UNIVERSIDAD TECNOLÓGICA DE LA MIXTECA

Instituto de Física y Matemáticas
Licenciatura en Matemáticas Aplicadas

Líderes de clases laterales de algunos códigos BCH antiprimitivos

TESIS
para obtener el título de
Licenciada en Matemáticas Aplicadas
presenta

Viridiana Itzel Méndez Vásquez

Director de tesis:
Dr. Adolfo Maceda Méndez

Huajuapan de León, Oaxaca *Noviembre de 2021*

Dedicatoria

A aquellos quienes incondicionalmente
han estado a mi lado;
Paula Vásquez y Rogelio Méndez,
para ustedes,
todo mi amor y gratitud por siempre.

A ellos que siempre han
confiado en mí;
Obed Méndez y Miguel Méndez.

Agradecimientos

Los grandes o pequeños logros que he obtenido a lo largo de mi vida tienen como base fundamental el apoyo y la confianza que han depositado en mí personas muy importantes y valiosas en mi vida, sin ellas no sería lo que hoy soy.

A mi madre Paula Vásquez López le agradezco por el apoyo incondicional que me ha brindado. Por siempre estar ahí, tomándome de la mano y por nunca soltarme. Gracias por darme esas alas para que pueda volar más allá incluso de donde usted ha llegado. Finalmente, le agradezco por todo el amor con el que ha guiado mis pasos, ese amor que sólo usted sabe brindar.

A mi padre, Rogelio Virgilio Méndez Serna, le agradezco por ser esa parte fuerte en mi vida. Por demostrarme que somos capaces de aprender cualquier cosa, con dedicación y atreviéndonos a hacerlo, sin tener miedo. Gracias por todo lo que me ha enseñado, incluso sin darse cuenta. Por confiar en mí y apoyar cada paso que doy.

A mis hermanos, Obed y Miguel, gracias por confiar y por estar al pendiente de mí. Por alegrarse y enorgullecerse de cada uno de mis logros. Por enseñarme que hay diferentes maneras de vivir la vida, cada quien sus gustos, cada quien sus intereses. Gracias por ser mis compañeros de vida.

A esa persona especial en mi vida, gracias por impulsarme a atraverme a vencer mis miedos, por confiar en mí y en mi capacidad. Gracias por la atención con la que siempre me escuchaste y por todos esas veces que con tanta dedicación escuchaste mis ensayos de exposición de este trabajo. Por tu amor, compañia y paciencia.

Al Dr. Adolfo Maceda Méndez le agradezco enormemente por haber confiado en mi para realizar este trabajo. Por la paciencia que tuvo a lo largo de la elaboración del mismo, pero sobre todo por su disposición a enseñarme todo lo necesario y más. Gracias por guiarme en cada uno de los pasos para la elaboración de esta tesis. Toda mi admiración y respeto para usted.

A mis sinodales, la Dra. Luz del Carmen Álvarez Marín, el Dr. Virgilio Vásquez Hi-

pólito y el Dr. Mario Lomelí Haro, les agradezco por el tiempo dedicado a la revisión de este trabajo. Gracias por sus comentarios y sugerencias tan atinadas que ayudaron al mejoramiento de esta tesis.

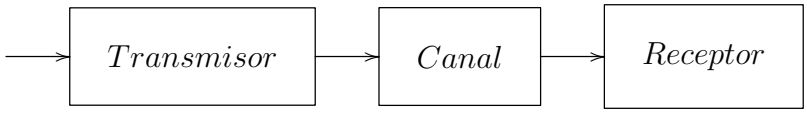
A todos mis profesores, los cuales contribuyeron a mi formación académica, en especial al Dr. Franco Barragán Mendoza por motivarme y enseñarme que las matemáticas requieren de mucha dedicación y práctica; a la Dra. Luz del Carmen Álvarez Marín, al M. C. Vulfrano Tochihuitl Bueno y al M. C. Juan Luis Hernández López, entre otros, porque posiblemente sin saber, hicieron que mi gusto por las matemáticas no hiciera más que crecer, porque quedaba fascinada con cada una de sus clases y mi admiración hacia ustedes fue creciendo.

A mis amigos, con los que llegué a Huajuapan y a los que a lo largo del camino se unieron, esas personas que se convirtieron en mi familia en Acatlima. Gracias porque sin ustedes estos años no habrían sido lo bonito que fueron.

Índice general

Introducción

La transmisión confiable de información a través de canales ruidosos, en el sentido en el que lo que se recibe no siempre es lo que se envió (veáse [20]), es uno de los requerimientos básicos de los sistemas de comunicación e información digital. Un sistema de comunicación cuenta con la siguiente estructura básica:



Dentro del Transmisor del sistema de comunicación se llevan a cabo las siguientes tareas (veáse [1]):

- Codificación de la fuente.
- Codificación del canal.
- Modulación.

Mientras que el Receptor realiza las tareas que se enlistan a continuación (veáse [1]):

- Demodulación.
- Decodificación del canal.
- Decodificación de la fuente.

El modulador genera la señal que se utiliza para transmitir la secuencia de símbolos b a través del canal. La señal se perturba debido al ruido del canal, por lo que esta señal con ruido es demodulada por el demodulador en el Receptor del sistema de comunicación, lo que lleva a la secuencia de símbolos recibidos r. La secuencia de símbolos recibidos r suele diferir de la secuencia de símbolos transmitida b, razón por la cual se utiliza un código de canal de modo que el receptor pueda detectar o incluso corregir errores. Para ello, el codificador del canal introduce redundancia en la secuencia de información u, dicha redundancia puede ser aprovechada por el decodificador del canal para la detección o correción de errores estimando la secuencia u de símbolos transmitidos (veáse [1]). En

la Teoría de códigos se estudian estos procesos de codificación y decodificación que se presentan en los sistemas de comunicación.

Nuestra investigación se centra en el estudio de la primera parte de la estructura de un sistema de comunicación: la transmisión, en el que la codificación juega el papel principal.

Los sistemas de comunicación modernos dependen en gran medida de potentes metodologías de codificación de canales, pero para su aplicación práctica estos esquemas de codificación no necesitan solamente tener buenas características de codificación con respecto a la capacidad de detectar o corregir errores que se introducen en el canal, sino que también se deben poder implementar de forma eficiente. Algunas de las aplicaciones prácticas de los códigos de canal se encuentran en las comunicaciones espaciales y por satélite, transmisión de datos, transmisión de audio y video digital y comunicaciones móviles, así como sistemas de almacenamiento como memorias de computadora o discos compactos (veáse [8]).

Los códigos lineales son un tipo de códigos con ciertas características que hacen que su codificación se pueda llevar a cabo de forma eficiente, sin embargo en general el problema de decodificación de códigos lineales es difícil de resolver. Los códigos cíclicos son un tipo de códigos lineales con propiedades algebraicas que hacen posible la existencia de algoritmos de decodificación algebraicas más eficientes (veáse [1]). Es importante mencionar que los procesos de codificación y decodificación se pueden llevar a cabo utilizando conceptos de Álgebra Moderna, particularmente de la teoría de campos finitos y de espacios vectoriales sobre dichos campos. Una de las características algebraicas más importantes de los códigos cíclicos es que estos se pueden describir mejor utilizando un anillo cociente de un anillo de polinomios sobre un campo finito.

Algunas de las propiedades de los códigos que hacen posible determinar cómo se puede llevar a cabo de forma más eficiente el proceso de decodificación son ciertos parámetros que tienen asociados, entre los que destacan la distancia mínima de Hamming y la dimensión del código.

Los códigos $\mathcal{BCH}$, los cuales son una familia de los códigos cíclicos, fueron descubiertos de forma independiente alrededor de 1960 por Bose-Chaudhuri-Hocquenghem (veáse [14, 16]). Dichos códigos pertenecen al tipo de códigos correctores de errores, estos cuentan con un algoritmo de decodificación eficiente que depende de lo que se conoce como distancia de diseño, la cual está determinada por las raíces de un polinomio. Este método depende además de lo conocido como clases laterales ciclotómicas. La teoría sobre códigos $\mathcal{BCH}$ es bien conocida cuando la longitud del código está dada por $n = q^l - 1$, donde q es una potencia de algún número primo. Cuando los códigos tienen esta característica se les denomina primitivos. Mientras que cuando su longitud está dada por $n = q^m + 1$ se les denomina antiprimitivos (veáse [6]).

Los códigos $\mathcal{BCH}$ se han estudiado y utilizado ampliamente en la práctica, como en la comunicación, el almacenamiento de datos y la seguridad de la información (veáse [19]), sin embargo, se sabe poco acerca de los parámetros de dichos códigos. En general es muy difícil determinar la dimensión y la distancia mínima de los códigos $\mathcal{BCH}$. Para un campo finito dado, la dimensión y la distancia mínima de los códigos $\mathcal{BCH}$ se conocen sólo para algunas longitudes de código especiales y distancias de diseño. Sólo se han desarrollado

algunos límites inferiores en la dimensión y la distancia mínima (veáse [20, 4, 18, 7, 12, 9]). Han tomado gran importancia los códigos $\mathcal{BCH}$ antiprimitivos, los cuales se pueden utilizar contra ataques de canal lateral y ataques no invasivos con fallos (veáse [15]). Cunsheng Ding señaló que es muy significativo encontrar el segundo y tercer líderes de clase lateral más grandes, módulo n, pues esto sería útil para deducir los parámetros de los códigos $\mathcal{BCH}$ (veáse [19]).

En este trabajo de investigación se estudiarán algunos códigos $\mathcal{BCH}$ antiprimitivos cuando $q = 2$ y m tiene algunas formas particulares, tomando como base el trabajo realizado por Yang Liu et. al en [19]. Para dicha investigación es indispensable conocer los líderes de clases laterales, así como los cinco líderes de clase lateral más grande, con el fin de determinar los parámetros de dichos códigos, por lo que el trabajo se ha estructurado de la siguiente forma:

En el Capítulo 1 se presentan conceptos básicos de Álgebra Moderna, mediante los cuales se construyen anillos cociente a partir de un anillo de polinomios sobre campos finitos. También se introducen las definiciones de raíz n-ésima primitiva de la unidad, polinomio mínimo y elementos conjugados sobre un campo que toman gran importancia en la construcción de códigos cíclicos.

El Capítulo 2 es una introducción a la Teoría de Códigos, en dicho capítulo se presentan definiciones como las de Código lineal y Código cíclico, además se explica cómo se construyen códigos cíclicos a partir de un ideal con la definición de determinadas funciones.

A lo largo del Capítulo 3 fundamentamos la construcción de los códigos $\mathcal{BCH}$, así como sus parámetros y algunas propiedades, justificamos además la relación de la distancia mínima de Hamming de estos códigos con la criptografía.

El Capítulo 4 está basado en el artículo [19], en dicho capítulo se presentan los códigos $\mathcal{BCH}$ de longitud $n = 2^m + 1$ para $m = 2t + 1$ para los cuales se determinan los cinco líderes de clases lateral más grande para después obtener los parámetros de dichos códigos.

Finalmente se presenta una sección sobre las Conclusiones obtenidas en este trabajo de tesis.

Capítulo 1

Conceptos preliminares de campos finitos

A lo largo de este capítulo, se presentan los conceptos básicos sobre Álgebra Moderna que se utilizarán en el desarrollo de la tesis.

1.1. Grupos y subgrupos

El primer concepto que presentamos es el de Grupo, pues a partir de dicho concepto se derivan el resto.

Definición 1.1.1. Un *grupo* es un conjunto no vacío G con una operación binaria, llamada producto y denotada por $(*)$, que satisface:

(1) Para todo $a, b \in G$, $a * b \in G$.

(2) El producto es asociativo.

(3) Existe un elemento $e \in G$ tal que para todo $a \in G$, $e * a = a * e = a$.

(4) Para cada $a \in G$ existe un único elemento $b \in G$ que satisface $a * b = b * a = e$.

El elemento e en (3) es único y se le llama: neutro aditivo del grupo G. Además, el elemento b en (4) se denota con a^{-1} y se le llama: el inverso multiplicativo de a.

Ejemplo 1.1.2. Si $G = \mathbb{Z}$ con $a * b = a + b$, entonces G es un grupo.

Definición 1.1.3. Se dice que el grupo G es *abeliano o conmutativo* si para cualesquiera $a, b \in G$, se cumple $a * b = b * a$.

Definición 1.1.4. Sea G un grupo y $H \subset G$ con $H \neq \emptyset$. Se dice que H es un *subgrupo* de G si H es un grupo con el producto de G.

Definición 1.1.5. Sea G un grupo y sea $a \in G$.

$$H = \{a^n : n \in \mathbb{Z}\}$$

es un subgrupo de G y es el menor subgrupo de G que contiene a a. H se denota por $\langle a \rangle$ y se le llama *subgrupo de G generado por a*.

Definición 1.1.6. Sea G un grupo. Se dice que G es *cíclico* si existe $g \in G$ tal que $G = \langle g \rangle$.

1.2. Anillos e ideales

Definición 1.2.1. Un *anillo* es un conjunto no vacío R con dos operaciones: $+$ (suma) y $\cdot$ (producto) tal que:

1. R es un grupo abeliano con la operación $+$.
2. Con la operación producto se satisface:
   - *a)* Para todo $x, y \in R$, $x \cdot y \in R$
   - *b)* Para todo $x, y, z \in R$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
   - *c)* Para todo $x, y, z \in R$, $x \cdot (y + z) = x \cdot y + x \cdot z$ y $(y + z) \cdot x = y \cdot x + z \cdot x$.

Ejemplo 1.2.2. El conjunto $R = \mathbb{Z}$ es un anillo con la suma y producto usuales de los números enteros.

Al trabajar sobre campos finitos, presentamos las siguientes definiciones que nos llevan a la definición de campo.

Definición 1.2.3. Sea R un anillo.

1. Se dice que R es *conmutativo* si $r_1 \cdot r_2 = r_2 \cdot r_1$ para cualesquiera $r_1, r_2 \in R$.
2. $u \in R$ con $u \neq 0$, se llama *divisor del cero* si existe $v \in R$ con $v \neq 0$ tal que $u \cdot v = 0$.
3. Para R conmutativo, R es un *dominio entero* si y sólo si R carece de divisores del cero.

Dadas las definiciones anteriores, presentamos la definición de campo.

Definición 1.2.4. Sea R dominio entero. R se llama *campo* si y sólo si $R - \{0\}$ es un grupo con la operación producto de R.

Definición 1.2.5. Sea R un anillo, $I \subseteq R$ con $I \neq \emptyset$. Se dice que I es un *ideal de R* si:

1. I es un grupo con la operación suma de R.

2. $ri, ir \in I$ para $i \in I$, $r \in R$ arbitrarios.

Definición 1.2.6. Si R es un anillo conmutativo unitario y $a \in R$, el ideal $\{ra : r \in R\}$ de todos los múltiplos de a es el *ideal principal generado por* a y se denota por $\langle a \rangle$. Un ideal N de R es un *ideal principal* si $N = \langle a \rangle$ para alguna $a \in R$.

Definición 1.2.7. Sea N un ideal de un anillo R y sea $a \in R$. La *clase* $a + N$ es el conjunto $\{a + n : n \in N\}$.

Las operaciones de clases que se definen son: Para $a, b \in R$

1. Suma: $(a + R) + (b + R) = a + b + R$

2. Multilicación: $(a + R)(b + R) = ab + R$

Definición 1.2.8. Si N es un ideal en un anillo R, el *anillo de las clases laterales* $r + N$ bajo las operaciones inducidas, es el anillo cociente y se denota por R/N. Las clases $r + N$ son las clases residuales módulo N.

1.3. Anillo de polinomios

Es bien sabido que en la definición de polinomio habitual, lo más importante son los coeficientes del mismo y el orden en el que se encuentran, por esta razón se presenta la siguiente definición de polinomio.

Definición 1.3.1. Sea R un anillo conmutativo con unidad, un *polinomio con coeficientes en* R es una función $f : \mathbb{N} \cup 0 \to R$ para la cual existe $N \in \mathbb{N}$ con $f(n) = 0$ para toda $n > N$. Si $f(n) \neq 0$ para algún $n \in \mathbb{N}$, al máximo valor que satisface dicha propiedad se le llama el grado de f y se denota por $grad(f)$.

Sobre polinomios se presentan las siguientes definiciones:

Definición 1.3.2. Si f y g son polinomios. Se denota y se define:

1. La *suma* de f con g mediante:

$$(f + g)(n) = f(n) + g(n)$$

2. El *producto* de f con g mediante:

$$(fg)(n) = \sum_{k=0}^{\infty} f(k)g(n - k)$$

Se satisface que $f+g$ y fg son polinomios, 0 representa la función constante 0 y la función 1 definida como $1(0)=1$ y $1(n)=0$ para todo $n>0$, así el conjunto de polinomios con coeficientes en R es un anillo conmutativo con identidad.

Consideremos la función $x:\mathbb{N}\to R$ definida por

$$x(n)=\begin{cases}1 & \text{si } n=1\\ 0 & \text{si } n\neq 1\end{cases}.$$

Se verifica, aplicando la definición de producto, que

$$x^k(n)=\begin{cases}1 & \text{si } n=k\\ 0 & \text{si } n\neq k\end{cases},$$

por lo que todo polinomio distinto de cero se puede escribir en la forma:

$$f=\sum_{k=0}^{\infty} f(k)x^k.$$

Observemos que la sumatoria en realidad es finita, pues por definición existe $N\in\mathbb{N}$ con $f(n)=0$ para toda $n>N$. Así,

$$f=\sum_{k=0}^{N} f(k)x^k,$$

o de forma explícita

$$f=a_0+a_1x+a_2x^2+\ldots+a_Nx^N.$$

Notación 1.3.3. A cada polinomio f se le denotará como $f(x)$ y con $R[x]$ se denota al conjunto de todos los polinomios con coeficientes en el anillo R.

Se presenta una propiedad importante cuando R es un campo.

Teorema 1.3.4. ([10, Teorema 31.5]) Si $\mathbb{F}$ es un campo, entonces todo ideal en $\mathbb{F}[x]$ es principal.

Teorema 1.3.5. Si $\mathbb{F}$ es un campo e I el ideal principal generado por $p(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n$ con $a_n\neq 0$, entonces para cada $r(x)+I\in\mathbb{F}[x]/I$, existe un único polinomio $q(x)=b_0+b_1x+b_2x^2+\ldots+b_{n-1}x^{n-1}$ tal que $r(x)+I=q(x)+I$.

Definición 1.3.6. Un polinomio no constante $p(x)$ sobre $\mathbb{F}[x]$ es *irreducible* sobre $\mathbb{F}$ si $p(x)$ no puede expresarse como producto $q(x)s(x)$ de dos polinomios $q(x)$ y $s(x)$ en $\mathbb{F}[x]$, ambos de grado menor que el grado de $p(x)$.

Teorema 1.3.7. Si $p(x)$ es un polinomio irreducible en $\mathbb{F}[x]$ con $\mathbb{F}$ campo, entonces $\mathbb{F}[x]/\langle p(x)\rangle$ es campo.

Definición 1.3.8. Sea $\mathbb{F}$ un campo, $\alpha\in\mathbb{F}$ y $p(x)\in\mathbb{F}[x]$. Se dice que α es una *raíz* de $p(x)$ si y sólo si $p(\alpha)=0$.

1.4. Campos finitos

Como los códigos con los que vamos a trabajar se desarrollan sobre campos finitos, en esta sección introduciremos cuestiones importantes sobre ellos.

Los campos finitos son aquellos campos con un número finito de elementos, es decir, si $\mathbb{F}$ es un campo, entonces $|\mathbb{F}| = q$.

Definición 1.4.1. Se define la *característica de un campo* $\mathbb{F}$, como el número entero positivo más pequeño p tal que $p \cdot 1 = 0$. Así, se dice que el campo $\mathbb{F}$ tiene característica p. Si dicho número no existe, se dice que el campo tiene característica 0. La operación $p \cdot 1$ representa p sumandos, es decir,

$$p \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{p-\text{veces}}.$$

Definición 1.4.2. Un *subcampo* es un subconjunto $\mathbb{K}$ de un campo $\mathbb{F}$ que es campo bajo las operaciones inducidas en $\mathbb{F}$.

Definición 1.4.3. Un campo $\mathbb{F}$ es un *campo de extensión* de un campo $\mathbb{K}$, si $\mathbb{K}$ es subcampo de $\mathbb{F}$. En este caso, $\mathbb{F}$ es un espacio vectorial sobre $\mathbb{K}$ con las operaciones adecuadas, además la extensión es finita si la dimensión de $\mathbb{F}$ sobre $\mathbb{K}$ es finita.

Teorema 1.4.4. Sea $\mathbb{F}$ un campo finito.

1. La característica de $\mathbb{F}$ es un número primo p.
2. $\mathbb{F}$ contiene al subcampo $\mathbb{F}_p$, donde $\mathbb{F}_p$ son los enteros módulo p.
3. $\mathbb{F}$ tiene p^m elementos, donde el número primo p es la característica de $\mathbb{F}$ y m es la dimensión de $\mathbb{F}$ sobre $\mathbb{F}_p$.

Definición 1.4.5. Sean n y p coprimos. Se define $ord_n(p)$ como el entero positivo más pequeño, a, tal que $p^a \equiv 1 \mod n$.

Observación 1.4.6. El Teorema de Euler nos asegura que, si n y p son coprimos, entonces $p^{\varphi(n)} \equiv 1 \mod n$, donde $\varphi(n)$ es la función de Euler que nos indica el número de enteros entre 1 y n que son primos relativos con n.

El Teorema del Buen Orden nos garantiza que existe $ord_n(p)$.

Ejemplo 1.4.7. Consideremos $n = 5$ y observemos que para $p = 2$

$$\begin{aligned} 2^0 &= 0 \cdot 5 + 1 \equiv 1 \mod 5 \\ 2^1 &= 0 \cdot 5 + 2 \equiv 2 \mod 5 \\ 2^2 &= 0 \cdot 5 + 4 \equiv 4 \mod 5 \\ 2^3 &= 1 \cdot 5 + 3 \equiv 3 \mod 5 \\ 2^4 &= 3 \cdot 5 + 1 \equiv 1 \mod 5 \end{aligned}$$

de modo que $ord_5(2) = 4$. De manera similar, se obtiene que $ord_5(3) = 4$ y $ord_5(4) = 2$.

Como $2, 3, 4 \in \mathbb{F}_5$ el orden de cada uno con respecto a n coincide con el orden de cada uno de los números en los enteros módulo 5.

Teorema 1.4.8. Si p es un número primo y m es un número natural, entonces existe un campo finito $\mathbb{F}$ con p^m elementos.

Teorema 1.4.9. Si el campo finito $\mathbb{F}$ tiene p^m elementos, entonces todo $a \in \mathbb{F}$ satisface $a^{p^m} = a$.

Definición 1.4.10. El *campo de descomposición* sobre $\mathbb{F}$ de un polinomio $f(x) \in \mathbb{F}[x]$ es la menor extensión de $\mathbb{F}$ que contiene a $\mathbb{F}$ y a todos los ceros de $f(x)$.

Teorema 1.4.11. Todo polinomio $f(x) \in \mathbb{F}[x]$ con $\mathbb{F}$ campo, tiene un campo de descomposición sobre $\mathbb{F}$.

Teorema 1.4.12. Sean n y p coprimos, donde p es un número primo. El campo de descomposición de $x^n - 1$ sobre $\mathbb{F}_p$ es $\mathbb{F}_{p^t}$ donde $t = ord_n(p)$.

Definición 1.4.13. Un elemento α de un campo es una *raíz n-ésima de la unidad* si $\alpha^n = 1$. Es una *raíz primitiva n-ésima de la unidad* si $\alpha^n = 1$ y $\alpha^m \neq 1$ para $0 < m < n$.

Notemos que en el Teorema 1.4.12, podemos concluir que $\mathbb{F}_{p^t}$ donde $t = ord_n(p)$, contiene una raíz primitiva n-ésima de la unidad.

Si $n = 2$ o $n = 3$, diremos que α es una raíz cuadrada y raíz cúbica, respectivamente. Para valores mayores de n, diremos que α es una raíz de orden n.

Si tenemos un campo finito $\mathbb{F}$, por el Teorema 1.4.4, $\mathbb{F}$ tiene p^n elementos donde p es un número primo, tenemos así $p^n - 1$ elementos distintos de cero. Del Teorema 1.4.9, todo elemento $\alpha \in \mathbb{F}$ cumple $\alpha^{p^n} = \alpha$, de donde $\alpha^{p^n-1} = 1$ si $\alpha \neq 0$, es decir, todos los elementos distintos de cero de un campo finito $\mathbb{F}$ con p^n elementos son raíces de la unidad de orden $(p^n - 1)$.

Teorema 1.4.14. [20, Teorema 3.3.1] Tenemos lo siguiente:

1. El grupo $\mathbb{F}_q^*$ de los elementos distintos de cero del campo $\mathbb{F}_q$, donde $q = p^m$ con p número primo, es cíclico de orden $q - 1$ bajo la multiplicación de $\mathbb{F}_q$.

2. Si γ es un generador de dicho grupo cíclico, entonces
$$\mathbb{F}_q = \{0, 1 = \gamma^0, \gamma, \gamma^2, \ldots, \gamma^{q-2}\}$$
y $\gamma^i = 1$ si y sólo si $(q-1)|i$.

Observemos que del teorema anterior, el campo $\mathbb{F}_q$ contiene una raíz primitiva de la unidad de orden n si y sólo si $n|(q-1)$, en dicho caso $\gamma^{\frac{q-1}{n}}$ es una raíz primitiva de la unidad de orden n.

Teorema 1.4.15. Sea $\mathbb{K}$ una extensión finita de $\mathbb{F}$. Si $\alpha \in \mathbb{K}$, entonces existe un polinomio no cero $f(x) \in \mathbb{F}[x]$ tal que $f(\alpha) = 0$.

Definición 1.4.16. Sea $\mathbb{K}/\mathbb{F}$ una extensión finita y $\alpha \in \mathbb{K}$. El *polinomio mínimo* de α es el polinomio mónico $M_\alpha(x)$ en $\mathbb{F}[x]$ de grado más pequeño que tiene a α como raíz.

Definición 1.4.17. Sea $\mathbb{K}/\mathbb{F}$ una extensión finita y $\alpha, \alpha' \in \mathbb{K}$. Dos elementos, α y α' los cuales tiene el mismo polinomio mínimo sobre $\mathbb{F}$ se llama *conjugados* sobre $\mathbb{F}$.

Capítulo 2

Introducción a la Teoría de Códigos

Un sistema de comunicación cuenta con la siguiente estructura básica:

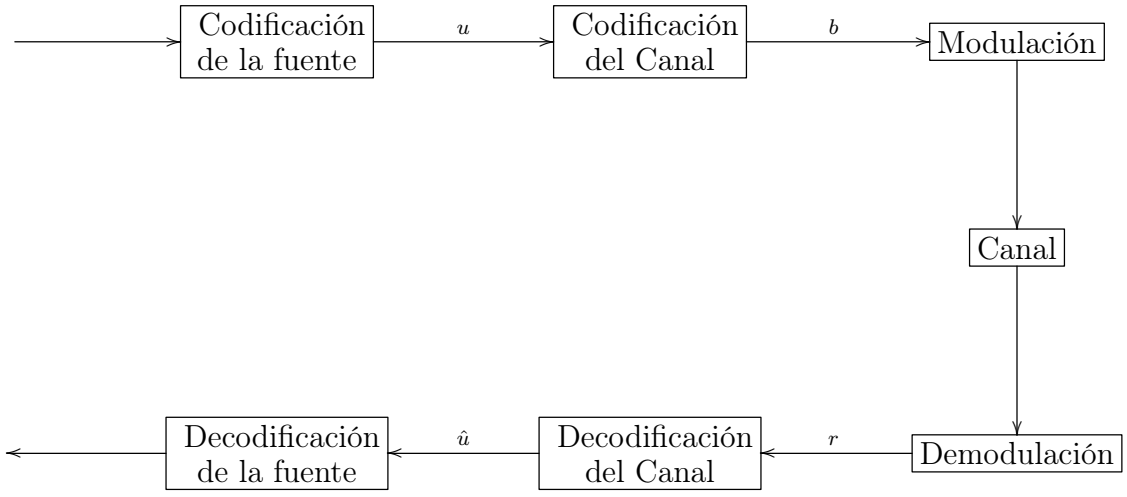


Figura 2.1

donde u es la secuencia de información que se codifica en la secuencia de símbolos b, la cual se transmite a través de un canal. La secuencia de símbolos recibidos r suele diferir de la secuencia de símbolos transmitida b, razón por la cual se utiliza un código de canal de modo que el receptor pueda detectar o incluso corregir errores. Para ello, el codificador del canal introduce redundancia en la secuencia de información u, dicha redundancia puede ser aprovechada por el decodificador del canal para la detección o correción de errores estimando la secuencia u, es decir, r recibidos se decodifica en la secuencia de símbolos de información $\hat{u}$ la cual es una estimación de los símbolos de información transmitidos originalmente (veáse [1]). En la Teoría de códigos se estudian estos procesos de codificación y decodificación que se presentan en los sistemas de comunicación.

2.1. Códigos lineales

Definición 2.1.1. Un *alfabeto* es un conjunto finito $\mathcal{A} = \{a_1, \cdots, a_q\}$, cuyos elementos son llamados símbolos y el número de elementos de $\mathcal{A}$ es la raíz de $\mathcal{A}$.

Con base en la definición anterior, se presenta la siguiente definición:

Definición 2.1.2. Una *palabra* de longitud n sobre $\mathcal{A}$ es una sucesión de n elementos de $\mathcal{A}$.

Notación 2.1.3. En general escribiremos las palabrasde longitud n sobre $\mathcal{A}$ de la siguiente forma:

$$u = u_{i_1} u_{i_2} \cdots u_{i_n}, \qquad u_{i_j} \in \mathcal{A}$$

Notación 2.1.4. Se denotará por $\mathcal{A}^n$ a todas las palabras de longitud n y por $\mathcal{A}^*$ al conjunto que contiene a todas las palabras, es decir, $\mathcal{A}^* = \bigcup_{n\in\mathbb{N}} \mathcal{A}^n$.

Definición 2.1.5. Si $\mathcal{A} = \{a_1, \cdots, a_q\}$ es un alfabeto, un *código q-ario* sobre $\mathcal{A}$ es un subconjunto $\mathcal{C}$ de $\mathcal{A}^*$. Los elementos de $\mathcal{C}$ son llamadas palabras de código. El número $M = |\mathcal{C}|$, el cardinal de $\mathcal{C}$, es el tamaño del código.

A lo largo de este trabajo, el alfabeto con el que trabajaremos será $\mathcal{A} = \mathbb{F}_q$, donde $q = p^m$ con p un número primo.

Consideremos ahora una secuencia de información $u_0u_1u_2u_3\ldots$ donde cada u_i es un símbolo de información. Esta secuencia se agrupará en bloques con k elementos cada uno, como se muestra a continuación

$$\underbrace{u_0u_1\ldots u_{k-1}}_{\text{bloque}}\underbrace{u_ku_{k+1}\ldots u_{2k-1}}_{\text{bloque}}\cdots$$

En lo que llamaremos *códigos de bloque* (n, k) q-arios, las palabras de información estarán dadas por cada uno de los bloques que mencionamos anteriormente, es decir, las palabras de información serán

$$\begin{aligned} &u_0u_1\ldots u_{k-1}\\ &u_ku_{k+1}\ldots u_{2k-1}\\ &u_{2k}u_{2k+1}\ldots u_{3k-1}\\ &\vdots \end{aligned}$$

cada una de longitud k con $u_i \in \{0, 1, \ldots, q-1\}$ las cuales se codifican por separado en las correspondientes palabras de código

$$\begin{aligned} &b_0b_1\ldots b_{n-1}\\ &b_nb_{n+1}\ldots b_{2n-1}\\ &b_{2n}b_{2n+1}\ldots b_{3n-1}\\ &\vdots \end{aligned}$$

de longitud n con $b_i \in \{0, 1, \ldots, q-1\}$. Representaremos como $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$ y $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$ a las palabras de información y de código, respectivamente.

Observemos que el número de posibles palabras de código está dado por

$$M = q^k.$$

La longitud n de una palabra de código es mayor que la longitud k de una palabra de información.

Definición 2.1.6. La tasa a la cual se transmite la información a través del canal se reduce por la llamada *tasa de código:*

$$R = \frac{log_q(M)}{n} = \frac{k}{n}.$$

Definición 2.1.7. El *peso*, $wt(b)$, de la palabra $b = (b_0, b_1, \ldots, b_{n-1})$ se define como el número de componentes b_i no cero.

$$wt(b) = |\{i : b_i \neq 0, 0 \leq i < n\}|.$$

Definición 2.1.8. El *peso mínimo* de un código de bloque $\mathcal{C}$ se define como

$$\min_{\forall b \neq 0} wt(b).$$

Una definicíon importante es la distancia mínima de Hamming.

Definición 2.1.9. La *Distancia de Hamming*, *dist(b,b')* entre dos palabras de código b y *b'*, ambas de longitud n, proporciona el número de componentes diferentes de b y *b'*.

$$dist(b, b') = |\{i : b_i \neq b_i', 0 \leq i < n\}|$$

Definición 2.1.10. Para un código $\mathcal{C}$ con M palabras de código, la *distancia mínima de Hamming* está dada por

$$d = \min_{\forall b \neq b'} dist(b, b').$$

La distancia mínima de Hamming de un código está completamente relacionada con las capacidades de detección y corrección de errores del código. Respecto a esto, se presentan los siguientes resultados

Teorema 2.1.11 ([17] Teorema 2.5.6)**.** Sea $\mathcal{C}$ un código con distancia mínima de Hamming d. El código $\mathcal{C}$ detecta exactamente $d-1$ errores.

Demostración. Sea $b \in \mathcal{C}$ una palabra de código transmitida, cuya palabra recibida sea r. Se sabe que r puede diferir de b. Si $dist(b, r) < d$, entonces $r \notin \mathcal{C}$, esto quiere decir que el código $\mathcal{C}$ puede detectar $d-1$ errores. ■

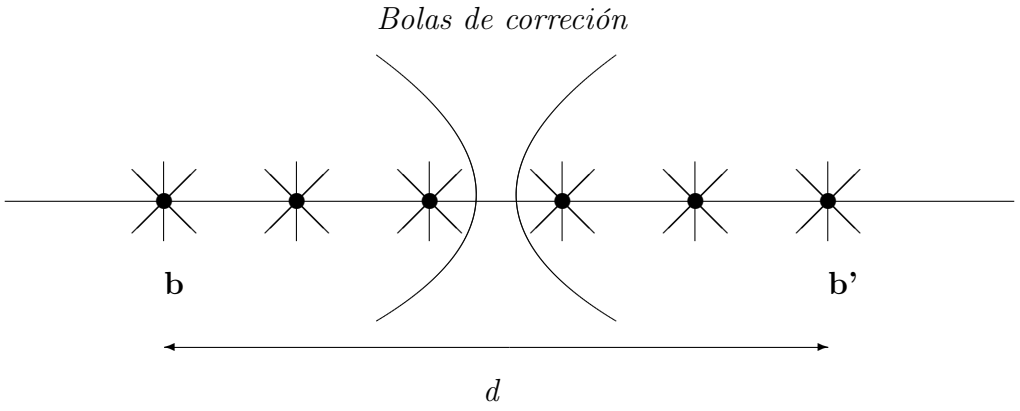


Figura 2.2: Bola de correción

Para el análisis de la capacidad de correción de errores de un código $\mathcal{C}$ con distancia de Hamming *dist* y distancia mínima de Hamming d, se define la *bola de corrección* para cada palabra de código b como:

$$H_r(b) = \{b' \in \mathcal{C} : dist(b, b') \leq r\}$$

Según el radio de las bolas de corrección, además de la palabra de código b, todas las palabras que difieren en $1, 2, \ldots, r$ componentes de b, son elementos de la bola de corrección correspondiente. Podemos decodificar de forma única todos los elementos de una bola de corrección en la palabra de código correspondiente b, siempre que las bolas de corrección no se intersecten. La condición se satisface si $r < \frac{d}{2}$.

Teorema 2.1.12 ([17], Teorema 2.5.10)**.** Sea $\mathcal{C}$ un código con distancia mínima de Hamming d. El número máximo de errores corregibles por el código $\mathcal{C}$ es

$$\lfloor \frac{d-1}{2} \rfloor.$$

Demostración. Suponga que b es una secuencia de información que se transmite a través del canal, recibiendo una secuencia de información r que difiere de b. Suponga que no se producen más de $\lfloor \frac{d-1}{2} \rfloor$ errores.

Consideremos el conjunto de 2^k esferas de radio $\lfloor \frac{d-1}{2} \rfloor$ con centro en las palabras de código en $\mathcal{C}$. Dada la definición de d, las esferas no se intersectan. Por tanto, r pertenece sólo a una esfera, aquella que tiene como centro a b. Así, el decodificador busca la esfera a la que pertenece r, y muestra el centro de la esfera como el vector decodificado. Se observa que, cuando el número de errores es a lo más $\lfloor \frac{d-1}{2} \rfloor$, el procedimiento proporciona la respuesta correcta. Además, el número máximo de errores que el código puede corregir es $\lfloor \frac{d-1}{2} \rfloor$. Sean $a, b \in \mathcal{C}$ tal que $dist(a, b) = d$. Sea también un vector u tal que $dist(a, u) = 1 + \lfloor \frac{d-1}{2} \rfloor$ y $dist(b, u) = d - 1 - \lfloor \frac{d-1}{2} \rfloor$. Se cumple que

$$dist(b, u) = d - 1 - \lfloor \frac{d-1}{2} \rfloor = \lfloor d - 1 - \frac{d-1}{2} \rfloor = \lfloor \frac{d-1}{2} \rfloor \leq 1 + \lfloor \frac{d-1}{2} \rfloor = dist(a, u).$$

Entonces si se transmite a y se recibe u, es decir, ocurren $1+\lfloor\frac{d-1}{2}\rfloor$ errores, el decodificador no puede concluir que la palabra transmitida era a, ya que la palabra de código b es al menos tan cercana a u como a. ■

Definición 2.1.13. Se define $\mathcal{C}(n,k,d)$ como el conjunto de códigos de bloque (n,k) $\mathcal{C} = \{b_1, b_2, \ldots, b_M\}$ donde $M = q^k$, con palabras de código de longitud n y distancia mínima de Hamming d.

Una definición indispensable en Teoría de códigos es la de códigos lineales, la cual se presenta a continuación.

Definición 2.1.14. Un código de bloque $\mathcal{C} \in \mathcal{C}(n,k,d)$ sobre el campo finito $\mathbb{F}_q$, donde $q = p^m$ con p un número primo, es llamado *lineal* si $\mathcal{C}$ es un subespacio de dimensión k del espacio vectorial $\mathbb{F}_q^n$.

La propiedad de linealidad de un código de bloque lineal en $\mathcal{C}(n,k,d)$ se puede utilizar para codificar de forma eficiente una palabra de información dada u=$(u_0, u_1, \ldots, u_{k-1})$. Tomemos una base $\{g_0, g_1, \ldots, g_{k-1}\}$ del subespacio $\mathcal{C}$, donde cada $g_i = (g_{i,0}, g_{i,1}, \ldots, g_{i,n-1})$ es un vector n-dimensional, con $0 \leq i \leq k-1$. La correspondiente palabra de código $b = (b_0, b_1, \ldots, b_{n-1})$ se puede escribir como

$$b = u_0 g_0 + u_1 g_1 + \cdots + u_{k-1} g_{k-1}$$

donde $u_i \in \mathbb{F}_q$.

Ejemplo 2.1.15. Consideremos al campo $\mathbb{F}_2$ y $n = 4$. Con dichos datos, se tiene el espacio vectorial $\mathbb{F}_2^4 = \{a_0a_1a_2a_3 : a_i \in \mathbb{F}_2, i = 0,1,2,3.\}$. Consideremos además el código $\mathcal{C}$ generado por $\{1010, 0101\}$.

Observemos que $\mathcal{C}$ es un código $(4,2)$ binario, más aún

$$\mathcal{C} = \{0000, 1010, 0101, 1111\}.$$

Utilizando este código, dada una secuencia de información, esta se puede codificar de acuerdo con el esquema mostrado en la Figura 2.1. Por ejemplo, la secuencia de información 1100100110 se agrupa en bloques con 2 elementos cada uno, es decir

$$\begin{array}{c} 11 \\ 00 \\ 10 \\ 01 \\ 10 \end{array}$$

Cada palabra de información se codifica por separado, por lo que

$$\begin{array}{rcl} 11 & \rightarrow & 1 \cdot 1010 + 1 \cdot 0101 = 1111 \\ 00 & \rightarrow & 0 \cdot 1010 + 0 \cdot 0101 = 0000 \\ 10 & \rightarrow & 1 \cdot 1010 + 0 \cdot 0101 = 1010 \\ 01 & \rightarrow & 0 \cdot 1010 + 1 \cdot 0101 = 0101 \\ 10 & \rightarrow & 1 \cdot 1010 + 0 \cdot 0101 = 1010 \end{array}$$

es decir, las correspondientes palabras de código son

$$\begin{array}{c} 1111 \\ 0000 \\ 1010 \\ 0101 \\ 1010 \end{array}$$

cada una de longitud 4. Con esto, se obtiene la secuencia final ya codificada 11110000101001011010.

Por otro lado,

$$\begin{array}{c} dist(0000, 1010) = 2 \\ dist(0000, 0101) = 2 \\ dist(0000, 1111) = 4 \\ dist(1010, 0101) = 4 \\ dist(1010, 1111) = 2 \\ dist(0101, 1111) = 2. \end{array}$$

Esto muestra que la distancia mínima de Hamming del código $\mathcal{C}$ es $d = 2$.

Definición 2.1.16. Sea $\mathcal{C}$ un código lineal de longitud n sobre $\mathbb{F}_q$, su código dual euclideano se define por

$$\mathcal{C}^{\perp} = \{x \in \mathbb{F}_q^n : (x, y) = xy^T = 0 \text{ para todo } y \in \mathcal{C}\}$$

donde y^T denota el vector transpuesto de $y = (y_1, y_2, \ldots, y_n)$.

La dimensión k de un código lineal juega un papel importante en la detección y correción de errores a través de la tasa de código, por lo que presentamos el siguiente resultado:

Teorema 2.1.17. *Teorema de Shannon.* Dado un código con tasa de código R menor a la capacidad C del canal de comunicación, entonces existe un bloque de código de longitud n con tasa de código R que se puede transmitir por el canal con una probabilidad de error arbitrariamente pequeña.

La capacidad del canal es un número que se obtiene de acuerdo a las características de dicho canal, para mayor información se puede consultar [1].

La tasa de código es la relación entre la cantidad de datos de información y datos totales transmitidos en las palabras de código. Una alta tasa de código significa que el contenido de información es alto y la carga de codificación es baja. Sin embargo, cuantos menos bits se utilicen para codificar redundancia, menos protección de error se proporciona. Se debe hacer una compensación entre la disponibilidad de ancho de banda del canal de transmisión y la cantidad de protección de error requerida para la comunicación.

Definición 2.1.18. Un código lineal $\mathcal{C}$ es un código lineal con dual complementario *(LCD)* si $\mathcal{C} \bigcap \mathcal{C}^{\perp} = \{0\}$, o de forma equivalente $\mathbb{F}_q^n = \mathcal{C} \bigoplus \mathcal{C}^{\perp}$.

Definición 2.1.19. Un código lineal $\mathcal{C}$ se llama *reversible* si $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ implica que $(c_{n-1}, c_{n-2}, \cdots, c_0) \in \mathcal{C}$.

2.2. Códigos cíclicos

En general es difícil decodificar un código de bloque lineal arbitrario, aunque hacen posible implementar una codificación eficaz, razón por la cual trabajaremos con una clase importante de los códigos lineales, pues permiten definir un algoritmo de decodificación algebraica más eficiente.

Definición 2.2.1. Un *código cíclico* es un código de bloque lineal $\mathcal{C}$ en $\mathcal{C}(n, k, d)$ con la propiedad adicional que para cada palabra de código

$$\mathbf{b} = (b_0, b_1, \ldots, b_{n-2}, b_{n-1})$$

todas las palabras desplazadas cíclicamente

$$\begin{array}{l}(b_{n-1}, b_0, \ldots, b_{n-3}, b_{n-2}) \\ (b_{n-2}, b_{n-3}, \ldots, b_{n-4}, b_{n-3}) \\ \vdots \\ (b_2, b_3, \ldots, b_0, b_1) \\ (b_1, b_2, \ldots, b_{n-1}, b_0)\end{array}$$

son palabras de código que pertenecen a $\mathcal{C}$.

Ejemplo 2.2.2. Considerando el código del Ejemplo 2.1.15. Se tienen las palabras de código

$$\begin{array}{c}1111 \\ 0000 \\ 1010 \\ 0101 \\ 1010\end{array}$$

Notemos que al desplazar cíclicamente a 1111 y 0000, obtenemos la misma palabra de código y así, pertenecen a $\mathcal{C}$.

Los desplazamientos cíclicos de 1010 son 0101 y la misma palabra de código 1010, ambas pertenecientes a $\mathcal{C}$. De manera similar, los desplazamientos cíclicos de 0101 pertenecen a $\mathcal{C}$, concluyendo así que dicho código lineal es además un código cíclico.

2.2.1. Construcción de códigos cíclicos a partir de un ideal

Los códigos cíclicos tienen una estrecha relación con los ideales de un anillo construido a partir de polinomios. Para establecer esta ralación se definen las siguientes funciones

$$\varphi : \mathbb{F}_q^n \to \mathbb{F}_q[x],$$

dada por,

$$\varphi(b_0, \ldots, b_{n-1}) = b_0 + b_1 x + \cdots + b_{n-2} x^{n-2} + b_{n-1} x^{n-1}.$$

y,

$$\pi : \mathbb{F}_q[x] \to \mathbb{F}_q[x]/\langle x^n - 1\rangle$$

dada por,

$$\pi(f(x)) = [f(x)],$$

donde $[f(x)]$ representa la clase de equivalencia de $f(x)$.

Teorema 2.2.3. La función

$$\pi \circ \varphi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/\langle x^n - 1\rangle$$

es una transformación lineal. Si $\mathcal{C}$ es un código cíclico, entonces $(\pi \circ \varphi)(\mathcal{C})$ es un ideal. Más aún, $\pi \circ \varphi|_{\mathcal{C}} : \mathcal{C} \to (\pi \circ \varphi)(\mathcal{C})$ es un isomorfismo de espacios vectoriales.

El teorema anterior nos da la opción de trabajar indistintamente con elementos en $\mathcal{C}$ o con la correspondiente clase de equivalencia de $c(x)$.

Teorema 2.2.4. Sea I un ideal no cero de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. El conjunto

$$\left\{(a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n : [a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}] \in I\right\}$$

es un código cíclico.

Teorema 2.2.5. Sea I un ideal no cero de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Existe un único polinomio mónico $g(x) \in \mathbb{F}_q[x]$ de grado r tal que,

1. $I = \langle g(x)\rangle/\langle x^n - 1\rangle$.
2. $g(x)$ divide a $x^n - 1$.

Además, si $\mathcal{C}$ es el código cíclico lineal correspondiente a I, entonces la dimensión de $\mathcal{C}$ es $n - r$.

Definición 2.2.6. Sea $\mathcal{C} = \langle g(x)\rangle$ un código cíclico, donde $g(x)$ es mónico y tiene el grado más pequeño entre todos los generadores de $\mathcal{C}$. Al polinomio $g(x)$ se le llama *polinomio generador* del código cíclico $\mathcal{C}$.

Teorema 2.2.7. [20, Teorema 4.2.1] Sea $\mathcal{C}$ un código cíclico no cero sobre $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Existe un polinomio $g(x) \in \mathcal{C}$ tal que

1. $g(x)$ es el único polinomio mónico de grado mínimo en $\mathcal{C}$.
2. $\mathcal{C} = \langle g(x)\rangle$.
3. $g(x)\,|(x^n - 1)$.

Ejemplo 2.2.8. Considerando nuevamente el código del Ejemplo 2.1.15. Se tienen que

$$\mathcal{C} = \{1111, 0000, 1010, 0101\}$$

Aplicando la función $\varphi : \mathbb{F}_2^4 \to \mathbb{F}_q[x]$ presentada anteriormente, a cada palabra de código del código $\mathcal{C}$, se obtiene

$$\begin{aligned}
&\varphi(1111) = 1 + x + x^2 + x^3 = (x+1)(1+x^2),\\
&\varphi(0000) = 0,\\
&\varphi(1010) = 1 + x^2,\\
&\varphi(0101) = x + x^3 = x(1+x^2).
\end{aligned}$$

Apliquemos ahora la función $\pi : \mathbb{F}_q[x] \to \mathbb{F}_2[x]/\langle x^4 - 1\rangle$ a la imagen de cada palabra de código bajo la función φ mostradas arriba, obteniendo

$$\begin{aligned}
&\pi(1 + x + x^2 + x^3) = [1 + x + x^2 + x^3] = [x+1][1+x^2]\\
&\pi(0) = [0]\\
&\pi(1 + x^2) = [1 + x^2]\\
&\pi(x + x^3) = [x + x^3] = [x][1+x^2]
\end{aligned}$$

Del Teorema 2.2.3, y puesto que el código $\mathcal{C}$ dado es un código cíclico, se concluye que $(\pi \circ \varphi)(\mathcal{C}) = \langle [x^2 + 1]\rangle$ es un ideal.

Por otro lado, el Teorema 2.2.7 nos garantiza que existe el polinomio generador $g(x)$ del código cíclico $\mathcal{C}$, en este caso $g(x) = 1 + x^2$.

Capítulo 3

Códigos $\mathcal{BCH}$

Los códigos $\mathcal{BCH}$ son una clase importante de códigos cíclicos. Estos códigos hacen posible derivar un algoritmo de decodificación algebraico eficiente.

3.1. Ceros de un código cíclico

Se sabe que un código cíclico $\mathcal{C}$ en $\mathcal{C}(n, k, d)$ sobre el campo finito $\mathbb{F}_q$ queda definido por el polinomio generador $g(x)$, según el Teorema 2.2.7, dicho polinomio es único y es divisor del polinomio $x^n - 1$, por lo que

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

Nos interesa encontrar los factores del polinomio $x^n - 1$ sobre $\mathbb{F}_q$. El estudio de los códigos cíclicos se ha centrado en el caso en el que el polinomio no tiene factores repetidos, por esta razón se supondrá que el polinomio $x^n - 1$ tiene sólo ceros simples, lo que es equivalente a la condición (Mc Eliece, 1987)

$$mcd(q, n) = 1$$

es decir, la cardinalidad del campo finito $\mathbb{F}_q$ y la longitud de la palabra de código son primos relativos.

El Teorema 1.4.12, nos garantiza que existe una raíz primitiva de la unidad de orden n, α en un campo de descomposición adecuado $\mathbb{F}_{q^l}$ donde l es el número más pequeño tal que $q^l \equiv 1 \mod n$, $\alpha^n = 1$ y $\alpha^r \neq 1$ para $r < n$. En el campo de extensión se cumple que $n|q^l - 1$. Los n ceros del polinomio $x^n - 1$ están dados por 1, α, α^2, ..., α^{n-1}, por lo que se puede factorizar como

$$x^n - 1 = (x - 1)(x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{n-1}) \tag{3.1.1}$$

Del Teorema 2.2.7, el polinomio generador $g(x)$ divide al polinomio $x^n - 1$, así $g(x)$ se puede definir con un conjunto de ceros α^{i_1}, α^{i_2}, ..., $\alpha^{i_{n-k}}$, por lo que

$$g(x) = (x - \alpha^{i_1})(x - \alpha^{i_2}) \cdots (x - \alpha^{i_{n-k}}). \tag{3.1.2}$$

Los coeficientes de este deben ser elementos de $\mathbb{F}_q$ por lo que no todas las opciones de α^{i_j} son posibles.

A continuación se presentan condiciones para que $g(x) \in \mathbb{F}_q[x]$:

Definición 3.1.1. La *clase lateral q-ciclotómica* de i es el conjunto de exponentes i, iq, iq^2, ... de la raíz primitiva de la unidad de orden n, $\alpha \in \mathbb{F}_{q^l}$. Se denota y define como

$$C_i = \{iq^j \mod (q^l - 1) : 0 \leq j \leq l - 1\}.$$

Definición 3.1.2. Al elemento más pequeño de C_i se le llama *líder de clase lateral*.

Observación 3.1.3. En adelante, cuando se dice que i *es líder de clase lateral* , significa que i es líder de su clase lateral C_i.

Teorema 3.1.4. Sea n un entero positivo tal que es primo relativo con q. Sea $t = ord_n(q)$. Sea α una raíz primitiva de la unidad de orden n en $\mathbb{F}_{q^t}$.

1. Para cada entero s, con $0 \leq s \leq n$, el polinomio mínimo 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 lateral q-ciclotómica de s módulo n.

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

Ahora, como $g(x) \in \mathbb{F}_q[x]$, entonces los coeficientes polinomiales deben ser elementos de $\mathbb{F}_q$ y dada su representación en 3.1.2, no todas las opciones de α^{i_j} son posibles. El Teorema 3.1.4, nos garantiza que las conjugadas de α^i son α^{iq}, α^{iq^2}, ..., además, estas son también ceros del polinomio generador $g(x)$. El producto de todos los factores lineales respectivos genera al polinomio mínimo

$$m_i(x) = (x - \alpha^i)(x - \alpha^{iq})(x - \alpha^{iq^2}) \ldots \tag{3.1.3}$$

con coeficientes en $\mathbb{F}_q$.

Ejemplo 3.1.5. Consideremos el campo finito $\mathbb{F}_2$, con $n = 7$. Queremos factorizar el polinomio $x^7 - 1 = x^7 + 1$ sobre $\mathbb{F}_2$.

Primero buscamos el entero más pequeño l, tal que $7 | \left(2^l - 1\right)$, el cual es $l = 3$. Se satisface que $\mathbb{F}_{2^3}$ contiene una raíz primitiva de la unidad de orden 7, α, además es el campo de extensión más pequeño de $\mathbb{F}_2$ que contiene todas las raíces de $x^7 - 1 = x^7 + 1$. Como $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$, podemos suponer que $\alpha^3 + \alpha + 1 = 0$. Los polinomios mínimos satisfacen 3.1.3, de modo que el primer polinomio mínimo es:

$$m_0(x) = x + 1$$

Para el segundo polinomio mínimo, se satisface

$$\begin{aligned} m_1(x) &= (x - \alpha)(x - \alpha^2)(x - \alpha^4) \\ &= x^3 - x^2\alpha(\alpha^3 + \alpha + 1) + x(\alpha^6 + \alpha^5 + \alpha^3) + 1 \end{aligned}$$

Puesto que α es una raíz primitiva de la unidad de orden 7, satisface que $\alpha^7 = 1$, o bien, $\alpha^7 - 1 = 0$. Se cumple que

$$\alpha^7 - 1 = (\alpha - 1)(\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)$$

y puesto que $\alpha \neq 1$, se sigue que $\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$. De aquí

$$\begin{aligned} \alpha^6 + \alpha^5 + \alpha^3 &= \alpha^4 + \alpha^2 + \alpha + 1 \\ &= \alpha(\alpha^3 + \alpha + 1) + 1 \\ &= 1. \end{aligned}$$

Así, el segundo polinomio mínimo toma la forma

$$m_1(x) = x^3 + x + 1.$$

Consideremos ahora α^3 para derivar el tercer polinomio mínimo. Sustituyendo en 3.1.3,

$$\begin{aligned} m_2(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12}) \\ &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^5) \\ &= x^3 + \alpha^3(\alpha^3 + \alpha^2 + 1)x^2 + \alpha(\alpha^3 + \alpha + 1)x + 1 \\ &= x^3 + x^2 + 1 \end{aligned}$$

Por lo tanto,

$$x^7 - 1 = m_0(x)m_1(x)m_2(x).$$

Por otro lado, las clases laterales ciclotómicas están dadas por:

$$C_i = \{i2^j \mod 7 : 0 \leq j \leq 2\}.$$

Así,

$$C_0 = \{0\}.$$

$$C_1 = \{2^j \mod 7 : 0 \leq j \leq 2\} = \{1 \mod 7, 2 \mod 7, 4 \mod 7\} = \{1, 2, 4\}.$$

$$C_3 = \{3 \cdot 2^j \mod 7 : 0 \leq j \leq 2\} = \{3 \mod 7, 6 \mod 7, 12 \mod 7\} = \{3, 6, 5\}.$$

Como cada polinomio mínimo es único, entonces el polinomio generador se puede construir utilizando los polinomios mínimos correspondientes, es decir

$$g(x) = mcm(m_{i_1}(x), m_{i_2}(x), \ldots, m_{i_{n-k}}(x))$$

Definición 3.1.6. Sea $\mathcal{C}$ un código cíclico. Al conjunto $T = \bigcup_i C_i$, la unión de las clases laterales q-ciclotómicas, se le llama *conjunto de definición* de $\mathcal{C}$.

Ejemplo 3.1.7. Consideremos de nuevo al polinomio $x^7 - 1 \in \mathbb{F}_2[x]$. Los códigos cíclicos que se pueden obtener a partir de dicho polinomio se enlistan a continuación.

En el ejemplo 3.1.5 encontramos los polinomios mínimos de $x^7 - 1$. Con ayuda de dichos polinomios generamos los códigos cíclicos.

1. $g(x) = x + 1$, $\mathcal{C}_2 = \langle x + 1 \rangle$ y $T_2 = \{0\}$.
2. $g(x) = x^3 + x + 1$, $\mathcal{C}_3 = \langle x^3 + x + 1 \rangle$, y $T_3 = \{1, 2, 4\}$.
3. $g(x) = x^3 + x^2 + 1$, $\mathcal{C}_4 = \langle x^3 + x^2 + 1 \rangle$ y $T_4 = \{3, 5, 6\}$.
4. $g(x) = (x+1)(x^3+x+1) = x^4+x^3+x^2+1$, $\mathcal{C}_5 = \langle x^4+x^3+x^2+1 \rangle$ y $T_5 = \{0, 1, 2, 4\}$.
5. $g(x) = (x+1)(x^3+x^2+1) = x^4+x^2+x+1$, $\mathcal{C}_6 = \langle x^4+x^2+x+1 \rangle$ y $T_6 = \{0, 3, 6, 5\}$.
6. $g(x) = (x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, $\mathcal{C}_7 = \langle x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \rangle$ y $T_7 = \{1, 2, 3, 4, 5, 6\}$.
7. $g(x) = (x+1)(x^3+x+1)(x^3+x^2+1) = x^7+1$, $\mathcal{C}_8 = \langle z^7+1 \rangle$ y $T_8 = \{0, 1, 2, 3, 4, 5, 6\}$. Es importante señalar que en este caso, $\mathcal{C}_8$ es el ideal cero en el anillo cociente $\mathbb{F}_2[x] \backslash \langle x^7 - 1 \rangle$.

Consideramos también el polinomio $g(x) = 1$, por lo que $\mathcal{C}_1 = \langle 1 \rangle = \mathbb{F}_2[x] \backslash \langle x^7 - 1 \rangle$ y $T_1 = \emptyset$, dicho código se puede analizar sin usar esta teoría pues la obtención de los polinomios mínimos se realiza tomando en cuenta que $g(x) \neq 1$.

Todos los códigos cíclicos anteriores tienen longitud $n = 7$.

Es importante señalar que las características del código cíclico $\mathcal{C}(n, k, d)$ y de su respectivo polinomio generador $g(x)$ quedan completamente determinadas por la clase lateral ciclotómica y los polinomios mínimos, respectivamente.

Teorema 3.1.8. [20, Teorema 4.4.2] Sea α una raíz primitiva de unidad de orden n en algún campo de extensión de $\mathbb{F}_q$. Sea $\mathcal{C}$ un código cíclico de longitud n sobre $\mathbb{F}_q$ con conjunto de definición T y polinomio generador $g(x)$. Se cumple lo siguiente:

1. T es la unión de clases laterales ciclotómicas módulo n.
2. $g(x) = \prod_{i \in T}(x - \alpha^i)$.
3. $c(x) \in \mathbb{F}_q[x]/\langle x^n - 1 \rangle$ está en $\mathcal{C}$ si y sólo si $c(\alpha^i) = 0$ para toda $i \in T$.
4. La dimensión de $\mathcal{C}$ es $n - |T|$.

Ejemplo 3.1.9. Aplicando el inciso 4 del Teorema anterior a los códigos cíclicos obtenidos en el Ejemplo 3.1.7, se obtienen los resultados mostrados en la Tabla 3.1.1

3.2. Límite $\mathcal{BCH}$ y definición de códigos $\mathcal{BCH}$

Bose, Ray-Chaudhai y Hocquenghem derivaron una cota inferior para la distancia mínima de Hamming de un código cíclico $\mathcal{C}(\alpha_1, \alpha_2, \ldots, \alpha_{n-k})$ basado en los ceros $\alpha_1, \alpha_2, \ldots, \alpha_{n-k}$ del polinomio generador $g(x)$. Dicha cota inferior se presenta en el siguiente resultado:

$\mathcal{C}_i$	Dimensión de $\mathcal{C}_i$
$\mathcal{C}_1$	$7 - \lvert T_1\rvert = 7 - 0 = 7$
$\mathcal{C}_2$	$7 - \lvert T_2\rvert = 7 - 1 = 6$
$\mathcal{C}_3$	$7 - \lvert T_3\rvert = 7 - 3 = 4$
$\mathcal{C}_4$	$7 - \lvert T_4\rvert = 7 - 3 = 4$
$\mathcal{C}_5$	$7 - \lvert T_5\rvert = 7 - 4 = 3$
$\mathcal{C}_6$	$7 - \lvert T_6\rvert = 7 - 4 = 3$
$\mathcal{C}_7$	$7 - \lvert T_7\rvert = 7 - 6 = 1$
$\mathcal{C}_8$	$7 - \lvert T_8\rvert = 7 - 7 = 0$

Tabla 3.1.1

Teorema 3.2.1. Sea $\mathcal{C}(\alpha_1, \alpha_2, \ldots, \alpha_{n-k})$ un código cíclico de longitud n sobre $\mathbb{F}_q$ con distancia mínima de Hamming d. Sea $\alpha \in \mathbb{F}_{q^{ord_n(q)}}$ una raíz de la unidad de orden n. Si el código cíclico incorpora $\delta - 1$ ceros sucesivos α^b, α^{b+1}, α^{b+2}, …, $\alpha^{b+\delta-2}$ del polinomio generador $g(x)$, entonces $d \geq \delta$.

Demostración. Sea $s(x)$ un polinomio de código de $\mathcal{C}$. Como $g(x)|s(x)$, por lo supuesto, $s(\alpha^b) = s(\alpha^{b+1}) = s(\alpha^{b+2}) = \ldots, s(\alpha^{b+\delta-2}) = 0$. Por lo visto en la Sección 2.2.1, $s(x) = s_0 + s_1 x + \cdots + s_{n-2}x^{n-2} + s_{n-1}x^{n-1}$. Se obtiene el siguiente sistema de ecuaciones:

$$\begin{array}{lllll}
s_0 & +s_1\alpha^{b} & +s_2\alpha^{b2} & +\cdots & +s_{n-2}\alpha^{b(n-2)} & +s_{n-1}\alpha^{b(n-1)} & = 0 \\
s_0 & +s_1\alpha^{b+1} & +s_2\alpha^{(b+1)2} & +\cdots & +s_{n-2}\alpha^{(b+1)(n-2)} & +s_{n-1}\alpha^{(b+1)(n-1)} & = 0 \\
s_0 & +s_1\alpha^{b+2} & +s_2\alpha^{(b+2)2} & +\cdots & +s_{n-2}\alpha^{(b+2)(n-2)} & +s_{n-1}\alpha^{(b+2)(n-1)} & = 0 \\
\vdots & & & & & & \\
s_0 & +s_1\alpha^{b+\delta-2} & +s_2\alpha^{(b+\delta-2)2} & +\cdots & +s_{n-2}\alpha^{(b+\delta-2)(n-2)} & +s_{n-1}\alpha^{(b+\delta-2)(n-1)} & = 0
\end{array}$$

cuya representación matricial es la siguiente

$$\begin{pmatrix}
1 & \alpha^{b} & \alpha^{b2} & \cdots & \alpha^{b(n-1)} \\
1 & \alpha^{b+1} & \alpha^{(b+1)2} & \cdots & \alpha^{(b+1)(n-1)} \\
1 & \alpha^{b+2} & \alpha^{(b+2)2} & \cdots & \alpha^{(b+2)(n-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha^{b+\delta-2} & \alpha^{(b+\delta-2)2} & \cdots & \alpha^{(b+\delta-2)(n-1)}
\end{pmatrix}
\begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ \vdots \\ s_{n-1} \end{pmatrix} =
\begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Consideremos el determinante de la matriz $(\delta-1)\times(\delta-1)$ la cual consiste de las primeras $\delta - 1$ columnas. Se obtiene [13]:

$$\begin{vmatrix}
1 & \alpha^{b} & \alpha^{b2} & \cdots & \alpha^{b(n-2)} \\
1 & \alpha^{b+1} & \alpha^{(b+1)2} & \cdots & \alpha^{(b+1)(n-2)} \\
1 & \alpha^{b+2} & \alpha^{(b+2)2} & \cdots & \alpha^{(b+2)(n-2)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha^{b+\delta-2} & \alpha^{(b+\delta-2)2} & \cdots & \alpha^{(b+\delta-2)(n-2)}
\end{vmatrix} =
\begin{vmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \alpha^{1} & \alpha^{2} & \cdots & \alpha^{\delta-2} \\
1 & \alpha^{2} & \alpha^{4} & \cdots & \alpha^{2(\delta-2)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha^{\delta-2} & \alpha^{(\delta-2)2} & \cdots & \alpha^{(\delta-2)(\delta-2)}
\end{vmatrix}
\alpha^{b(\delta-1)(\delta-2)/2}$$

El resultado del determinante de la matriz que se obtuvo del lado derecho de la igualdad corresponde a la matriz de Vandermonde, el cual es distinto de cero. Además, $\alpha^{b(\delta-1)(\delta-2)/2} \neq 0$, con esto, la matriz $(\delta-1)\times(\delta-1)$ la cual consiste de las primeras $\delta-1$ columnas tiene determinante distinto de cero, es decir, es una matriz no singular. Puesto que $s(x)$ tiene al menos d componentes distintos de cero, entonces $d \geq \delta$. ■

Observación 3.2.2. Los Teoremas 2.1.11 y 2.1.12 nos garantizan que la capacidad de un código $\mathcal{C}$ de detectar y corregir errores depende de la distancia mínima de Hamming del código, presentado el Teorema anterior se concluye que si el valor de δ es grande, entonces el código ciclico $\mathcal{C}$ tiene una capacidad de detectar y corregir un mayor número de errores.

Ejemplo 3.2.3. Apliquemos el resultado anterior a los códigos cíclicos obtenidos en el Ejemplo 3.1.7. El conjunto de definición de cada código cíclico nos indica si tiene raíces consecutivas.

$\mathcal{C}_i$	b	δ	d_i
$\mathcal{C}_1$			
$\mathcal{C}_2$			
$\mathcal{C}_3$	1	3	$d_3 \geq 3$
$\mathcal{C}_4$	5	3	$d_4 \geq 3$
$\mathcal{C}_5$	0	3	$d_5 \geq 3$
$\mathcal{C}_6$	5	3	$d_6 \geq 3$
$\mathcal{C}_7$	1	7	$d_7 \geq 7$
$\mathcal{C}_8$	0	8	$d_8 \geq 8$

Observemos que para la distancia mínima de Hamming de cualquier código cíclico de longitud 7 debe ser menor o igual a 7, de modo que $d_7 = 7$ y para d_8 no es posible.

Definición 3.2.4. Al parámetro δ establecido en el límite $\mathcal{BCH}$ se le llama *distancia de diseño* del código cíclico.

Finalmente se definen los códigos $\mathcal{BCH}$.

Definición 3.2.5. Al código cíclico sobre el campo finito $\mathbb{F}_q$ definido con una distancia mínima de Hamming d con $d \geq \delta$, preescribiendo $\delta-1$ potencias sucesivas α^b, α^{b+1}, α^{b+2}, $\ldots$, $\alpha^{b+\delta-2}$ de una raíz apropiada, α, de la unidad de orden n como ceros del polinomio generador $g(x)$, se le denomina *código* $\mathcal{BCH}$ y se denota por $\mathcal{C}(\alpha^b, \alpha^{b+1}, \alpha^{b+2}, \ldots, \alpha^{b+\delta-2})$.

Ejemplo 3.2.6. Dada la definición de códigos $\mathcal{BCH}$ y obtenidos los valores de δ en el Ejemplo 3.2.3, se obtienen los siguientes códigos $\mathcal{BCH}$.

Con $\delta = 3$:

1. $\mathcal{C}(\alpha, \alpha^2)$.
2. $\mathcal{C}(\alpha^5, \alpha^6)$.
3. $\mathcal{C}(1, \alpha)$.

Con $\delta = 7$, se obtiene $\mathcal{C}(\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$.

3.3. Propiedades sobre códigos $\mathcal{BCH}$

Podemos dar una definición de los códigos $\mathcal{BCH}$ basada en el conjunto de definición, la cual se enuncia a continuación.

Teorema 3.3.1. Sea δ un entero con $2 \leq \delta \leq n$. Un código $\mathcal{BCH}$, $\mathcal{C} \in \mathcal{C}(n, q, \delta, b)$ sobre $\mathbb{F}_q$, de longitud n y distancia de diseño δ. $\mathcal{C}$ tiene conjunto de definición

$$T = C_b \cup C_{b+1} \cup \cdots \cup C_{b+\delta-2} \tag{3.3.1}$$

donde C_i es la clase lateral ciclotómica que contiene i.

Si $b = 1$, $\mathcal{C}$ es un código $\mathcal{BCH}$ de sentido estrecho, y de sentido no estrecho en cualquier otro caso. Además, si $n = q^m - 1$, $\mathcal{C}$ se llama primitivo, y se llama no primitivo en caso contrario, pero si $n = q^m + 1$, entonces $\mathcal{C}$ se llama antiprimitivo.

Observación 3.3.2. Como se muestra en [4] y [12], todos los códigos $\mathcal{BCH}$ antiprimitivos son códigos lineales con código dual complementario, es decir, son códigos LCD.

Teorema 3.3.3. [20, Teorema 4.1.4] El tamaño de cada clase lateral q-ciclotómica es un divisor de $ord_n(q)$.

Los siguientes resultados muestran cotas inferiores en la dimensión de los códigos $\mathcal{BCH}$.

Proposición 3.3.4. Sea k la dimensión de $\mathcal{C} \in \mathcal{C}(n, q, \delta, b)$. Entonces

1. $k \geq n - ord_n(q)(\delta - 1)$
2. Si $q = 2$, $b = 1$ y δ es impar, entonces $k \geq n - ord_n(q)(\delta - 1)/2$.

Demostración. Como el conjunto de definición de un código $\mathcal{BCH}$ con distancia de diseño δ es la unión de a lo más $\delta - 1$ clases laterales ciclotómicas, cada una, por el Teorema 3.3.3, tiene tamaño a lo más $ord_n(q)$. Por lo tanto, la dimensión del código satisface $k \leq n - ord_n(q)(\delta - 1)$.

Ahora, suponga $b = 0$ y $q = 2$. Si $\delta = 2\omega + 1$, entonces

$$T = C_1 \cup C_2 \cup \cdots \cup C_{2\omega} = C_1 \cup C_3 \cup \cdots \cup C_{2\omega-1}$$

pues $C_{2i} = C_i$. Observemos que T es la unión de a lo más $\omega = (\delta - 1)/2$ clases laterales 2-ciclotómicas de tamaño a lo más $ord_n(q)$, así $k \leq n - ord_n(q)(\delta - 1)/2$. ■

Para enunciar otra proposición importante, consideremos primero los siguientes lemas:

Lema 3.3.5. [18, Lema 8] Sea n un entero positivo y q la potencia de un número primo tal que $mcd(n, q) = 1$, $q^{\lfloor m/2 \rfloor} \leq n \leq q^m - 1$ y $m = ord_n(q)$. La clase lateral ciclotómica $C_x = \{xq^j \mod n | 0 \leq j \leq m\}$ tiene cardinalidad m para toda x en el rango $1 \leq x \leq nq^{\lceil m/2 \rceil}/(q^m - 1)$.

Lema 3.3.6. [18, Lema 9] Sea $n \geq 1$ un entero positivo y q la potencia de un número primo tal que $mcd(n,q) = 1$, $q^{\lfloor m/2 \rfloor} \leq n \leq q^m - 1$ y $m = ord_n(q)$. Si x, y son dos enteros distintos en el rango $1 \leq x, y \leq \text{mín}\{\lfloor nq^{\lceil m/2 \rceil}/(q^m-1) - 1 \rfloor, n-1\}$ tal que $x, y \not\equiv 0$ mód q, entonces las clases laterales q-arias de x y $y \mod n$, son distintas.

Proposición 3.3.7. Sea $mcd(q,n) = 1$, $q^{\lfloor m/2 \rfloor} \leq n \leq q^m - 1$ y $m = ord_n(q)$. Si $2 \leq \delta \leq \text{mín}\{nq^{\lceil m/2 \rceil}/(q^m-1), n\}$, entonces la dimensión k de $\mathcal{C} \in \mathcal{C}(n,q,\delta,1)$ es $k = n - m\lceil(\delta - 1)/(1-1/q)\rceil$.

Demostración. Sea $T = C_1 \cup C_2 \cup \cdots \cup C_{\delta-1}$ el conjunto de definición del código BCH $\mathcal{C}(n,q,\delta,1)$, el cual es una unión de a lo más $\delta - 1$ clases laterales ciclotómicas. Cuando $1 \leq x \leq \delta - 1$ es un múltiplo de q, se satisface que $C_{x/q} = C_x$, por lo que el número de clases laterales se reduce en $\lfloor(\delta-1)/q\rfloor$. Por el Lema 3.3.6, si $x, y \not\equiv 0 \mod q$ y $x \neq y$, entonces C_x y C_y son disjuntas. Luego, T es la unión de $(\delta-1) - \lfloor(\delta-1)/q\rfloor = \lceil(\delta-1)(1-1/q)\rceil$ clases laterales ciclotómicas distintas. Por el Lema 3.3.5, todas las clases laterales tienen cardinalidad m. Así, el grado del polinomio generador es $m\lceil(\delta-1)/(1-1/q)\rceil$, obteniendo que $k = n - m\lceil(\delta-1)/(1-1/q)\rceil$. ■

Lema 3.3.8. [4, Lema 15] Sea $l \geq 2$. Cada entero positivo $a \leq q^{\lfloor (l-1)/2 \rfloor} + 1$ y $a \not\equiv 0$ mód q es un líder de clase lateral y $|C_a| = 2l$. Todos los enteros positivos restantes en este rango no son líderes de clase lateral. En particular, estos C_a son pares disjuntos para todos esos $a's$.

Teorema 3.3.9. [4, Teorema 16] Sea $n = q^l + 1$ y $m = 2l$. El código $\mathcal{C} \in \mathcal{C}(q,n,\delta,0)$ tiene distancia mínima $d \geq 2(\delta - 1)$.

Algunos resultados conocidos en la dimensión de códigos $\mathcal{BCH}$, pertenecientes a $\mathcal{C}(q^m + 1, q, \delta, 1)$ y $\mathcal{C}(q^m+1, q, \delta+1, 0)$ se presentan en los siguientes dos lemas.

Lema 3.3.10. Para cualquier entero δ con $3 \leq \delta \leq q^{\lfloor (l-1)/2 \rfloor} + 3$, el código reversible $\mathcal{C} \in \mathcal{C}(q,n,\delta,0)$ tiene parámetros $[q^l + 1, q^l - 2l(\delta - 2 - \lfloor(\delta-2)/q\rfloor), d \geq 2(\delta-1)]$.

Demostración. Notemos que $0 \leq \delta - 2 \leq q^{\lfloor (l-1)/2 \rfloor} + 1$. Por el Lema 3.3.8, cada entero a con $1 \leq a \leq \delta - 2$ y $a \not\equiv 0 \mod q$ es un líder de clase lateral y todos los enteros restantes en este rango no son líderes de clase lateral. El número total de enteros a tal que $1 \leq a \leq \delta - 2$ y $a \equiv 0 \mod q$ es igual a $\lfloor(\delta-2)/q\rfloor$. De este modo, hay $\delta - 2 - \lfloor(\delta-2)/q\rfloor$ clases laterales, y según el Lema 3.3.8, cada una de cardinalidad $2l$, obteniendo así que la dimensión está dada por $q^l - 2l(\delta - 2 - \lfloor(\delta-2)/q\rfloor)$. Del Teorema 3.3.9, se obtiene que $d \geq 2(\delta-1)$. ■

Lema 3.3.11. Sea $m \geq 3$ un entero y $h = \lfloor \frac{m-1}{2} \rfloor$. Se tienen los siguientes resultados para $2 \leq \delta \leq q^{h+1}$.

1. Si $m \geq 4$ es un número entero par, entonces $\mathcal{C} \in \mathcal{C}(n,q,\delta,1)$ tiene parámetros $[q^m + 1, q^m + 1 - 2m\left(\delta - 1 - \lfloor\frac{\delta-1}{q}\rfloor\right), d \geq \delta]$ y $\mathcal{C}' \in \mathcal{C}(n,q,\delta+1,0)$ tiene parámetros $[q^m + 1, q^m - 2m\left(\delta - \lfloor\frac{\delta}{q}\rfloor\right), d \geq 2\delta]$.

2. Si $m \geq 3$ es un entero impar, para $2 \leq \delta \leq q^{h+1}$, $\mathcal{C} \in \mathcal{C}(n, q, \delta, 1)$ tiene dimensión

$$k = \begin{cases} q^m + 1 - 2m\left(\delta - 1 - \lfloor \frac{\delta-1}{q} \rfloor\right) & \text{si } \delta \leq q^{h+1} - q; \\ q^m + 1 - 2m\left(q^{h+1} - q - \lfloor \frac{\delta-1}{q} \rfloor\right) & \text{si } q^{h+1} - q \leq \delta \leq q^{h+1}; \end{cases}$$

En lo siguiente, tomamos $n = 2^m + 1$ con $m \geq 10$. Se considerarán sólo códigos $\mathcal{BCH}$ de longitud n con conjuntos de definición $T_\delta = C_1 \cup C_2 \cup \cdots \cup C_{\delta-1}$ y $T'_\delta = C_0 \cup C_2 \cup \cdots \cup C_{\delta-1}$ para δ impar, los cuales se denotan por $\mathcal{C}(n, 2, \delta, 1)$ y $\mathcal{C}(n, 2, \delta + 1, 0)$ respectivamente. Luego, $\mathcal{C}(n, 2, \delta, 1) = [n, k, d] = [n, n - |T_\delta|, d \geq \delta]$ y $\mathcal{C}(n, 2, \delta + 1, 0) = [n, k_0, d_0] = [n.n - 1 - |T'_\delta|, d_0 \geq 2\delta]$.

3.3.1. Mínima distancia de Hamming de códigos $\mathcal{BCH}$ y su relación con la criptografía

Los códigos LCD toman un papel muy importante en la implementación de protección en la seguridad de la información procesada por dispositivos sensibles, de forma particular, contra los llamados ataques de canal lateral (SCA, por sus siglas en inglés) y ataques no invasivos de fallas. La implementación de algoritmos criptográficos son propensos a ataques no invasivos de fallos y a ataques de canal lateral, los cuales tienen como objetivo extraer la clave.

Los ataques no invasivos observan alguna fuga (como las emanaciones electromagnéticas) o perturban los datos internos (por ejemplo, con impulsos electromagnéticos), sin dañar el sistema. Constituyen una preocupación especial en la medida en que no dejan evidencia de que han sido perpetrados. Estos ataques pueden clasificarse en dos categorías:

- Ataques de canal lateral (SCA) : Consisten en registrar pasivamente alguna fuga, que es la fuente de información para recuperar la clave.
- Los ataques de inyección de fallos (FIA): Consisten en perturbar activamente el cálculo para obtener diferencias aprovechables en la salida.

Hacer que un código $\mathcal{C}$ sea LCD de la mayor distancia mínima posible mejora simultáneamente la resistencia contra SCA y FIA.

Por otro lado, los caballos de Troya de hardware (HTH) constituyen una amenaza especial. Los HTH son puertas agregadas por un adversario (por ejemplo, una fundición de silicio) en el diseño en el momento de la fabricación. Esas puertas permiten entregar una carga útil maliciosa en una condición de activación diseñada. La activación resulta de un disparo, decidido en función del valor de algunos bits del circuito. Para evitar de manera preventiva la inserción de la lógica de activación HTH y para detectar de manera proactiva el efecto de la carga útil HTH, la distancia mínima d de los códigos LCD debe

establecerse lo más grande posible.

Como se observa en los casos mencionados anteriormente, el mejoramiento de la protección depende en gran medida del tamaño de la distancia mínima de Hamming, todo esto para códigos LCD, pero por la Observación 3.3.2, todos los códigos $\mathcal{BCH}$ son LCD, y dado el Límite $\mathcal{BCH}$, la distancia de diseño del código juega un papel fundamental (veáse [3]).

Capítulo 4

Códigos $\mathcal{BCH}$ de longitud $n = 2^m + 1$ para $m = 2t + 1$

En este capítulo, consideramos $n = 2^m+1$ con $m = 2t+1 \geq 11$, es decir, para $t \geq 5$. Se obtendrán todos los líderes de clase lateral para $1 \leq i \leq 2^{t+2}+7$, después se determinarán los cinco líderes de clase lateral más grandes. Estos líderes son muy importantes porque permiten hallar la dimensión y establecer una cota inferior de la distancia mínima de Hamming de los códigos $\mathcal{BCH}$ de longitud $n = 2^m + 1$ para $m = 2t + 1$.

Notación 4.0.1. Sean a, b, c enteros no negativos, con $a \leq b$, denotamos $[a, b] = \{a, a + 1, \ldots, b\}$ y $[a, b] + c = [a + c, b + c]$.

Observación 4.0.2. Suponga que C_i es la clase lateral 2-ciclotómica que contiene i. De acuerdo con la definición de C_i, como sus elementos son de la forma $i \cdot 2^k$, definamos

$$D_i = \{y_{i,k} | y_{i,k} \equiv i \cdot 2^k; k = 0, 1, \ldots, m-1; y_{i,k} \in \mathbb{Z}_n\}.$$

Veamos que $C_i = D_i \cup \{n - y : y \in D_i\}$.

Sea $y \in C_i$. Dada la forma de $n = 2^m + 1$, se cumple que $2^m \equiv -1$, luego $2^{2m} \equiv 1$. Además, $ord_n(2)|2m$, por lo que las opciones para $ord_n(2)$ son números entre 1 y m, y $2m$, de donde se concluye que $ord_n(2) = 2m$, de esta forma

$$C_i = \{i \cdot 2^k | 0 \leq k \leq 2m - 1\} \mod n.$$

Por lo que $y \equiv i \cdot 2^k \mod n$ para algún $0 \leq k \leq 2m - 1$. Si $0 \leq k \leq m - 1$, entonces $y \in D_i$, pero si $m \leq k \leq 2m - 1$, notemos que

$$y \equiv 2^k i = 2^{k-m}(2^m + 1 - 1)i \equiv -2^{k-m} i \equiv n - y_{i,k-m} \in \mathbb{Z}_n,$$

donde $y_{i,k-m} \in D_i$, así $y \in \{n - y : y \in D_i\}$.

Sea ahora $y_{i,k} \in D_i$, luego $y_{i,k} \equiv 2^k i$ para algún $0 \leq k \leq m - 1$, es claro que $y_{i,k} \in C_i$. Tomemos $t \in \{n - y : y \in D_i\}$, luego $t = n - y_{i,k}$ con $y_{i,k} \in D_i$. Se satisface que

$$n - y_{i,k} \equiv -2^k i = 2^k(2^m - 2^m - 1)i \equiv 2^{k+m} i,$$

por lo que $n - y_{i,k} \in C_i$. Se concluye así que, $C_i = D_i \cup \{n - y : y \in D_i\}$.

Notación 4.0.3. Mostrado lo anterior, la clase lateral q-ciclotómica C_i, se puede denotar como

$$C_i = \{y_{i,k}, n - y_{i,k} | 0 \leq k \leq m-1\}.$$

Definición 4.0.4. i es un líder de la clase lateral C_i si y sólo si $y_{i,k} - i \geq 0$ y $n - y_{i,k} - i \geq 0$ para $0 \leq k \leq m-1$.

Observemos que cuando i es par, entonces $\frac{i}{2} \in C_i$, por lo que i no es un líder de clase lateral. Para encontrar los líderes de clase lateral en T_δ y T'_δ se necesita considerar solo i impar.

Ejemplo 4.0.5. Consideremos $n = 2^3 + 1 = 9$. En este caso, $m = 3$.

$$\begin{aligned} C_1 &= \{y_{1,0}, y_{1,1}, y_{1,2}, y_{1,3}, y_{1,4}, y_{1,5}\} \\ &= \{1, 2, 4, 8, 7, 5\} \\ &= C_5 \\ &= C_7 \end{aligned}$$

Notemos que

- Como $y_{1,0} \equiv 2^0 \mod 9$, entonces $y_{1,0} = 1$.
- $y_{1,1} \equiv 2^1 \mod 9$. Así, $y_{1,1} = 2$.
- $y_{1,2} \equiv 2^2 \mod 9$, por lo que $y_{1,2} = 4$.
- $y_{1,3} \equiv 2^3 \mod 9$, entonces $y_{1,3} = 8$.
- $y_{1,4} \equiv 2^4 \mod 9$, $y_{1,4} = 7$.
- $y_{1,5} \equiv 2^5 \mod 9$, así $y_{1,5} = 5$

$$\begin{aligned} C_3 &= \{y_{3,0}, y_{3,1}, y_{3,2}, y_{3,3}, y_{3,4}, y_{3,5}\} \\ &= \{3, 6\} \end{aligned}$$

- Como $y_{3,0} \equiv 3 \cdot 2^0 \mod 9$, entonces $y_{3,0} = 3$ y $9 - y_{3,0} = 6$.
- $y_{3,1} \equiv 3 \cdot 2^1 \mod 9$. Así, $y_{3,1} = 6$ y $9 - y_{3,1} = 3$.
- $y_{3,2} \equiv 3 \cdot 2^2 \mod 9$, por lo que $y_{3,2} = 3$ y $9 - y_{3,2} = 6$.

Observando los elementos de estas clases laterales, notamos que 1 y 3 son líderes de la clase lateral C_1 y C_3, respectivamente, pero 5 y 7 no son líderes de su clase lateral, pues estas coinciden con C_1 y el líder en C_1 es 1.

El siguiente teorema nos muestra algunos valores de i para los cuales este es líder de clase lateral y también algunos valores para los cuales no lo es, esto es importante porque conocerlos es la base para determinar la dimensión y una cota inferior para la distancia mínima de Hamming de los códigos $\mathcal{BCH}$ de longitud $n = 2^m + 1$ para $m = 2t + 1$.

Para la demostración de los incisos dos y tres de dicho teorema, se representará i de la forma $i = 2^{t+1} + 1 + 2l$ donde $l \in [1, 2^{t-1} - 2]$ y como $i = 2^{t+1} + 2^t + 1 + 2l$ con $l \in [1, 2^{t-1} - 5]$, respectivamente, para después determinar $y_{i,k}$ y como lo indica la Definición 4.0.4, verificar que $y_{i,k} - i \geq 0$ y $n - y_{i,k} - i \geq 0$ para $0 \leq k \leq m - 1$. Para algunos valores de k es complicado determinar $y_{i,k}$ por lo que para cada k se dividirá el intervalo en el que toma valores l en 2^{k-1-t} intervalos disjuntos, los cuales se denotan como $I_{\lambda,k}$ donde $\lambda \in [1, 2^{k-t-1}]$ y recibe el nombre de *etiqueta de identidad* del subintervalo $I_{\lambda,k}$.

Por último, para el inciso cuatro del Teorema se demostrará que para cada valor de i, existe un entero impar $y \in [1, i-1]$ que satisface que $y \in C_i$, es decir, se muestra que existe un elemento en C_i menor a i, por lo que i no es líder de clase lateral.

Teorema 4.0.6. Sea i impar.

1. Si $1 \leq i \leq 2^{t+1} - 3$, entonces i es un líder de clase lateral.

2. Si $2^{t+1} + 3 \leq i \leq 2^{t+1} + 2^t - 3$, entonces i es un líder de clase lateral.

3. Si $2^{t+1} + 2^t + 3 \leq i \leq 2^{t+2} - 9$, entonces i es un líder de clase lateral.

4. Si $i = 2^{t+1} - 1, 2^{t+1} + 1, 2^{t+1} + 2^t - 1, 2^{t+1} + 2^t + 1$ o $2^{t+2} - t \leq i \leq 2^{t+2} + 7$, entonces i no es un líder de clase lateral.

Demostración. 1. El Lema 15 en [4] justifica este inciso.

2. Como i es impar, lo podemos denotar como $i = 2^{t+1} + 1 + 2l$, donde $l \in I = [1, 2^{t-1} - 2]$. Para verificar que i es líder de clase lateral es necesario probar que $y_{i,k} - i \geq 0$ y $n - y_{i,k} - i \geq 0$ para $k \in [0, m - 1 = 2t]$. Se determinará primero $y_{i,k}$.

   - Cuando $k = 0, 1, 2, \cdots, t-1$, de $2^{t+1} + 3 \leq i \leq 2^{t+1} + 2^t - 3$, tenemos que $i \leq 2^k i < n$. De donde $y_{i,k} = 2^k i \geq i$ y así, $y_{i,k} - i \geq 0$. Además

$$\begin{aligned} n - y_{i,k} - i &\geq n - 2^k i - i \\ &\geq n - 2^{t-1} i - i \\ &= 2^{2t+1} + 1 - (2^{t-1} + 1)i \\ &\geq 2^{2t+1} + 1 - (2^{t-1} + 1)(2^{t+1} + 2^t - 3) \\ &= 2^{2t+1} + 1 - (2^{2t} + 2^{2t-1} - 3 \cdot 2^{t-1} + 2^{t+1} + 2^t - 3) \\ &= 2^{2t-1}(2^2 - 1 - 2) - 2^{t-1}(2^2 - 3) - 2^t + 4 \\ &= 2^{2t-1} - 2^{t-1} - 2^t + 4 > 0. \end{aligned}$$

- Cuando $k = t, t+1$, tenemos $y_{i,k} = 2^k i - 2^{k-t} n$. Se sigue que

$$\begin{aligned} y_{i,k} - i &= 2^k(2^{t+1} + 1 + 2l) - 2^{k-t}(2^{2t+1} + 1) - 2^{t+1} - 1 - 2l \\ &= (2^{k+1} - 2)l + 2^k - 2^{t+1} - 1 - 2^{k-t} \\ &\geq (2^{k+1} - 2) + 2^k - 2^{t+1} - 1 - 2^{k-t} \\ &= (3 - 2^{-t}) \cdot 2^k - 2^{t+1} - 3 \\ &\geq (3 - 2^{-t}) \cdot 2^t - 2^{t+1} - 3 \\ &= 2^t - 4 > 0, \end{aligned}$$

$$\begin{aligned} n - y_{i,k} - i &= 2^{2t+1} + 1 - 2^k i + 2^{k-t}(2^{2t+1} + 1) - 2^{t+1} - 1 - 2l \\ &= 2^{k-t} + 2^{2t+1} - 2^{t+1} - 2^k - (2^{k+1} + 2)l \\ &\geq 2^{k-t} + 2^{2t+1} - 2^{t+1} - 2^k - (2^{k+1} + 2)(2^{t-1} - 2) \\ &= 2^{k-t} + 2^{2t+1} - 2^{t+1} - 2^k - (2^{k+1} - 2^{k+2} + 2^t - 4) \\ &= 2^{2t+1} - 2^t - 2^{t+1} + 4 - (2^t - 2^{-t} - 3)2^k \\ &\geq 2^{2t+1} - 2^t - 2^{t+1} + 4 - (2^t - 2^{-t} - 3)2^{t+1} \\ &= 3(2^t + 2) > 0. \end{aligned}$$

- Cuando $k = t+2, t+3, \cdots, 2t-1$, es complicado determinar $y_{i,k}$. Para esto, para cada k, se dividirá el intervalo $I = [1, 2^{t-1} - 2]$ de l en 2^{k-1-t} intervalos disjuntos, como sigue:

$$\begin{aligned} &I_{1,k} = [1, 2^{2t-k} - 1], \\ &I_{\lambda,k} = [(\lambda - 1)2^{2t-k}, \lambda 2^{2t-k} - 1] \text{ para } \lambda \in [2, 2^{k-t-1} - 1], \\ &I_{\lambda,k} = [(\lambda - 1)2^{2t-k}, 2^{t-1} - 2] \text{ para } \lambda = 2^{k-t-1}. \end{aligned}$$

  Fijando k, a λ se le llama *etiqueta de identidad* del subintervalo $I_{\lambda,k} = [l_{\lambda,b}, l_{\lambda,e}]$. Así, para $\lambda \in [1, 2^{k-t-1}]$, si $i = 2^{t+1} + 1 + 2l$ con $l \in I_{\lambda,k}$, se deriva que $y_{i,k} = 2^k i - (2^{k-t} + \lambda - 1)n$. Verifiquemos ahora que $y_{i,k} - i \geq 0$ y $n - y_{i,k} - i \geq 0$.

  a) Veamos que $y_{i,k} - i \geq 0$. Para cada λ, se tiene que

$$\begin{aligned} y_{i,k} - i &= 2^k i - (2^{k-t} + \lambda - 1)n - i \\ &= (2^k - 1)(2^{t+1} + 1 + 2l) - (2^{k-t} + \lambda - 1)(2^{2t+1} + 1) \\ &= (2^k - 1)(1 + 2l) - 2^{t+1} - 2^{k-t} - (\lambda - 1)(2^{2t+1} + 1) \end{aligned}$$

  Cuando $\lambda = 1$, $l \geq 1$ y $k \geq t+2$, se tiene

$$\begin{aligned} y_{i,k} - i &= (2^k - 1)(1 + 2l) - 2^{t+1} - 2^{k-t} \\ &\geq (2^k - 1)(1 + 2) - 2^{t+1} - 2^{k-t} \\ &= (3 - 2^{-t})2^k - 2^{t+1} - 3 \\ &\geq (3 - 2^{-t})2^{t+2} - 2^{t+1} - 3 \\ &= 5 \cdot 2^{t+2} - 7 > 0. \end{aligned}$$

Para $\lambda \in [2, 2^{k-t-1}]$, $l \in I_{\lambda,k} = [l_{\lambda,b} = (\lambda-1)2^{2t-k}, l_{\lambda,e}]$ tenemos

$$\begin{aligned}
y_{i,k} - i &= (2^k-1)(1+2l) - 2^{t+1} - 2^{k-t} - (\lambda-1)(2^{2t+1}+1) \\
&\geq (2^k-1)(1+2l_{\lambda,b}) - 2^{t+1} - 2^{k-t} - (\lambda-1)(2^{2t+1}+1) \\
&= (2^k-1)(1+2(\lambda-1)2^{2t-k}) - 2^{t+1} - 2^{k-t} - (\lambda-1)(2^{2t+1}+1) \\
&= 2^{2t+1-k} + 2^k - 2^{t+1} - 2^{k-t} - (2^{2t-k+1}+1)\lambda \\
&\geq 2^{2t+1-k} + 2^k - 2^{t+1} - 2^{k-t} - (2^{2t-k+1}+1)\cdot 2^{k-t-1} \\
&= 2^{2t+1-k} + 2^k(1 - 2^{-t} - 2^{-t-1}) - 2^{t+1} - 2^t \\
&\geq 2^{2t+1-(t+2)} + 2^{t+2}(1 - 2^{-t} - 2^{-t-1}) - 2^{t+1} - 2^t \\
&= 2^t + 2^{t-1} - 6 > 0.
\end{aligned}$$

b) Veamos ahora que $n - y_{i,k} - i \geq 0$. Observemos que para λ general,

$$\begin{aligned}
n - y_{i,k} - i &= n - 2^k i + (2^{k-t} + \lambda - 1)n - i \\
&= 2^{2t+1} + 1 - (2^k+1)(2^{t+1}+1+2l) + (2^{k-t}+\lambda-1)(2^{2t+1}+1) \\
&= (2^{k-t}+\lambda)(2^{2t+1}+1) - (2^k+1)(2^{t+1}+1+2l).
\end{aligned}$$

Si $1 \leq \lambda \leq 2^{k-t-1} - 1$ y $l \in I_{\lambda,k} = [l_{\lambda,b}, l_{\lambda,e} = \lambda 2^{2t-k-1}]$ entonces

$$\begin{aligned}
n - y_{i,k} - i &= (2^{k-t}+\lambda)(2^{2t+1}+1) - (2^k+1)(2^{t+1}+1+2l) \\
&\geq (2^{k-t}+\lambda)(2^{2t+1}+1) - (2^k+1)(2^{t+1}+1+2l_{\lambda,e}) \\
&= 2^{k-t}+\lambda)(2^{2t+1}+1) - (2^k+1)(2^{t+1}+1+2(\lambda 2^{2t-k-1})) \\
&= 2^{k-t} - 2^{t+1} + 2^k + 1 - (2^{2t+1-k}-1)\lambda \\
&\geq 2^{k-t} - 2^{t+1} + 2^k + 1 - (2^{2t+1-k}-1)(2^{k-t-1}-1) \\
&= 2^{2t+1-k} + 2^k(1 + 2^{-t} + 2^{-t-1}) - 2^{t+1} - 2^t \\
&\geq 2^{2t+1-(t+2)} + 2^{t+2}(1 + 2^{-t} + 2^{-t-1}) - 2^{t+1} - 2^t \\
&= 3(2^{t-1}+2) > 0.
\end{aligned}$$

Si $\lambda = 2^{k-t-1}$, sea $l \in I_{\lambda,k} = [l_{\lambda,b} = (\lambda-1)2^{2t-k}, l_{\lambda,e} = 2^{t-1} - 2]$, entonces tenemos

$$\begin{aligned}
n - y_{i,k} - i &= (2^{k-t}+\lambda)(2^{2t+1}+1) - (2^k+1)(2^{t+1}+1+2l) \\
&\geq (2^{k-t}+\lambda)(2^{2t+1}+1) - (2^k+1)(2^{t+1}+1+2l_{\lambda,e}) \\
&= 2^{k-t}+\lambda)(2^{2t+1}+1) - (2^k+1)(2^{t+1}+1+2(2^{t-1}-2)) \\
&= 2^k(3 + 2^{-t} + 2^{-t-1}) - 2^{t+1} - 2^t + 3 \\
&\geq 2^{t+2}(3 + 2^{-t} + 2^{-t-1}) - 2^{t+1} - 2^t + 3 \\
&= 9(2^t+1) > 0.
\end{aligned}$$

- Cuando $k = 2t$, para $i = 2^{t+1} + 1 + 2l$ con $l \in I = [1, 2^{t-1} - 2]$, tenemos

$$\begin{aligned} y_{i,k} &= 2^k i - (2^{k-t} + l)n \\ &= 2^{2t}(2^{t+1} + 1 + 2l) - (2^t + l)(2^{2t+1} + 1) \\ &= 2^{2t} - 2^t - l. \end{aligned}$$

  Observemos que

$$\begin{aligned} y_{i,k} - i &= 2^{2t} - 2^t - l - (2^{t+1} + 1 + 2l) \\ &= 2^{2t} - 2^t - 2^{t+1} - 1 - 3l \\ &\geq 2^{2t} - 2^t - 2^{t+1} - 1 - 3 \cdot (2^{t-1} - 2) \\ &= 2^{2t} - 2^t - 2^{t+1} - 1 - 3 \cdot 2^{t-1} + 6 \\ &= 2^{2t} - 2^t - 2^{t+1} - (2+1) \cdot 2^{t-1} + 5 \\ &= 2^{2t} - 2^t - 2^{t+1} - 2^t - 2^{t-1} + 5 \\ &= 2^{2t} - 2^{t+2} - 2^{t-1} + 5 > 0, \end{aligned}$$

$$\begin{aligned} n - y_{i,k} - i &= 2^{2t+1} + 1 - 2^{2t} + 2^t + l - 2^{t+1} - 1 - 2l \\ &= 2^{2t} + 2^t - 2^{t+1} - l \\ &\geq 2^{2t} + 2^t - 2^{t+1} - (2^{t-1} - 2) \\ &= 2^{2t} - 2^{t+1} + 2^{t-1} + 2 > 0. \end{aligned}$$

3. Para $i \in [2^{t+1} + 2^t + 3, 2^{t+2} - 9]$ impar, tomamos $i = 2^{t+1} + 2^t + 1 + 2l$ con $l \in J = [1, 2^{t-1} - 5]$. De forma similar al inciso anterior, se determinará $y_{i,k}$ y se probará que $y_{i,k} - i \geq 0$ y $n - y_{i,k} - i \geq 0$ para todo $k \in [0, m - 1 = 2t]$.

   - Cuando $k = 0, 1, 2, \cdots, t-1$, se tiene que $i \leq 2^k i < n$, por lo que $y_{i,k} = 2^k i \geq i$ o bien, $y_{i,k} - i \geq 0$. Además

$$\begin{aligned} n - y_{i,k} - i &= 2^{2t+1} + 1 - (2^k + 1)i \\ &\geq 2^{2t+1} + 1 - (2^k + 1)(2^{t+2} - 9) \\ &\geq 2^{2t+1} + 1 - (2^{t-1} + 1)(2^{t+2} - 9) \\ &= 2^{2t+1} + 1 - 2^{2t+1} + 9 \cdot 2^{t-1} + 2^{t+2} + 9 \\ &= 2^{t-1} + 10 > 0. \end{aligned}$$

   - Cuando $k = t$, tenemos que $y_{i,k} = 2^k i - n$, entonces

$$\begin{aligned} y_{i,k} - i &= 2^k i - n - i \\ &= (2^k - 1)(2^{t+1} + 2^t + 1 + 2l) - 2^{2t+1} - 1 \\ &\geq (2^k - 1)(2^{t+1} + 2^t + 1 + 2) - 2^{2t+1} - 1 \\ &= (2^t - 1)(2^{t+1} + 2^t + 3) - 2^{2t+1} - 1 \\ &= 2^{2t+1} + 2^{2t} + 3 \cdot 2^t - 2^{t+1} - 2^t - 3 - 2^{2t+1} - 1 \\ &= 2^{2t} - 4 \geq 0. \end{aligned}$$

$$\begin{aligned} n - y_{i,k} - i &= n - 2^k i + n - i \\ &= 2n - (2^k + 1)i \\ &= 2n - (2^t + 1)i \\ &\geq 2n - (2^t + 1)(2^{t+2} - 9) \\ &= 2(2^{2t+1} + 1) - (2^t + 1)(2^{t+2} - 9) \\ &= 2^{2t+2} + 2 - 2^{2t+2} + 9 \cdot 2^t - 2^{t+2} + 9 \\ &= 5 \cdot 2^t + 11 > 0. \end{aligned}$$

- Cuando $k = t + 1$, tenemos $y_{i,k} = 2^k i - 3n$. Se sigue que

$$\begin{aligned} y_{i,k} - i &= (2^{t+1} - 1)i - 3n \\ &\geq (2^{t+1} - 1)(2^{t+2} - 9) - 3n \\ &= (2^{t+1} - 1)(2^{t+2} - 9) - 3 \cdot (2^{2t+1} + 1) \\ &= 2^{2t+2} + 2^{2t+1} + 3 \cdot 2^{t+1} - 2^{t+1} - 2^t - 3 - 3 \cdot 2^{2t+1} - 3 \\ &= 3(2^t - 2) > 0, \end{aligned}$$

$$\begin{aligned} n - y_{i,k} - i &= 4n - (2^{t+1} + 1)i \\ &\geq 4n - (2^{t+1} + 1)(2^{t+2} - 9) \\ &= 4(2^{2t+1} + 1) - (2^{t+1} + 1)(2^{t+2} - 9) \\ &= 2^{2t+3} + 4 - 2^{2t+3} + 9 \cdot 2^{t+1} - 2^{t+2} + 9 \\ &= 7 \cdot 2^{t+1} + 13 > 0. \end{aligned}$$

- Para cada $k = t+2, t+3, \cdots, 2t-3$, para determinar $y_{i,k}$, dividimos el intervalo $J = [1, 2^{t-1} - 5]$ de valores de l en 2^{k-1-t} subintervalos como sigue:

$$\begin{aligned} &J_{\lambda,k} = [1, \lambda 2^{2t-k} - 1] \text{ para } \lambda = 1, \\ &J_{\lambda,k} = [(\lambda - 1)2^{2t-k}, \lambda 2^{2t-k} - 1] \text{ para } \lambda \in [2, 2^{k-t-1} - 1], \\ &J_{\lambda,k} = [(\lambda - 1)2^{2t-k}, 2^{t-1} - 5] \text{ para } \lambda = 2^{k-t-1}. \end{aligned}$$

De forma similar al inciso anterior, para k dado, se define $\lambda \in [1, 2^{k-t-1}]$ la cual se llama *etiqueta de identidad* del subintervalo $J_{\lambda,k} = [l_{\lambda,b}, l_{\lambda,e}]$. Fijando λ, si $i = 2^{t+1} + 2^t + 1 + 2l$ con $l \in J_{\lambda,k}$, se sigue que

$$y_{i,k} = 2^k i - (2^{k-t} + 2^{k-t-1} + \lambda - 1)n.$$

a) Primero veamos que $y_{i,k} - i > 0$. Observemos que

$$\begin{aligned} y_{i,k} - i &= (2^k - 1)i - (2^{k-t} + 2^{k-t-1} + \lambda - 1)n \\ &= (2^k - 1)(2^{t+1} + 2^t + 1 + 2l) - (2^{k-t} + 2^{k-t-1} + \lambda - 1)(2^{2t+1} + 1) \\ &= (2^k - 1)(1 + 2l) + (2^k - 1)(2^{t+1} + 2^t) - (2^{k-t} + 2^{k-t-1})(2^{2t+1} + 1) \\ &\quad -(\lambda - 1)(2^{2t+1} + 1) \\ &= (2^k - 1)(1 + 2l) + 2^{k+t+1} + 2^{k+t} - 2^{t+1} - 2^t - 2^{k+t+1} - 2^{k-t} - 2^{k+t} \\ &\quad -2^{k-t-1} - (\lambda - 1)(2^{2t+1} + 1) \\ &= (2^k - 1)(1 + 2l) - 2^{t+1} - 2^t - 2^{k-t} - 2^{k-t-1} - (\lambda - 1)(2^{2t+1} + 1). \end{aligned}$$

Cuando $\lambda = 1$, notemos que $l \in J_{\lambda,k} = [1, 2^{2t-k} - 1]$ y $k \geq t + 2$, se tiene que

$$\begin{aligned} y_{i,k} - i &= (2^k - 1)(1 + 2l) - 2^{t+1} - 2^t - 2^{k-t} - 2^{k-t-1} \\ &\geq (2^k - 1)(1 + 2) - 2^{t+1} - 2^t - 2^{k-t} - 2^{k-t-1} \\ &= 3 \cdot 2^k - 3 - 2^{t+1} - 2^t - 2^{k-t} - 2^{k-t-1} \\ &= 2^k(3 - 2^{-t} - 2^{-t-1}) - 2^{t+1} - 2^t - 3 \\ &\geq 2^{t+2}(3 - 2^{-t} - 2^{-t-1}) - 2^{t+1} - 2^t - 3 \\ &= 3 \cdot 2^{t+2} - 2^{t+1} - 2^t - 9 > 0. \end{aligned}$$

Para $\lambda \in [2, 2^{k-t-1}]$ cuando $l \in J_{\lambda,k} = [l_{\lambda,b} = (\lambda - 1)2^{2t-k}, l_{\lambda,e}]$, se tiene el siguiente proceso

$$\begin{aligned} y_{i,k} - i &= (2^k - 1)(1 + 2l) - 2^{t+1} - 2^t - 2^{k-t} - 2^{k-t-1} - (\lambda - 1)(2^{2t+1} + 1) \\ &\geq (2^k - 1)(1 + 2l_{\lambda,b}) - 2^{t+1} - 2^t - 2^{k-t} - 2^{k-t-1} - (\lambda - 1)(2^{2t+1} + 1) \\ &= (2^k - 1)(1 + (\lambda - 1)2^{2t-k+1}) - 2^{t+1} - 2^t - 2^{k-t} - 2^{k-t-1} \\ &\quad -(\lambda - 1)(2^{2t+1} + 1) \\ &= 2^k + (\lambda - 1)2^{2t+1} - 1 - (\lambda - 1)2^{2t-k+1} - 2^{t+1} - 2^t - 2^{k-t} - 2^{k-t-1} \\ &\quad -(2^{2t+1} + 1)\lambda + 2^{2t+1} + 1 \\ &= 2^{2t+1-k} + 2^k - 2^{t+1} - 2^t - 2^{k-t} - 2^{k-t-1} - (2^{2t-k+1} + 1)\lambda \\ &\geq 2^{2t+1-k} + 2^k - 2^{t+1} - 2^t - 2^{k-t} - 2^{k-t-1} - (2^{2t-k+1} + 1) \cdot 2^{k-t-1} \\ &= 2^{2t+1-k} + 2^k - 2^{t+1} - 2^t - 2^{k-t} - 2^{k-t-1} - 2^t - 2^{k-t-1} \\ &= 2^{2t+1-k} + 2^k(1 - 2^{1-t}) - 2^{t+2} \\ &\geq 2^{2t+1-(t+2)} + 2^{t+2}(1 - 2^{1-t}) - 2^{t+2} \\ &= 2^{t-1} + 2^{t+2}1 - 2^3 - 2^{t+2} \\ &= 2^{t-1} - 8 > 0. \end{aligned}$$

b) Mostremos ahora que $n - y_{i,k} - i > 0$. Observemos que

$$\begin{aligned} n - y_{i,k} - i &= n - (2^k + 1)i + (2^{k-t} + 2^{k-t-1} + \lambda - 1)n \\ &= (2^{k-t} + 2^{k-t-1} + \lambda)n - (2^k + 1)i \\ &= (2^{k-t} + 2^{k-t-1} + \lambda)(2^{2t+1} + 1) - (2^k + 1)(2^{t+1} + 2^t + 1 + 2l). \end{aligned}$$

Tomando $\lambda \in [1, 2^{k-t-1} - 2^{k+2-2t}]$, desde que $l \in J_{\lambda,k} = [l_{\lambda,b}, l_{\lambda,e} = \lambda 2^{2t-k} - 1]$, se deduce que

$$\begin{aligned} n - y_{i,k} - i &= (2^{k-t} + 2^{k-t-1} + \lambda)(2^{2t+1} + 1) - (2^k + 1)(2^{t+1} + 2^t + 1 + 2l) \\ &\geq (2^{k-t} + 2^{k-t-1} + \lambda)(2^{2t+1} + 1) - (2^k + 1)(2^{t+1} + 2^t + 1 + 2l_{\lambda,e}) \\ &= (2^{k-t} + 2^{k-t-1} + \lambda)(2^{2t+1} + 1) - (2^k + 1)(2^{t+1} + 2^t + 1 + 2(\lambda 2^{2t-k} - 1)) \\ &= 2^{t+k+1} + 2^{k-t} + 2^{t+k} + 2^{k-t-1} + \lambda 2^{2t+1} + \lambda - 2^{t+k+1} - 2^{t+k} - 2^k \\ &\quad -\lambda 2^{2t+1} + 2^{k+1} - 2^{t+1} - 2^t - \lambda 2^{2t-k+1} + 1 \\ &= 2^{k-t} + 2^{k-t-1} - 2^{t+1} - 2^t + 2^j + 1 - (2^{2t+1-k} - 1)\lambda \\ &\geq 2^{k-t} + 2^{k-t-1} - 2^{t+1} - 2^t + 2^j + 1 - (2^{2t+1-k} - 1)(2^{k-t-1} - 2^{k+2-2t}) \\ &= 2^{k-t} + 2^{k-t-1} - 2^{t+1} - 2^t + 2^j + 1 - 2^t + 2^3 + 2^{k-t-1} - 2^{k+2-2t} \\ &= 2^k(1 + 2^{1-t} - 2^{2-2t}) - 2^{t+2} + 9 \\ &\geq 2^{2t-2}(1 + 2^{1-t} - 2^{2-2t}) - 2^{t+2} + 9 \\ &= 2^{2t-2} + 2^{t-1} - 2^{t+2} + 8 > 0. \end{aligned}$$

- Cuando $k = 2t$, y teniendo $i = 2^{t+1} + 2^t + 1 + 2l$ con $l \in J = [1, 2^{t-1} - 5]$, se obtiene

$$\begin{aligned} y_{i,k} &= 2^k i - (2^{k-t} + 2^{t-1} + l)n \\ &= 2^{2t}(2^{t+1} + 2^t + 1 + 2l) - (2^t + 2^{t-1} + l)(2^{2t+1} + 1) \\ &= 2^{3t+1} + 2^{3t} + 2^{2t} + 2^{2t+1}l - (2^{3t+1} + 2^t + 2^{3t} + 2^{t-1} + 2^{2t+1}l + l) \\ &= 2^{2t} - 2^t - 2^{t-1} - l, \end{aligned}$$

por lo tanto, para $l \in J = [1, 2^{t-1} - 5]$ se puede derivar que

$$\begin{aligned} y_{i,k} - i &= 2^{2t} - 2^t - 2^{t-1} - l - i \\ &= 2^{2t} - 2^t - 2^{t-1} - l - 2^{t+1} - 2^t - 1 - 2l \\ &= 2^{2t} - 2^{t+2} - 2^{t-1} - 1 - 3l \\ &\geq 2^{2t} - 2^{t+2} - 2^{t-1} - 1 - 3(2^{t-1} - 5) \\ &= 2^{2t} - 2^{t+2} - 2^{t-1} - 1 - 3 \cdot 2^{t-1} + 15 \\ &= 2^{2t} - 2^{t+2} - 2^{t+1} + 14 > 0. \end{aligned}$$

$$\begin{aligned} n - y_{i,k} - i &= 2^{2t+1} + 1 - (2^{2t} - 2^t - 2^{t-1} - l) - (2^{t+1} + 2^t + 1 + 2l) \\ &= 2^{2t} - 2^{t+1} + 2^{t-1} - l \\ &\geq 2^{2t} - 2^{t+1} + 2^{t-1} - (2^{t-1} - 5) \\ &= 2^{2t} - 2^{t+1} + 5 > 0. \end{aligned}$$

4. Observemos que para $i = 2^{t+1} - 1$,

$$\begin{aligned} i \cdot 2^{3t+1} &= (2^{t+1} - 1)2^{3t+1} \\ &= (2^{t+1} - 1)2^t \cdot 2^{2t+1} \\ &= (2^{2t+1} - 2^t) \cdot 2^{2t+1} \\ &= (2^{2t+1} + 1 - 1 - 2^t) \cdot (2^{2t+1} + 1 - 1) \\ &= (n - 1 - 2^t)(n - 1) \\ &= n^2 - 2n - 2^t n + 2^t + 1 \\ &= n(n - 2 - 2^t) + 2^t + 1 \\ &\equiv 2^t + 1 \mod n. \end{aligned}$$

Ahora, para $i = 2^{t+1} + 1$,

$$\begin{aligned} i \cdot 2^t &= (2^{t+1} + 1)2^t \\ &= 2^{2t+1} + 2^t \\ &= 2^{2t+1} + 1 + 2^t - 1 \\ &= n + 2^t - 1 \\ &\equiv 2^t - 1 \mod n. \end{aligned}$$

Considerando $i = 2^{t+1} + 2^t - 1$,

$$\begin{aligned} i \cdot 2^{2t+2} &= (2^{t+1} + 2^t - 1)2^{2t+2} \\ &= (2^{t+1} + 2^t - 1)2^{t+1} \cdot 2^{2t+1} \\ &= (2^{2t+2} + 2^{2t+1} - 2^{t+1})2^{2t+1} \\ &= (3 \cdot 2^{2t+1} + 3 - 3 - 2^{t+1})(2^{2t+1} + 1 - 1) \\ &= (3n - 3 - 2^{t+1})(n - 1) \\ &= (3n - 6 - 2^{t+1})n + 2^{t+1} + 3 \\ &\equiv 2^{t+1} + 3 \mod n. \end{aligned}$$

Con $i = 2^{t+1} + 2^t + 1$, se tiene que

$$\begin{aligned} i \cdot 2^{t+1} &= (2^{t+1} + 2^t + 1)2^{t+1} \\ &= 2^{2t+2} + 2^{2t+1} + 2^{t+1} \\ &= 3 \cdot 2^{2t+1} + 3 + 2^{t+1} - 3 \\ &= 3n + 2^{t+1} - 3 \\ &\equiv 2^{t+1} - 3 \mod n. \end{aligned}$$

Por último, para $2^{t+2} - 7 \leq i \leq 2^{t+2} + 7$, consideramos $j = 1, 3, 5, 7$ en

$$\begin{aligned}(2^{t+2} - j)2^{3t} &= (2^{t+2} - i)2^{t-1} \cdot 2^{2t+1} \\ &= (2^{2t+1} - j2^{t-1})2^{2t+1} \\ &= (2^{2t+1} - j2^{t-1})2^{2t+1} \\ &= (2^{2t+1} + 1 - 1 - j2^{t-1})(2^{2t+1} + 1 - 1) \\ &= (n - 1 - j2^{t-1})(n - 1) \\ &= (n - 2 - j2^{t-1})n + j \cdot 2^{t-1} + 1 \\ &\equiv j \cdot 2^{t-1} + 1 \quad \text{mód } n;\end{aligned}$$

$$\begin{aligned}(2^{t+2} + j)2^{t-1} &= 2^{2t+1} + j \cdot 2^{t-1} \\ &= 2^{2t+1} + 1 + j \cdot 2^{t-1} - 1 \\ &= n + j \cdot 2^{t-1} - 1 \\ &\equiv j \cdot 2^{t-1} - 1 \quad \text{mód } n.\end{aligned}$$

En las congruencias presentadas anteriormente se puede observar que para cada i presentada en el inciso 4, existe un entero impar $y \in [1, i - 1]$ que satisface que $y \in C_i$, es decir, i no es líder de la clase lateral. Por lo tanto, la prueba está completa. ■

Uno de los objetivos principales de esta investigación es encontrar los cinco líderes de clase lateral más grandes, pero la primera pregunta a responder es: ¿Quiénes son los candidatos a ser los cincos líderes de clase lateral más grandes? En el siguiente Teorema se presentan δ_i con $i = 1, 2, 3, 4, 5$, los cuales son valores que dependen de n, el Teorema nos garantiza que cada uno de ellos son líderes de clase lateral.

Para la demostración del Teorema, se verifica primero que cada δ_i es impar. Para ver que δ_1 es líder de clase lateral se observarán los elementos de C_{δ_1} donde efectivamente δ_1 será el elemento más pequeño. Con δ_i para $i = 2, 3, 4, 5$ se obtiene primero $y_{\delta_i,k}$ para los distintos valores de k y se aplica la Definición 4.0.4, pues se mostrará que $y_{\delta_i,k} - \delta_i \geq 0$ y $n - y_{\delta_i,k} - \delta_i \geq 0$ para garantizar que son líderes de clases lateral.

Teorema 4.0.7. Los números $\delta_1 = \frac{n}{3}$, $\delta_2 = \frac{n-3}{6}$, $\delta_3 = \delta_2 - 2$, $\delta_4 = \delta_2 - 8$, $\delta_5 = \delta_2 - 10$ son líderes de clase lateral y $\delta_1 > \delta_2 > \delta_3 > \delta_4 > \delta_5$.

Demostración. Notemos que

$$\begin{aligned}\delta_1 = \frac{n}{3} &= \frac{2^{2t+1} + 1}{3} \\ &= 2^{2t} - 2^{2t-1} + \cdots + 4 - 2 + 1,\end{aligned}$$

y

$$\begin{aligned}\delta_2 = \frac{n-3}{6} &= \frac{2^{2t+1}-2}{6} \\ &= \frac{2^{2t}-1}{3} \\ &= 2^{2t-2}+2^{2t-4}+\cdots+4+1.\end{aligned}$$

Así,

$$\begin{aligned}\delta_3 &= \delta_2 - 2 \\ &= 2^{2t-2}+2^{2t-4}+\cdots+4+1-2 \\ &= 2^{2t-2}+2^{2t-4}+\cdots+2+1,\end{aligned}$$

$$\begin{aligned}\delta_4 &= \delta_2 - 8 \\ &= 2^{2t-2}+2^{2t-4}+\cdots+4+1-8 \\ &= 2^{2t-2}+2^{2t-4}+\cdots-4+1,\end{aligned}$$

$$\begin{aligned}\delta_5 &= \delta_2 - 10 \\ &= 2^{2t-2}+2^{2t-4}+\cdots+4+1-10 \\ &= 2^{2t-2}+2^{2t-4}+\cdots-6+1.\end{aligned}$$

Se observa que $\delta_1, \delta_2, \delta_3, \delta_4$ y δ_5 son números impares.

Calculemos ahora C_{δ_1}. Es claro que $\delta_1 \in C_{\delta_1}$, también $n-\delta_1 = n-\frac{n}{3} = \frac{2n}{3} = 2\delta_1 \in C_{\delta_1}$. De hecho $C_{\delta_1} = \{\delta_1, 2\delta_1\}$, lo que implica que $|C_{\delta_1}| = 2$ y δ_1 es un líder de clase lateral.

Veamos que δ_2 es un líder de clase lateral. Se probará que $y_{\delta_2,k}-\delta_2 \geq 0$ y $n-y_{\delta_2,k}-\delta_2 \geq 0$ en los siguientes tres casos.

1. Si $k = 0, 1, 2$, es claro que $y_{\delta_2,k} = 2^k\delta_2 \geq \delta_2$, de modo que $y_{\delta_2,k} - \delta_2 \geq 0$. Además

$$\begin{aligned}n - y_{\delta_2,k} - \delta_2 &= n - 2^k\delta_2 - \delta_2 \\ &= n - 3 - 2^k\delta_2 - \delta_2 + 3 \\ &= (6 - 2^k - 1)\delta_2 + 3 \\ &= (5 - 2^k)\delta_2 + 3 > 0\end{aligned}$$

2. Si $k = 3, 5, \cdots, 2t-1$, tenemos que

$$y_{\delta_2,k} = \frac{n}{3} - 2^{k-1} = \frac{2n}{6} - 1 - 2^{k-1} + 1 = 2\delta_2 - 2^{k-1} + 1.$$

Así,

$$\begin{aligned}y_{\delta_2,k} - \delta_2 &= 2\delta_2 - 2^{k-1} + 1 - \delta_2 \\ &= \delta_2 - 2^{k-1} + 1 \\ &\geq \delta_2 - 2^{(2t-1)-1} + 1 \\ &= \delta_2 - 2^{2t-2} + 1 > 0,\end{aligned}$$

$$\begin{aligned} n - y_{\delta_2,k} - \delta_2 &= n - 2\delta_2 + 2^{k-1} - 1 - \delta_2 \\ &= n - 3\delta_2 + 2^{k-1} - 1 \\ &= n - 3 - 3\delta_2 + 2^{k-1} - 1 + 3 \\ &= 6\delta_2 - 3\delta_2 + 2^{k-1} + 2 \\ &= 3\delta_2 + 2^{k-1} + 2 > 0. \end{aligned}$$

3. Si $k = 4, 6, \cdots, 2t$, entonces

$$y_{\delta_2,k} = \frac{2n}{3} - 2^{k-1} = \frac{4n}{6} - 2 - 2^{k-1} + 2 = 4\delta_2 - 2^{k-1} + 2.$$

De donde

$$\begin{aligned} y_{\delta_2,k} - \delta_2 &= 4\delta_2 - 2^{k-1} + 2 - \delta_2 \\ &= 3\delta_2 - 2^{k-1} + 2 \\ &\geq 3\delta_2 - 2^{2t-1} + 2 > 0, \end{aligned}$$

y

$$\begin{aligned} n - y_{\delta_2,k} - \delta_2 &= n - 4\delta_2 + 2^{k-1} - 2 - \delta_2 \\ &= n - 5\delta_2 + 2^{k-1} - 2 \\ &= n - 3 - 5\delta_2 + 2^{k-1} - 2 + 3 \\ &= 6\delta_2 - 5\delta_2 + 2^{k-1} + 1 \\ &= \delta_2 + 2^{k-1} + 1 > 0. \end{aligned}$$

Con los casos anteriores se demuestra que δ_2 es un líder de clase lateral.

El siguiente paso es demostrar que δ_3 es un líder de clase lateral. Para esto se presentan los siguientes casos:

1. Si $k = 0, 1, 2$, entonces $y_{\delta_3,k} = 2^k\delta_3 \geq \delta_3$, por lo que $y_{\delta_3,k} - \delta_3 \geq 0$. Además

$$n - y_{\delta_3,k} - \delta_3 = n - (2^k + 1)\delta_3$$

$$\begin{aligned} n - y_{\delta_3,k} - \delta_3 &= n - (2^k + 1)\delta_3 \\ &= n - (2^k + 1)(\frac{n-3}{6} - 2) \\ &\geq n - (2^2 + 1)(\frac{n-3}{6} - 2) \\ &= n - 5\frac{n-3}{6} + 10 \\ &= \frac{n+15}{6} + 10. \end{aligned}$$

2. Si $k = 3, 5, \cdots, 2t-3$, entonces se obtiene que

$$y_{\delta_3,k} = 2\delta_2 - 2^{k+1} - 2^{k-1} + 1.$$

A partir de donde,

$$\begin{aligned} y_{\delta_3,k} - \delta_3 &= 2\delta_2 - 2^{k+1} - 2^{k-1} + 1 - (\delta_2 - 2) \\ &= \delta_2 - 2^{k+1} - 2^{k-1} + 3 \\ &\geq \delta_2 - 2^{(2t-3)+1} - 2^{(2t-3)-1} + 3 \\ &= \delta_2 - 2^{2t-2} - 2^{2t-4} + 3 > 0, \end{aligned}$$

y

$$\begin{aligned} n - y_{\delta_3,k} - \delta_3 &= n - (2\delta_2 - 2^{k+1} - 2^{k-1} + 1) - (\delta_2 - 2) \\ &= n - 3\delta_2 + 2^{k+1} + 2^{k-1} + 1 \\ &= n - 3 - 3\delta_2 + 2^{k+1} + 2^{k-1} + 4 \\ &= 3\delta_2 + 2^{k+1} + 2^{k-1} + 4 > 0. \end{aligned}$$

3. Si $k = 4, 6, \cdots, 2t-2$, se deduce que

$$y_{\delta_3,x} = 4\delta_2 - 2^{k+1} - 2^{k-1} + 2.$$

Luego,

$$\begin{aligned} y_{\delta_3,k} - \delta_3 &= 4\delta_2 - 2^{k+1} - 2^{k-1} + 2 - (\delta_2 - 2) \\ &= 3\delta_2 - 2^{k+1} - 2^{k-1} + 4 \\ &\geq 3\delta_2 - 2^{(2t-2)+1} - 2^{(2t-2)-1} + 4 \\ &= 3\delta_2 - 2^{2t-1} - 2^{2t-3} + 4 > 0. \end{aligned}$$

4. Si $k = 2t-1$, entonces

$$y_{\delta_3,k} = n + 2\delta_2 - 2^{2t-2} - 2^{2t} + 1.$$

Así,

$$\begin{aligned} y_{\delta_3,k} - \delta_3 &= n + 2\delta_2 - 2^{2t-2} - 2^{2t} + 1 - (\delta_2 - 2) \\ &= n + \delta_2 - 2^{2t-2} - 2^{2t} + 3 \\ &= 2^{2t+1} + 1 + \delta_2 - 2^{2t-2} - 2^{2t} + 3 \\ &= \delta_2 + 2^{2t} - 2^{2t-2} + 4 > 0. \end{aligned}$$

$$\begin{aligned} n - y_{\delta_3,k} - \delta_3 &= n - (n + 2\delta_2 - 2^{2t-2} - 2^{2t} + 1) - (\delta_2 - 2) \\ &= 2^{2t-2} + 2^{2t} + 1 - 3\delta_2 \\ &= 2^{2t-2} + 2^{2t} + 1 - 3\left(\frac{n-3}{6}\right) \\ &= 2^{2t-2} + 2^{2t} + 1 - \frac{2^{2t+1} - 2}{2} \\ &= 2^{2t-2} + 2^{2t} + 1 - 2^{2t} + 1 \\ &= 2^{2t-2} + 2 > 0. \end{aligned}$$

5. Si $k = 2t$, entonces

$$y_{\delta_3,k} = 4\delta_2 - 2^{2t-1} + 3.$$

Luego,

$$\begin{aligned} y_{\delta_3,k} - \delta_3 &= 4\delta_2 - 2^{2t-1} + 3 - (\delta_2 - 2) \\ &= 3\delta_2 - 2^{2t-1} + 5 \\ &= \frac{2^{2t+1} - 2}{2} - 2^{2t-1} + 5 \\ &= 2^{2t} - 2^{2t-1} + 4 \\ &= 2^{2t-1} + 4 > 0, \end{aligned}$$

$$\begin{aligned} n - y_{\delta_3,k} - \delta_3 &= n - (4\delta_2 - 2^{2t-1} + 3) - (\delta_2 - 2) \\ &= n - 5\delta_2 + 2^{2t-1} - 1 \\ &= n - 3 - 5\delta_2 + 2^{2t-1} + 2 \\ &= 6\delta_2 - 5\delta_2 + 2^{2t-1} + 2 \\ &= \delta_2 + 2^{2t-1} + 2 > 0. \end{aligned}$$

Con los casos anteriores se mostró que δ_3 es un líder de clase lateral.

Mostremos ahora que $y_{\delta_4,k} - \delta_4 \geq 0$ y $n - y_{\delta_4,k} - \delta_4 \geq 0$.

1. Si $k = 0, 1, 2$, entonces $y_{\delta_4,k} = 2^k\delta_4 \geq \delta_4$, de modo que $y_{\delta_4,k} - \delta_4 \geq 0$. Además

$$\begin{aligned} n - y_{\delta_4,k} - \delta_4 &= n - 2^k(\delta_2 - 8) - (\delta_2 - 8) \\ &= n - (2^k + 1)(\delta_2 - 8) \\ &= n - 3 - (2^k + 1)\delta_2 + 2^{k+3} + 8 + 3 \\ &= 6\delta_2 - (2^k + 1)\delta_2 + 2^{k+3} + 11 \\ &= (6 - 2^k - 1)\delta_2 + 2^{k+3} + 11 > 0. \end{aligned}$$

2. Si $k = 3, 5, \cdots, 2t-5$, tenemos que

$$y_{\delta_4,k} = 2\delta_2 - 2^{k+3} - 2^{k-1} + 1.$$

A partir de donde

$$\begin{aligned} y_{\delta_4,k} - \delta_4 &= 2\delta_2 - 2^{k+3} - 2^{k-1} + 1 - (\delta_2 - 8) \\ &= \delta_2 - 2^{k+3} - 2^{k-1} + 9 \\ &\geq \delta_2 - 2^{(2t-5)+3} - 2^{(2t-5)-1} + 9 \\ &= \delta_2 - 2^{2t-2} - 2^{2t-6} + 9 > 0, \end{aligned}$$

y

$$\begin{aligned} n - y_{\delta_4,k} - \delta_4 &= n - (2\delta_2 - 2^{k+3} - 2^{k-1} + 1) - (\delta_2 - 8) \\ &= n - 3\delta_2 + 2^{k+3} + 2^{k-1} + 7 \\ &= n - 3 - 3\delta_2 + 2^{k+3} + 2^{k-1} + 10 \\ &= 6\delta_2 - 3\delta_2 + 2^{k+3} + 2^{k-1} + 10 \\ &= 3\delta_2 + 2^{k+3} + 2^{k-1} + 10 > 0. \end{aligned}$$

3. Si $k = 4, 6, \cdots, 2t-4$, se tiene que

$$y_{\delta_4,k} = 4\delta_2 - 2^{k+3} - 2^{k-1} + 2.$$

De modo que

$$\begin{aligned} y_{\delta_4,k} - \delta_4 &= 4\delta_2 - 2^{k+3} - 2^{k-1} + 2 - (\delta_2 - 8) \\ &= 3\delta_2 - 2^{k+3} - 2^{k-1} + 10 \\ &\geq 3\delta_2 - 2^{(2t-4)+3} - 2^{(2t-4)-1} + 10 \\ &= 3\delta_2 - 2^{2t-1} - 2^{2t-5} + 10 \\ &= \frac{2^{2t+1} - 2}{2} - 2^{2t-1} - 2^{2t-5} + 10 \\ &= 2^{2t} - 2^{2t-1} - 2^{2t-5} + 9 \\ &= 2^{2t-1} - 2^{2t-5} + 9 > 0. \end{aligned}$$

$$\begin{aligned} n - y_{\delta_4,k} - \delta_4 &= n - (4\delta_2 - 2^{k+3} - 2^{k-1} + 2) - (\delta_2 - 8) \\ &= n - 5\delta_2 + 2^{k+3} + 2^{k-1} + 6 \\ &= n - 3 - 5\delta_2 + 2^{k+3} + 2^{k-1} + 9 \\ &= 6\delta_2 - 5\delta_2 + 2^{k+3} + 2^{k-1} + 9 \\ &= \delta_2 + 2^{k+3} + 2^{k-1} + 9 > 0. \end{aligned}$$

4. Si $k = 2t - 3$, entonces

$$y_{\delta_4,k} = 5\delta_2 - 2^{2t-4} + 3,$$

por lo que

$$\begin{aligned} y_{\delta_4,k} - \delta_4 &= 5\delta_2 - 2^{2t-4} + 3 - (\delta_2 - 8) \\ &= 4\delta_2 - 2^{2t-4} + 11 \\ &= 4\delta_2 - 2^{2t-4} - (2^{2t} + 1) + 2^{2t} + 12 \\ &= 4\delta_2 - 2^{2t-4} - 3\delta_2 + 2^{2t} + 12 \\ &= \delta_2 - 2^{2t-4} + 2^{2t} + 12 > 0, \end{aligned}$$

además

$$\begin{aligned} n - y_{\delta_4,k} - \delta_4 &= n - 5\delta_2 + 2^{2t-4} - 3 - (\delta_2 - 8) \\ &= n - 6\delta_2 + 2^{2t-4} + 5 \\ &= n - (n - 3) + 2^{2t-4} + 5 \\ &= 2^{2t-4} + 8 > 0. \end{aligned}$$

5. Si $k = 2t - 2$, obtenemos que

$$y_{\delta_4,k} = 4\delta_2 - 2^{2t-3} + 3,$$

así

$$\begin{aligned} y_{\delta_4,k} - \delta_4 &= 4\delta_2 - 2^{2t-3} + 3 - (\delta_4 - 8) \\ &= 3\delta_2 - 2^{2t-3} + 11 \\ &= 3 \cdot \frac{2^{2t+1} - 2}{6} - 2^{2t-3} + 11 \\ &= 2^{2t} - 1 - 2^{2t-3} + 11 \\ &= 2^{2t} - 2^{2t-3} + 10 > 0, \end{aligned}$$

y

$$\begin{aligned} n - y_{\delta_4,k} - \delta_4 &= n - 4\delta_2 + 2^{2t-3} - 3 - (\delta_2 - 8) \\ &= n - 5\delta_2 + 2^{2t-3} + 5 \\ &= n - 3 - 5\delta_2 + 2^{2t-3} + 8 \\ &= 6\delta_2 - 5\delta_2 + 2^{2t-3} + 8 \\ &= \delta_2 + 2^{2t-3} + 8 > 0. \end{aligned}$$

6. Si $k = 2t - 1$ obtenemos que

$$y_{\delta_4,k} = 2\delta_2 - 2^{2t-2} + 3,$$

de modo que

$$\begin{aligned} y_{\delta_4,k} - \delta_4 &= 2\delta_2 - 2^{2t-2} + 3 - (\delta_2 - 8) \\ &= \delta_2 - 2^{2t-2} + 11 > 0, \end{aligned}$$

además

$$\begin{aligned} n - y_{\delta_4,k} - \delta_4 &= n - 2\delta_2 + 2^{2t-2} - 3 - (\delta_2 - 8) \\ &= n - 3\delta_2 + 2^{2t-2} + 5 \\ &= n - 3 - 3\delta_2 + 2^{2t-2} + 8 \\ &= 6\delta_2 - 3\delta_2 + 2^{2t-2} + 8 \\ &= 3\delta_2 + 2^{2t-2} + 8 > 0. \end{aligned}$$

7. Si $k = 2t$ se puede derivar que

$$y_{\delta_4,k} = 4\delta_2 - 2^{2t-1} + 6,$$

por lo que

$$\begin{aligned} y_{\delta_4,k} - \delta_4 &= 4\delta_2 - 2^{2t-1} + 6 - (\delta_2 - 8) \\ &= 3\delta_2 - 2^{2t-1} + 14 \\ &= 2^{2t} - 1 - 2^{2t-1} + 14 \\ &= 2^{2t} - 2^{2t-1} + 13 > 0, \end{aligned}$$

$$\begin{aligned} n - y_{\delta_4,k} - \delta_4 &= n - (4\delta_2 - 2^{2t-1} + 6) - (\delta_2 - 8) \\ &= n - 5\delta_2 + 2^{2t-1} + 2 \\ &= n - 3 - 5\delta_2 + 2^{2t-1} + 5 \\ &= 6\delta_2 - 5\delta_2 + 2^{2t-1} + 5 \\ &= \delta_2 + 2^{2t-1} + 5 > 0. \end{aligned}$$

Con los casos anteriores se demuestra que δ_4 es un líder de clase lateral.

Resta probar que $y_{\delta_5,k} - \delta_5 \geq 0$ y $n - y_{\delta_5,k} - \delta_5 \geq 0$. Se presentan los siguientes casos:

1. Si $k = 0, 1, 2$, entonces $y_{\delta_5,k} = 2^k\delta_5 \geq \delta_5$. De modo que $y_{\delta_5,k} - \delta_5 \geq 0$. Además,

$$\begin{aligned} n - y_{\delta_5,k} - \delta_5 &= n - 2^k(\delta_2 - 10) - (\delta_2 - 10) \\ &= n - (2^k + 1)\delta_2 + 2^k \cdot 10 + 10 \\ &= n - 3 - (2^k + 1)\delta_2 + 2^k \cdot 10 + 13 \\ &= 6\delta_2 - (2^k + 1)\delta_2 + 2^k \cdot 10 + 13 \\ &= (6 - 2^k - 1)\delta_2 + 2^{k+3} + 2^{k+1} + 13 > 0. \end{aligned}$$

2. Si $k = 3, 5, \cdots, 2t - 5$, entonces

$$y_{\delta_5,k} = 2\delta_2 - 2^{k+3} - 2^{k+1} - 2^{k-1} + 1,$$

$$\begin{aligned} y_{\delta_5,k} - \delta_5 &= 2\delta_2 - 2^{k+3} - 2^{k+1} - 2^{k-1} + 1 - (\delta_5 - 10) \\ &= \delta_2 - 2^{k+3} - 2^{k+1} - 2^{k-1} + 11 \\ &\geq \delta_2 - 2^{(2t-5)+3} - 2^{(2t-5)+1} - 2^{(2t-5)-1} + 11 \\ &= \delta_2 - 2^{2t-2} - 2^{2t-4} - 2^{2t-6} + 11 > 0, \end{aligned}$$

$$\begin{aligned} n - y_{\delta_5,k} - \delta_5 &= n - (2\delta_2 - 2^{k+3} - 2^{k+1} - 2^{k-1} + 1) - (\delta_2 - 10) \\ &= n - 3\delta_2 + 2^{k+3} + 2^{k+1} + 2^{k-1} + 9 \\ &= n - 3 - 3\delta_2 + 2^{k+3} + 2^{k+1} + 2^{k-1} + 12 \\ &= 3\delta_2 - 3\delta_2 + 2^{k+3} + 2^{k+1} + 2^{k-1} + 12 \\ &= 3\delta_2 + 2^{k+3} + 2^{k+1} + 2^{k-1} + 12 > 0. \end{aligned}$$

3. Si $k = 4, 6, \cdots, 2t - 4$, entonces deducimos

$$y_{\delta_5,k} = 4\delta_2 - 2^{k+3} - 2^{k+1} - 2^{k-1} + 2,$$

de donde

$$\begin{aligned} y_{\delta_5,k} - \delta_5 &= 4\delta_2 - 2^{k+3} - 2^{k+1} - 2^{k-1} + 2 - (\delta_2 - 10) \\ &= 3\delta_2 - 2^{k+3} - 2^{k+1} - 2^{k-1} + 12 \\ &\geq 3\delta_2 - 2^{(2t-4)+3} - 2^{(2t-4)+1} - 2^{(2t-4)-1} + 12 \\ &= 3\delta_2 - 2^{2t-1} - 2^{2t-3} - 2^{2t-5} + 12 \\ &= 2^{2t} - 1 - 2^{2t-1} - 2^{2t-3} - 2^{2t-5} + 12 \\ &= 2^{2t-1} - 2^{2t-3} - 2^{2t-5} + 11, \end{aligned}$$

$$\begin{aligned} n - y_{\delta_5,k} - \delta_5 &= n - (4\delta_2 - 2^{k+3} - 2^{k+1} - 2^{k-1} + 2) - (\delta_2 - 10) \\ &= n - 5\delta_2 + 2^{k+3} + 2^{k+1} + 2^{k-1} + 8 \\ &= (n - 3) - 5\delta_2 + 2^{k+3} + 2^{k+1} + 2^{k-1} + 11 \\ &= 6\delta_2 - 5\delta_2 + 2^{k+3} + 2^{k+1} + 2^{k-1} + 11 \\ &= \delta_2 + 2^{k+3} + 2^{k+1} + 2^{k-1} + 11 > 0. \end{aligned}$$

4. Si $k = 2t - 3$, entonces se obtiene que

$$y_{\delta_5,k} = 5\delta_2 - 2^{2t-2} - 2^{2t-4} + 3,$$

luego

$$\begin{aligned} y_{\delta_5,k} - \delta_5 &= 5\delta_2 - 2^{2t-2} - 2^{2t-4} + 3 - (\delta_2 - 10) \\ &= 4\delta_2 - 2^{2t-2} - 2^{2t-4} + 13 \\ &= 4\delta_2 - (2^{2t} - 1) + 2^{2t} - 2^{2t-2} - 2^{2t-4} + 12 \\ &= 4\delta_2 - 3\delta_2 + 2^{2t} - 2^{2t-2} - 2^{2t-4} + 12 \\ &= \delta_2 + 2^{2t} - 2^{2t-2} - 2^{2t-4} + 12 > 0. \end{aligned}$$

5. Si $k = 2t - 2$, se obtiene que

$$y_{\delta_5,k} = 4\delta_2 - 2^{2t-1} - 2^{2t-3} + 3,$$

así

$$\begin{aligned} y_{\delta_5,k} - \delta_5 &= 4\delta_2 - 2^{2t-1} - 2^{2t-3} + 3 - (\delta_2 - 10) \\ &= 3\delta_2 - 2^{2t-1} - 2^{2t-3} + 13 \\ &= 2^{2t} - 1 - 2^{2t-1} - 2^{2t-3} + 13 \\ &= 2^{2t-1} - 2^{2t-3} + 12 > 0, \end{aligned}$$

$$\begin{aligned} n - y_{\delta_5,k} - \delta_5 &= n - (4\delta_2 - 2^{2t-1} - 2^{2t-3} + 3) - (\delta_2 - 10) \\ &= n - 5\delta_2 + 2^{2t-1} + 2^{2t-3} + 7 \\ &= (n-3) - 5\delta_2 + 2^{2t-1} + 2^{2t-3} + 10 \\ &= 6\delta_2 - 5\delta_2 + 2^{2t-1} + 2^{2t-3} + 10 \\ &= \delta_2 + 2^{2t-1} + 2^{2t-3} + 10 > 0. \end{aligned}$$

6. Si $k = 2t - 1$, tenemos que

$$y_{\delta_5,k} = 5\delta_2 - 2^{2t-2} + 5,$$

por lo que

$$\begin{aligned} y_{\delta_5,k} - \delta_5 &= 5\delta_2 - 2^{2t-2} + 5 - (\delta_2 - 10) \\ &= 4\delta_2 - 2^{2t-2} + 15 \\ &= 4\delta_2 - (2^{2t} - 1) + 2^{2t} - 2^{2t-2} + 14 \\ &= 4\delta_2 - 3\delta_2 + 2^{2t} - 2^{2t-2} + 14 \\ &= \delta_2 + 2^{2t} - 2^{2t-2} + 14 > 0, \end{aligned}$$

$$\begin{aligned} n - y_{\delta_5,k} - \delta_5 &= n - (5\delta_2 - 2^{2t-2} + 5) - (\delta_2 - 10) \\ &= n - 6\delta_2 + 2^{2t-2} + 5 \\ &= n - (n-3) + 2^{2t-2} + 5 \\ &= 2^{2t-2} + 8 > 0. \end{aligned}$$

7. Si $k = 2t$, se deduce que

$$y_{\delta_5,k} = 4\delta_2 - 2^{2t-1} + 7,$$

$$\begin{aligned} y_{\delta_5,k} - \delta_5 &= 4\delta_2 - 2^{2t-1} + 7 - (\delta_2 - 10) \\ &= 3\delta_2 - 2^{2t-1} + 17 \\ &= 2^{2t} - 1 - 2^{2t-1} + 17 \\ &= 2^{2t-1} + 16 > 0, \end{aligned}$$

$$\begin{aligned} n - y_{\delta_5,k} - \delta_5 &= n - (4\delta_2 - 2^{2t-1} + 7) - (\delta_2 - 10) \\ &= n - 5\delta_2 + 2^{2t-1} + 3 \\ &= (n-3) - 5\delta_2 + 2^{2t-1} + 6 \\ &= 6\delta_2 - 5\delta_2 + 2^{2t-1} + 6 \\ &= \delta_2 + 2^{2t-1} + 6 > 0. \end{aligned}$$

Mostrados los casos anteriores se concluye que δ_5 es un líder de clase lateral.

■

Los siguientes resultados se utilizarán para demostrar que si i es líder de clase lateral e $i \notin \{\delta_1, \delta_2, \delta_3, \delta_4, \delta_5\}$, entonces $i < \delta_5$.

Se introducirá un algoritmo iterativo para particionar el conjunto $I^{(t)} = [1, 2^{2t-5}]$, para $t \geq 5$, en 2^{t-3} subintervalos disjuntos $I_1, I_2, \ldots, I_{2^{t-3}}$ tales que $I^{(t)} = I_1 \cup I_2 \cdots \cup I_{2^{t-3}}$.

Algoritmo Iterativo 1:

1. Si $t = 5$, entonces $I^{(5)} = [1, 2^{2\cdot 5-5}] = [1, 2^5]$ se puede particionar en los siguientes $2^{5-3} = 2^2$ subintervalos.

   $I_1 = I_{2^0} = [1, 2^1] = [1, 2] = [a_1, b_1]$,

   $I_2 = I_{2^1} = [a_1 + 2^1, 2^{2\cdot 1+1}] = [3, 8] = [a_2, b_2]$,

   $I_3 = I_{1+2^1} = I_1 + 2^{2\cdot 1+1} = I_1 + 2^3 = [9, 10] = [a_3, b_3]$.

   $I_4 = I_{2^2} = [a_{2^1} + 2^{2\cdot 1+1}, 2^{2\cdot 2+1}] = [a_2 + 2^3, 2^5] = [11, 32] = [a_4, b_4]$.

2. Si $t = 6$, entonces $I^{(6)} = [1, 2^7]$ puede ser particionado en 2^3 subintervalos. Sea $I_s = [a_s, b_s]$ para $1 \leq s \leq 4$ como en el inciso 1).

   Para $s = j + 2^2 \leq 2^{2+1}$ con $1 \leq j \leq 2^2 - 1$, consideremos los siguientes conjuntos:

   $$I_s = I_j + 2^{2\cdot 2+1} = I_j + 2^5 = [a_s, b_s] \text{ para } 5 \leq s \leq 7.$$

   Es decir,

   $I_5 = I_1 + 2^5 = [33, 34] = [a_5, b_5]$,

$I_6 = I_2 + 2^5 = [35, 40] = [a_6, b_6]$,

$I_7 = I_3 + 2^5 = [41, 42] = [a_7, b_7]$.

Además,

$I_8 = I_{2^3} = [a_{2^2} + 2^{2\cdot 2+1}, 2^{2\cdot 3+1}] = [a_4 + 2^5, 2^7] = [43, 128]$.

3. Cuando $t \geq 7$. Si la partición de $I^{(t-1)}$ está dada por

$$I^{(t-1)} = [1, 2^{2t-7}] = I_1 \cup I_2 \cdots \cup I_{2^{t-4}}$$

donde $I_j = [a_j, b_j]$.

Para $u = j + 2^{t-4}$ con $1 \leq j \leq 2^{t-4} - 1$, consideramos los siguientes conjuntos:

$$I_u = I_j + 2^{2\cdot(t-4)+1} = I_j + 2^{2t-7} = [a_j + 2^{2t-7}, b_j + 2^{2t-7}].$$

Sea $I_{2^{t-3}} = [a_{2^{t-4}} + 2^{2\cdot(t-4)+1}, 2^{2\cdot(t-3)+1}] = [a_{2^{t-4}} + 2^{2t-7}, 2^{2t-5}]$.

Entonces, la partición de $I^{(t)} = [1, 2^{2t-5}]$ se obtiene de forma iterativa como

$$I^{(t)} = I^{(t-1)} \bigcup \left(\bigcup_{u=2^{t-4}+1}^{2^{t-3}} I_u \right) = (I_1 \cup I_2 \cdots \cup I_{2^{t-4}}) \cup I_{2^{t-4}+1} \cdots \cup I_{2^{t-3}}.$$

Observación 4.0.8. Del Algoritmo Iterativo 1, se puede derivar lo siguiente:

1. Para $0 \leq r \leq t-3$, I_{2^r} tiene la forma

$$I_{2^r} = \begin{cases} [1, 2] = [1, 2^{2r+1}], & \text{si } r = 0 \\ [1 + (2 + 2^3 + \cdots + 2^{2r-1}), 2^{2r+1}], & \text{si } 1 \leq r \leq t-3 \end{cases}$$

2. Para cada $s \in [1, 2^{t-3} - 1]$, sea la expansión $2-$ádica de s

$$s = a_0 2^0 + a_1 2^1 + a_2 2^2 + \cdots + a_{t-4} 2^{t-4} = (a_0 a_1 a_2 \cdots a_{t-4})_2.$$

Se define $r = r_s = \text{mín}\{j | a_j = 1, 0 \leq j \leq t-4\}$. Podemos derivar que

$$\begin{aligned} I_s &= I_{2^r} + a_{r+1} 2^{2r+3} + a_{1+2} 2^{2r+5} + \cdots + a_{t-a} 2^{2t-7} \\ &= I_{2^r} + 2^{2r+3}(a_{r+1} + a_{r+2} 2^2 + \cdots + a_{t-4} 2^{2(t-r-5)}) \\ &= I_{2^r} + 2^{2r+3}\lambda, \end{aligned}$$

donde $\lambda = a_{r+1} + a_{r+2} 2^2 + \cdots + a_{t-4} 2^{2(t-r-5)}$. Se puede observar que $0 \leq \lambda \leq 1 + 2^2 + \cdots + 2^{2(t-r-5)} < 2^{2(t-r-4)}$ para $s \leq 2^{t-3} - 1$.

Notemos también que $I_{2^{t-3}} = I_{2^{t-3}} + 2^{2r+3}\lambda$ con $\lambda = 0$.

De 1. y 2. se deriva que para cualquier $s \in [1, 2^{t-3}]$ existe un entero $0 \leq \lambda \leq 2^{2(t-r-4)}$ de forma que

$$I_s = I_{r,\lambda} = I_{2^r} + 2^{2r+3}\lambda, \qquad \text{donde } 0 \leq r \leq t-3.$$

Lema 4.0.9. Sea $\delta_2 = \frac{n-3}{6}$. Si $i \in [\delta_2 + 2, \delta_2 + 2^{2t-4}]$ es impar, entonces i no es un líder de clase lateral.

Demostración. Se consideran todos los valores de i impares. Se puede representar i como

$$i = \delta_2 + 2l \qquad \text{con } l \in I^{(t)} = [1, 2^{2t-5}].$$

Sea $I^{(t)} = \bigcup_{s=1}^{2^{t-3}} I_s$ una partición de $I^{(t)}$ obtenida del Algoritmo Iterativo 1. Como $l \in I^{(t)}$, entonces existe un entero $s \in [1, 2^{t-3}]$ tal que $l \in I_s$. De la Observación 4.0.8, sabemos que $I_s = I_{2^r} + 2^{2r+3}\lambda$, donde $0 \leq r \leq t-3$ está determinada por s y $0 \leq \lambda \leq 2^{2(t-r-4)}$. Así, i se denota por

$$i = \delta_2 + 2l = \delta_2 + 2(l_0 + 2^{2r+3}\lambda), \qquad \text{donde } l_0 \in I_{2^r}.$$

Eligiendo $k = 2t - 2r - 3$, derivamos lo siguiente

$$\begin{aligned} y_{i,k} \equiv 2^k i &= 2^{2t-2r-3}(\delta_2 + 2(l_0 + 2^{2r+3}\lambda)) \\ &= 2^{2t-2r-3}\delta_2 + 2^{2t-2r-2}l_0 + 2^{2t+1}\lambda \\ &\equiv 2\delta_2 - 2^{2t-2r-4} + 1 + 2^{2t-2r-2}l_0 + 2^{2t+1}\lambda \\ &= 2\delta_2 - 2^{2(t-r-2)} + 2^{2(t-r-1)}l_0 + 1 - \lambda + \lambda(2^{2t+1} + 1) \\ &= 2\delta_2 - 2^{2(t-r-2)} + 2^{2(t-r-1)}l_0 + 1 - \lambda + \lambda n. \end{aligned}$$

De donde

$$y_{i,k} = 2\delta_2 - 2^{2(t-r-2)} + 2^{2(t-r-1)}l_0 + 1 - \lambda.$$

De acuerdo a los intervalos en los que se encuentran r, l_0 y λ, cuando $k = 2t - 2r - 3$, se muestra que $\frac{n-\delta_2}{2} < y_{i,k} < \frac{n+\delta_2}{2}$. Primero observemos que

$$\begin{aligned} \frac{n+\delta_2}{2} &= \frac{n-3+\delta_2+3}{2} \\ &= \frac{6\delta_2+\delta_2+3}{2} \\ &= \frac{4\delta_2+3\delta_2+3}{2} \\ &= \frac{4\delta_2+2^{2t}-1+3}{2} \\ &= 2\delta_2 + 2^{2t-1} + 1, \end{aligned}$$

y

$$\begin{aligned} \frac{n-\delta_2}{2} &= \frac{n-3-\delta_2+3}{2} \\ &= \frac{6\delta_2-\delta_2+3}{2} \\ &= \frac{4\delta_2+\delta_2+3}{2} \\ &= 2\delta_2 + (2^{2t-3} + 2^{2t-5} + \cdots + 2^3 + 2) + 2. \end{aligned}$$

La cota superior de $y_{i,k}$:

$$\begin{aligned} y_{i,k} &= 2\delta_2 - 2^{2(t-r-2)} + 2^{2(t-r-1)}l_0 + 1 - \lambda \\ &\leq 2\delta_2 - 2^{2(t-r-2)} + 2^{2(t-r-1)}l_0 + 1 \\ &\leq 2\delta_2 - 2^{2(t-r-2)} + 2^{2(t-r-1)} \cdot 2^{2r+1} + 1 \\ &= 2\delta_2 - 2^{2(t-r-2)} + 2^{2t-1} + 1 \\ &< \frac{n+\delta_2}{2} \end{aligned}$$

Analicemos ahora la cota inferior de $y_{i,k}$:

Si $i = 0$, entonces $l_0 \in [1, 2]$, obtenemos que

$$\begin{aligned} y_{i,k} &= 2\delta_2 - 2^{2(t-r-2)} + 2^{2(t-r-1)}l_0 + 1 - \lambda \\ &> 2\delta_2 - 2^{2(t-r-2)} + 2^{2(t-r-1)}l_0 + 1 - 2^{2(t-4)} \\ &\geq 2\delta_2 - 2^{2(t-r-2)} + 2^{2(t-r-1)} \cdot 1 + 1 - 2^{2(t-4)} \\ &> \frac{n-\delta_2}{2}. \end{aligned}$$

Si $1 \leq r \leq t-3$, entonces $l_0 \in [1 + (2 + 2^3 + \cdots + 2^{2r-1}), 2^{2r+1}]$. Así

$$\begin{aligned} y_{i,k} &= 2\delta_2 - 2^{2(t-r-2)} + 2^{2(t-r-1)}l_0 + 1 - \lambda \\ &> 2\delta_2 - 2^{2(t-r-2)} + 2^{2(t-r-1)}l_0 + 1 - 2^{2(t-r-4)} \\ &\geq 2\delta_2 - 2^{2(t-r-2)} + 2^{2(t-r-1)}\left[1 + (2 + 2^3 + \cdots + 2^{2r-1})\right] + 1 - 2^{2(t-r-4)} \\ &= 2\delta_2 - 2^{2(t-r-2)} + 2^{2(t-r-1)} + \left(2^{2t-3} + 2^{2t-5} + \cdots + 2^{2t-2r-1}\right) + 1 - 2^{2(t-r-4)} \\ &\geq 2\delta_2 - 2^{2(t-(t-3)-2)} + 2^{2(t-(t-3)-1)} + \left(2^{2t-3} + 2^{2t-5} + \cdots + 2^{2t-2(t-3)-1}\right) + 1 - 2^{2(t-(t-3)-4)} \\ &= 2\delta_2 - 2^2 + 2^4 + \left(2^{2t-3} + 2^{2t-5} + \cdots + 2^5\right) + 1 - 2^{-2} \\ &= 2\delta_2 + \left(2^{2t-3} + 2^{2t-5} + \cdots + 2^5 + 2^4\right) - 2^2 + 1 - 2^{-2} \\ &> \frac{n-\delta_2}{2}. \end{aligned}$$

Con lo mostrado, se verifica que $\frac{n-\delta_2}{2} < y_{i,k} < \frac{n+\delta_2}{2}$.

Si $\frac{n-\delta_2}{2} < y_{i,k} \leq \frac{n-1}{2}$, entonces $n - \delta_2 < 2y_{i,k} < n - 1$. Se sigue que $1 - n < -2y_{i,k} < \delta_2 - n$, más aún $1 < n - 2y_{i,k} < \delta_2$. Es decir, existe $j_{i,k} = n - 2y_{i,k}$ con $j_{i,k} \in C_{y_{i,k}}$ y $j_{i,k} \in C_i$ tal que $1 \leq j_{i,k} < \delta_2$.

Si $\frac{n+1}{2} \leq y_{i,k} < \frac{n+\delta_2}{2}$, entonces $n + 1 \leq 2y_{i,k} < n + \delta_2$, de donde $1 \leq 2y_{i,k} - n < \delta_2$. Así, existe un entero $j_{i,k} = 2y_{i,k} - n \equiv 2y_{i,k}$ con $j_{i,k} \in C_{y_{i,k}}$ y $j_{i,k} \in C_i$ tal que $1 \leq j_{i,k} < \delta_2$.

Con la discusión previa tenemos que cuando $i \in [\delta_2 + 2, \delta_2 + 2^{2t-4}]$, existe un entero $j_{i,k} \in [1, \delta_2)$ tal que $j_{i,k} \in C_i$. Es decir, existe un entero en la clase lateral ciclotómica de i menor a i, cuando $i \in [\delta_2 + 2, \delta_2 + 2^{2t-4}]$.

Se concluye que i no es un líder de clase lateral cuando $i \in [\delta_2 + 2, \delta_2 + 2^{2t-4}]$. ■

Lema 4.0.10. Sean $\delta_1 = \frac{n}{3}$ y $\delta_2 = \frac{n-3}{6}$ dados como antes. Si un entero impar $i > \delta_2$ y $i \neq \delta_1$, entonces i no es un líder de clase lateral.

Demostración. Es suficiente verificar que existe $k \in [0, m-1]$ tal que $y_{i,k} < i$ o $n - y_{i,k} < i$ para $i > \delta_2$ y $i \neq \delta_1$. Se presentan los siguientes casos:

1. $i \in \left[\frac{n+1}{2}, n-1\right]$. Observemos que $i \leq n-1 < n$ y como $\frac{n+1}{2} \leq i$, entonces $n < n+1 \leq 2i$. De donde, $i < n < 2i$. Tomando $k = 0$, se tiene que $y_{i,0} = i$, de modo que $n - y_{i,0} = n - i < i$.

2. $i \in \left[\frac{n}{3} + 1, \frac{n-1}{2}\right]$. Notemos que $\frac{n}{3} < \frac{n}{3} + 1 \leq i$, por lo que $n < 3i$, además $i \leq \frac{n-1}{2}$, de donde $2i \leq n - 1 < n$. Resumiendo, se tiene que $2i < n < 3i$. Considerando $k = 1$, $n - y_{i,1} = n - 2i < i$.

3. $i \in \left[\lceil \frac{n}{4} \rceil, \frac{n}{3} - 1\right]$. Se satisface que $\frac{n}{4} < \lceil \frac{n}{4} \rceil \leq i$, por lo que $n < 4i$. Además $i \leq \frac{n}{3} - 1 < \frac{n}{3}$, y así $3i < n$. De lo anterior, $3i < n < 4i$ y eligiendo $k = 2$, $y_{i,2} = 4i - n < i$.

4. $x \in [\lceil \frac{n}{5} \rceil, \lfloor \frac{n}{4} \rfloor]$. Tenemos que $\frac{n}{5} < i < \frac{n}{4}$, a partir de donde $4i < n < 5i$. Tomando $k = 2$, se obtiene que $n - y_{i,2} = n - 4i < i$.

5. $i \in [\lceil \frac{3n}{16} \rceil, \lfloor \frac{n}{5} \rfloor]$. Se cumple que $\frac{3n}{16} < i < \frac{n}{5}$, por lo que $15i < n < 16i$. Considerando $k = 4$, se tiene que $y_{i,4} = 16i - 3n < i$.

Del Lema 4.0.9 y de los casos anteriores, se infiere que para cada $i \in [\delta_2 + 2, \delta_2 + 2^{2t-4}] \bigcup [\lceil \frac{3n}{16} \rceil, n-1] \setminus \left\{\frac{n}{3}\right\}$, i no es un líder de clase lateral.

Notemos que

$$\begin{aligned}
\lceil \frac{3n}{16} \rceil &= \lceil \frac{3n}{16} - \frac{9}{16} \rceil \\
&= \lceil \frac{3(n-3)}{16} \rceil \\
&= \lceil \frac{9}{8} \frac{n-3}{6} \rceil \\
&= \lceil \frac{n-3}{6} + \frac{n-3}{6 \cdot 8} \rceil \\
&= \lceil \delta_2 + \frac{\delta_2}{8} \rceil \\
&= \delta_2 + \lceil \frac{\delta_2}{8} \rceil \\
&= \delta_2 + \lceil \frac{2^{2t+1} - 2}{3 \cdot 2^4} \rceil \\
&= \delta_2 + \lceil \frac{2^{2t-3} - 2^{-3}}{3} \rceil \\
&< \delta_2 + 2^{2t-4}.
\end{aligned}$$

Se deduce que si $i \in [\delta_2 + 2, n-1] \setminus \{\delta_1\}$, entonces i no es un líder de clase lateral. ■

Teorema 4.0.11. Sean v, como en el Teorema 4.0.7. Si i es un líder de clase lateral e $i \notin \{\delta_1, \delta_2, \delta_3, \delta_4, \delta_5\}$, entonces $i < \delta_5$.

Demostración. Sea i un líder de clase lateral distinto de $\delta_1, \delta_2, \delta_3, \delta_4, \delta_5$.

Por el Lema 4.0.10, i no está entre δ_1 y δ_2. Sólo falta probar que $\delta_2 - 4$ y $\delta_2 - 6$ no son un líderes de clase lateral. Observemos que

$$\begin{aligned} 2^{2t-3}(\delta_2 - 4) &\equiv 2^{2t-3}(\delta_2 - 4) - \frac{2^{2t-4}-1}{3}n \\ &= 2^{2t-3} + 2^{2t-5} + \cdots + 2 + 2^{2t-4} \\ &< \delta_2 - 4, \end{aligned}$$

$$\begin{aligned} -2^{2t-3}(\delta_2 - 6) &\equiv \frac{2^{2t-4}-1}{3}n - 2^{2t-3}(\delta_2 - 6) \\ &= \delta_2 - 2^{2t-2} + 2^{2t-4} \\ &= \delta_2 - 6, \end{aligned}$$

de donde se concluye que ni $\delta_2 - 4$ ni $\delta_2 - 6$ son un líder de clase lateral. Por lo tanto, δ_3, δ_4 y δ_5 son el tercer, cuarto y quinto líder de clase lateral más grande, respectivamente. ■

Lema 4.0.12. Si $1 \leq i \leq 2^{t+2}+7$ o $i \in \{\delta_2, \delta_3, \delta_4, \delta_5\}$ con $\delta_2 = \frac{n-3}{6}, \delta_3 = \delta_2 - 2, \delta_4 = \delta_2 - 8$ y $\delta_5 = \delta_2 - 10$, entonces $|C_i| = 2m$.

Demostración. La demostración se realizará por contradicción. Supongamos que $|C_i| = k$ con $k < 2m$, entonces $2^k i \equiv i$, es decir $i(2^k - 1) \equiv 0$. Desde que $k|2m$ y m es impar, se tiene que $k = m, \frac{2m}{3}$ o $k \leq \frac{2m}{5}$.

1. Si $k = m$, entonces $(2^k - 1, n) = (2^m - 1, 2^m + 1) = 1$. Supongamos que $i(2^k - 1) \equiv 0$. Dado que $(2^m - 1, 2^m + 1) = 1$, entonces $i \equiv 0$, pero $1 \leq i \leq 2^{t+2} + 7 < n$, por lo tanto $i(2^k - 1) \not\equiv 0$.

2. Si $k = \frac{2m}{3}$, entonces $m \equiv 0 \mod 3$. Notemos que $2^m + 1 = (2^{\frac{2m}{3}} - 1)2^m + (2^{\frac{m}{3}} + 1)$, por lo que $(2^m + 1, 2^{\frac{2m}{3}} - 1) = (2^{\frac{2m}{3}} - 1, 2^{\frac{m}{3}} + 1) = 2^{\frac{m}{3}} + 1$. Por otro lado, $1 \leq i \leq 2^{t+2} + 7 < \frac{n}{2^{\frac{m}{3}}+1} = 2^{\frac{2m}{3}} - 2^{\frac{m}{3}} + 1$, así $i(2^k - 1) \not\equiv 0$.

3. Si $k \leq \frac{2m}{5}$, se obtiene que $1 \leq i(2^k - 1) \leq (2^{t+2} + 7)(2^{\frac{2m}{5}} - 1) < n$, por lo que $i(2^k - 1) \not\equiv 0$.

Con los casos mostrados anteriormente se concluye que cuando $1 \leq i \leq 2^{t+2}+7$, $i(2^k-1) \not\equiv 0$, lo cual es una contradicción. Por lo tanto, para $1 \leq i \leq 2^{t+2} + 7$, $|C_i| = 2m$.

De la prueba del Teorema 4.0.7, cuando $i \in \{\delta_2, \delta_3, \delta_4, \delta_5\}$ se deriva que $y_{i,k} > i$ para $1 \leq k \leq 2m - 1$, por lo que $i(2^k - 1) \not\equiv 0$ y así, $|C_i| = 2m$. ■

La investigación realizada hasta el momento nos conduce al siguiente Teorema en el que se obtiene la dimensión y una cota inferior para la distancia de los códigos binarios

$\mathcal{BCH}$ antiprimitivos $\mathcal{C}(n, 2, \delta, 1)$ y $\mathcal{C}(n, 2, \delta + 1, 0)$ donde $n = 2^{2t+1} + 1$.

La dimensión de los códigos se determina haciendo uso del Lema 4.0.12 en el que se conoce la cardinalidad de la clase lateral ciclotómica en los que los δ_i (para $i = 2, 3, 4, 5$) son líderes de clase lateral, mientras que la cota $\mathcal{BCH}$ nos da una cota inferior para la distancia del código.

Teorema 4.0.13. Sean $\delta_1 = \frac{n}{3}, \delta_2 = \frac{n-3}{6}, \delta_3 = \delta_2 - 2, \delta_4 = \delta_2 - 8$ y $\delta_5 = \delta_2 - 10$ como en el Teorema 4.0.7. Sea además δ impar.

1. El código $\mathcal{BCH}$ de sentido estrecho $\mathcal{C}(n, 2, \delta, 1)$ tiene parámetros

$$\begin{cases} [n, n - m\delta + 5m, d \geq \delta] & \text{si } 2^{t+1} + 3 \leq \delta \leq 2^{t+1} + 2^t - 3; \\ [n, n - m\delta + 9m, d \geq \delta] & \text{si } 2^{t+1} + 2^t + 3 \leq \delta \leq 2^{t+2} - 9; \\ [n, n - 2^{t+2}m + 16m, d \geq 2^{t+2} + 9] & \text{si } 2^{t+2} - 7 \leq \delta \leq 2^{t+2} + 9; \\ [n, 2m(i-1) + 3, d \geq \delta_i] & \text{si } \delta_{i+1} + 2 \leq \delta \leq \delta_i (i = 1, 2, 3, 4); \\ [n, 1, n] & \text{si } \delta_1 + 2 \leq \delta \leq n. \end{cases}$$

2. El código $\mathcal{BCH}$ $\mathcal{C}(n, 2, \delta + 1, 0)$ tiene parámetros

$$\begin{cases} [n, 2^m - m\delta + 5m, d \geq 2\delta] & \text{si } 2^{t+1} + 3 \leq \delta \leq 2^{t+1} + 2^t - 3; \\ [n, 2^m - m\delta + 9m, d \geq 2\delta] & \text{si } 2^{t+1} + 2^t + 3 \leq \delta \leq 2^{t+2} - 9; \\ [n, 2^m - 2^{t+2}m + 16m, d \geq 2(2^{t+2} + 9)] & \text{si } 2^{t+2} - 7 \leq \delta \leq 2^{t+2} + 9; \\ [n, 2m(i-1) + 2, d \geq 2\delta_i] & \text{si } \delta_{i+1} + 2 \leq \delta \leq \delta_i (i = 1, 2, 3, 4). \end{cases}$$

Demostración. 1. Sea T_δ el conjunto de definición de $\mathcal{C}(n, 2, \delta, 1)$ y $T_\delta = \bigcup_{i \in S_\delta} C_i$, donde

$$S_\delta = \{i : i \text{ es un líder de clase lateral}, C_i \subseteq T_\delta\}.$$

Del inciso 4 del Teorema 3.1.8, se sigue que $\mathcal{C}(n, 2, \delta, 1)$ tiene dimensión $k = n - |T_\delta| = n - \sum_{i \in S_\delta} |C_i|$.

(i): Cuando $2^{t+1} + 3 \leq \delta \leq 2^{t+1} + 2^t - 3$, del Teorema 4.0.6, tenemos que

$$S_\delta = \{i : i \text{ es impar y } i \in [1, \delta - 1] \backslash \{2^{t+1} \pm 1\}\},$$

donde $|S_\delta| = \frac{\delta - 1}{2} - 2$. De acuerdo al Lema 4.0.12, todas las clases laterales ciclotómicas en T_δ tienen cardinalidad $2m$, se sigue que

$$\begin{aligned} k &= n - \sum_{i \in S_\delta} |C_i| \\ &= n - 2m \cdot \left(\frac{\delta - 1}{2} - 2 \right) \\ &= n - m\delta + 5m. \end{aligned}$$

Claramente existen $\delta - 1$ enteros consecutivos, de acuerdo al Límite $\mathcal{BCH}$, la distancia mínima $d \geq \delta$.

(ii): De forma similar a (i), cuando $2^{t+1}+2^t+3 \leq \delta \leq 2^{t+2}-9$, del Teorema 4.0.6 y el Lema 4.0.12,

$$S_\delta = \{i : i \text{ es impar y } i \in [1, \delta-1] \backslash \{2^{t+1} \pm 1, 2^{t+1}+2^t \pm 1\}\},$$

se tiene que $|S_\delta| = \frac{\delta-1}{2} - 4$ y así

$$\begin{aligned} k &= n - \sum_{i \in S_\delta} |C_i| \\ &= n - 2m \cdot \left(\frac{\delta-1}{2} - 4\right) \\ &= n - m\delta + 9m. \end{aligned}$$

Además, $d \geq \delta$.

(iii): Similarmente a (i), cuando $2^{t+2}-7 \leq \delta \leq 2^{t+2}+9$, del Teorema 4.0.6 y el Lema 4.0.12,

$$S_\delta = \{i : i \text{ es impar y } i \in [1, 2^{t+2}-9] \backslash \{2^{t+1} \pm 1, 2^{t+1}+2^t \pm 1\}\},$$

se tiene que $|S_\delta| = 2^{t+1} - 8$ y así

$$\begin{aligned} k &= n - \sum_{i \in S_\delta} |C_i| \\ &= n - 2m \cdot \left(2^{t+1} - 8\right) \\ &= n - 2^{t+2}m + 16m. \end{aligned}$$

Además, $d \geq 2^{t+2} + 9$.

(iv): Cuando $\delta_{i+1} + 2 \leq \delta \leq \delta_i$, $(i = 1, 2, 3, 4)$, podemos inferir del Teorema 4.0.11 que $T_\delta = \bigcup_{i \in S_\delta} C_i = \{1, 2, \cdots, n-1\} \backslash \bigcup_{j=1}^{i} C_{\delta_j}$. En la prueba del Teorema 4.0.7 se vió que $|C_{\delta_1}| = 2$. Por el Lema 4.0.12, cada $C_{\delta_i} (i = 2, 3, 4, 5)$ tiene cardinalidad $2m$, de donde se sigue que

$$\begin{aligned} k &= n - \sum_{i \in S_\delta} |C_i| \\ &= n - [n - 1 - 2m(i-1) - 2] \\ &= 2m(i-1) + 3. \end{aligned}$$

Por otro lado, existen $\delta_i - 1$ enteros consecutivos en T_δ, así la distancia mínima satisface $d \geq \delta_i$.

(v): Cuando $\delta_1 + 2 \leq \delta \leq n$. Del Teorema 4.0.11 se infiere que $T_\delta = \bigcup_{i \in S_\delta} C_i = \{1, 2, \cdots, n-1\}$, de modo que $k = n - |T_\delta| = n - (n-1) = 1$.

Claramente, la distancia mínima $d = n$.

2. De forma similar a 1., sea T_δ el conjunto de definición de $\mathcal{C}(n, 2, \delta+1, 0)$. $T_\delta = \bigcup_{i \in S_\delta}$ donde

$$S_\delta = \{i : i \text{ es un líder de clase lateral}, C_i \subseteq T_\delta\}.$$

Del inciso 4 del Teorema 3.1.8, se sigue que $\mathcal{C}(n, 2, \delta + 1, 0)$ tiene dimensión $k = n - |T_\delta| = n - \sum_{i \in S_\delta} |C_i|$.

(i)': Cuando $2^{t+1} + 3 \leq \delta \leq 2^{t+1} + 2^t - 3$, del Teorema 4.0.6, tenemos que

$$S_\delta = \{i : i \text{ es impar y } i \in [0, \delta - 1] \backslash \{2^{t+1} \pm 1\}\}.$$

Se sabe que $|C_0| = 1$ y de acuerdo al Lema 4.0.12, el resto de las clases laterales ciclotómicas en T_δ tienen cardinalidad $2m$, se sigue que

$$\begin{aligned} k &= n - \sum_{i \in S_\delta} |C_i| \\ &= n - \left[2m \cdot \left(\frac{\delta - 1}{2} - 2\right) + 1\right] \\ &= 2^m - m\delta + 5m. \end{aligned}$$

Claramente existen $2\delta - 1$ enteros consecutivos, de acuerdo al Límite $\mathcal{BCH}$, la distancia mínima $d \geq 2\delta$.

(ii)': De manera similar a $(i)'$, cuando $2^{t+1} + 2^t + 3 \leq \delta \leq 2^{t+2} - 9$, del Teorema 4.0.6 y el Lema 4.0.12,

$$S_\delta = \{i : i \text{ es impar y } i \in [0, \delta - 1] \backslash \{2^{t+1} \pm 1, 2^{t+1} + 2^t \pm 1\}\},$$

se tiene que $|S_\delta| = \frac{\delta - 1}{2} - 4$ y así

$$\begin{aligned} k &= n - \sum_{i \in S_\delta} |C_i| \\ &= n - \left[2m \cdot \left(\frac{\delta - 1}{2} - 4\right) + 1\right] \\ &= 2^m - m\delta + 9m. \end{aligned}$$

Además, $d \geq 2\delta$.

(iii)': Similarmente a (i)', cuando $2^{t+2} - 7 \leq \delta \leq 2^{t+2} + 9$, del Teorema 4.0.6 y el Lema 4.0.12,

$$S_\delta = \{i : i \text{ es impar y } i \in [0, 2^{t+2} - 9] \backslash \{2^{t+1} \pm 1, 2^{t+1} + 2^t \pm 1\}\},$$

se tiene que $|S_\delta| = 2^{t+1} - 8$ y así

$$\begin{aligned} k &= n - \sum_{i \in S_\delta} |C_i| \\ &= n - \left[2m \cdot \left(2^{t+1} - 8\right) + 1\right] \\ &= 2^m - 2^{t+2}m + 16m. \end{aligned}$$

Además, $d \geq 2(2^{t+2} + 9)$.

(iv)': Cuando $\delta_{i+1}+2 \leq \delta \leq \delta_i$, $(i=1,2,3,4)$, podemos inferir del Teorema 4.0.11 que $T_\delta = \bigcup_{i\in S_\delta} C_i = \{0,1,2,\cdots,n-1\} \setminus \bigcup_{j=1}^{i} C_{\delta_j}$. En la prueba del Teorema 4.0.7 se vió que $|C_{\delta_1}| = 2$. Por el Lema 4.0.12, cada $C_{\delta_i} (i = 2,3,4,5)$ tiene cardinalidad $2m$, de donde se sigue que

$$\begin{aligned} k &= n - \sum_{i\in S_\delta} |C_i| \\ &= n - [n - 2m(i-1) - 2] \\ &= 2m(i-1) + 2. \end{aligned}$$

Por otro lado, existen $2\delta_i - 1$ enteros consecutivos en T_δ, así la distancia mínima satisface $d \geq 2\delta_i$.

■

Se presentan a continuación algunos ejemplos sobre la aplicación del Teorema 4.0.13.

Ejemplo 4.0.14. Consideremos el valor de $t = 5$. Se tiene que $m = 11$ y así, $n = 2^{11}+1$. Los valores de δ_i para $i = 1,2,3,4$ y 5, dados como en el Teorema 4.0.7, para este ejemplo son:

$$\delta_1 = \frac{n}{3} = 683, \qquad \delta_2 = \frac{n-3}{6} = 341, \qquad \delta_3 = \delta_2 - 2 = 339,$$

$$\delta_4 = \delta_2 - 8 = 333, \qquad \delta_5 = \delta_2 - 10 = 331.$$

- Si tomamos $\delta = 71$, entonces $2^6+3 \leq \delta \leq 2^6+2^5-3$. El Teorema 4.0.13 indica que la dimensión del código $\mathcal{C}(2^{11}+1, 2, \delta, 1)$ es $k = 2^{11}+1-11\cdot 71+5\cdot 11 = 1323$, con una distancia mínima de Hamming $d \geq 71$, mientras que el código $\mathcal{C}(2^{11}+1, 2, \delta+1, 0)$ tiene parámetros: $k = 2^{11} - 11\cdot 71 + 5\cdot 11 = 1322$ y distancia mínima de Hamming $d \geq 2\cdot 71 = 142$.

- Tomemos ahora $\delta = 117$. Se cumple que $2^6 + 2^5 + 3 \leq \delta \leq 2^7 - 9$, por lo que el Teorema 4.0.13 indica que la dimensión del código $\mathcal{C}(2^{11}+1, 2, \delta, 1)$ es $k = 2^{11}+1-11\cdot 71+9\cdot 11 = 1367$, con distancia mínima de Hamming $d \geq 117$.

  Por otro lado, el código $\mathcal{C}(2^{11}+1, 2, \delta+1, 0)$ tiene parámetros: $k = 2^{11}-11\cdot 71+9\cdot 11 = 860$ y distancia mínima de Hamming $d \geq 2\cdot 71 = 234$.

- Si $\delta = 135$, entonces $2^7 - 7 \leq \delta \leq 2^7 + 9$. El Teorema 4.0.13 indica que la dimensión del código $\mathcal{C}(2^{11}+1, 2, \delta, 1)$ es $k = 2^{11}+1-11\cdot 2^7+16\cdot 11 = 817$, con una distancia mínima de Hamming $d \geq 2^7 + 9 = 137$. Y el código $\mathcal{C}(2^{11}+1, 2, \delta+1, 0)$ tiene dimensión $k = 2^{11} - 11\cdot 2^7 + 16\cdot 11 = 816$, con distancia mínima de Hamming $d \geq 2(2^7+9) = 274$.

- Con $\delta = 341$, se tiene que $\delta_3 + 2 \leq \delta \leq \delta_2$, por lo que el Teorema 4.0.13 nos dice que la dimensión de $\mathcal{C}(2^{11}+1, 2, \delta, 1)$ es $k = 2\cdot 11\cdot(2-1)+3 = 25$, con distancia mínima de Hamming $d \geq \delta_2 = 341$. Además, el código $\mathcal{C}(2^{11}+1, 2, \delta+1, 0)$ tiene dimensión $k = 2\cdot 11\cdot(2-1)+2 = 24$ y distancia mínima de Hamming $d \geq 2\cdot\delta_2 = 682$.

- Tomando $\delta = 2045$, se satisface que $\delta_1 + 2 \leq \delta \leq n$, concluyendo así, por el Teorema 4.0.13 se obtiene que el código $\mathcal{C}(2^{11} + 1, 2, \delta, 1)$ tiene dimensión $k = 1$ y distancia mínima de Hamming $d = n = 2049$.

El polinomio generador $g(x)$ del código $\mathcal{C}$ tiene grado $n - k = 2049 - k$, además $g(x)$ divide al polinomio $x^n - 1 = x^{2049} + 1$.

Por último, con estas distancias de Hamming se logra detectar y corregir un número importante de errores, de acuerdo con los resultados enunciados en el Capítulo 2.

Conclusiones

A lo largo de este trabajo de investigación se han presentado teoremas que permiten obtener los líderes de algunas clases 2-ciclotómicas módulo n más grandes, los cuales son una herramienta fundamental para determinar la dimensión de algunos códigos $\mathcal{BCH}$ antiprimitivos $\mathcal{C}(n, 2, \delta, 1)$ y $\mathcal{C}(n, 2, \delta + 1, 0)$ para algunos valores de δ y m, basándonos en el trabajo realizado por Yang Liu, et. al. en [19]. Los teoremas presentados requieren del uso de conceptos, tales como los de campos finitos y anillos cociente, que se estudian en los cursos de Álgebra Moderna, es aquí donde se obtiene el primer éxito de esta investigación, presentar cómo se utilizan temas de un área tan abstracta en un ejemplo de una aplicación importante como lo es el estudio de códigos en los sistemas de comunicación.

No es fácil determinar los parámetros de los códigos $\mathcal{BCH}$ antiprimitivos, en la sección 3.3 se presentaron resultados que proporcionan cotas inferiores para la dimensión de dichos códigos $\mathcal{BCH}$, razón por la cual el Teorema 4.0.13 cobra tanta importancia al presentar la dimensión de dichos códigos completamente determinada.

Uno de los logros importantes de esta tesis es presentar de manera detallada los cálculos que demuestran para qué valores de i este es líder de clase lateral, utilizando diferentes técnicas, además de los cálculos explicitos para determinar que los δ_i (para $i = 1, 2, 3, 4, 5$) presentados son líderes de clase lateral y más aún, que son los cinco líderes de clase lateral más grandes.

Por otro lado, explicamos el significado e importancia de los teoremas que nos aportan la información más importante así como el significado de los parámetros de los códigos desde el punto de vista de su aplicación en la detección y correción de errores, así como de la protección en la seguridad de la información procesada, aplicaciones que son fundamentales en los sistemas de comunicación.

Como trabajo a futuro se espera desarrollar más y nuevas técnicas sobre códigos $\mathcal{BCH}$ antiprimitivos sobre campos finitos, además de discutir las construcciones de códigos LCD.

Bibliografía

[1] A. Naubauer; J. Freudenberger; V. Kühn. *Coding Theory, Algorithms, Architectures and Applications*. John Wiley & Sons Ltd. 2007.

[2] Blaum, Mario. *A Short Course on Error-Correcting Codes*. 2009.

[3] C. Carlet, S. Guilley. *Complementary dual codes for counter-measures to side-channel attacks*, in: E.R. Pinto, et al. (Eds.), Coding Theory and Applications, in: CIM Series in Mathematical Sciences, Springer Verlag, vol. 3, 2014, pp. 97–105

[4] C. Li, C. Ding, S. Li. *LCD cyclic codes over finite fields*, IEEE Trans. Inf. Theory 63 (7) (2017), pp. 4344−4356.

[5] Charles P. Shelton, *Coding for Error Detection and Correction* , Carnegie Mellon University, 1999.

[6] C. Ding. *BCH codes in the past 55 years, in: The 7th International Workshop on Finite Fields and Their Applications*, Tianjin, China, 2016.

[7] C. Ding, C. Fan, Z. Zhou. *The dimension and minimum distance of two classes of primitive BCH codes*, Finite Fields Appl. 45 (2017), pp. 237–263.

[8] Costello D., Hagenauer J., Imai H. and Wicker S. *Applications of error-control coding*. IEEE Transactions on Information Theory,(1998), pp. 2531–2560.

[9] F. J. Macwilliams, N. J. A. Sloane. *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, the Netherlands, 1977.

[10] Fraleigh, John B. *Álgebra Abstracta: Primer curso*, Addison-Wesley Iberoamericana, Versión en español, (1992).

[11] González M. Nayeli A. *Códigos cíclicos basados en campos finitos para desarrollar algoritmos de ADN*, Universidad Tecnológica de la Mixteca, 2019.

[12] H. Liu, C. Ding, C. Li. *Dimensions of three types of BCH codes over* $\mathbb{F}_q$, Discrete Math. 340 (2017) 1910−1927.

[13] Jungnickel, D. *Codierungstheorie*, Spektrum Akademischer Verlag, Heidelberg, Germany, 1995.

[14] R. C. Bose and D. K. Ray-Chaudhuri. *On a class of error correcting binary group codes*, Inform. and Control 3 (1960), pp. 68–79.

[15] K. Guenda. *Dimension and minimum distance of a class of BCH codes*, Ann. Sci. Québec 32 (2008), pp. 57–62.

[16] R. C. Bose and D. K. Ray-Chaudhuri. *Further results on error correcting binary group codes*, Inform. and Control 3 (1960), pp. 279–290.

[17] S. Ling, C. Xing, *Coding Theory: A First Course* , Cambridge University Press, 2004.

[18] S.A. Aly, A. Klappenecker, P.K. Sarvepalli. *On quantum and classical BCH codes*, IEEE Trans. Inf. Theory 53 (3) (2007), pp. 1183−1188.

[19] Yang Liu, Ruihu Li, Qiang Fu, Liangdong Lu, Yi Rao. *Some binary BCH codes with length* $n = 2^m + 1$. Finite Fields and Their Applications 55 (2019) 109?133.

[20] W.C. Huffman, V. Pless. *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.