se tiene que $\frac{nm(m+1)}{2} = 45$ y el valor más pequeño de δ para que $45 < \boldsymbol{N_5(\delta)}$ es $\delta = 18$, en cuyo caso $\boldsymbol{N_5(18)} = 46$, según el lema anterior. Entonces $t = \lfloor \frac{\delta}{m} \rfloor + 1 = 10$ y por el teorema 5.12, este algoritmo puede corregir $15 - 10 = 5$ errores.

EJEMPLO 5.11. Si C_1 es el código anterior. Tomando $m = 6$ en el Algoritmo de Decodificación Sudan-Guruswami, se tiene que $\frac{nm(m+1)}{2} = 315 < \boldsymbol{N_5(\delta)}$ con $\delta = 53$, en cuyo caso $\boldsymbol{N_5(53)} = 319$, usando el lema anterior. Entonces $t = \lfloor \frac{\delta}{m} \rfloor + 1 = 9$ y por el teorema 5.12, este algoritmo puede corregir $15 - 9 = 6$ errores con estos parámetros.

EJEMPLO 5.12. Sea C_2 un código Reed-Solomon con parámetros $[31, 8, 24]_{32}$. Si se selecciona $m = 1$ en el Algoritmo de Decodificación Sudan-Guruswami, se tiene que $\frac{nm(m+1)}{2} = 31$ y el menor valor de δ para que $31 < \boldsymbol{N_7(\delta)}$ es $\delta = 17$, en cuyo caso $\boldsymbol{N_7(17)} = 33$, por lema 5.4. Entonces $t = \lfloor \frac{\delta}{m} \rfloor + 1 = 18$ y por el teorema 5.12, el Algoritmo de Decodificación Sudan-Guruswami puede corregir $31 - 18 = 13$ errores.

EJEMPLO 5.13. Sea C_2 el código anterior. Si se toma $m = 2$ en el Algoritmo de Decodificación Sudan-Guruswami, se tiene que $\frac{nm(m+1)}{2} = 93$ y el menor valor de δ para que $93 < \boldsymbol{N_7(\delta)}$ es $\delta = 32$, en cuyo caso $\boldsymbol{N_7(32)} = 95$, por lema 5.4. Entonces $t = \lfloor \frac{\delta}{m} \rfloor + 1 = 17$ y por el teorema 5.12 este algoritmo puede corregir $31 - 17 = 14$ errores con estos parámetros.

EJEMPLO 5.14. Si C_2 es el código del ejemplo 5.12. Tomando $m = 3$ en el Algoritmo de Decodificación Sudan-Guruswami, se tiene que $\frac{nm(m+1)}{2} = 186$ y el menor valor de δ para que $186 < \boldsymbol{N_7(\delta)}$ es $\delta = 47$, en cuyo caso $\boldsymbol{N_7(47)} = 189$, por lema 5.4. Entonces $t = \lfloor \frac{\delta}{m} \rfloor + 1 = 16$ y por el teorema 5.12 este algoritmo puede corregir $31 - 16 = 15$ errores con estos parámetros.

Como vimos en los ejemplos 5.10; 5.11; 5.12; 5.13 y 5.14 la capacidad de corregir errores del Algoritmo de Decodificación Sudan-Guruswami crece si m aumenta. Para una mayor capacidad de corregir errores se aumenta el grado-$(1, k-1)$ de $p(x, y)$, que por supuesto incrementa la dificultad

de este algoritmo. El siguiente corolario nos da una idea de como la capacidad para corregir errores varía dependiendo del m seleccionado.

Corolario 5.2. *El Algoritmo de Decodificación Sudan-Guruswami aplicado al* $RSG_k(\gamma, \mathbf{v})$ $[n, k, n-k+1]_q$*-código producirá todas las n-cadenas tal que la distancia de Hamming entre los vectores recibidos es menor o igual que e con* $e \leq n - 1 - n\sqrt{R(m+1)/m}$*, en donde el número* $R = \frac{k}{n}$ *es la tasa de información del código.*

En el corolario anterior, si m es grande, vimos que la fracción $\frac{e}{n}$ de los errores que la Decodificación Sudan-Guruswami puede corregir, es de aproximadamente $1 - \sqrt{R}$.

Para llevar a cabo este algoritmo se debe tener un método para calcular el polinomio $p(x, y)$ del paso 2 y luego encontrar los factores de $p(x, y)$ de la forma $y - f(x)$ en el paso 3. Para encontrar el polinomio no trivial $p(x, y)$ en $\mathbb{F}_q[x, y]$ de grado-$(1, k-1)$, se resuelven las $\frac{nm(m+1)}{2}$ ecuaciones lineales homogéneas en los coeficientes desconocidos $p_{j,l}$ de

$$\sum_{j \geq a} \sum_{l \geq b} \binom{j}{a} \binom{l}{b} \gamma_i^{j-a} y_i^{l-b} p_{j,l} = 0; \ \forall a, b \geq 0 \text{ con } (a, b) \in \mathbb{Z}^2, \ a + b < m, \ 0 \leq i \leq n-1$$

pero el número de ecuaciones e incógnitas aumentan con gran rapidez, como se reseñó en los ejemplos 5.12; 5.13 y 5.14.

5. Estudio comparativo

VAMOS A ESTUDIAR VARIOS CÓDIGOS REED-SOLOMON 5-ario DE LONGITUD $n = 4$, EL CONJUNTO DEFINIDO T, ELEMENTO PRIMITIVO α.

Ejemplo 5.15. Hay 2 elementos primitivos en $\mathbb{F}_5$, las cuales son $\alpha \in \{2, 3\}$. Sea $\alpha = 3$ un elemento primitivo de $\mathbb{F}_5$. Sea C_1 el código Reed-Solomon narrow-sense con los parámetros $[4, 1, 4]_5$, distancia diseñada $\delta = 4$ y conjunto definido $T = \{1, 2, 3\}$ con $\delta - 1 = 3$ elementos consecutivos. Su polinomio generador es

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

con matriz generadora $G \in \mathbb{F}_5^{1\times 4}$ de C_1 (usando el teorema 3.5) y matriz de control de paridad $H \in \mathbb{F}_5^{3\times 4}$ de C_1,

$$G = (I_1 \mid A) = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}_{1\times 4}, \qquad H = (A \mid I_3) = \begin{pmatrix} 4 & 1 & 0 & 0 \\ 4 & 0 & 1 & 0 \\ 4 & 0 & 0 & 1 \end{pmatrix}_{3\times 4}$$

Este código tiene $M = 5$ palabras, usando la matriz generadora G de C_1 se obtienen estas palabras, las cuales son

$$C_1 = \{0000,\ 1111,\ 2222,\ 3333,\ 4444\} = Rep_5(4).$$

Ejemplo 5.16. Sea $\alpha = 3$ un elemento primitivo de $\mathbb{F}_5$. Sea C_2 el código Reed-Solomon (non-narrow-sense) con los parámetros $[4, 1, 4]_5$, distancia diseñada $\delta = 4$ y conjunto definido $T = \{0, 1, 2\}$ con $\delta - 1 = 3$ elementos consecutivos. Su polinomio generador es

$$g(x) = (x - 3^0)(x - 3)(x - 3^2) = x^3 + 2x^2 + 4x + 3.$$

La matriz generadora $G \in \mathbb{F}_5^{1\times 4}$ de C_2 (usando el teorema 3.5) y la matriz generadora en forma estándar $G' \in \mathbb{F}_5^{1\times 4}$ de C_2 son,

$$G = \begin{pmatrix} 3 & 4 & 2 & 1 \end{pmatrix}_{1\times 4}, \qquad G' = (I_1 \mid A) = \begin{pmatrix} 1 & 3 & 4 & 2 \end{pmatrix}_{1\times 4}$$

La matriz de paridad $H \in \mathbb{F}_5^{3\times 4}$ de C_2 es

$$H = (A \mid I_3) = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 3 & 0 & 0 & 1 \end{pmatrix}_{3\times 4}$$

Este código, al igual que C_1, tiene tamaño $M = 5$, usando la matriz generadora G de C_2 se obtienen las palabras código, las cuales son

$$C_2 = \{0000,\ 3421,\ 1342,\ 4213,\ 2134\}.$$

Además, el código $C_1 = Rep_5(4)$ es equivalente a C_2. Aplicando al código C_2 las permutaciones $\pi = (01234) \in Biy(\mathbb{F}_5)$ del alfabeto en todas las coordenadas se tiene el resultado. Aquí lo vemos:

$$C_2 = \begin{Bmatrix} 0000 \\ 3421 \\ 1342 \\ 4213 \\ 2134 \end{Bmatrix} \xrightarrow{\pi} \begin{Bmatrix} 0000 \\ 1111 \\ 2222 \\ 3333 \\ 4444 \end{Bmatrix} = C_1 \quad \Rightarrow \quad C_2 \simeq C_1.$$

Ejemplo 5.17. Sea $\alpha = 3$ un elemento primitivo de $\mathbb{F}_5$. Sea C_3 el código Reed-Solomon narrow-sense con los parámetros $[4, 2, 3]_5$, distancia diseñada $\delta = 3$ y conjunto definido $T = \{1, 2\}$ con $\delta - 1 = 2$ elementos consecutivos. Este código no es auto-dual. Tiene el polinomio generador

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

con matrices generadora (usando el teorema 3.5) y generadora en forma estándar (la matriz G reducida por filas), $G, G' \in \mathbb{F}_5^{2\times 4}$, respectivamente

$$G = \begin{pmatrix} 2 & 3 & 1 & 0 \\ 0 & 2 & 3 & 1 \end{pmatrix}_{2\times 4}, \qquad G' = (I_2 \mid A) = \begin{pmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 4 & 3 \end{pmatrix}_{2\times 4}$$

Entonces, usando la matriz G la transformación lineal con $u \in \mathbb{F}_5^2$ es

$$uG = (x_1,\ x_2)_{1\times 2} \begin{pmatrix} 2 & 3 & 1 & 0 \\ 0 & 2 & 3 & 1 \end{pmatrix}_{2\times 4} = (2x_1,\ 3x_1 + 2x_2,\ x_1 + 3x_2,\ x_2)_{1\times 4}$$

Codificando, se tienen las $M = 5^2 = 25$ palabras código, las cuales son

$$\begin{array}{lllll} 00 \longrightarrow 0000, & 01 \longrightarrow 0231, & 02 \longrightarrow 0412, & 03 \longrightarrow 0143, & 04 \longrightarrow 0324 \\ 10 \longrightarrow 2310, & 11 \longrightarrow 2041, & 12 \longrightarrow 2222, & 13 \longrightarrow 2403, & 14 \longrightarrow 2134 \\ 20 \longrightarrow 4120, & 21 \longrightarrow 4301, & 22 \longrightarrow 4032, & 23 \longrightarrow 4213, & 24 \longrightarrow 4444 \\ 30 \longrightarrow 1430, & 31 \longrightarrow 1111, & 32 \longrightarrow 1342, & 33 \longrightarrow 1023, & 34 \longrightarrow 1204 \\ 40 \longrightarrow 3240, & 41 \longrightarrow 3421, & 42 \longrightarrow 3102, & 43 \longrightarrow 3333, & 44 \longrightarrow 3014 \end{array}$$

Por tanto, el $[4, 2, 3]_5$-código Reed-Solomon narrow-sense C_3 con distancia diseñada $\delta = 3$ y conjunto definido $T = \{1, 2\}$ es

$$C_3 = \left\{ \begin{array}{lllll} 0000, & 0231, & 0412, & 0143, & 0324 \\ 2310, & 2041, & 2222, & 2403, & 2134 \\ 4120, & 4301, & 4032, & 4213, & 4444 \\ 1430, & 1111, & 1342, & 1023, & 1204 \\ 3240, & 3421, & 3102, & 3333, & 3014 \end{array} \right\}$$

La matriz de control de paridad $H \in \mathbb{F}_5^{2\times 4}$ de C_3 usando la observación 17 es

$$H = (-A^\top \mid I_2) = \begin{pmatrix} 3 & 1 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{pmatrix}_{2\times 4}$$

Tomando las palabras even-like de C_3, resulta el $[4,1,4]_5$-código C_2 even-like, que es Reed-Solomom (non-narrow-sense) con el conjunto definido $T = \{0,1,2\}$.

Como el código C_3 es cíclico entonces es lineal y podemos decodificar por síndrome, en su forma vectorial. Además, C_3 es 1-corrector. Supongamos que se recibe la palabra $x = 4124$, calculamos su síndrome $s(x) = xH^\top = 04 = 4.(01) = 4 \times$ (columna 4 de H). Por lo tanto, se detecta un error de magnitud 4 en la cuarta coordenada de la palabra recibida x. Luego, la palabra se decodifica como la palabra en el código Reed-Solomon narrow-sense

$$c = x - 4e_4 = 4124 - 0004 = 4120 \in C_3.$$

Pero si queremos decodificar por síndrome, en su forma polinómica, usando el hecho de que C_3 es un código cíclico, sólo necesitamos la tabla con el único líder de peso 1 y grado 3 que es x^3, entonces la tabla líder-síndrome es

Líder	Síndrome
x^3	$2x+1$

Supongamos que, como antes se recibe la palabra $u(x) = 4 + x + 2x^2 + 4x^3 = 4124$. Como $syn(u(x)) = 3x + 4 = 4(2x+1)$ está en la tabla, se deduce que el coeficiente de x^3 en $u(x)$ es incorrecto y tiene un error de magnitud 4. Por lo tanto, se decodifica como

$$c(x) = u(x) - a(x) = 4x^3 + 2x^2 + x + 4 - 4x^3 = 2x^2 + x + 4 = 4120 \in C_3.$$

Considerando el $[4,2,3]_5$-código Reed-Solomon narrow-sense C_3 como un código RSG con parámetros $[4,2,3]_5$, $\alpha = 3$, $\gamma = \{1,3,4,2\}$ y $\mathbf{v} = (1,1,1,1)$; se puede hallar la matriz generadora G de C_3, (que es equivalente a la anterior), usando de la definición 5.5, entonces

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 4 & 2 \end{pmatrix}_{2\times 4}$$

Usando la ecuación (5.1) del teorema 5.10, para luego hallar la matriz de paridad H de C_3, se tiene $\mathbf{w}$ cualquier palabra código no nula en el código 1-dimensional $RSG_3^{\perp}(\gamma, \mathbf{v})$ con $h \in \mathcal{P}_3$. Tomando $\mathbf{w} = 3421 \in RSG_3^{\perp}(\gamma, \mathbf{v})$ con $h(x) = x$, entonces la matriz de paridad H de C_3 es

$$H = \begin{pmatrix} 3 & 4 & 2 & 1 \\ 3 & 2 & 3 & 2 \end{pmatrix}_{2\times 4}$$

Para el código extendido $\ddot{C}_3$, tenemos la matriz generadora extendida $\ddot{G} \in \mathbb{F}_5^{2\times 5}$ de $\ddot{C}_3$ con $\mathbf{u} = (0,4) \in \mathbb{F}_5^2$

$$\ddot{G} = (G\mathbf{u}^\top) = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 3 & 4 & 2 & 4 \end{pmatrix}_{2\times 5}$$

La matriz de paridad extendida $\ddot{H} \in \mathbb{F}_5^{2\times 5}$ de $\ddot{C}_3$ es

$$\ddot{H} = \begin{pmatrix} 3 & 4 & 2 & 1 & 0 \\ 3 & 2 & 3 & 2 & 2 \end{pmatrix}_{2\times 5}$$

El código extendido $\ddot{C}_3$ con parámetros $[5,2,4]_5$ es RSG y MDS. Notemos que el peso aumentó con respecto a C_3, pero sigue siendo un código 1-corrector.

Ejemplo 5.18. Sea $\alpha = 2$ un elemento primitivo de $\mathbb{F}_5$. Sea C_4 el código Reed-Solomon narrow-sense con parámetros $[4,3,2]_5$, distancia diseñada $\delta = 2$ y conjunto definido $T = \{4\}$ con $\delta - 1 = 1$ elemento. Su polinomio generador es $g(x) = x - 2^4 = x + 4$, las matrices generadora $G \in \mathbb{F}_5^{3\times 4}$ y de paridad $H \in \mathbb{F}_5^{1\times 4}$ de C_4 son

$$G = \begin{pmatrix} 4 & 1 & 0 & 0 \\ 0 & 4 & 1 & 0 \\ 0 & 0 & 4 & 1 \end{pmatrix}_{3\times 4}, \qquad H = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}_{1\times 4}$$

Este código tiene tamaño $M = 125$ y todas sus palabras son even-like. Además, C_4 es el código even-like $P_5(4)$, es decir, $C_4 = P_5(4) \subset \mathbb{F}_5^4$.

Ejemplo 5.19. Sea $\alpha = 3$ un elemento primitivo de $\mathbb{F}_5$. Sea C_5 el código Reed-Solomon narrow-sense con parámetros $[4,3,2]_5$, distancia diseñada $\delta = 2$ y conjunto definido $T = \{1\}$ con $\delta - 1 = 1$ elemento. Tiene el polinomio generador $g(x) = x - 3 = x + 2$ y usando el teorema 3.5 se tiene la matriz generadora G de C_5, y la matriz de paridad H de C_5,

$$G = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 \end{pmatrix}_{3\times 4}, \qquad H = \begin{pmatrix} 3 & 4 & 2 & 1 \end{pmatrix}_{1\times 4}$$

Este código detecta 1 error pero no corrige ninguno. Además, tiene $M = 5^3 = 125$ palabras código que no son even-like pero es equivalente a $P_5(4)$, es decir, $C_5 \simeq P_5(4)$. El $[4,1,4]_5$-código dual $C_5^\perp$ es 1-dimensional de peso mínimo 4, conjunto definido $T = \{0,1,2\}$ con $\delta - 1 = 3$ elementos consecutivos, tiene $M = 5$ palabras y coincide con el código C_2 del ejemplo 5.16.

Para finalizar este estudio, usando el teorema 5.3 se tiene que $C_1 \subset C_3 \subset C_5$.

6. Aplicaciones interesantes

Observación 35.

(1) En la grabación de discos se utilizan los códigos acortados Reed-Solomon con longitud $n = 255$ sobre $\mathbb{F}_{256}$.
(2) Un CD de música utiliza el código Reed-Solomon para corregir rayadura y polvo.
(3) Para limpiar las imagénes de los errores de transmisión introducidos por la atmósfera de la Tierra, (la turbulencia de la atmósfera de la Tierra produce errores en la transmisión, incluso cuando el cielo se encuentra despejado), los científicos aplicaron Goddard Reed-Solomon, usado comúnmente en CD y DVD. Los errores típicos incluyen píxeles perdidos y señales falsas.
(4) En el año 1977, la agencia del gobierno estadounidense responsable de programas espaciales NASA (National Aeronautics and Space Administration) utilizó los códigos Reed-Solomon en las misiones Galileo, Magallanes y Ulises.
(5) En las misiones espacio profundo de la NASA, se utilizan los códigos Reed-Solomon acortados, como el código externo perteneciente a los códigos concatenados. Este código fue usado por primera vez en la misión de la sonda Mariner Mars lanzado en el año 1971. Se utilizó un código biortogonal con parámetros $[32, 6, 16]_2$ para transmitir imágenes digitales de la superficie marciana, (el código biortogonal $\mathcal{B}(\boldsymbol{r})$ es el dual de un código binario extendido de Hamming y tiene parámetros $[2^r, r + 1, 2^{r-1}]_2$, consiste en los vectores $\mathbf{0}$, $\mathbf{1}$ y $2^{r+1} - 2$ palabras código con peso $w = 2^{r-1}$, el código binario extendido de Hamming tiene parámetros $[2^r, 2^r - r - 1, 4]_2$), pero para la transmisión de datos del espectrómetro infrarojo (IRIS) se usó un código concatenado que comprende un código biortogonal y un $[6, 4]_{64}$-código Reed-Solomon acortado sobre $\mathbb{F}_{2^6}$. Esto es porque los datos del IRIS se comprimen antes de la transmisión y requiere una tasa de error menor que 5×10^{-5} mientras que los datos de las imágenes eran capaz de tolerar una tasa de error de 5×10^{-3}.
(6) En el Voyager lanzado en el verano del año 1977, un código de convolución con longitud de $n = 7$ y una tasa de información de $\frac{1}{2}$ fue usado en el enlace principal comunicacional para la transmisión de imágenes de Júpiter y Saturno, pero para la transmisión de las

imágenes de Plutón y Neptuno, este código se concatena con un $[255, 223, 32]_{256}$-código Reed-Solomon.

(7) Una vez que la compresión de imagen se comenzó a utilizar, una tasa de error binario de 1×10^{-6} se hizo necesaria, inferior a la tasa anterior de error binario de 5×10^{-3} y códigos concatenados fueron usados para cumplir con este requisito. El código Reed-Solomon usado por el Voyager era un $[255, 223, 32]_{256}$-código sobre $\mathbb{F}_{2^8}$ con el polinomio primitivo

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

y polinomio generador

$$g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)\dots(x - \alpha^{30})(x - \alpha^{31})(x - \alpha^{32})$$

donde α es una raíz de $M(x)$. Por consiguiente, puesto que $n = 2^8 - 1 = 255$ y el grado de $g(x)$ es $r = 32$, $k = n - r = 223$, lo que resulta un código con parámetros $[255, 223, 32]_{256}$. La tasa de error binario BER (Bit Error Rate), usada en telecomunicaciones con el fin de modelar un canal de comunicación, define la velocidad a la que se producen errores en el canal de transmisión (fibra óptica), esto puede interpretarse como el número de bits recibidos de forma incorrecta respecto al total de bits enviados durante un intervalo específico de tiempo. La tasa de error binario es igual a la cantidad de errores de bits dividido por el número total de bits enviados. Por ejemplo, supongamos que se transmite la siguiente cadena de bits 0110001011 por un canal y se recibe la palabra $0\underline{0}10\underline{1}010\underline{0}1$. Para determinar el BER se divide 3 (número de bits con errores) entre 10 (número total de bits transmitidos), entonces la tasa de error binario en este caso es 3×10^{-1}.

(8) Entre los años 1986 y 1989, la sonda Voyager 2 tomó fotos en color de alta calidad de los planetas Urano y Neptuno usando códigos Reed-Solomon. Esta sonda transmitía 115.200 bits por segundo.

(9) Los que han visto las imágenes enviadas por la sonda espacial Voyager 2, han sido sorprendidos por la gran calidad de las imágenes recibidas. En 1980, cuando la Voyager fue cerca de aproximadamente 3 mil millones de kilómetros de la Tierra, era capaz de transmitir imágenes de alta resolución de Tritón, la luna más grande de Neptuno. Esta enorme hazaña fue en gran medida debido al hecho de que el sofisticado sistema de comunicación en el Voyager tenía un esquema de corrección de errores muy elaborado construido en él. Se utilizó un código de Reed-Solomon para mejorar la fiabilidad de la transmisión. Cada

palabra código contiene 223 bytes de datos (1 byte consiste en 8 bits) y 32 bytes de redundancia. Sin el esquema de corrección de errores, el Voyager no habría sido capaz de enviar el volumen de datos que hizo, utilizando una potencia de transmisión de sólo 20 vatios. Las naves espaciales Galileo (1991), Mars Global Surveyor (1997), Mars Pathfinder (1997) y Mars Exploration Rover (2004) usaron códigos Reed-Solomon en sus esquemas de transmisión de datos. No estaría fuera de lugar afirmar que los códigos Reed-Solomon han ido a los confines del sistema solar y más allá.

Conclusiones

Se puede afirmar que la teoría de códigos es un área de la matemática que contribuye al mundo en donde vivimos, ya que se utilizan en las memorias RAM y los modems; mejoran las conexiones a las redes de Wifi, evitan las interferencias en comunicaciones satelitales, corrigen rayaduras a la hora de escuchar algún CD o ver algún DVD en el reproductor. Cada día se transmite un mayor volumen de información digital, por lo que, se requieren códigos más eficientes para codificarlos, implementarlos y decodificarlos, para que de esta manera la información enviada y recibida coincidan, por ejemplo, en youtube se suben 20 horas de videos por minutos.

Los códigos son usados en aplicaciones tecnológicas por empresas como IBM, Philips, Sony, la NASA y la AEE. Una de las aplicaciones más importantes son en las misiones espaciales de la NASA y la Agencia Espacial Europea (AEE) tomar fotografías de otros planetas, primero en el 1965 las fotografías eran en blanco y negro, once años después en el año 1976 se empezaron a enviar fotografías a color en alta resolución desde Marte. Los códigos Reed-Solomon son los que más se utilizan para estos propósitos.

Entre los códigos usados en este trabajo se encuentran los códigos lineales y los códigos cíclicos, se demostraron varios teorema usados en la detección y corrección de errores, se vio que que entre mayor es la distancia d de un código, es mayor su capacidad detectora y correctora, unos de los más usados fue el teorema 1.6, que dice, si C es un código entonces s-detector si, y sólo si $d = s + 1$ y es t-corrector si, y sólo si $d = 2t + 1$ ó $d = 2t + 2$.

Se estudió la compresión de datos, usando la matriz generadora, donde se buscan representaciones que usen pocos bits para la información que se quiere enviar, conservando los datos de interés, para que de esa forma se pueda transmitir rapidamente o almacenarla en poco espacio en el disco duro, por ejemplo, el formato MP3 logra comprimir más de 10 veces lo que seria una canción sin compresión y asi se puede almacenar mas música en el MP3 por lo que el tamaño total del archivo será menor.

Analizamos también la decodificación de códigos para la corrección de errores, aqui se buscan representaciones tales que si se pierden o se alteran algunos de sus símbolos por acción del ruido

en el canal, de todas formas se pueda recuperar el contenido original que se tenia almacenado, esto se hizo mediante la redundancia, calculada a partir de los datos naturales y esto permite reconstruir la información sin repetir muchas veces la información original. Los códigos cíclicos son los más faciles para decodificarlos que los códigos lineales por su estructura.

Adicionalmente, presentamos algunos tipos de equivalencias, usadas para establecer cuando dos códigos son iguales, vimos que dos códigos son equivalentes entonces tienen los mismo parámetros.

Para finalizar, esta es un área que se esta desarrollando rapidamente, de ínteres para aquellos que quieren hacer trabajo científico o tecnológico tanto en la ingenieria eléctrica, computación y matemática, vimos que detrás de toda la tecnologia siempre hay un trabajo matemático que le antecede. Una tarea a futuro, es estudiar los tipos de ruidos que aparecen en el canal y de qué manera afecta a la información enviada. Hay un gran futuro en el estudio de todos estos fenómenos.

Bibliografía

[1] R. Hill. *A First Course in Coding Theory*. Oxford Applied Mathematics and Computing Science Series, (1986).

[2] Herstein. *Algebra Moderna*.

[3] K. Hoffman y R. Kunze. *Algebra lineal*. Prentice Hall Inc.

[4] Joseph J. Rotman. *A First Course In Abstract Algebra*, tercera edición. University of Illinois at Urbana-Champaign.

[5] R. Podestá. *Introducción a la Teoría de Códigos Autocorrectores*. Notas del curso dado en el ENAIII, Vaquerias, agosto 2006.

[6] R. Podestá. *Algunos aspectos combinatorios de la Teoría de Códigos*. Notas del curso dado en la Primera Escuela Puntana de Combinatoria, San Luis, julio 2012.

[7] T. W. Hungerford, *Abstract Algebra An Introduction*. Cleveland State University, (1974).

[8] Juan Jacobo Simón Pinero. *Apuntes codigos correctores de errores*, (2011-2012).

[9] W. Cary Huffman and Vera Pless. *Fundamentals of Error Correcting Codes*. Cambridge, (2003).

[10] Henk C.A van Tilborg. *Coding Theory A First Course*.