CÓDIGOS CÍCLICOS Y DE RESIDUOS CUADRÁTICOS SOBRE ANILLOS DE GALOIS

TESIS QUE PRESENTA

HAYDEE HERNÁNDEZ SORIANO

PARA OBTENER EL TÍTULO DE
LICENCIADA EN MATEMÁTICAS

DIRECTOR DE TESIS: DR. CARLOS ALBERTO LÓPEZ ANDRADE

BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA ⟨BUAP⟩
Facultad de Ciencias Físico Matemáticas ⟨FCFM⟩
http://www.fcfm.buap.mx/
Junio 2018

Haydee Hernández Soriano : *Códigos cíclicos y de residuos cuadráticos sobre anillos de Galois ,* Benemérita Universidad Autónoma de Puebla (BUAP) , Facultad de Ciencias Físico Matemáticas (FCFM) © Junio 2018.

WEBSITE:
http://www.fcfm.buap.mx/

E-MAIL:
haydeehs03@gmail.com

"No es el conocimiento, sino el acto de aprendizaje, y no la posesión, sino el acto de llegar ahí, lo que concede el mayor disfrute."
Carl Friedrich Gauss

El camino no ha sido fácil, pero ha válido la pena, ustedes jamás dudaron de mi, y aún en la tribulación no dejaron de apoyarme, Dios me concede llegar hasta acá tomada de las manos de las personas a las que más amo.
A mis padres y hermano.

AGRADECIMIENTOS

Primero que nada doy gracias a Dios por la vida que me permite disfrutar, por la familia que me ha dado y por cada una de las personas que me ha permitido conocer a lo largo de mi vida, cada una de ellas ha aportado algo que hoy me ha traído hasta este punto.

Agradezco a mis padres por el apoyo incondicional que me han brindado en estos años, por tenerme paciencia pero sobre todo por todo el amor que me han brindado, hoy el logro también es de ustedes, han sido un ejemplo de superación, valentía y amor para mi, los amo y gracias por estar presentes, por sus palabras de aliento y su presencia en mi vida aun en la distancia.

A mi hermano gracias por no dejarme sola, apoyarme siempre, incluso hasta en lo más mínimo, por ser mi compañero de aventuras, confidente y apoyo incondicional, gracias por las noches en las que te quedaste conmigo estudiando, por las palabras de aliento que me brindaste y la sonrisa que me sacabas cuando me sentía cansada. Gracias por compartir esta aventura conmigo, te amo hermanito.

A cada miembro de mi familia, a mis abuelos, tíos, primos, gracias por apoyarme y hacerse presentes, gracias de manera especial a mi tío Francisco J. y a mi tía Columba por recibirme en su casa durante mi estancia en Puebla, gracias a mis primos Laura y Octavio por apoyarme en los primeros años, hacerme compañía y sentirme amada por ustedes, gracias por compartir conmigo momentos agradables que han hecho de esta etapa una de las mejores.

A mi asesor, Dr. Carlos Alberto López Andrade, le agradezco la oprtunidad que me ha dado de trabajar con usted durante estos años, ha sido uno de los pilares mas importantes durante mi formación como profesionista, gracias de manera especial por su tiempo y dedicación a este trabajo y mas aún, gracias por sus consejo, confianza y apoyo.

Agradezco a mis sinodales, Dr. Carlos Guillén Galvaán, Dr. Iván Fernando Vilchis Montalvo y Dr. César Cejudo Castilla, por su disposición y tiempo dedicado a la revisión de este trabajo, así como sus comentarios y observaciones que sirvieron para el enriquecimiento del mismo.

De manera muy especial agradezco a mi tutora, M.C. María Guadalupe Raggi Cárdenas, por su preocupación y constante atención a mis actividades escolares, gracias profesora por estar al pendiente de mí desde primer semestre, por sus consejos y apoyo.

A mis amigos

* *Ángel, sensei gracias por tu amistad, eres una persona muy especial para mi, siempre te agradeceré por ser mi "tutor" en los primeros semestres de la licenciatura, cuando me ayudaste a comprender muchas de las cosas de cálculo, gracias por tantas risas, tantas caídas y tan buenos momentos juntos, fuiste mi primer amigo en la facultad y eso te hace muy especial, te quiero.*

* *Abraham, gracias por tu amistad, por escucharme, por aconsejarme y por permitirme conocerte, es muy graciosa la historia de como nos empezamos a hablar, en fin, eres mi compañero de escuelas, viajes y demás, gracias por tu amistad y compañía en estos años.*

* *Marisol, gracias por tu apoyo, por explicarme aquellas cosas que algunas veces no entendía, por los largos momentos que pasamos haciendo tarea, sacrificando muchas cosas, por hacerme parte de tus equipos y por permitirme conocerte.*

* *Mónica, sabes que eres mi beffi, te has hecho parte importante en mi vida, te admiro mucho como persona, contigo he compartído los secretos mas profundos de mi vida como estudiante, me has escuchado, aconsejado y hasta regañado pero gracias por eso, te quiero a montones, gracias por invitarme a formar parte del equipo Jace, me permitiste conocer personas incríbles, con las cuales tambien estoy super agradecida.*

A cada uno de los profesores con los que tuve la oportunidad de aprender, muchas gracias, gracias por su esmero y amor a está profesión, por enamorarme de las matemáticas, gracias porque tuve la dicha de aprender de grandes matemáticos, gracias por compartir su tiempo y conocomiento conmigo.

A cada uno de mis compañeros, con los que tuve la oportunidad de compartir, muchas gracias por hacer de esta aventura algo aun más divertido.

Y a todas aquellas personas que conocí a lo largo de mi estancia en Puebla, amigos y hermanos de comunidad, gracias por su apoyo y aliento, por no dejarme bajar los brazos y hacer de esta etapa una de las mejores en mi vida.

INTRODUCCIÓN

La Teoría de Códigos y la Criptografía inmersas en las Matemáticas y en otras disciplinas tales como las Ciencias de la Computación e Ingenieria Eléctrica, están enfocadas en la optimización de la fiabilidad y seguridad de las comunicaciones dígitales. A grandes rasgos, la fiabilidad significa corrección de errores mientras que la seguridad significa prevenir el acceso no autorizado de intrusos.

La Teoría de Códigos Algebraicos es vista como una rama de las matemáticas puras, sus fundamentos pueden encontrarse en el Álgebra, la Teoría de Números, la Geometría Finita y la Combinatoria. Los códigos detectores-correctores de errores son estudiados para dar solución al problema central de la teoría de la información, cuyo objetivo es lograr construir un sistema de codificación y de decodificación que haga posible la comunicación confiable, eficaz y segura; y además, que sea aceptable para las aplicaciones prácticas, es decir, requerimos buenos códigos detectores-correctores de errores capaces de ser implementados para recuperar el mensaje original produciendo así, una buena transmisión de la información.

Por lo anterior, el estudio de este tipo de problemas es interesante no sólo desde el punto de vista teórico dado que tiene aplicaciones prácticas, i.e., el estudio de la Teoría de Códigos Algebraicos es un tema de investigación actual que es de utilidad para la sociedad en general.

En los años 90 del siglo pasado, se inició el estudio de la caracterización de la estructura algebraica de los códigos cíclicos lineales sobre anillos finitos, en particular sobre anillos de Galois (cf. [JKC+94], [PQ96], [KLP97] [LB02], [DLP04], [LATR11]). La representación p-ádica de los elementos de un anillo de Galois es imprescindible en la definición de la función de Gray en esta clase de anillos, así como la correspondiente representación π-ádica en la clase de los anillos finitos de cadena (cf. [GS99]), de las cuales, los primeros son una subclase. Hammons et. al en [JKC+94] demostraron que el código de Kerdock es la imagen de Gray de un código cíclico lineal extendido sobre el anillo de Galois $\mathbb{Z}_4$. Ellos usan este hecho para resolver un problema "viejo", explicar la dualidad formal entre dos códigos no lineales binarios, los famosos códigos de Kerdock y Preparata. Este trabajo abrió la puerta al estudio de la Teoría de Códigos Algebraicos sobre anillos finitos, y en particular, sobre los anillos de Galois.

Este trabajo tiene como base el artículo de Pless y Qian [PQ96], del cual se ha estudiado a detalle la primera sección, donde se habla de las principales propiedades de un código cíclico sobre $\mathbb{Z}_4$, nuestro objetivo será comprender la estructura de dichos códigos y sus claras diferencias con los códigos cíclicos sobre campos finitos, además de poder dar un pequeño vistazo a los códigos de residuos cuadráticos sobre campos finitos que son una familia muy particular de códigos cíclicos con propiedades muy interesantes, las cuales nos llevan a revisar algunos conceptos de la Teoría de Números y algunas propiedades importantes de los campos finitos (cf.[MA78]).

Esta tesis consta de cuatro capítulos, en el primer capítulo se abordan algunas definiciones importantes que serán de gran utilidad en los capítulos 2 y 3, además se encuentran resultados muy interesantes como lo es el Teorema chino del residuo y algunos resultados que se derivan del mismo; el tema central del capítulo 2 es dar algunas propiedades importantes sobre los códigos cíclicos sobre campos finitos, comenzando por definir lo que es un código y un código lineal, así como los características mas importantes que definen a un código lineal, como lo son la longitud, el peso y sus matrices generadoras y de chequeo de paridad y finalmente abordar un par de ejemplos. El tercer capítulo es el que merece de una singular atención, se comienza dando algunas definiciones importantes del anillo de polinomios $\mathbb{Z}_4[x]$, y discutimos la estructura que tiene el anillo cociente $\frac{\mathbb{Z}_4[x]}{\langle f(x)\rangle}$ donde $f(x)$ es un polinomio básico irreducible, enseguida, se discute la estructura de un $\mathbb{Z}_4-$código cíclico, se muestra como son sus polinomios generadores y cual es la cardinalidad del mismo, hablamos del código dual y de los generadores idempotentes. Por útlimo, el capítulo 4 da una pequeña introducción a la estructura de códigos de residuos cuadráticos sobre campos finitos, para ello, se comienza definiendo un residuo cuadrático módulo p y se recuerdan algunos resultados de teoría de números, finalmente, se definen a los códigos de residuos cuadráticos y se prueban algunas propiedades importantes de los mismos.

ÍNDICE GENERAL

1 PRELIMINARES

En este capítulo se presentan algunos conceptos básicos y resultados importantes que serán de gran utilidad en los capítulos posteriores. Cabe señalar que en este manuscrito todos los anillos son conmutativos.

Definición 1.1. *Sea* R *un anillo arbitrario y sea* D *un ideal en* R. *Entonces* D *es llamado primario si las condiciones* $a, b \in R$, $ab \in D$ *y* $a \notin D$ *implican que existe un entero* m *tal que* $b^m \in D$.

En $\mathbb{Z}$, el ideal $\langle p^s \rangle$ donde p es un primo y $s \geqslant 2$, es un ideal primario.

Sean $p-$ primo, $s \in \mathbb{N}$, $\mathbb{Z}_{p^s} = \frac{\mathbb{Z}_{p^s}}{p^s\mathbb{Z}}$, el anillo de enteros módulo p^s, es un anillo local cuyo único ideal máximal es $M = \langle \bar{p} \rangle$ y con campo residual $\frac{\mathbb{Z}_{p^s}}{\langle \bar{p} \rangle} \simeq \mathbb{F}_p$ ($\mathbb{F}_p$ es el campo primo con p elementos). Haciendo abuso de la notación, a los elementos de $\mathbb{Z}_{p^s}$ los denotaremos sin hacer uso de la barra de clase.

$$\begin{array}{ccc} \mu\colon \mathbb{Z}_{p^s} & \longrightarrow & \frac{\mathbb{Z}_{p^s}}{\langle p \rangle} \\ a & \longmapsto & a + \langle p \rangle \end{array} \tag{1}$$

Sabemos que μ es un homomorfismo sobreyectivo natural

$$\begin{array}{ccc} \bar{\mu}\colon \mathbb{Z}_{p^s}[x] & \longrightarrow & \frac{\mathbb{Z}_{p^s}}{\langle p \rangle}[x] \\ f(x) = \sum_{i=0}^{n} a_i x^i & \longmapsto & \sum_{i=0}^{n} \mu(a_i) x^i = \bar{f}(x) \end{array} \tag{2}$$

donde dicha función es un homomorfismo sobreyectivo de anillos (cf.[Ram17]), esto se prueba a detalle en la Observación 3.1, para $p = 2$ y $s = 2$.

Definición 1.2. *Sean* $f_1, f_2 \in \mathbb{Z}_{p^s}[x]$. *Diremos que* f_1 *y* f_2 *son coprimos en* $\mathbb{Z}_{p^s}[x]$ *si existen* $q_1, q_2 \in \mathbb{Z}_{p^s}[x]$ *tales que*

$$q_1 f_1 + q_2 f_2 = 1$$

Lema 1.1. *Sean* $f_1, f_2 \in \mathbb{Z}_{p^s}[x]$. *Entonces* f_1 *y* f_2 *son coprimos en* $\mathbb{Z}_{p^s}[x]$ *si y sólo si* $\bar{f}_1$, $\bar{f}_2$ *son coprimos en* $\mathbb{F}_p[x]$.

Demostración. $\Rightarrow$] Sean f_1 y f_2 polinomios coprimos en $\mathbb{Z}_{p^s}[x]$, entonces por la Definición 1.2 existen $q_1, q_2 \in \mathbb{Z}_{p^s}[x]$ tales que $q_1 f_1 + q_2 f_2 = 1$ y aplicando (2) tenemos que $\overline{q_1 f_1 + q_2 f_2} = \bar{1}$, luego, $\bar{q}_1 \bar{f}_1 + \bar{q}_2 \bar{f}_2 = \bar{1}$, de ahí que $\bar{f}_1$ y $\bar{f}_2$ son coprimos en $\mathbb{F}_p[x]$.

$\Leftarrow$] Ahora, sean $\bar{f}_1$, $\bar{f}_2$ coprimos en $\mathbb{F}_q[x]$ entonces existen $g_1', g_2' \in \mathbb{F}_q[x]$ tales que $g_1' \bar{f}_1 + g_2' \bar{f}_2 = 1'$ pero como $\bar{\mu}$ es sobreyectiva entonces existen $q_1, q_2 \in \mathbb{Z}_{p^s}[x]$ tales que $\bar{q}_1 = g_1$ y $\bar{q}_2 = g_2'$ y $\bar{1} = 1'$ así, $\bar{q}_1 \bar{f}_1 + \bar{q}_2 \bar{f}_2 = \bar{1}$, luego $\overline{q_1 f_1 + q_2 f_2 - 1} = 0$ y de ahí que $\overline{q_1 f_1 + q_2 f_2} - \bar{1} = \bar{0}$, es decir, $q_1 f_1 + q_2 f_2 - 1 \in \langle p \rangle$, por lo que existe $k \in \mathbb{Z}_{p^s}[x]$ tal que $q_1 f_1 + q_2 f_2 - 1 = kp$, luego $q_1 f_1 + q_2 f_2 = 1 + kp$.

Definimos $h = \sum_{i=0}^{s-1} (-kp)^i$, tenemos que $h(q_1 f_1 + q_2 f_2) = h(1 + kp)$, entonces

$$\begin{aligned} hq_1 f_1 + hq_2 f_2 &= h + h(kp) \\ &= h + (\sum_{i=0}^{s-1} (-kp)^i)kp \\ &= h + ((-kp)^0 + (-kp) + (-kp)^2 + \cdots + (-kp)^{s-1})kp \\ &= h + (1 - kp + k^2p^2 + \cdots + (-1)^{s-1}k^{s-1}p^{s-1})kp \\ &= h + kp - k^2p^2 + k^3p^3 + \cdots + (-1)^{s-2}k^{s-1}p^{s-1} + (-1)^{s-1}k^s p^s \\ &= 1 - kp + k^2p^2 + \cdots + (-1)^{s-1}k^{s-1}p^{s-1} + \\ &\quad + kp - k^2p^2 + k^3p^3 + \cdots + (-1)^{s-2}k^{s-1}p^{s-1} + (-1)^{s-1}k^s p^s \\ &= 1 \text{ (ya que } p^s = 0) \end{aligned}$$

Así $(hq_1)f_1 + (hq_2)f_2 = 1$, por lo que f_1 y f_2 son coprimos en $\mathbb{Z}_{p^s}[x]$.

□

Sean A, B ideales en un anillo R, entonces

$$AB = \{c \in R : c = \sum_{j=1}^{n} a_j b_j \text{ para algún } n \in \mathbb{N} \text{ y con } a_j \in A \text{ y } b_j \in B\}$$

Teorema 1.1 (Teorema Chino del Residuo). *Sean $A_1, A_2, \ldots, A_n$ ideales en un anillo conmutativo R tales que $R^2 + A_i = R$ para toda i y $A_i + A_j = R$ para toda $i \neq j$. Si $b_1, \ldots, b_n \in R$ entonces existe $b \in R$ tal que*

$$b \equiv b_i \pmod{A_i}$$

con $i \in \{1, 2, \ldots, n\}$. Además b es determinado de manera única por la congruencia módulo el ideal $\bigcap_{i=1}^{n} A_i$.

Observación 1.1. *Si R tiene identidad, entonces $R^2 = R$, de ahí $R^2 + A = R$ para cada ideal A de R. (c.f. [Hun74])*

Demostración. Probemos que para cada $k \in \{1, 2, \ldots, n\}$, $R = A_k + \bigcap_{i \neq k} A_i$.

Tomemos $k = 1$ y veamos que $R = A_1 + \bigcap_{i \neq 1} A_i$ inductivamente.

Para $n = 3$, sean A_1, A_2, A_3 ideales de R tales que $A_1 + A_2 = R$, $A_1 + A_3 = R$ y $A_2 + A_3 = R$. Entonces $R^2 = (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1A_3 + A_2A_1 + A_2A_3$. Notemos que

- $A_1^2 \subseteq A_1$. Sea $c \in A_1^2 = A_1A_1$ entonces existe un $n \in \mathbb{N}$ tal que $c = \sum_{j=1}^{n} a_j b_j$ donde $a_j, b_j \in A_1$ pero A_1 es ideal por lo que $a_j b_j \in A_1$ para cada $j = 1, 2, \ldots n$ y así $\sum_{j=1}^{n} a_j b_j \in A_1$, por lo que $c \in A_1$.
- A_1A_3 y A_2A_1 están contenidos en A_1. Sean $c \in A_1A_3$ y $d \in A_2A_1$ entonces, existen $n, m \in \mathbb{N}$ tales que $c = \sum_{j=1}^{n} a_j b_j$ y $d = \sum_{i=1}^{m} h_i f_i$ donde $a_j, f_i \in A_1$, $b_j \in A_3$ y $h_i \in A_2$ para cada $i = 1, \ldots, m$ y $j = 1, \ldots, n$, y como A_1 es un ideal y $A_2, A_3 \subseteq R$ entonces para cada i y j se tiene que $h_i f_i \in A_1$ y $a_j b_j \in A_1$ y ya que A_1 es cerrado bajo la suma entonces $c = \sum_{j=1}^{n} a_j b_j \in A_1$ y $d = \sum_{i=1}^{m} h_i f_i \in A_1$.
- $A_2A_3 \subseteq A_2 \cap A_3$. Sea $c \in A_2A_3$, entonces $c = \sum_{j=1}^{n} a_j b_j$ para algún $n \in \mathbb{N}$ y para cada j, $a_j \in A_2$ y $b_j \in A_3$, luego por ser A_2 y A_3 ideales entonces $a_j b_j \in A_2$ y $a_j b_j \in A_3$, así que $c \in A_2$ y $c \in A_3$ por lo que $c \in A_2 \cap A_3$.

Así, $R^2 = A_1^2 + A_1A_3 + A_2A_1 + A_2A_3 \subseteq A_1 + A_1 + A_1 + (A_2 \cap A_3) = A_1 + (A_2 \cap A_3)$ ya que A_1 es un ideal. Entonces $R^2 \subseteq A_1 + (A_2 \cap A_3)$. Como $R = A_1 + R^2$ entonces $R = A_1 + R^2 \subseteq A_1 + A_1 + (A_2 \cap A_3) = A_1 + (A_2 \cap A_3)$, por lo que $R \subseteq A_1 + (A_2 \cap A_3)$, pero $A_1 + (A_2 \cap A_3) \subseteq R$ pues son ideales de R, así,

$$R = A_1 + (A_2 \cap A_3)$$

Asumimos inductivamente que $R = A_1 + (A_2 \cap A_3 \cap \ldots \cap A_{k-1})$ y ya que $R = A_1 + A_k$. Entonces

$$\begin{aligned} R^2 &= (A_1 + (A_2 \cap A_3 \cap \ldots \cap A_{k-1}))(A_1 + A_k) \\ &= A_1^2 + (A_2 \cap A_3 \cap \ldots \cap A_{k-1})A_1 + A_1A_K + (A_2 \cap A_3 \cap \ldots \cap A_{k-1})A_K \end{aligned}$$

Y como ya vimos $A_1^2 \subseteq A_1$, además $B_1 = A_2 \cap A_3 \cap \ldots \cap A_{k-1}$ es un ideal en R, por lo que $B_1A_1 \subseteq A_1$ y también $A_1A_k \subseteq A_1$ y la justificación de esto es análoga a la que hizo en el segundo punto cuando n=3, por otro lado tenemos que $B_1A_k \subseteq B_1 \cap A_k = (A_2 \cap A_3 \cap \ldots \cap A_{k-1}) \cap A_k$ ya que B_1 es un ideal en R y la prueba de ello se remite al tercer punto, cuando $n = 3$. Así

$$R^2 \subseteq A_1 + A_1 + A_1 + (A_2 \cap A_3 \cap \ldots \cap A_k) = A_1 + (A_2 \cap A_3 \cap \ldots \cap A_k)$$

luego

$$R = R^2 + A_1 \subseteq A_1 + (A_2 \cap A_3 \cap \ldots \cap A_k) + A_1 = A_1 + (A_2 \cap A_3 \cap \ldots \cap A_k) \subseteq R$$

Por tanto, $R = A_1 + (A_2 \cap A_3 \cap \ldots \cap A_k)$. Consecuentemente

$$R = A_1 + \bigcap_{i \neq 1} A_i$$

con $i \in \{1, 2, \ldots, n\}$.

De manera similar se prueba que para cada $k = 1, 2 \ldots, n$ $R = A_k + \bigcap_{i \neq k} A_i$. Luego, existen $a_k \in A_k$ y $r_k \in \bigcap_{i \neq k} A_i$, tales que $b_k = a_k + r_k$. Más aún, $b_k - r_k = a_k \in A_k$, por lo que $b_k \equiv r_k \pmod{A_k}$ y como $r_k \in \bigcap_{i \neq k} A_i$, entonces $r_k \in A_i$ con $i \neq k$, así $r_k \equiv 0 \pmod{A_i}$, para cada $i \neq k$. Sea $b = r_1 + r_2 + \cdots + r_n$. Ya que $r_i \equiv b_i \pmod{A_i}$ y $r_j \equiv 0 \pmod{A_i}$ para cada $j \neq i$, entonces $r_1 + r_2 + \cdots + r_i + \cdots + r_n \equiv b_i \pmod{A_i}$ para cada i, de ahí que

$$b \equiv b_i \pmod{A_i}$$

Si $c \in R$ es tal que $c \equiv b_i \pmod{A_i}$ para cada i, entonces $c \equiv b \pmod{A_i}$, por lo que $c - b \in A_i$ para cada i, luego $c - b \in \bigcap_{i=1}^{n} A_i$ y por lo tanto $c \equiv b \pmod{\bigcap_{i=1}^{n} A_i}$.

□

Corolario 1.1. *Si $A_1, \ldots, A_n$ son ideales en un anillo R, entonces existe un monomorfismo de anillos*

$$\theta\colon \frac{R}{A_1 \cap \ldots \cap A_n} \longrightarrow \frac{R}{A_1} \times \cdots \times \frac{R}{A_n}$$

Si $R^2 + A_i = R$, para cada i y $A_i + A_j = R$ para cada $i \neq j$, entonces θ es un isomorfismo de anillos.

Demostración. Sabemos que para cada $k = 1, 2, \ldots, n$, la función

$$\begin{array}{rccc} \pi_k\colon & R & \longrightarrow & \dfrac{R}{A_k} \\ & r & \longmapsto & r + A_k \end{array}$$

es un homomorfismo sobreyectivo de anillos. Sea

$$\begin{array}{rccc} \theta_1\colon R & \longrightarrow & \dfrac{R}{A_1} \times \cdots \times \dfrac{R}{A_n} \\ r & \longmapsto & \theta_1(r) = (r + A_1, r + A_2, \ldots, r + A_n) \end{array}$$

Notemos que $\theta_1(r) = (\pi_1(r), \pi_2(r), \ldots, \pi_n(r))$, por lo que, sean $r, s \in R$ si $r = s$, como cada π_k está bien definida entonces $\pi_k(r) = \pi_k(s)$, por lo que $(\pi_1(r), \pi_2(r), \ldots, \pi_n(r)) = (\pi_1(s), \pi_2(s), \ldots, \pi_n(s))$, de ahí que $\theta_1(r) = \theta_1(s)$, así θ_1 está bien definida. Además se tiene que

$$\begin{aligned} \theta_1(r+s) &= (\pi_1(r+s), \pi_2(r+s), \ldots, \pi_n(r+s)) \\ &= (\pi_1(r) + \pi_1(s), \pi_2(r) + \pi_2(s), \ldots, \pi_n(r) + \pi_n(s)) \\ &\qquad \text{(ya que para cada } k,\ \pi_k \text{ es un homomorfismo)} \\ &= (\pi_1(r), \pi_2(r), \ldots, \pi_n(r)) + (\pi_1(s), \pi_2(s), \ldots, \pi_n(s)) \\ &= \theta_1(r) + \theta_1(s) \end{aligned}$$

y

$$\begin{aligned} \theta_1(rs) &= (\pi_1(rs), \pi_2(rs), \ldots, \pi_n(rs)) \\ &= (\pi_1(r)\pi_1(s), \pi_2(r)\pi_2(s), \ldots, \pi_n(r)\pi_n(s)) \text{ (ya que para cada } k,\ \pi_k \text{ es un homomorfismo)} \\ &= (\pi_1(r), \pi_2(r), \ldots, \pi_n(r))(\pi_1(s), \pi_2(s), \ldots, \pi_n(s)) \\ &= \theta_1(r)\theta_1(s) \end{aligned}$$

por lo que θ_1 también es un homomorfismo de anillos. Veamos que $\mathrm{Ker}(\theta_1) = A_1 \cap \ldots \cap A_n$. Sea $r \in \mathrm{Ker}(\theta_1)$

$$\begin{aligned}
&\Rightarrow \quad \theta_1(r) = (0 + A_1, 0 + A_2, \ldots, 0 + A_n) \\
&\Rightarrow \quad (r + A_1, r + A_2, \ldots, r + A_n) = (0 + A_1, 0 + A_2, \ldots, 0 + A_n) \\
&\Rightarrow \quad r + A_i = 0 + A_i \text{ para cada } i \in \{1, 2, \ldots, n\} \\
&\Rightarrow \quad r \in A_i, \text{ para cada } i \in \{1, 2, \ldots, n\} \\
&\Rightarrow \quad r \in A_1 \cap A_2 \cap \ldots \cap A_n
\end{aligned}$$

por lo que $\mathrm{Ker}(\theta_1) \subseteq A_1 \cap A_2 \cap \ldots \cap A_n$. Ahora, sea $s \in A_1 \cap A_2 \cap \ldots \cap A_n$, entonces $s \in A_i$ para cada $i \in \{1, 2, \ldots, n\}$, luego $\pi_i(s) = s + A_i = 0 + A_i$, de ahí que $\theta_1(s) = (\pi_1(s), \pi_2(s), \ldots, \pi_n(s)) = (0 + A_1, 0 + A_2, \ldots, 0 + A_n)$, y así $s \in \mathrm{Ker}(\theta_1)$. Por lo tanto

$$A_1 \cap A_2 \cap \ldots \cap A_n \subseteq \mathrm{Ker}(\theta_1)$$

Sea

$$\begin{array}{rccc}
\theta\colon & \dfrac{R}{A_1 \cap \ldots \cap A_n} & \longrightarrow & \dfrac{R}{A_1} \times \cdots \times \dfrac{R}{A_n} \\
& r + A_1 \cap \ldots \cap A_n & \longmapsto & \theta_1(r)
\end{array}$$

Veamos que θ está bien definida. Sean $r + A_1 \cap \ldots \cap A_n, s + A_1 \cap \ldots \cap A_n \in \dfrac{R}{A_1 \cap \ldots \cap A_n}$ con $r + A_1 \cap \ldots \cap A_n = s + A_1 \cap \ldots \cap A_n$

$$\begin{aligned}
&\Rightarrow \quad r - s \in A_1 \cap \ldots \cap A_n = \mathrm{Ker}(\theta_1) \\
&\Rightarrow \quad r - s \in A_i \ \ (\text{para cada } i = 1, 2 \ldots, n) \\
&\Rightarrow \quad r + A_i = s + A_i \\
&\Rightarrow \quad (r + A_1, r + A_2, \ldots, r + A_n) = (s + A_1, s + A_2, \ldots, s + A_n) \\
&\Rightarrow \quad \theta_1(r) = \theta_1(s) \\
&\Rightarrow \quad \theta(r + A_1 \cap \ldots \cap A_n) = \theta(s + A_1 \cap \ldots \cap A_n)
\end{aligned}$$

por lo que θ está bien definido. Además, es un homomorfismo de anillos ya que

$$\begin{aligned}
\theta((r + A_1 \cap \ldots \cap A_n) + (s + A_1 \cap \ldots \cap A_n)) &= \theta((r + s) + A_1 \cap \ldots \cap A_n) \\
&= \theta_1(r + s) \\
&= \theta_1(r) + \theta_1(s) \ \ (\text{ya que } \theta_1 \text{ es un morfimos de anillos}) \\
&= \theta(r + A_1 \cap \ldots \cap A_n) + \theta(s + A_1 \cap \ldots \cap A_n)
\end{aligned}$$

y

$$\begin{aligned}
\theta((r + A_1 \cap \ldots \cap A_n)(s + A_1 \cap \ldots \cap A_n)) &= \theta(rs + A_1 \cap \ldots \cap A_n) \\
&= \theta_1(rs) \\
&= \theta_1(r)\theta_1(s) \ \ (\text{ya que } \theta_1 \text{ es un morfimos de anillos}) \\
&= \theta(r + A_1 \cap \ldots \cap A_n)\theta(s + A_1 \cap \ldots \cap A_n)
\end{aligned}$$

Ahora probemos que $\mathrm{Ker}(\theta) = \{0 + A_1 \cap \ldots \cap A_n\}$. Sea $r + A_1 \cap \ldots \cap A_n \in \mathrm{Ker}(\theta)$,

$$\begin{aligned}
&\Rightarrow \quad \theta(r + A_1 \cap \ldots \cap A_n) = (0 + A_1, \ldots, 0 + A_n) \\
&\Rightarrow \quad (r + A_1, \ldots, r + A_n) = (0 + A_1, \ldots, 0 + A_n) \\
&\Rightarrow \quad r \in A_i \ \ (\text{para cada } \ i = 1, 2 \ldots, n) \\
&\Rightarrow \quad r \in A_1 \cap \ldots \cap A_n \\
&\Rightarrow \quad r + A_1 \cap \ldots \cap A_n = 0 + A_1 \cap \ldots \cap A_n
\end{aligned}$$

por lo que $\mathrm{Ker}(\theta) \subseteq \{0 + A_1 \cap \ldots \cap A_n\}$, ahora si tomamos un $r \in A_1 \cap \ldots \cap A_n$, tenemos que $r + A_1 \cap \ldots \cap A_n = 0 + A_1 \cap \ldots \cap A_n$, así

$$\theta(0 + A_1 \cap \ldots \cap A_n) = \theta(r + A_1 \cap \ldots \cap A_n) = (r + A_1, \ldots, r + A_n) = (0 + A_1, \ldots, 0 + A_n)$$

pues $r \in A_i$, para cada i y de ahí que $0 + A_1 \cap \ldots \cap A_n \in \mathrm{Ker}(\theta)$. Por lo tanto $\mathrm{Ker}(\theta) = \{0 + A_1 \cap \ldots \cap A_n\}$, luego θ es un homomorfismo inyectivo pero no necesariamente es sobreyectivo.

Si $R^2 + A_i = R$, para cada i, y $A_i + A_j = R$ con $i \neq j$, sea $(b_1 + A_1, b_2 + A_2, \ldots, b_n + A_n) \in \frac{R}{A_1} \times \frac{R}{A_2} \times \cdots \times \frac{R}{A_n}$, por el Teorema 1.1 existe un $b \in R$ tal que para cada i, se cumple que $b \equiv b_i \pmod{A_i}$, es decir, $b + A_i = b_i + A_i$, y así

$$\theta(b + A_1 \cap \ldots \cap A_n) = (b + A_1, b + A_2, \ldots, b + A_n) = (b_1 + A_1, b_2 + A_2, \ldots, b_n + A_n)$$

Por lo que bajo estas condiciones θ es sobreyectiva y así, es un isomorfismo de anillos. □

Teorema 1.2. *Si R_1, R_2, ..., R_n son anillos con identidad y A es un ideal en $R_1 \times R_2 \times \cdots \times R_n$ entonces $A = A_1 \times A_2 \times \cdots \times A_n$ donde cada A_i es un ideal en R_i.*

Demostración. Se tiene que

$$\begin{aligned} \varphi_k \colon R_1 \times \cdots \times R_k \times \cdots \times R_n &\longrightarrow R_k \\ (r_1, \ldots, r_k, \ldots, r_n) &\longmapsto r_k \end{aligned}$$

es un homomorfismo sobreyectivo canónico. Así, sea A un ideal en $R_1 \times R_2 \times \cdots \times R_n$ para cada $i \in \{1, 2 \ldots, n\}$, definimos

$$A_i = \{a_i \in R_i \colon (a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n) \in A\} = \varphi_k(A)$$

Luego, tenemos que

- Para cada $i \in \{1, 2 \ldots, n\}$, A_i es un ideal de R_i, puesto que $\varphi_i(A) = A_i$ y φ_i es un homomorfismo sobreyectivo de anillos.
- Como cada A_i es un ideal de R_i, entonces, $A_1 \times \cdots \times A_n$ es un ideal de $R_1 \times \cdots \times R_n$.
- Veamos que $A = A_1 \times \cdots \times A_n$

  Sea $a \in A_1 \times \cdots \times A_n$, entonces $a = (a_1, \ldots, a_n)$, donde cada $a_i \in A_i$. Como φ_i es un homomorfismo sobreyectivo, entonces existe $\alpha_i \in A$ tal que $\varphi_i(\alpha_i) = a_i$, luego, sea $e_i \in R$ tal que $e_i = (0, \ldots, 0, 1_i, 0, \ldots)$ donde 1_i es el elemento identidad de R_i, para cada $i = 1, 2, \ldots, n$, entonces

  $$a = \alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_n e_n$$

  por lo que $a \in A$ puesto que A es un ideal en R, así $A_1 \times \cdots \times A_n \subseteq A$. Por otro lado, $A \subseteq A_1 \times \cdots \times A_n$ debido a la definición de cada A_i. Por lo tanto

  $$A = A_1 \times \cdots \times A_n$$

De ahí que, si A es un ideal de R entonces $A = A_1 \times A_2 \times \cdots \times A_n$ donde cada A_i es un ideal en R_i. □

Definición 1.3. *Si R es un anillo, un R—módulo izquierdo es un grupo abeliano M junto con una función $(a, x) \to ax$ de $R \times M$ en M que satisface, para cada $a, b \in R$ y $x, y \in M$*

i) $a(x + y) = ax + ay$

ii) $(a + b)x = ax + bx$

iii) $(ab)x = a(bx)$

Si R tiene identidad, 1_R y

iv) $1_r x = x$ *entonces M es un R—módulo izquierdo unitario.*

A partir de este momento R siempre denotará un anillo conmutativo con identidad. Un ideal I de R es un R-módulo izquierdo unitario, más aún, R es un R-módulo izquierdo unitario.

Definición 1.4. *Sean M y N R-módulos, una función $f : M \to N$ es un homomorfismo de R-módulos (o es R-lineal) si:*

- $f(x+y) = f(x) + f(y)$,
- $f(ax) = af(x)$,

para cada $a \in R$ *y* $x, y \in M$.

Sea $f : M \to N$ un homomorfismo de R- módulos. Si f es biyectiva entonces f es un isomorfismo de R−módulos (cf. [Roto3], [DF04], [Kas82]).

Definición 1.5. *Un submódulo* M' *de* M *es un subgrupo de* M *que es cerrado bajo multiplicación por elementos de* R.

El grupo abeliano M/M' hereda de M una estructura de R-módulo definida por:

- $(x + M') + (y + M') = (x + y) + M'$
- $a(x + M') = ax + M'$.

Definición 1.6. *Si* M *es un* R*-módulo y* L, N *son submódulos de* M*, entonces*

$$L + N = \{x + y | x \in L, y \in N\}$$

es el submódulo más pequeño de M *que contiene a* L *y* N *(c.f. [AM69]), mientras que* $L \cap N$ *es el submódulo más grande de* M *que está contenido en* L *y* N *(c.f. [Wis91]), bajo la inclusión.*

Si M es un R-módulo y L, N son submódulos de M tales que $M = L + N$ y $L \cap N = \{0\}$ entonces M es la suma directa de L y N, lo cual se denota por $M = L \oplus N$.

2 CÓDIGOS CÍCLICOS SOBRE CAMPOS FINITOS

Los códigos cíclicos fueron estudiados por primera vez por Prange en 1957. Desde entonces, los teóricos de la codificación algebraica han hecho grandes progresos en el estudio de estos códigos. Los códigos cíclicos incluyen la importante familia de códigos BCH y muchas clases importantes de códigos, entre éstas se encuentran los códigos de Hamming y códigos de Golay.

La idea en los códigos correctores de errores consiste en añadir información redundante de tal manera que es posible detectar o incluso corregir errores después de la transmisión.

Imaginemos a dos individuos, el remitente (emisor) y el receptor. El remitente debe tratar de transmitir al receptor con la mayor precisión posible la salida de la fuente, esto es, el mensaje, y el único vínculo de comunicación permitido entre los dos es un canal simétrico q-ario (cf. [McE04]). Para tal efecto, se codifica el mensaje para darle alguna protección contra errores en el canal.

Supóngase que el mensaje $\mathbf{u}$ es codificado en la palabra-código $\mathbf{x}$ la cual es enviada por el canal, debido al ruido del canal, el vector recibido $\mathbf{y}$, quizá sea diferente de $\mathbf{x}$, esto es, $\mathbf{y} = \mathbf{x} + \mathbf{e}$ donde $\mathbf{e}$ es un vector error, la decodificación debe decidir a partir de $\mathbf{y}$ que mensaje $\mathbf{u}$ o (usualmente más simple) que palabra-código $\mathbf{x}$ fué transmitida. En la Figura 1 se muestra un sistema general de transmisión de información como el que se acaba de describir.

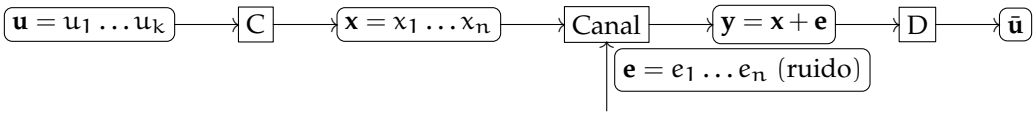

Figura 1: Sistema general de transmisión de información

Definiciones y conceptos básicos relacionados con los códigos lineales sobre campos finitos son dados en la sección **1**, la estructura de los códigos cíclicos lineales se describe en la sección **2** y **3** (cf. [MA78], [Rom92], [McE04]).

2.1 CÓDIGOS LINEALES

Sea $\mathbb{F}_q$ un campo finito con q elementos, donde $q = p^m$, p-primo, $m \in \mathbb{N}$ y sea $\mathbb{F}_q^n$ el conjunto de n-adas de elementos de $\mathbb{F}_q$.

Definición 2.1. *Se dice que $\mathcal{C}$ es un código de longitud n sobre $\mathbb{F}_q$ ó que $\mathcal{C}$ es un $\mathbb{F}_q$- código de longitud n si $\mathcal{C}$ es un subconjunto de $\mathbb{F}_q^n$. Un (n, M)-código $\mathcal{C}$ sobre $\mathbb{F}_q$ es un código de longitud n y tamaño M. A los elementos de un código $\mathcal{C}$ se les llama palabras-código.*

Definición 2.2. *Sea $H \in \mathcal{M}_{(n-k)\times n}(\mathbb{F}_q)$ arbitraria. Llamamos a $\mathcal{C}$ código lineal de longitud n sobre $\mathbb{F}_q$ con matriz de chequeo de paridad H al conjunto que consiste de todos los vectores $\mathbf{x} \in \mathbb{F}_q^n$ tales que $H\mathbf{x}^t = \mathbf{0}$, i.e.,*

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_q^n : H\mathbf{x}^t = \mathbf{0}\}.$$

Definición 2.3. *Sea $\mathcal{C}$ un código lineal sobre $\mathbb{F}_q$. Una matriz G cuyo espacio fila es igual a $\mathcal{C}$ es llamada una matriz generadora para $\mathcal{C}$. Recíprocamente, si G es una matriz con entradas en $\mathbb{F}_q$, su espacio fila es llamado el código lineal generado por G.*

Teorema 2.1. *Si $\mathcal{C}$ es un código lineal sobre $\mathbb{F}_q$ con matriz de chequeo de paridad $H = [A|I_{n-k}] \in \mathcal{M}_{(n-k)\times n}(\mathbb{F}_q)$, entonces su matriz generadora está dada por $G = [I_k|-A^t]$ y viceversa.*

Demostración. Si el mensaje es $\mathbf{u} = (u_1, \ldots, u_k)$, entonces $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{C}$ es tal que $x_1 = u_1, ...,$ $x_k = u_k$, de ahí que,

$$\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = I_k \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}$$

Partiendo de que $H\mathbf{x}^t = 0$ y que $H = [A|I_{n-k}]$, tenemos que

$$[A|I_{n-k}] \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$$

entonces

$$0 = A \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} + I_{n-k} \begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix}$$

esto implica que,

$$\begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix} = -A \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = -A \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}$$

por consiguiente,

$$\begin{pmatrix} x_1 \\ \vdots \\ x_k \\ x_{k+1} \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} I_k \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix} \\ -A \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix} \end{pmatrix} = \begin{pmatrix} I_k \\ -A \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}, \text{i.e.,} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} I_k \\ -A \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix},$$

transponiendo, la última ecuación, obtenemos $\mathbf{x} = [x_1x_2...x_n] = [u_1u_2...u_k][I_k|-A^t] = \mathbf{u}G$, donde $G = [I_k|-A^t]$. □

A las matrices H y G que se enuncian en el Teorema 2.1 se les llaman matriz de chequeo de paridad estándar y matriz generadora estándar, respectivamente.

Teorema 2.2. *Si $\mathcal{C}$ es un código lineal con matriz de chequeo de paridad $H = [A|I_{n-k}] \in \mathcal{M}_{(n-k)\times n}(\mathbb{F}_q)$, entonces $dim\mathcal{C} = k$ y $|\mathcal{C}| = q^k$.*

Demostración. Como *rango*$(H) = n-k$ entonces *nulidad*$(H) = n-(n-k) = k$, por consiguiente, $dim\mathcal{C} = k$ y toda palabra-código se puede escribir como combinación lineal de k vectores en $\mathcal{C}$, i.e., $\mathbf{x} = \sum_{i=1}^{n} \alpha_i \mathbf{x_i}$ donde $\alpha_i \in \mathbb{F}_q$ y $\mathbf{x_i} \in \mathcal{C}, i = 1, ..., k$. Hay q^k de tales combinaciones lineales, por lo tanto, $|\mathcal{C}| = q^k$. □

Definición 2.4. *Un $[n, k]$-código lineal sobre $\mathbb{F}_q$ es un subespacio k-dimensional del espacio vectorial $\mathbb{F}_q^n$; n es llamado la longitud del código y k la dimensión .*

Usualmente la matriz de chequeo de paridad H de un $[n, k]$-código lineal $\mathcal{C}$ es una matriz de tamaño $(n-k) \times n$ de la forma $H = [A|I_{n-k}]$, sin embargo, H no necesariamente debe tener esta forma ya que si H es equivalente a una matriz escalonada reducida por filas H', entonces el espacio nulo de H' es igual al espacio nulo de H.

Definición 2.5. *Se dice que dos códigos lineales $\mathcal{C}_1$ y $\mathcal{C}_2$ son equivalentes por permutación si existe una permutación de sus coordenadas, la cual envía $\mathcal{C}_1$ a $\mathcal{C}_2$, ver Ejemplo 2.2. Esta permutación puede ser descrita usando una matriz de permutación, la cual es una matriz cuadrada con exactamente un 1 en cada fila y columna y 0's en todo lo demás. Sean G_1 la matriz generadora de $\mathcal{C}_1$ y G_2 la matriz generadora de $\mathcal{C}_2$, $\mathcal{C}_1$ y $\mathcal{C}_2$ son equivalentes por permutación si y sólo si existe una matriz de permutación P tal que $G_1P = G_2$ (c.f. [HP03]).*

Teorema 2.3. *Si $\mathcal{C}$ es un $[n,k]$-código lineal sobre $\mathbb{F}_q$ con matriz de chequeo de paridad H y matriz generadora G entonces $HG^t = 0$ o $GH^t = 0$.*

Demostración. Como $\mathbf{x} = \mathbf{u}G$ para cada $\mathbf{x} \in \mathcal{C}$ y $\mathbf{u} \in \mathbb{F}_q^n$ entonces $\mathbf{x}^t = G^t\mathbf{u}^t$, pero $H\mathbf{x}^t = 0$, de ahí que, $0 = H\mathbf{x}^t = HG^t\mathbf{u}^t$, i.e., $0 = HG^t\mathbf{u}^t$ para cada $\mathbf{u} \in \mathbb{F}_q^n$, por consiguiente, $HG^t = 0$ o bien, $GH^t = 0$. □

Definición 2.6. *Sean $n \in \mathbb{N}$ y $\mathbf{x} \in \mathbb{F}_q^n$*

(i) El peso de Hamming de $\mathbf{x}$, denotado por $w_H(\mathbf{x})$, se define como $w_H(\mathbf{x}) := |\{1 \leqslant j \leqslant n \mid x_j \neq 0\}|$.

(ii) La distancia de Hamming entre $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, denotada por $d_H(\mathbf{x}, \mathbf{y})$, se define como:

$$d_H(\mathbf{x}, \mathbf{y}) = w_H(\mathbf{x} - \mathbf{y})$$

(iii) Si C es un código sobre $\mathbb{F}_q$, la distancia mínima de Hamming

$$\begin{aligned} d_C &= \text{mín}\{d_H(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C \text{ y } \mathbf{x} \neq \mathbf{y}\} \\ &= \text{mín}\{w_H(\mathbf{x} - \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C \text{ y } \mathbf{x} \neq \mathbf{y}\} \end{aligned}$$

La distancia mínima de un $[n,k]$-código lineal es de suma importancia en la teoría de códigos detectores-correctores de errores, uno de los resultados más relevantes respecto a este parámetro se enuncia a continuación, cuya demostración se puede encontrar en cualquier libro de Teoría de Códigos.

Teorema 2.4 ([LA14] Teorema 3.9, pág. 16)**.** *Un $[n,k,d]$-código lineal $\mathcal{C}$ sobre $\mathbb{F}_q$, puede corregir $\left[\frac{1}{2}(d-1)\right]$ o menos errores.*

Definición 2.7. *Sean $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ y $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ vectores en $\mathbb{F}_q^n$. El producto escalar de $\mathbf{u}$ y $\mathbf{v}$ está definido por $u_1v_1 + u_2v_2 + \cdots + u_nv_n$ y se denota por $\mathbf{u} \cdot \mathbf{v}$. Dos vectores $\mathbf{u}$ y $\mathbf{v}$ en $\mathbb{F}_q^n$ son ortogonales si $\mathbf{u} \cdot \mathbf{v} = 0$.*

Definición 2.8. *Si $\mathcal{C}$ es un $\mathbb{F}_q$-código lineal su código dual u ortogonal $\mathcal{C}^\perp$ puede ser definido como el conjunto de vectores que son ortogonales a todas las palabras-código de $\mathcal{C}$, es decir,*

$$\mathcal{C}^\perp = \left\{\mathbf{u} \in \mathbb{F}_q^n : \mathbf{u} \cdot \mathbf{v} = 0 \text{ para todo } \mathbf{v} \in \mathcal{C}\right\},$$

un $\mathbb{F}_q$-código lineal $\mathcal{C}$ es auto-dual si $\mathcal{C} = \mathcal{C}^\perp$.

2.2 CÓDIGOS CÍCLICOS LINEALES

Un *corrimiento cíclico* es una función:

$$\begin{aligned} \sigma : \mathbb{F}_q^n &\to \mathbb{F}_q^n \\ \mathbf{a} = (a_0, \ldots, a_{n-1}) &\mapsto \sigma(\mathbf{a}) = (a_{n-1}, a_0, \ldots, a_{n-2}) \end{aligned}$$

Definition 2.1. *Un código $\mathcal{C} \subseteq \mathbb{F}_q^n$ es cíclico si es lineal y si un corrimiento cíclico de una palabra-código es también una palabra-código, i.e., $\sigma(\mathcal{C}) = \mathcal{C}$.*

Sea $\mathcal{R}_n = \dfrac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle}$.

Recordemos lo siguiente sobre el anillo $\mathcal{R}_n$,

- Cada polinomio con coeficientes en $\mathbb{F}_q$ de grado menor o igual que $n-1$ pertenece a una clase diferente, estos polinomios serán los representantes de las clases residuales.
- La suma y el producto en $\mathcal{R}_n$ son las usuales, i.e., en la suma se suman los polinomios representantes y en el producto se multiplican los polinomios representantes, recordando que en este último caso el producto obtenido se reduce módulo x^n-1. Obsérvese que $x^n+\langle x^n-1\rangle = 1+\langle x^n-1\rangle$ en $\mathcal{R}_n$ ya que $x^n-1 \in \langle x^n-1\rangle$, lo cual se denota por $x^n \equiv 1 \pmod{x^n-1}$, en este contexto, abusando de la notación, se suele reemplazar a $x^n \equiv 1 \pmod{x^n-1}$ por $x^n = 1$ en $\mathcal{R}_n$.

Definimos la siguiente función

$$\begin{aligned} \psi : \mathbb{F}_q^n &\to \mathcal{R}_n \\ \mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) &\mapsto c(x)+I = (c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) + I \end{aligned} \tag{3}$$

donde $I = \langle x^n-1\rangle$ y ψ es un isomorfismo que va del $\mathbb{F}_q$ espacio vectorial $\mathbb{F}_q^n$ al $\mathbb{F}_q$ espacio vectorial $\mathcal{R}_n$. Para probar que es un isomofismo de espacios vectoriales primero veamos que ψ es transformación lineal, sean $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ con $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ y $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$ y $\lambda \in \mathbb{F}_q$ tenemos que

$$\begin{aligned} \psi(\mathbf{a}+\lambda\mathbf{b}) &= \psi((a_0+\lambda b_0, a_1+\lambda b_1, \ldots, a_{n-1}+\lambda b_{n-1})) \\ &= ((a_0+\lambda b_0) + (a_1+\lambda b_1)x + \ldots + (a_{n-1}+\lambda b_{n-1})x^{n-1}) + I \\ &= ((a_0 + a_1x + \ldots + a_{n-1}x^{n-1}) + I) + (\lambda(b_0 + b_1x + \ldots + b_{n-1}x^{n-1}) + I) \\ &= \psi(\mathbf{a}) + \lambda\psi(\mathbf{b}) \end{aligned}$$

Por lo que ψ es tranformación lineal, ahora bien , por el recordatorio que hicimos previamente sobre el anillo $\mathcal{R}_n$ entonces cada elemento $f(x)+I \in \mathcal{R}_n$ es de la forma $f(x)+I = (f_0 + f_1x + \cdots + f_{n-1}x^{n-1}) + I$, luego, existe $\mathbf{f} = (f_0, f_1, \ldots, f_{n-1}) \in \mathbb{F}_q^n$ tal que $\psi(\mathbf{f}) = f(x)+I$, por lo que ψ es sobreyectiva. Para ver que ψ es inyectiva tomemos dos elementos, $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ con $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ y $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$, y supongamos que $\psi(\mathbf{a}) = \psi(\mathbf{b})$

$$\begin{aligned} &\Rightarrow \quad a(x)+I = b(x)+I \\ &\Rightarrow \quad a(x)-b(x) \in I = \langle x^n-1\rangle \\ &\Rightarrow \quad a(x)-b(x) = 0 \text{ en } \mathbb{F}_q[x] \text{ (ya que } grad(a(x)-b(x)) < n) \\ &\Rightarrow \quad a(x) = b(x) \\ &\Rightarrow \quad a_i = b_i \text{ para cada } i \in \{0,1,\ldots,n-1\} \\ &\Rightarrow \quad \mathbf{a} = \mathbf{b} \end{aligned}$$

por lo que ψ es un isomorfismo de espacios vectoriales. Así que a cada elemento $\mathbf{a} \in \mathcal{C}$ lo podemos ver como $a(x)+I$ donde $I = \langle x^n-1\rangle$ y vicecersa.

Teorema 2.5. *Sea ψ como la definimos en (3) y $\mathcal{C}$ un subconjunto no vacío de $\mathbb{F}_q^n$. $\mathcal{C}$ es un código cíclico si y sólo si, $\psi(\mathcal{C})$ es un ideal del anillo $\mathcal{R}_n$.*

Demostración. $\Leftarrow$] Supongamos que $\psi(\mathcal{C})$ es un ideal de $\mathcal{R}_n$, entonces para cualesquiera $\alpha+I, \beta+I \in \mathcal{R}_n$, con $\alpha, \beta \in \mathbb{F}_q$ y $\mathbf{a}, \mathbf{b} \in \mathcal{C}$ se cumple que $\alpha\psi(\mathbf{a})+I, \beta\psi(\mathbf{b})+I \in \psi(\mathcal{C})$, así $(\alpha\psi(\mathbf{a})+\beta\psi(\mathbf{b}))+I$ está en $\psi(\mathcal{C})$ y como ψ es tranformación $\mathbb{F}_q$-lineal, tenemos que $(\alpha\psi(\mathbf{a})+\beta\psi(\mathbf{b}))+I = \psi(\alpha\mathbf{a}+\beta\mathbf{b})$ es un elemento de $\psi(\mathcal{C})$, por lo que $\alpha\mathbf{a}+\beta\mathbf{b}$ está en $\mathcal{C}$, de ahí que $\mathcal{C}$ es subespacio vectorial, y por tanto es un código lineal. Resta ver que $\mathcal{C}$ es cíclico, para ello consideremos la palabra código $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ en $\mathcal{C}$, tenemos que

$$\psi(\mathbf{c}) = c(x)+I = c_o + c_1x + \ldots + c_{n-1}x^{n-1} + I$$

y ya que $\psi(\mathcal{C})$ es un ideal de $\mathcal{R}_n$ y $x+I$ está en $\mathcal{R}_n$ entonces

$$\begin{aligned} (c(x)+I)(x+I) &= (c_0 + c_1x + \ldots + c_{n-1}x^{n-1} + I)(x+I) \\ &= (c_0 + c_1x + \ldots + c_{n-1}x^{n-1})x + I \\ &= (c_0x + c_1x^2 + \ldots + c_{n-2}x^{n-1} + c_{n-1}x^n) + I \\ &= (c_0x + c_1x^2 + \ldots + c_{n-2}x^{n-1} + c_{n-1}) + I \text{ (ya que } x^n = 1 \text{ en } \mathcal{R}_n) \\ &= (c_{n-1} + c_0x + c_1x^2 + \ldots + c_{n-2}x^{n-1}) + I \end{aligned}$$

está en $\psi(\mathcal{C})$, y mas aún, ya que éste es el polinomio asociado con el vector $\mathbf{c}' = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$, entonces $\mathbf{c}'$ está en $\mathcal{C}$. Por tanto, $\mathcal{C}$ es un código cíclico.

$\Rightarrow$] Supongamos que $\mathcal{C}$ es un código cíclico. Sean $a(x) + I, b(x) + I$ elementos de $\psi(\mathcal{C})$, existen $\mathbf{a}$, $\mathbf{b}$ en $\mathcal{C}$ tales que $\psi(\mathbf{a}) = a(x) + I$ y $\psi(\mathbf{b}) = b(x) + I$, así

$$\begin{aligned}(a(x) - b(x)) + I &= \psi(\mathbf{a}) - \psi(\mathbf{b}) \\ &= \psi(\mathbf{a} - \mathbf{b}) \text{ (ya que } \psi \text{ es } \mathbb{F}_q - \text{lineal)}\end{aligned}$$

y como $\mathbf{a} - \mathbf{b}$ está en $\mathcal{C}$ entonces $\psi(\mathbf{a} - \mathbf{b})$ está en $\psi(\mathcal{C})$, así $(a(x) + I) - (b(x) + I)$ es un elemento de $\psi(\mathcal{C})$, de ahí que $(\psi(\mathcal{C}), +) \leqslant (\mathcal{R}_n, +)$. Por otro lado, sea $f(x) + I = f_0 + f_1 x + \ldots + f_{n-1}x^{n-1} + I$ elemento de $\psi(\mathcal{C})$, entonces $f(x) + I = \psi((f_0, f_1, \ldots, f_{n-1}))$, donde $(f_0, f_1, \ldots, f_{n-1})$ es una palabra código de $\mathcal{C}$, tenemos que el polinomio

$$(x + I)(f(x) + I) = f_{n-1} + f_0 x + f_1 x^2 + \cdots + f_{n-2}x^{n-1} + I$$

es también un elemento de $\psi(\mathcal{C})$ puesto que el vector $(f_{n-1}, f_0, f_1, \ldots, f_{n-2})$ es un elemento de $\mathcal{C}$ ya que este es cíclico. De manera análoga

$$(x^2 + I)(f(x) + I) = (x + I)(xf(x) + I) = f_{n-2} + f_{n-1}x + f_0 x^2 + f_1 x^3 + \cdots + f_{n-3}x^{n-1} + I$$

es un elemento de $\psi(\mathcal{C})$, ya que el vector $(f_{n-2}, f_{n-1}, f_0, f_1, \ldots, f_{n-3})$ está en $\mathcal{C}$. Supongamos que $(x^k + I)(f(x) + I)$ está en $\psi(\mathcal{C})$ con k un entero positivo, veamos que $(x^{k+1} + I)(f(x) + I)$ también lo está. Tenemos que

$$(x^{k+1} + I)(f(x) + I) = (x + I)(x^k f(x) + I)$$

y como $(x^k f(x) + I)$ está en $\psi(\mathcal{C})$ entonces existe un vector $\mathbf{f^k} = (f_{n-k}, f_{n-(k-1)}, \ldots, f_{n-1}, f_0, f_1, \ldots$ $\ldots, f_{n-(k+1)})$ en $\mathcal{C}$ tal que $\psi(\mathbf{f^k}) = (x^k f(x) + I)$, luego

$$\begin{aligned}(x + I)(x^k f(x) + I) &= (x + I)(f_{n-k} + f_{n-(k-1)}x + \cdots + f_0 x^k + f_1 x^{k+1} + \cdots f_{n-(k+1)}x^{n-1} + I) \\ &= (f_{n-(k+1)} + f_{n-k}x + f_{n-(k-1)}x^2 + \cdots + f_0 x^{k+1} + f_1 x^{k+2} + \cdots \\ &\quad \cdots + f_{n-(k+2)}x^{n-1}) + I\end{aligned}$$

pero $\mathbf{f^{k+1}} = (f_{n-(k+1)}, f_{n-k}, f_{n-(k-1)}, \ldots, f_{n-1}, f_0, f_1, \ldots, f_{n-(k+2)}) \in \mathcal{C}$ ya que $\mathbf{f^k} \in \mathcal{C}$ y $\mathcal{C}$ es cíclico, entonces $x^{k+1}f(x) + I$ está en $\mathcal{C}$. Por lo que, para toda $k \geqslant 0$ se cumple que $(x^k + I)(f(x) + I)$ pertenece a $\psi(\mathcal{C})$. Sea $g(x) + I = g_0 + g_1 x + \cdots + g_{n-1}x^{n-1} + I$ un elemento de $\mathcal{R}_n$ entonces

$$\begin{aligned}g(x)f(x) + I &= (g_0 + g_1 x + \cdots + g_{n-1}x^{n-1} + I)(f(x) + I) \\ &= \sum_{i=0}^{n-1} g_i(x^i f(x) + I)\end{aligned}$$

y como $x^i f(x) + I$ está en $\psi(\mathcal{C})$ para cada $0 \leqslant i \leqslant n-1$, existe $\mathbf{f^i}$ para cada i, tal que $\psi(\mathbf{f^i}) = x^i f(x) + I$, y ya que ψ es isomorfismo de espacios vectoriales y cada g_i está en $\mathbb{F}_q$ se sigue que

$$\begin{aligned}g(x)f(x) + I &= \sum_{i=0}^{n-1} g_i \psi(\mathbf{f^i}) \\ &= \sum_{i=0}^{n-1} \psi(g_i \mathbf{f^i}) \\ &= \psi(\sum_{i=0}^{n-1} g_i \mathbf{f^i})\end{aligned}$$

y como $\mathcal{C}$ es un código lineal entonces $\sum_{i=0}^{n-1} g_i \mathbf{f^i}$ está en $\mathcal{C}$, por lo que $f(x)g(x) + I$ es un elemento de $\psi(\mathcal{C})$. Por tanto, $\psi(\mathcal{C})$ es un ideal de $\mathcal{R}_n$

□

A partir de ahora, cuando hablemos de un código cíclico $\mathcal{C}$ lo veremos como un ideal del anillo $\mathcal{R}_n$ y viceversa, según nos convenga.

Notar que, de acuerdo a la definición de código cíclico, un código lineal $\mathcal{C}$ es cíclico si es cerrado bajo todo corrimiento cíclico, es decir,

$$(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \Rightarrow (c_k, \ldots, c_{n-1}, c_0, c_1, \ldots, c_{k-1}) \in \mathcal{C}$$

Si $p(x) + I \in \mathcal{R}_n$, entonces el ideal generado por $p(x) + I$, denotado por $\langle p(x) + I \rangle$ (donde I es el ideal $I = \langle x^n - 1 \rangle$), es, abusando del lenguaje, el ideal generado por $p(x)$ en $\mathcal{R}_n$

2.2.1 El Polinomio Generador de un Código Cíclico

En el siguiente teorema exhibiremos que $\mathcal{R}_n$ es un anillo de ideales principales y por ende que cada código cíclico tiene un polinomio generador.

Teorema 2.6. *Sea $\mathcal{C}$ un ideal en $\mathcal{R}_n$ distinto de cero, esto es, un código cíclico de longitud n.*

i) Hay un único polinomio mónico $g(x)$ de grado mínimo tal que $\mathcal{C} = \langle g(x) + I \rangle$ y $g(x)$ es llamado el polinomio generador de $\mathcal{C}$.

ii) El polinomio generador $g(x)$ divide a $x^n - 1$.

iii) Si el $\mathtt{grad}(g(x)) = r$, entonces $\mathcal{C}$ tiene dimensión $n - r$. De hecho,

$$\mathcal{C} = \langle g(x) + I \rangle = \{(r(x) + I)(g(x) + I) : \mathtt{grad}(r(x)) < n - r\}.$$

iv) Si $g(x) = g_0 + g_1 x + \cdots + g_r x^r$ entonces $g_0 \neq 0$ y $\mathcal{C}$ tiene matriz [1] generadora

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_r & & \\ & g_0 & g_1 & \cdots & g_r & \\ & & \ddots & & & \ddots \\ & & & g_0 & g_1 & \cdots & g_r \end{pmatrix}$$

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

Demostración. i) Sean los polinomios $g_1(x), g_2(x) \in \mathbb{F}_q[x]$ mónicos y de grado mínimo r distintos, tales que $g_1(x) + I, g_2(x) + I \in \mathcal{C}$ y $g_1(x) + I \neq g_2(x) + I$, entonces $(g_1(x) + I) - (g_2(x) + I) \neq 0$ y $(g_1(x) + I) - (g_2(x) + I) \in \mathcal{C}$ pero $\mathtt{grad}(g_1(x) - g_2(x)) < r$ lo cual no puede ser posible, así, $g_1(x) + I = g_2(x) + I$. Por lo tanto, hay un único polinomio mónico $g(x)$ de grado mínimo r tal que $g(x) + I \in \mathcal{C}$.

Veamos que $\mathcal{C} = \langle g(x) + I \rangle$.

$\supseteq$]Sea $g(x) \in \mathbb{F}_q[x]$ mónico y de grado mínimo r tal que $g(x) + I \in \mathcal{C}$, como $\mathcal{C}$ es un ideal de $\mathcal{R}_n$, entonces $\langle g(x) + I \rangle \subseteq \mathcal{C}$.

$\subseteq$] Supongamos que $p(x) + I \in \mathcal{C}$ para algún $p(x) \in \mathbb{F}_q[x]$, por el algoritmo de la división existen $q(x), r(x) \in \mathbb{F}_q[x]$ tales que $p(x) = q(x)g(x) + r(x)$ donde $r(x) = 0$ ó $\mathtt{grad}(r(x)) < \mathtt{grad}(g(x))$ entonces $p(x) + I = (q(x) + I)(g(x) + I) + (r(x) + I)$ para algún $q(x) + I, r(x) + I \in \mathcal{R}_n$. Como $\mathcal{C}$ es un ideal que contiene a $g(x) + I$, tenemos, $p(x) + I, (q(x) + I)(g(x) + I) \in \mathcal{C}$, por consiguiente, $r(x) + I = p(x) + I - (q(x) + I)(g(x) + I) \in \mathcal{C}$, i.e., $r(x) + I \in \mathcal{C}$ pero $\mathtt{grad}(r(x)) < \mathtt{grad}(g(x))$ ésto sólo es posible si $r(x) = 0$, de ahí que $p(x) = q(x)g(x)$ entonces $p(x) + I = q(x)g(x) + I = (q(x) + I)(g(x) + I) \in \langle g(x) + I \rangle$, por consiguiente, $p(x) + I \in \langle g(x) + I \rangle$, en consecuencia, $\mathcal{C} \subseteq \langle g(x) + I \rangle$.

Por lo tanto, $\mathcal{C} = \langle g(x) + I \rangle$.

1 Los espacios en blanco en la matriz representan los ceros omitidos

ii) Dividiendo $x^n - 1$ por $g(x)$ obtenemos $x^n - 1 = q(x)g(x) + r(x)$ para algunos $q(x), r(x) \in \mathbb{F}_q[x]$ donde $r(x) = 0$ ó $grad(r(x)) < r$. Como en $\mathcal{R}_n$ $(x^n - 1) + I = 0 + I$. Entonces

$$\begin{aligned}(x^n - 1) + I &= (q(x)g(x) + r(x)) + I \text{ en } \mathcal{R}_n \\ &= (q(x) + I)(g(x) + I) + (r(x) + I)\end{aligned}$$

si $f(x) + I = (q(x) + I)(g(x) + I) \in \mathcal{C}$ para $f(x) = q(x)g(x) \in \mathbb{F}_q[x]$

$$\begin{aligned}&\Rightarrow 0 + I = (f(x) + I) + (r(x) + I) \\ &\Rightarrow r(x) + I \in \mathcal{C} \text{ donde } grad(r(x)) < r \\ &\Rightarrow r(x) = 0 \\ &\Rightarrow x^n - 1 = q(x)g(x)\end{aligned}$$

Por lo tanto, $g(x)|x^n - 1$.

iii) El ideal generado por $g(x) + I$ es $\langle g(x) + I\rangle = \{(f(x) + I)(g(x) + I) : f(x) + I \in \mathcal{R}_n\}$ con la reducción usual módulo $x^n - 1$ y debemos mostrar que es suficiente restringir $f(x)$ a polinomios de grado menor que $n - r$. Como $g(x)|x^n - 1$ entonces $x^n - 1 = h(x)g(x)$ para algún $h(x) \in \mathbb{F}_q[x]$ de grado $n - r$. Dividamos $f(x)$ por $h(x)$ luego $f(x) = q(x)h(x) + r(x)$ donde $grad(r(x)) < grad(h(x)) = n - r$

$$\begin{aligned}&\Rightarrow f(x)g(x) = q(x)h(x)g(x) + r(x)g(x) \\ &\Rightarrow f(x)g(x) = q(x)(x^n - 1) + r(x)g(x) \\ &\Rightarrow f(x)g(x) - r(x)g(x) = q(x)(x^n - 1) \in (x^n - 1) = I \\ &\Rightarrow f(x)g(x) - r(x)g(x) \in I \\ &\Rightarrow f(x)g(x) \equiv r(x)g(x) \pmod{I}\end{aligned}$$

lo que queríamos demostrar. Sólo resta probar que el conjunto

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

genera a $\mathcal{C}$ y es linealmente independiente, formando así una base para $\mathcal{C}$. Veamos que dicho conjunto genera a $\mathcal{C}$. Sea $u(x) + I \in \mathcal{C}, u(x) + I = (f(x) + I)(g(x) + I)$ donde $grad(f(x)) < n - r$ y $f(x) = a_0 + a_1x + \ldots + a_{n-r-1}x^{n-r-1}$

$$\begin{aligned}\Rightarrow u(x) + I &= ((a_0 + a_1x + \ldots + a_{n-r-1}x^{n-r-1}) + I)(g(x) + I) \\ &= ((a_0 + a_1x + \ldots + a_{n-r-1}x^{n-r-1})g(x)) + I \\ &= (a_0g(x) + a_1xg(x) + \ldots + a_{n-r-1}x^{n-r-1}g(x)) + I \\ &= (a_0g(x) + I) + (a_1xg(x) + I) + \ldots + (a_{n-r-1}x^{n-r-1}g(x) + I) \\ &= (a_0 + I)(g(x) + I) + (a_1 + I)(xg(x) + I) + \ldots + \\ &\quad (a_{n-r-1} + I)(x^{n-r-1}g(x) + I)\end{aligned}$$

así $\{g(x) + I, xg(x) + I, \ldots, x^{n-r-1}g(x) + I\}$ genera a $\mathcal{C}$, donde como sabemos los $a_i + I$ están en una copia isomofa de $\mathbb{F}_q$ en $\mathcal{R}_n$.
Ahora probemos que $\{g(x) + I, xg(x) + I, \ldots, x^{n-r-1}g(x) + I\}$ es un conjunto linealmente indepen-

diente.
Supongamos que

$$\begin{aligned}
0+I &= (b_0+I)(g(x)+I)+(b_1+I)(xg(x)+I)+\ldots+(b_{n-r-1}+I)(x^{n-r-1}g(x)+I)\\
&\Rightarrow\quad (b_0g(x)+b_1xg(x)+\ldots+b_{n-r-1}x^{n-r-1}g(x))+I=0+I\\
&\Rightarrow\quad (b_0g(x)+b_1xg(x)+\ldots+b_{n-r-1}x^{n-r-1}g(x))\in I=\langle x^n-1\rangle\\
&\Rightarrow\quad (b_0+b_1x+\ldots+b_{n-r-1}x^{n-r-1})g(x)\in\langle x^n-1\rangle\\
&\Rightarrow\quad (b_0+b_1x+\ldots+b_{n-r-1}x^{n-r-1})g(x)=0\\
&\qquad (\text{ ya que este polinomio tiene grado menor que } n)\\
&\Rightarrow\quad b_0+b_1x+\ldots+b_{n-r-1}x^{n-r-1}=0\\
&\Rightarrow\quad b_i=0, i=0,\ldots,n-r-1\\
&\Rightarrow\quad b_i+I=0+I, i=0,\ldots,n-r-1
\end{aligned}$$

así $\{g(x)+I, xg(x)+I,\ldots,x^{n-r-1}g(x)+I\}$ es linealmente independiente. De ahí que $\{g(x)+I, xg(x)+I,\ldots,x^{n-r-1}g(x)+I\}$ es una base para $\mathcal{C}$. Por lo tanto, $\dim\mathcal{C}=n-r$.

iv) Supongamos que $g_0=0$, entonces $g(x)=xh(x)$ donde $h(x)\in\mathbb{F}_q[x]$ y $\mathrm{grad}(h(x))<r$ pero $h(x)=1\cdot h(x)$, y en $\mathcal{R}_n$ se tiene que:

$$h(x)+I=1\cdot h(x)+I=x^n\cdot h(x)+I=x^{n-1}(xh(x))+I=(x^{n-1}+I)(g(x)+I)\in\mathcal{C}\Rightarrow h(x)+I\in\mathcal{C},$$

lo cual no puede ser posible. Por lo tanto, $g_0\neq 0$. Finalmente, recordando que $\{g(x)+I, xg(x)+I,\ldots,x^{n-r-1}g(x)+I\}$ es una base de $\mathcal{C}$ y que a una clase polinomial la podemos ver como una palabra-código luego tenemos las siguientes relaciones:

$$\begin{aligned}
g(x)+I &\leftrightarrow (g_0,g_1,\ldots,g_r,0,0,\ldots,0)\\
xg(x)+I &\leftrightarrow (0,g_0,g_1,\ldots,g_r,0,\ldots,0)\\
&\vdots\qquad\qquad \vdots\\
x_{n-r-1}g(x)+I &\leftrightarrow (0,0,\ldots,0,g_0,g_1,\ldots,g_r)
\end{aligned}$$

así el conjunto de palabras-código

$$\{(g_0,g_1,\ldots,g_r,0,0,\ldots,0),(0,g_0,g_1,\ldots,g_r,0,\ldots,0),\ldots,(0,0,\ldots,0,g_0,g_1,\ldots,g_r)\}$$

genera a $\mathcal{C}$ y por la Definición 2.3 tenemos que si G es la matriz

$$\begin{pmatrix}
g_0 & g_1 & \cdots & g_r & & \\
 & g_0 & g_1 & \cdots & g_r & \\
 & & \ddots & & & \ddots \\
 & & & g_0 & g_1 & \cdots & g_r
\end{pmatrix}$$

entonces el espacio fila de G debe generar a $\mathcal{C}$.

□

A partir de ahora haremos uso de la notación $\mathcal{C}=\langle\langle p(x)+I\rangle\rangle$ para denotar el hecho de que $\mathcal{C}$ es el ideal generado por $p(x)+I$ y que $p(x)$ es el polinomio generador para $\mathcal{C}$.

Teorema 2.7. *Un polinomio mónico* $p(x)$ *en* $\mathcal{R}_n$ *es el polinomio generador para un código cíclio si y sólo si* $p(x)|x^n-1$.

Demostración. Debemos establecer dos implicaciones.
$\Rightarrow$] Ya probamos en el teorema anterior que si $p(x)+I\in\mathcal{R}_n$ es el polinomio generador de un código cíclico $\mathcal{C}$ entonces $p(x)|x^n-1$.
$\Leftarrow$] Supongamos que $p(x)|x^n-1$ y sea $g(x)+I$ el polinomio generador para $\mathcal{C}=\langle p(x)+I\rangle$ con $p(x)\neq$

$g(x)$, entonces tenemos que $grad(g(x)) < grad(p(x))$.
Por hipótesis

$$x^n - 1 = p(x)f(x), \text{ para algún } f(x) \in \mathbb{F}_q[x]$$

Además como $g(x) + I \in \mathcal{C} \Rightarrow g(x) + I \in \langle p(x) + I\rangle \Rightarrow g(x) + I = (h(x) + I)(p(x) + I)$ para algún $h(x) \in \mathbb{F}_q[x] \Rightarrow (g(x) + I)(f(x) + I) = (h(x) + I)(p(x) + I)(f(x) + I) = (h(x) + I)((x^n - 1) + I) = 0 + I$. Pero $grad(g(x)f(x)) < grad(p(x)f(x)) = n$ y además $g(x)f(x) + I = 0 + I$ lo cual no puede ser posible, así $p(x) + I = g(x) + I$. Por lo tanto, si $p(x)|x^n - 1$ entonces $p(x)$ es el polinomio generador de un código cíclico.

□

Sean $\mathcal{D}_n = \{m(x) \in \mathbb{F}_q[x] : m(x)|x^n - 1$ y $m(x)$ es mónico$\}$ y $\mathcal{G}_n$ el conjunto de todos los códigos cíclicos en $\mathcal{R}_n$, es decir, $\mathcal{G}_n = \{\mathcal{C} \subseteq \mathcal{R}_n : \mathcal{C}$ es un ideal$\}$. Tenemos que la función

$$\begin{array}{rcl} \gamma : \mathcal{D}_n & \to & \mathcal{G}_n \\ g(x) & \to & \langle\langle g(x)\rangle\rangle \end{array}$$

es una correspondecia uno-a-uno entre el conjunto de todos los divisores mónicos, $\mathcal{D}_n$, y el conjunto de todos los códigos cíclicos, $\mathcal{G}_n$, en $\mathcal{R}_n$, donde envía a cada divisor mónico $g(x)$ de $x^n - 1$ al código $\langle\langle g(x)\rangle\rangle$. De los Teoremas 2.6 y 2.7 tenemos que γ es sobreyectiva, por lo que resta ver que γ es inyectiva. Sean $\mathcal{C}_1, \mathcal{C}_2 \in \mathcal{G}_n$, supongamos que $\mathcal{C}_1 = \mathcal{C}_2$ donde $\mathcal{C}_1 = \langle\langle m_1(x)\rangle\rangle$ y $\mathcal{C}_2 = \langle\langle m_2(x)\rangle\rangle$. Sea $c_1 = m_1(x) \in \mathcal{C}_1$, entonces $m_1(x) = c_1 \in \mathcal{C}_2$, por lo que $m_1(x) = f_1(x)m_2(x)$, luego $m_2(x)|m_1(x)$ y como $m_1(x)$ y $m_2(x)$ son mónicos del mismo grado entonces $m_1(x) = m_2(x)$

La función γ tiene algunas propiedades adicionales relacionadas con un orden parcial natural en $\mathcal{D}_n$ y $\mathcal{G}_n$. Notemos que si $\mathcal{C}_1$ y $\mathcal{C}_2$ son códigos cíclicos en $\mathcal{R}_n$, entonces la suma

$$\mathcal{C}_1 + \mathcal{C}_2 = \{\mathbf{c_1} + \mathbf{c_2} | \mathbf{c_1} \in \mathcal{C}_1, \mathbf{c_2} \in \mathcal{C}_2\}$$

es el código cíclico más pequeño en $\mathcal{R}_n$ que contiene a $\mathcal{C}_1$ y $\mathcal{C}_2$. Probemos esto último, sea $\mathcal{C}$ un ideal en $\mathcal{R}_n$ que contiene a $\mathcal{C}_1$ y $\mathcal{C}_2$, veamos que $\mathcal{C}_1 + \mathcal{C}_2 \subseteq \mathcal{C}$. Tomemos $\mathbf{c_1} + \mathbf{c_2} \in \mathcal{C}_1 + \mathcal{C}_2$, entonces $\mathbf{c_1} \in \mathcal{C}_1 \subseteq \mathcal{C}$ y $\mathbf{c_2} \in \mathcal{C}_2 \subseteq \mathcal{C}$, de ahí que $\mathbf{c_1} + \mathbf{c_2} \in \mathcal{C}$, lo que queríamos demostrar, en consecuencia $\mathcal{C}_1 + \mathcal{C}_2$ es el ideal más pequeño en $\mathcal{R}_n$ que contiene a $\mathcal{C}_1$ y $\mathcal{C}_2$.

Teorema 2.8. *Sea* $\mathcal{C}_1 = \langle\langle g_1(x) + I\rangle\rangle$ *y* $\mathcal{C}_2 = \langle\langle g_2(x) + I\rangle\rangle$ *códigos cíclicos en* $\mathcal{R}_n$. *Entonces*

i) $\mathcal{C}_1 \subseteq \mathcal{C}_2 \Leftrightarrow g_2(x)|g_1(x)$,

ii) $\mathcal{C}_1 \cap \mathcal{C}_2 = \langle\langle mcm(g_1(x), g_2(x))\rangle\rangle$,

iii) $\mathcal{C}_1 + \mathcal{C}_2 = \langle\langle mcd(g_1(x), g_2(x))\rangle\rangle$.

Demostración. i) Es fácil ver que se sigue el resultado. $\mathcal{C}_1 \subseteq \mathcal{C}_2 \Leftrightarrow \langle\langle g_1(x)\rangle\rangle \subseteq \mathcal{C}_2 \Leftrightarrow g_1(x) \in \mathcal{C}_2$ y ya que $\mathcal{C}_2 = \langle\langle g_2(x)\rangle\rangle \Leftrightarrow g_1(x) = m(x)g_2(x)$ para algún $m(x) \in \mathbb{F}_q[x] \Leftrightarrow g_2(x)|g_1(x)$.

$$\therefore \mathcal{C}_1 \subseteq \mathcal{C}_2 \Leftrightarrow g_2(x)|g_1(x)$$

ii) Dado que $\mathcal{C}_1 \cap \mathcal{C}_2$ es un ideal en $\mathcal{R}_n$ entonces es un código cíclico lineal sobre $\mathbb{F}_q$, luego $\mathcal{C}_1 \cap \mathcal{C}_2 = \langle\langle m(x)\rangle\rangle$ y solo resta porbar que $m(x) = mcm(g_1(x), g_2(x))$ para ello veamos que i) $m(x)$ es múltiplo de $g_1(x)$ y $g_2(x)$ y que ii) si $g_1(x)|u(x)$ y $g_2(x)|u(x)$ entonces $m(x)|u(x)$.
i) $m(x) \in \mathcal{C}_1 \cap \mathcal{C}_2 \Rightarrow m(x) \in \mathcal{C}_1$ y $m(x) \in \mathcal{C}_2 \Rightarrow m(x) = v_1(x)g_1(x)$ y $m(x) = v_2(x)g_2(x)$ para algunos $v_1, v_2 \in \mathcal{R}_n \Rightarrow m(x)$ es un múltiplo de $g_1(x)$ y de $g_2(x)$
ii) Supongamos que $g_1(x)|u(x)$ y $g_2(x)|u(x) \Rightarrow u(x) = z_1(x)g_1(x)$ y $u(x) = z_2(x)g_2(x) \Rightarrow u(x) \in \mathcal{C}_1$ y $u(x) \in \mathcal{C}_2 \Rightarrow u(x) \in \mathcal{C}_1 \cap \mathcal{C}_2 = \langle\langle m(x)\rangle\rangle \Rightarrow u(x) = h(x)m(x)$ para algún $h(x) \in \mathcal{R}_n \Rightarrow m(x)|u(x)$.
Así,$m(x) = mcm(g_1(x), g_2(x))$. Por lo tanto, $\mathcal{C}_1 \cap \mathcal{C}_2 = \langle\langle mcm(g_1(x), g_2(x))\rangle\rangle$.

iii) Dado que $\mathcal{C}_1 + \mathcal{C}_2$ es un ideal en $\mathcal{R}_n$, entonces es un código cíclico lineal sobre $\mathbb{F}_q$, luego $\mathcal{C}_1 + \mathcal{C}_2 = \langle\langle d(x)\rangle\rangle$ y sólo resta probar que $d(x) = mcd(g_1(x), g_2(x))$, para ello veamos que

a) $d(x)|g_1(x)$ y $d(x)|g_2(x)$,

b) Si $\nu(x)|g_1(x)$ y $\nu(x)|g_2(x)$, entonces $\nu(x)|d(x)$.

a) Sean $g_1(x) \in \mathcal{C}_1 \subseteq \mathcal{C}_1 + \mathcal{C}_2 = \langle\langle d(x)\rangle\rangle$ y $g_2(x) \in \mathcal{C}_2 \subseteq \mathcal{C}_1 + \mathcal{C}_2 = \langle\langle d(x)\rangle\rangle$

$$\Rightarrow g_1(x) = t_1(x)d(x) \text{ y } g_2(x) = t_2(x)d(x)$$

para algunos $t_1(x), t_2(x) \in \mathcal{R}_n$

$$\Rightarrow d(x)|g_1(x) \text{ y } d(x)|g_2(x).$$

b) Si $\nu(x)|g_1(x)$ y $\nu(x)|g_2(x)$ entonces $g_1(x) = u_1(x)\nu(x)$ y $g_2(x) = u_2(x)\nu(x)$ para algunos $u_1(x), u_2(x) \in \mathcal{R}_n$. Sea $d(x) = c \in \mathcal{C}_1 + \mathcal{C}_2$ entonces $c = c_1 + c_2$ con $c_1 \in \mathcal{C}_1$ y $c_2 \in \mathcal{C}_2$, por lo que existen $s_1(x), s_2(x) \in \mathcal{R}_n$ tales que $c_1 = s_1(x)g_1(x)$ y $c_2 = s_2(x)g_2(x)$

$$\begin{aligned} &\Rightarrow \quad d(x) = s_1(x)u_1(x)\nu(x) + s_2(x)u_2(x)\nu(x) = (m_1(x)u_1(x) + m_2(x)u_2(x))\nu(x) \\ &\Rightarrow \quad \nu(x)|d(x) \end{aligned}$$

Así, $d(x) = mcd(g_1(x), g_2(x))$. Por lo tanto, $\mathcal{C}_1 + \mathcal{C}_2 = \langle\langle mcd(g_1(x), g_2(x))\rangle\rangle$.

□

2.2.2 El Polinomio de Chequeo de un Código Cíclico

Como el polinomio generador $g(x)$ de un $[n, n-r]$-código cíclico en $\mathcal{R}_n$ divide a $x^n - 1$, tenemos que

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

donde $h(x)$ es un polinomio de grado $n - r$, llamado el polinomio de chequeo de $\mathcal{C}$.

Teorema 2.9. *Sea $h(x)$ el polinomio de chequeo de un código cíclico $\mathcal{C}$ en $\mathcal{R}_n$.*

i) El código $\mathcal{C}$ puede ser descrito de la siguente forma

$$\mathcal{C} = \{p(x) + I \in \mathcal{R}_n | (p(x) + I)(h(x) + I) = 0 + I\},$$

ii) Si $h(x) = h_0 + h_1x + \ldots + h_{n-r}x^{n-r}$, entonces una matriz de chequeo de paridad para $\mathcal{C}$ esta dada por

$$H = \begin{pmatrix} h_{n-r} & h_{n-r-1} & \cdots & h_0 & & \\ & h_{n-r} & h_{n-r-1} & \cdots & h_0 & \\ & & \ddots & & & \ddots \\ & & & h_{n-r} & h_{n-r-1} & \cdots & h_0 \end{pmatrix},$$

iii) El código dual $\mathcal{C}^\perp$ es el código cíclico de dimensión r con polinomio generador

$$h^\perp(x) = {h_0}^{-1}x^{n-r}h(x^{-1}) = {h_0}^{-1}(h_0x^{n-r} + h_1xn - r - 1 + \cdots + h_{n-r}),$$

donde el último polinomio en paréntesis es el polinomio reverso, ó contrario u opuesto del polinomio de chequeo $h(x)$. (Notar que $\mathcal{C}^\perp$ no es generado por $h(x)$).

Demostración. i) Sea $g(x) + I$ el polinomio generador de $\mathcal{C}$, si $p(x) + I \in \mathcal{C}$, entonces $p(x) + I = (f(x) + I)(g(x) + I)$ para algún $f(x) + I \in \mathcal{R}_n$. Así

$$\begin{aligned} (p(x) + I)(h(x) + I) &= (f(x) + I)(g(x) + I)(h(x) + I) \\ &= (f(x) + I)(g(x)h(x) + I) \\ &= (f(x)(x^n - 1) + I) \\ &= 0 + I \end{aligned}$$

por lo que $\mathcal{C} \subseteq \{p(x)+I \in \mathcal{R}_n | (p(x)+I)(h(x)+I) = 0+I\}$.

Por otro lado, sea $p(x)+I \in \mathcal{R}_n$ tal que $(p(x)+I)(h(x)+I) = 0+I$. Por el algoritmo de la división existen, $q(x), r(x) \in \mathbb{F}_q[x]$ tales que

$$p(x) = q(x)g(x) + r(x)$$

donde $r(x) = 0$ ó $grad(r(x)) < grad(g(x)) = r$. Supongamos que $grad(r(x)) < r$, multiplicando por $h(x)$, tenemos

$$p(x)h(x) = q(x)g(x)h(x) + r(x)h(x)$$

entonces, $p(x)h(x) - r(x)h(x) \in I$, así que $p(x)h(x)+I = r(x)h(x)+I$, de ahí que $r(x)h(x)+I = 0+I$, es decir, $r(x)h(x) \in \langle x^n - 1\rangle$ pero $grad(r(x)h(x)) < r + (n-r) = n$, lo cual es una contradicción por lo que $r(x) = 0$ y así $p(x) = q(x)g(x)$, lo que nos lleva a que $p(x)+I = (q(x)+I)(g(x)+I)$, por tanto $p(x)+I \in \mathcal{C}$.

ii) Sea $c(x)+I \in \mathcal{C}$, con $c(x)+I = c_0 + c_1x + c_2x^2 + \cdots + c_tx^t + I$ donde $t = grad(c(x)) < n$, tenemos por el inciso i) que $c(x)h(x)+I = 0+I$, es decir, $c(x)h(x) \in I$ por lo que existe $a(x) \in \mathbb{F}_q[x]$, con $a(x) = a_0 + a_1x + a_2x^2 \cdots + a_mx^m$ tal que $c(x)h(x) = a(x)(x^n-1)$ y como $grad(c(x)h(x)) < n + (n-r) = 2n-r$, entonces $m = grad(a(x)) < n-r$, por lo que existe $k \in \mathbb{N}$ tal que $m+k = n-r$. Notemos que

$$\begin{aligned}
a(x)(x^n-1) &= a_0x^n + a_1x^{n+1} + a_2x^{n+2} + \cdots + a_mx^{n+m} - a_0 - a_1x - a_2x^2 \cdots - a_mx^m \\
&= -a_0 - a_1x - a_2x^2 - \cdots - a_mx^m + a_{m+1}x^{m+1} + \cdots + a_{m+k-1}x^{m+k-1} \\
&\quad + a_{m+k}x^{m+k} + a_{m+k+1}x^{m+k+1} + \cdots + a_{n-1}x^{n-1} + \\
&\quad + a_0x^n + a_1x^{n+1} + a_2x^{n+2} \cdots + a_mx^{n+m} \\
&= -a_0 - a_1x - a_2x^2 - \cdots - a_mx^m + a_{m+1}x^{m+1} + \cdots + a_{n-r-1}x^{n-r-1} \\
&\quad + a_{n-r}x^{n-r} + a_{(n-r)+1}x^{(n-r)+1} + \cdots + a_{(n-r)+(r-1)}x^{n-r+(r-1)} + \\
&\quad + a_0x^n + a_1x^{n+1} + a_2x^{n+2} \cdots + a_mx^{n+m}
\end{aligned}$$

donde $a_{(n-r)+i} = 0$ para cada $i \in \{0,1,2,\ldots,r-1\}$, por lo que en el producto de $c(x)h(x)$, los coeficientes de $x^{n-r}, x^{n-r+1}, \ldots, x^{n-1}$ son iguales a 0, es decir, para toda $j \in \{n-r, n-r+1, \ldots, n-1\}$ se cumple $\sum_{i=0}^{j} c_ih_{j-i} = 0$, desarrollando la suma para cada j podemos ver que

$$\begin{aligned}
0 &= c_0h_{n-r} + c_1h_{n-r-1} + \cdots + c_{n-r}h_0 \\
0 &= c_0h_{n-r+1} + c_1h_{n-r} + c_2h_{n-r-1} + \cdots + c_{n-r+1}h_0 \\
&\vdots \\
0 &= c_0h_{n-1} + c_1h_{n-2} + \cdots + c_{r-1}h_{n-r} + c_rh_{n-1-r} + \cdots c_{n-1}h_0
\end{aligned}$$

y ya que $grad(h(x)) = n-r$, entonces $h_{n-1} = h_{n-2} = \cdots = h_{n-r+1} = 0$ por lo que, tenemos lo siguiente

$$\begin{aligned}
0 &= c_0h_{n-r} + c_1h_{n-r-1} + \cdots + c_{n-r}h_0 \\
0 &= c_1h_{n-r} + c_2h_{n-r-1} + \cdots + c_{n-r+1}h_0 \\
&\vdots \\
0 &= c_{r-1}h_{n-r} + c_rh_{n-1-r} + \cdots c_{n-1}h_0
\end{aligned}$$

de aqui, podemos ver que

$$\begin{pmatrix}
h_{n-r} & h_{n-r-1} & \cdots & h_0 & & & \\
 & h_{n-r} & h_{n-r-1} & \cdots & h_0 & & \\
 & & \ddots & & & \ddots & \\
 & & & h_{n-r} & h_{n-r-1} & \cdots & h_0
\end{pmatrix}
\begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} =
\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Por tanto, por la Definición 2.2 tenemos que H es una matriz de chequeo de paridad del código $\mathcal{C}$.

iii) Primero probemos que $h^{\perp}(x)$ divide a x^n-1. Tenemos que $h(x)g(x)=x^n-1$

$$\begin{aligned}
&\Rightarrow \quad h(x^{-1})g(x^{-1})=x^{-n}-1\\
&\Rightarrow \quad x^n h(x^{-1})g(x^{-1})=x^n(x^{-n}-1)\\
&\Rightarrow \quad (x^{n-r}h(x^{-1}))(x^r g(x^{-1}))=1-x^n\\
&\Rightarrow \quad h^{\perp}(x)(-f(x))=x^n-1 \text{ donde } f(x)=x^r g(x^{-1})\\
&\Rightarrow \quad h^{\perp}(x)|x^n-1
\end{aligned}$$

Así, por el Teorema 2.7, $\langle h^{\perp}(x)+I\rangle = \mathcal{C}'$ es un código cíclico y por el Teorema 2.6 su matriz generadora es H (como en el inciso ii)) y $\dim(\mathcal{C})=n-(n-r)=r$, ahora como $H\mathbf{c}^t=\mathbf{o}$ entonces para cada vector $\mathbf{h}$ generado por el espacio fila de la matriz H, es $\mathbf{h}\cdot\mathbf{c}=\mathbf{o}$, por lo que $\mathcal{C}'\subseteq\mathcal{C}^{\perp}$ y como $\dim(\mathcal{C}^{\perp})=r$ entonces $\mathcal{C}'=\mathcal{C}^{\perp}$

□

Ejemplo 2.1. *Sean* $\mathcal{R}=\mathbb{F}_2[x]$ *e* $I=x^9-1$, *tenemos que*

$$\mathcal{R}_9=\frac{\mathbb{F}_2[x]}{\langle x^9-1\rangle}=\{f(x)+(x^9-1) : f(x)\in\mathbb{F}_2[x]\}$$

Se tiene que $x^9-1=(1+x)(1+x+x^2)(1+x^3+x^6)$ *es producto de factores irreducibles sobre* $\mathbb{F}_2$. *De ahí que hay* $2^3=8$ *códigos cíclicos en* $\mathcal{R}_9$. *Uno de ellos es el código cíclico* $\mathcal{C}_1=\langle\langle(1+x^3+x^6)+(x^9-1)\rangle\rangle$ *que tiene dimensión* $\dim\mathcal{C}_1=9-6=3$ *y matriz generadora*

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

Existen códigos lineales muy famosos, uno de ellos es el $[7,4,3]-$código lineal de Hamming y en este ejemplo, abordaremos las principales características de dicho código.

Ejemplo 2.2. *Veamos que el* $[7,4,3]$*-código lineal de Hamming es un código cíclico lineal. Considérese el polinomio* $x^7-1=(1+x)(1+x^2+x^3)(1+x+x^3)$ *como producto de irreducibles sobre* $\mathbb{F}_2$ *y construyamos el anillo cociente* $\mathcal{R}_7=\dfrac{\mathbb{F}_2[x]}{\langle x^7-1\rangle}$. *Sea* $g(x)=1+x+x^3$ *tenemos que* $\langle\langle g(x)+(x^7-1)\rangle\rangle$ *es un ideal principal en* $\mathcal{R}_7$ *por lo que* $\langle\langle g(x)+(x^7-1)\rangle\rangle=\mathcal{C}$ *donde* $\mathcal{C}$ *es un código cíclico. Así* $g(x)$ *genera un* $[7,4]$*-código lineal cíclico con matriz generadora*

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

Sea $x\in\mathcal{C}$ *y* $u\in\mathbb{F}_2^4$ *con* $u=(u_1,u_2,u_3,u_4)$ *tenemos que* $x=u_1(1,1,0,1,0,0,0)+u_2(0,1,1,0,1,0,0)+u_3(0,0,1,1,0,1,0)+u_4(0,0,0,1,1,0,1)$. *Luego, todas las palabras códigos de* $\mathcal{C}$ *son*

0000000	0001101
0011010	0010111
0110100	0111001
0101110	0100011
1101000	1100101
1110010	1111111
1011100	1010001
1000110	1001011

Por otro lado, construyamos una matriz de chequeo de paridad del código de Hamming. Ésta se construye tomando los coficientes que resultan al expresar los números $1,2,3,4,5,6$ *y* 7 *a través de una expansión en base* 2, *como se muestra*

$$\begin{aligned}
1 &= 1\cdot 2^0 + 0\cdot 2^1 + 0\cdot 2^2\\
2 &= 0\cdot 2^0 + 1\cdot 2^1 + 0\cdot 2^2\\
3 &= 1\cdot 2^0 + 1\cdot 2^1 + 0\cdot 2^2\\
4 &= 0\cdot 2^0 + 0\cdot 2^1 + 1\cdot 2^2\\
5 &= 1\cdot 2^0 + 0\cdot 2^1 + 1\cdot 2^2\\
6 &= 0\cdot 2^0 + 1\cdot 2^1 + 1\cdot 2^2\\
7 &= 1\cdot 2^0 + 1\cdot 2^1 + 1\cdot 2^2
\end{aligned}$$

Posteriormente formamos la matriz H

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

y de aquí podemos obtener la matriz generadora que es

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

Así, todas las palabras código del código de Hamming, $\mathcal{H}$ *son:*

0000000	1110000
1101001	0011001
0101010	1011010
1000011	0110011
1001100	0111100
0100101	1010101
1100110	0010110
0001111	1111111

Podemos ver que mediante la permutación

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7\\ 1 & 6 & 3 & 7 & 5 & 4 & 2 \end{pmatrix}$$

Los códigos $\mathcal{C}$ *y* $\mathcal{H}$ *son equivalentes. Por lo tanto el [7,4,3]-código de Hamming es un código cíclico.*

2.3 IDEMPOTENTES

En esta sección daremos la definición y un resultado principal de idempotentes de un código cíclico sobre $\mathbb{F}_2$, por lo que $\mathcal{R}_n = \frac{\mathbb{F}_2[x]}{\langle x^n-1\rangle}$ con n impar.

Definición 2.9. *Un polinomio* $e(x)$ *en* $\mathcal{R}_n$ *es un idempotente si*

$$e(x) = e^2(x) = e(x^2)$$

Teorema 2.10. *Un código cíclico* $\mathcal{C} = \langle g(x) + 1\rangle$ *contiene un único idempotente* $e(x)$ *tal que* $\mathcal{C} = \langle e(x) + 1\rangle$

Demostración. Sea $x^n - 1 = g(x)h(x)$, donde $g(x)$ y $h(x)$ son primos relativos. Por el Algoritmo de Euclides existen polinomios $p(x)$ y $q(x)$ únicos en $\mathbb{F}_2[x]$ tales que

$$p(x)g(x) + q(x)h(x) = 1$$

Sea $e(x) = p(x)g(x)$ entonces sustituyendo y multiplicando por $e(x)$ en la igualdad de arriba tenemos que

$$e(x)e(x) - q(x)h(x)e(x) = e(x)$$

pero $q(x)h(x)e(x) = q(x)p(x)h(x)g(x) = q(x)p(x)(x^n - 1)$, por lo que

$$e^2(x) - e(x) \in \langle x^n - 1 \rangle$$

y así, en $\mathcal{R}_n$ se cumple que

$$e^2(x) = e(x)$$

Por otro lado, podemos ver que $e(x) + I = p(x)g(x) + I \in \langle g(x) + I \rangle$ donde $I = \langle x^n - 1 \rangle$, por lo que resta probar que $g(x) + I \in \langle e(x) + I \rangle$. Como $p(x)g(x) + q(x)h(x) = 1$, multiplicando por $g(x)$ y sustituyendo $e(x)$ tenemos que

$$e(x)g(x) + q(x)h(x)g(x) = g(x)$$

pero $q(x)h(x)g(x) \in \langle x^n - 1 \rangle$, por lo que

$$e(x)g(x) - g(x) \in \langle x^n - 1 \rangle$$

por lo que en $\mathcal{R}_n$ tenemos que $e(x)g(x) = g(x)$ y así $g(x) + I \in \langle e(x) + I \rangle$. Por lo tanto

$$\mathcal{C} = \langle e(x) + I \rangle.$$

□

3 CÓDIGOS CÍCLICOS SOBRE ANILLOS DE GALOIS

A lo largo de este capítulo estudiaremos las principales propiedades de los códigos cíclicos sobre anillos de Galois, en particular sobre el anillo $\mathbb{Z}_4$.

Recordemos que $\mathbb{Z}_4 = \frac{\mathbb{Z}}{4\mathbb{Z}}$ denota a los enteros módulo 4 y es un anillo local cuyo único ideal maximal es $M = \langle 2 \rangle$. Un conjunto de n-adas sobre $\mathbb{Z}_4$ es llamado un código sobre $\mathbb{Z}_4$ y es un $\mathbb{Z}_4-$código lineal si es un $\mathbb{Z}_4$-submódulo de $\mathbb{Z}_4^n$.

En este capítulo probaremos que cualquier código cíclico sobre $\mathbb{Z}_4$, $\mathcal{C}$, tiene generadores de la forma $(fh, 2fg)$ donde $fgh = x^n - 1$ sobre $\mathbb{Z}_4[x]$ y $|\mathcal{C}| = 4^{grad(g)}2^{grad(h)}$. Además probaremos que $\mathcal{C}^\perp$ tiene generadores de la forma $(g^*h^*, 2f^*g^*)$.

3.1 GENERADORES

Sea

$$\begin{array}{ccc} \mu\colon \mathbb{Z}_4 & \longrightarrow & \frac{\mathbb{Z}_4}{\langle 2 \rangle} \\ a & \longmapsto & a + \langle 2 \rangle \end{array} \tag{4}$$

Sabemos que μ es un homomorfismo sobreyectivo natural, además cabe recordar que $\frac{\mathbb{Z}_4}{\langle 2 \rangle}$ es isomorfo a $\mathbb{Z}_2$, y este a su vez es isomorfo a $\mathbb{F}_2$ por lo que en adelante haremos uso de esto de manera indistinta. La siguiente función, $\bar{\mu}$ manda a cada coeficiente de un polinomio $f(x) = \sum_{i=0}^{n} a_i x^i$ en $\mathbb{Z}_4[x]$ a su imagen bajo la función μ, es decir

$$\begin{array}{ccc} \bar{\mu}\colon \mathbb{Z}_4[x] & \longrightarrow & \frac{\mathbb{Z}_4}{\langle 2 \rangle}[x] \\ \sum_{i=0}^{n} a_i x^i & \longmapsto & \sum_{i=0}^{n} \mu(a_i) x^i \end{array} \tag{5}$$

Observación 3.1. *La función $\bar{\mu}$ es un homomorfismo sobreyectivo de anillos.*

Demostración. Sean $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{j=0}^{m} b_j x^j$ polinomios en $\mathbb{Z}_4[x]$, con $n \geqslant m$

$$\begin{aligned} \bar{\mu}(f(x) + g(x)) &= \bar{\mu}(\sum_{i=0}^{n} (a_i + b_i)x^i), \text{ donde } b_{m+1} = b_{m+2} = \ldots = b_n = 0 \\ &= \sum_{i=0}^{n} \mu(a_i + b_i)x^i \\ &= \sum_{i=0}^{n} (\mu(a_i) + \mu(b_i))x^i \text{ ya que } \mu \text{ es homorfismo.} \\ &= \sum_{i=0}^{n} \mu(a_i)x^i + \sum_{i=0}^{m} \mu(b_i))x^i \\ &= \bar{\mu}(f(x)) + \bar{\mu}(g(x)) \end{aligned}$$

Así, $\bar{\mu}(f(x) + g(x)) = \bar{\mu}(f(x)) + \bar{\mu}(g(x))$.

Por otro lado,

$$\begin{aligned}
\bar{\mu}(f(x)g(x)) &= \bar{\mu}(\sum_{j=0}^{m+n} c_j x^j), \text{ donde } c_j = \sum_{i=0}^{j} a_i b_{j-i} \\
&= \sum_{j=0}^{m+n} \mu(c_j)x^j \\
&= \sum_{j=0}^{m+n} \mu(\sum_{i=0}^{j} a_i b_{j-i})x^j \\
&= \sum_{j=0}^{m+n} \sum_{i=0}^{j} \mu(a_i b_{j-i})x^j \\
&= \sum_{j=0}^{m+n} \sum_{i=0}^{j} \mu(a_i)\mu(b_{j-i})x^j \\
&= (\sum_{i=0}^{n} \mu(a_i)x^i)(\sum_{j=0}^{m} \mu(b_j)x^j) \\
&= \bar{\mu}(f(x))\bar{\mu}(g(x))
\end{aligned}$$

De ahí, $\bar{\mu}(f(x)g(x)) = \bar{\mu}(f(x))\bar{\mu}(g(x))$.

Sea $\bar{f}(x) \in \frac{\mathbb{Z}_4}{\langle 2\rangle}[x]$, ya que μ es sobreyectivo para cada coeficiente de $\bar{f}(x) = \sum_{i=0}^{n} a_i' x^i$ existe un elemento en $\mathbb{Z}_4$ tal que $\mu(a_i) = a_i'$, por lo que existe un polinomio en $\mathbb{Z}_4[x]$, $f(x) = \sum_{i=0}^{n} a_i x^i$, tal que $\bar{\mu}(f(x)) = \bar{f}(x)$. Así, $\bar{\mu}$ es un homomorfismo sobreyectivo.

□

Es importante mencionar que a partir de ahora denotaremos a $\bar{\mu}(f(x))$ por $\bar{f}(x)$.

Definición 3.1. *Un poloniomio $f(x)$ en $\mathbb{Z}_4[x]$ es básico irreducible si $\mu(f(x))$ es irreducible en $\mathbb{F}_2[x]$; $f(x)$ es primario si $\langle f(x)\rangle$ es un ideal primario.*

Lema 3.1. *Si $f(x)$ es un polinomio básico irreducible, entonces $f(x)$ es primario.*

Demostración. Supongamos que $g(x)h(x) \in \langle f(x)\rangle$ para algunos $g(x), h(x) \in \mathbb{Z}_4[x]$, entonces $f(x)$ divide a $g(x)h(x)$, por lo que exite $k(x) \in \mathbb{Z}_4[x]$ tal que $g(x)h(x) = f(x)k(x)$, ya que $\bar{\mu}$ es homomorfismo de anillos, tenemos que $\bar{\mu}(g(x))\bar{\mu}(h(x)) = \bar{\mu}(f(x))\bar{\mu}(k(x))$, es decir $\bar{\mu}(f(x))$ divide a $\bar{\mu}(g(x))\bar{\mu}(h(x))$ y ya que $f(x)$ es básico irreducible entonces $\bar{\mu}(f(x))$ es irreducible en $\mathbb{F}_2[x]$, de ahí que sucede uno de los siguientes casos,

i) $mcd(\bar{\mu}(g(x)), \bar{\mu}(f(x))) = 1$

ii) $mcd(\bar{\mu}(g(x)), \bar{\mu}(f(x))) = \bar{\mu}(f(x))$

Si ocurre i), es decir, si $\bar{\mu}(g(x))$ y $\bar{\mu}(f(x))$ son coprimos, por el Lema 1.1 tenemos que $g(x)$ y $f(x)$ tambien son coprimos, luego, $f(x)$ divide a $h(x)$, de ahí que $h(x) \in \langle f(x)\rangle$ y así, $\langle f(x)\rangle$ es ideal primario. Por otro lado, si ocurre ii) tenemos que, $\bar{\mu}(f(x))$ divide a $\bar{\mu}(g(x))$, de ahí que existe $u(x) + \langle 2\rangle \in \frac{\mathbb{Z}_4}{\langle 2\rangle}[x]$ tal que $g(x) + \langle 2\rangle = (f(x) + \langle 2\rangle)(u(x) + \langle 2\rangle)$, entonces $g(x) - f(x)u(x) \in \langle 2\rangle$, es decir, $g(x) - f(x)u(x) = 2v(x)$ para algún $v(x) \in \mathbb{Z}_4[x]$, despejando $g(x)$, vemos que $g(x) = f(x)u(x) - 2v(x)$, elevando al cuadrado ambos lados tenemos $g^2(x) = f^2(x)u^2(x) + 4f(x)u(x)v(x) + 4v^2(x) = f^2(x)u^2(x)$ en $\mathbb{Z}_4[x]$, de esto se sigue el hecho de que $\langle f(x)\rangle$ es un ideal primario, pues $g^2(x) \in \langle f(x)\rangle$. Por tanto, $f(x)$ es un polinomio primario.

□

Un *anillo local* es un anillo que tiene un único ideal maximal. Si $\mathcal{R}$ es un anillo local, el anillo polinomial puede no ser un dominio de factorización única. Un ejemplo de tales polinomios son los

polinomios regulares. Un *polinomio regular* es un polinomio que no es divisor de cero en $\mathcal{R}[x]$. En nuestro caso el anillo local es $\mathbb{Z}_4$ y cualquier polinomio que tenga algún coeficiente distinto de cero y de 2 es regular. En particular, $x^n - 1$ es regular. Por el lema de Hensel (cf [Ram17][Wan03]) $x^n - 1$ es producto de polinomios básicos irreducibles y tales polinomios son primarios por el Lema 3.1. Por lo tanto por el teorema de factorización (cf [Ram17][Wan03], para un resultado más general cf [McD74]), tenemos lo siguiente.

Lema 3.2. *Si* $x^n - 1 = f_1 f_2 \dots f_r$ *donde los* f_i *son polinomios básicos irreducibles y coprimos por pares, entonces esta factorización es única.*

Demostración. Supongamos que $x^n - 1 = f_1 f_2 \dots f_r$ con los f_i básicos irreducibles y coprimos por pares y además $x^n - 1 = g_1 g_2 \dots g_r$ donde los g_i son básicos irreducibles y coprimos por pares, entonces por el teorema de factorización tenemos que $\langle f_i \rangle = \langle g_i \rangle$, luego f_i divide a g_i y tambien g_i divide a f_i, de ahí que $g_i = a f_i$ con a una unidad en $\mathbb{Z}_4[x]$ pero las únicas unidades en $\mathbb{Z}_4[x]$ son 1 y 3, así que $a = 1$ ó $a = 3$. Por tanto la factorización es única salvo asociados. □

El siguiente lema muestra la estructura del anillo $\frac{\mathbb{Z}_4[x]}{\langle f(x) \rangle}$ para un polinomio básico irreducible $f(x)$.

Lema 3.3. *Si* $f(x)$ *está en* $\mathbb{Z}_4[x]$ *y es un polinomio básico irreducible, entonces los únicos ideales de* $\frac{\mathbb{Z}_4[x]}{\langle f(x) \rangle}$ *son* $\langle 0 + I \rangle$, $\langle 1 + I \rangle$ *y* $\langle 2 + I \rangle$, *donde* I *es el ideal generado por* $f(x)$, *es decir,* $I = \langle f(x) \rangle$.

Demostración. Supongamos que J es un ideal del anillo $\frac{\mathbb{Z}_4[x]}{\langle f(x) \rangle}$, distinto de $\langle 0 + I \rangle$ y $g(x) + \langle f(x) \rangle$ está en J, para algún $g(x)$ que no está en $I = \langle f(x) \rangle$. Como $f(x)$ es un polinomio básico irreducible, entonces por la Definición 3.1, $\bar{f}(x)$ es irreducible en $\mathbb{F}_2[x]$, así que tenemos los siguientes casos, i) $\bar{g}(x)$ y $\bar{f}(x)$ son coprimos ó ii) $\bar{g}(x)$ es divisible por $\bar{f}(x)$. Analicemos cada uno de ellos:

i) Si $\bar{f}(x)$ y $\bar{g}(x)$ son coprimos en $\mathbb{F}_2[x]$, por el Lema 1.1 tenemos que $f(x)$ y $g(x)$ también lo son pero en $\mathbb{Z}_4[x]$, por lo que existen $t(x)$ y $s(x)$ en $\mathbb{Z}_4[x]$ tales que $t(x)g(x) + s(x)f(x) = 1$ luego, $t(x)g(x) - 1 = -s(x)f(x)$ y como $-s(x)f(x)$ está en $\langle f(x) \rangle$ entonces $t(x)g(x) - 1 \in \langle f(x) \rangle$, esto significa que $t(x)g(x) + \langle f(x) \rangle = 1 + \langle f(x) \rangle$, y así $[t(x) + \langle f(x) \rangle][g(x) + \langle f(x) \rangle] = 1 + \langle f(x) \rangle$, de esto último se sigue que $g(x) + \langle f(x) \rangle$ es invertible en $\frac{\mathbb{Z}_4[x]}{\langle f(x) \rangle}$ y como a $g(x) + \langle f(x) \rangle$ lo tomamos en J entonces $1 + \langle f(x) \rangle$ está en J , así $J = \langle 1 + I \rangle$

ii) Si $\bar{f}(x)$ divide a $\bar{g}(x)$ entonces $\bar{g}(x) = \bar{f}(x)q'(x)$ para algún $q'(x)$ en $\mathbb{F}_2[x]$ y ya que $\bar{\mu}$ es sobreyectiva, entonces existe $q(x)$ en $\mathbb{Z}_4[x]$ tal que $\bar{\mu}(q(x)) = \bar{q}(x) = q'(x)$. Así $\bar{g}(x) = \bar{f}(x)\bar{q}(x)$

$$
\begin{aligned}
&\Rightarrow \quad \bar{g}(x) - \bar{f}(x)\bar{q}(x) = 0' \\
&\Rightarrow \quad \overline{g(x) - f(x)q(x)} = 0' \\
&\Rightarrow \quad g(x) - f(x)q(x) \in \mathrm{Ker}(\bar{\mu}) = \langle 2 \rangle \\
&\Rightarrow \quad g(x) - f(x)q(x) = 2\nu(x) \ \text{ para algún } \nu(x) \text{ en } \mathbb{Z}_4[x] \\
&\Rightarrow \quad g(x) - 2\nu(x) = f(x)q(x) \text{ donde } f(x)q(x) \text{ está en } \langle f(x) \rangle \\
&\Rightarrow \quad g(x) - 2\nu(x) \in \langle f(x) \rangle \\
&\Rightarrow \quad g(x) + \langle f(x) \rangle = 2\nu(x) + \langle f(x) \rangle \\
&\Rightarrow \quad g(x) + \langle f(x) \rangle = [2 + \langle f(x) \rangle][\nu(x) + \langle f(x) \rangle], \text{ este último se encuentra en } \langle 2 + I \rangle \\
&\Rightarrow \quad g(x) + \langle f(x) \rangle \in \langle 2 + I \rangle
\end{aligned}
$$

Por lo que el ideal J está contenido en el ideal $\langle 2 + I \rangle$, debido a esto tenemos que existe un elemento de la forma $2r(x) + \langle f(x) \rangle$ distinto de la clase del cero en J (ya que J no es el ideal $\langle 0 + I \rangle$) para algún $r(x)$ en $\mathbb{Z}_4[x]$. Podemos suponer que $\bar{r}(x)$ no está en $\langle \bar{f}(x) \rangle$, de lo contrario, si $\bar{r}(x)$ estuviera en $\langle \bar{f}(x) \rangle$ existiría un polinomio $u'(x)$ en $\mathbb{Z}_4[x]$ tal que $\bar{r}(x) = u'(x)\bar{f}(x)$ y como $\bar{\mu}$ es sobreyectiva, entonces $u'(x) = \bar{u}(x)$ para algún $u(x)$ en $\mathbb{Z}_4[x]$, luego, restando $\bar{f}(x)u'(x)$ y sustituyendo $u'(x)$ tendríamos que $0' = \bar{r}(x) - \bar{f}(x)\bar{u}(x) = \overline{r(x) - f(x)u(x)}$ lo que nos dice

que $r(x) - f(x)u(x) = 2v(x)$ para algún $v(x)$ en $\mathbb{Z}_4[x]$ y despejando $r(x)$ se sigue que $r(x) = f(x)u(x) + 2v(x)$, al multiplicar por 2 tenemos $2r(x) = 2f(x)u(x) + 4v(x)$ y como estamos en $\mathbb{Z}_4[x]$ entonces $2r(x) = 2f(x)u(x)$, esto implica que $2r(x)$ está en $\langle f(x)\rangle$ y así, tendríamos que $2r(x) + \langle f(x)\rangle = 0 + \langle f(x)\rangle$, lo cual no es posible pues $2r(x) + \langle f(x)\rangle$ lo tomamos distinto de la clase del 0. Como $\bar{r}(x)$ no está en $\langle \bar{f}(x)\rangle$ y $\bar{f}(x)$ es irreducible en $\mathbb{F}_2[x]$ entonces $\bar{r}(x)$ y $\bar{f}(x)$ son coprimos, por lo que existen $s'(x)$ y $t'(x)$ en $\mathbb{F}_2[x]$ tales que $s'(x)\bar{r}(x) + t'(x)\bar{f}(x) = 1'$ pero como $\bar{\mu}$ es sobreyectivo tenemos que existen $s(x)$ y $t(x)$ en $\mathbb{Z}_4[x]$ tales que $s'(x) = \bar{s}(x)$ y $t'(x) = \bar{t}(x)$ y además $1' = \bar{1}$, sustituyendo $s'(x), t'(x)$ y $1'$,

$$
\begin{aligned}
&\Rightarrow \quad \bar{s}(x)\bar{r}(x) + \bar{t}(x)\bar{f}(x) = \bar{1} \\
&\Rightarrow \quad \overline{s(x)r(x) + t(x)f(x) - 1} = 0' \\
&\Rightarrow \quad s(x)r(x) + t(x)f(x) - 1 \in \ker(\bar{\mu}) = \langle 2\rangle \\
&\Rightarrow \quad s(x)r(x) + t(x)f(x) - 1 = 2w(x) \text{ para algún } w(x) \text{ en } \mathbb{Z}_4[x] \\
&\Rightarrow \quad 2s(x)r(x) + 2t(x)f(x) - 2 = 4w(x) \text{ pero } 4 = 0 \text{ en } \mathbb{Z}_4 \\
&\Rightarrow \quad 2s(x)r(x) + 2t(x)f(x) - 2 = 0 \\
&\Rightarrow \quad 2s(x)r(x) - 2 = -2t(x)f(x) \text{ este último se encuentra en } \langle f(x)\rangle \\
&\Rightarrow \quad 2s(x)r(x) - 2 \in \langle f(x)\rangle \\
&\Rightarrow \quad 2s(x)r(x) + \langle f(x)\rangle = 2 + \langle f(x)\rangle
\end{aligned}
$$

Y dado que $2r(x) + \langle f(x)\rangle$ es un elemento del ideal J, entonces $2 + \langle f(x)\rangle$ también está en J y así, $\langle 2 + I\rangle$ está contenido en J.

Por tanto $J = \langle 2 + I\rangle$.

□

Sea $\mathcal{R}_n = \frac{\mathbb{Z}_4[x]}{\langle x^n - 1\rangle}$.

De manera similar a cuando hablamos de códigos cíclicos sobre campos finitos en el Capítulo 2, tenemos que $\mathcal{C}$ es un $\mathbb{Z}_4$-código cíclico de longitud n, si y sólo si, es un ideal del anillo $\mathcal{R}_n$. Para esto primero definimos la función

$$
\begin{aligned}
\phi : \mathbb{Z}_4^n &\to \mathcal{R}_n \\
\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) &\mapsto c(x) + I = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + I
\end{aligned}
\tag{6}
$$

donde $I = \langle x^n - 1\rangle$ el cual es un isomorfismo de $\mathbb{Z}_4-$módulos y cuya prueba resulta ser igual a la que se realizó cuando definimos la función ψ, de esta misma forma tenemos que la prueba de la caracterización de códigos cíclicos sobre $\mathbb{Z}_4$ es similar a la que se da en el Teorema 2.5 puesto que una vez más, al estudiar dicha demostración podemos darnos cuenta que ésta no depende del hecho de que trabajamos sobre un campo finito.

El siguiente teorema nos muestra como son los ideales del anillo $\mathcal{R}_n$ partiendo de una factorización del polinomio $x^n - 1$, pero antes de enunciarlo probaré el siguiente resultado, el cual me será de mucha utilidad en la demostración del teorema.

Proposición 3.1. *Sean $f_1, f_2, \ldots, f_r$ polinomios coprimos por pares en $\mathbb{Z}_4[x]$, se cumple que*

i) Para todo $i, j \in \{1, 2, \ldots, r\}$ con $i \neq j$, $\langle f_i\rangle + \langle f_j\rangle = \langle 1\rangle$,

ii) $\langle f_1 f_2 \cdots f_r\rangle = \langle f_1\rangle \cap \langle f_2\rangle \cap \cdots \cap \langle f_r\rangle$.

Demostración. i) Como para cada $i, j \in \{1, 2, \ldots, r\}$ se tiene que f_i, f_j son coprimos siempre que $i \neq j$, entonces existen α, β en $\mathbb{Z}_4[x]$ tales que $\alpha f_i + \beta f_j = 1$. Sea h en $\mathbb{Z}_4[x] = \langle 1\rangle$, tenemos

$$
\begin{aligned}
h &= h(\alpha f_i + \beta f_j) \\
&= h(\alpha f_i) + h(\beta f_j) \\
&= (h\alpha) f_i + (h\beta) f_j
\end{aligned}
$$

y ya que $(h\alpha)f_i \in \langle f_i\rangle$ y $(h\beta)f_j \in \langle f_j\rangle$ se sigue que h es elemento de $\langle f_i\rangle + \langle f_j\rangle$, por lo que $\langle 1\rangle \subseteq \langle f_i\rangle + \langle f_j\rangle$. Por otro lado, como $\langle f_i\rangle$ y $\langle f_j\rangle$ son ideales de $\mathbb{Z}_4[x]$ entonces $\langle f_i\rangle + \langle f_j\rangle \subseteq \langle 1\rangle = \mathbb{Z}_4[x]$.

ii) Podemos ver que $f_1 f_2 \cdots f_r$ es un elemento de cada ideal generado por f_i por lo que $f_1 f_2 \cdots f_r$ está en $\langle f_1\rangle \cap \langle f_2\rangle \cap \cdots \cap \langle f_r\rangle$ y así $\langle f_1 f_2 \cdots f_r\rangle \subseteq \langle f_1\rangle \cap \langle f_2\rangle \cap \cdots \cap \langle f_r\rangle$. Para probar la otra contención haremos inducción sobre r, que es el número de polinomios involucrados. Para $r = 2$, sea g en $\langle f_1\rangle \cap \langle f_2\rangle$ entonces f_1 y f_2 dividen a g y como f_1 y f_2 son coprimos tenemos que el producto de ambos divide a g, por lo que g se encuentra en $\langle f_1 f_2\rangle$. Supongamos que el resultado se cumple para r, es decir, $\langle f_1\rangle \cap \langle f_2\rangle \cap \cdots \cap \langle f_r\rangle \subseteq \langle f_1 f_2 \cdots f_r\rangle$, veamos que el resultado también se sigue para $r+1$ Sea g en $\langle f_1\rangle \cap \langle f_2\rangle \cap \cdots \cap \langle f_r\rangle \cap \langle f_{r+1}\rangle = (\langle f_1\rangle \cap \langle f_2\rangle \cap \cdots \cap \langle f_r\rangle) \cap \langle f_{r+1}\rangle$ por lo que, g está en $\langle f_1\rangle \cap \langle f_2\rangle \cap \cdots \cap \langle f_r\rangle$ y también es elemento de $\langle f_{r+1}\rangle$, por nuestra hipótesis inductiva tenemos que g se encuentra en $\langle f_1 f_2 \cdots f_r\rangle$, y como todos los f_i son coprimos por pares, se sigue que $\prod_{i=1}^{r} f_i$ es coprimo con f_{r+1}, y ya que $f_1 f_2 \cdots f_r$ y f_{r+1} dividen a g, entonces existen $s, q \in \mathbb{Z}_4[x]$ tales que $g = s f_1 f_2 \cdots f_r$ y $g = q f_{r+1}$, luego $f_{r+1} | s f_1 f_2 \cdots f_r$ por lo que $s = k f_{r+1}$ para algún $k \in \mathbb{Z}_4[x]$, así $f_1 f_2 \cdots f_r f_{r+1}$ divide a g, por lo que $\langle f_1\rangle \cap \langle f_2\rangle \cap \cdots \cap \langle f_r\rangle \subseteq \langle f_1 f_2 \cdots f_r\rangle\langle f_{r+1}\rangle \subseteq \langle f_1 f_2 \cdots f_r f_{r+1}\rangle$. Por lo tanto, se cumple que $\langle f_1 f_2 \cdots f_r\rangle = \langle f_1\rangle \cap \langle f_2\rangle \cap \cdots \cap \langle f_r\rangle$

□

Teorema 3.1. *Sea $x^n - 1 = f_1 f_2 \cdots f_r$ un producto de polinomios básicos irreducibles y coprimos por pares en $\mathbb{Z}_4[x]$ para n impar, y sea $\hat{f}_i$ el producto de todos los f_j excepto f_i. Entonces cualquier ideal del anillo $\mathcal{R}_n$ es suma de algunos $\langle \hat{f}_i + \langle x^n - 1\rangle\rangle$ y $\langle 2\hat{f}_j + \langle x^n - 1\rangle\rangle$*

Demostración. Por el Lema de Hensel tal factorización de $x^n - 1$ existe y además es única por el Lema 3.2. Como los f_i son coprimos por pares tenemos que $\langle f_1 f_2 \cdots f_r\rangle = \langle f_1\rangle \cap \langle f_2\rangle \cap \cdots \cap \langle f_r\rangle$ y para cada $i \neq j, \langle f_i\rangle + \langle f_j\rangle = \langle 1\rangle$ Además ya que $\mathbb{Z}_4[x]$ tiene unidad se cumple que $(\mathbb{Z}_4[x])^2 = \mathbb{Z}_4[x]$ y así $(\mathbb{Z}_4[x])^2 + \langle f_i\rangle = \mathbb{Z}_4[x]$ para cada $i \in 1, 2, \ldots, r$, luego por el Teorema 1.1 y el Corolario 1.1 se sigue que

$$\mathcal{R}_n = \frac{\mathbb{Z}_4[x]}{\langle x^n - 1\rangle} = \frac{\mathbb{Z}_4[x]}{\langle f_1 f_2 \cdots f_r\rangle} = \frac{\mathbb{Z}_4[x]}{\langle f_1\rangle \cap \langle f_2\rangle \cap \cdots \cap \langle f_r\rangle} \simeq \frac{\mathbb{Z}_4[x]}{\langle f_1\rangle} \oplus \frac{\mathbb{Z}_4[x]}{\langle f_2\rangle} \oplus \cdots \oplus \frac{\mathbb{Z}_4[x]}{\langle f_r\rangle}$$

es decir,

$$\mathcal{R}_n \simeq \frac{\mathbb{Z}_4[x]}{\langle f_1\rangle} \oplus \frac{\mathbb{Z}_4[x]}{\langle f_2\rangle} \oplus \cdots \oplus \frac{\mathbb{Z}_4[x]}{\langle f_r\rangle}.$$

Si I es un ideal de $\mathcal{R}_n$, por el Teorema 1.2 entonces,

$$I \simeq I_1 \oplus I_2 \oplus \cdots \oplus I_r$$

donde, para cada $i \in \{1, 2, \ldots, r\}$, I_i es un ideal de $\frac{\mathbb{Z}_4[x]}{\langle f_i\rangle}$. Como cada f_i es un básico irreducible en $\mathbb{Z}_4[x]$, entonces por el Lema 3.3 los únicos ideales de $\frac{\mathbb{Z}_4[x]}{\langle f_i\rangle}$ son $\langle 0 + \langle f_i\rangle\rangle$, $\langle 1 + \langle f_i\rangle\rangle$ y $\langle 2 + \langle f_i\rangle\rangle$.

A continuación se definen tres funciones que establecen un isomorfismo entre los ideales I_i y los ideales de $\mathcal{R}_n$, donde cada función es un isomorfismo de anillos.

Para ello, primero consideremos lo siguiente, como $\hat{f}_i$ y f_i son coprimos entonces existen $a_i, b_i \in \mathbb{Z}_4[x]$ tales que $a_i\hat{f}_i + b_i f_i = 1$, consideremos $e_i = a_i\hat{f}_i$, entonces $e_i = 1 - b_i f_i$ luego $e_i^2 = e_i - b_i f_i e_i = e_i - b_i f_i \hat{f}_i a_i = e_i - b_i a_i(x^n - 1)$, luego $e_i^2 - e_i \in \langle x^n - 1\rangle$), así $e_i^2 \equiv e_i \pmod{x^n - 1}$ y además $e_i\hat{f}_i = \hat{f}_i - b_i f_i \hat{f}_i = \hat{f}_i - b_i(x^n - 1)$ de ahí que $e_i\hat{f}_i - \hat{f}_i \in \langle x^n - 1\rangle$, entonces $e_i\hat{f}_i + \langle x^n - 1\rangle = \hat{f}_i + \langle x^n - 1\rangle$ por lo que $\langle \hat{f}_i + \langle x^n - 1\rangle\rangle \subseteq \langle e_i + \langle x^n - 1\rangle\rangle$ y como $e_i = a_i\hat{f}_i$, entonces $\langle e_i + \langle x^n - 1\rangle\rangle \subseteq \langle \hat{f}_i + \langle x^n - 1\rangle\rangle$, así $\langle e_i + \langle x^n - 1\rangle\rangle = \langle \hat{f}_i + \langle x^n - 1\rangle\rangle$, luego se tiene que:

i) Si $I_j = \langle 1 + \langle f_j\rangle\rangle = \frac{\mathbb{Z}_4[x]}{\langle f_j\rangle}$, definimos

$$\begin{aligned} \varphi_1 : I_j &\to \langle e_j + \langle x^n - 1\rangle\rangle \\ h + \langle f_j\rangle &\mapsto h e_j + \langle x^n - 1\rangle \end{aligned}$$

Sean $h+\langle f_j\rangle$, $g+\langle f_j\rangle$ en I_j, tenemos las siguientes equivalencias

$$\begin{aligned} h+\langle f_j\rangle = g+\langle f_j\rangle &\Leftrightarrow h-g\in\langle f_j\rangle \\ &\Leftrightarrow h-g = f_j k \text{ para algún } k\in\mathbb{Z}_4[x] \\ &\Leftrightarrow (h-g)e_j = e_j f_j k \\ &\Leftrightarrow (h-g)e_j = a_j\hat{f}_j f_j k \\ &\Leftrightarrow he_j - ge_j = a_j(x^n-1)k \text{ para algún } k\in\mathbb{Z}_4[x] \\ &\Leftrightarrow he_j - ge_j \in\langle x^n-1\rangle \\ &\Leftrightarrow he_j+\langle x^n-1\rangle = ge_j+\langle x^n-1\rangle \\ &\Leftrightarrow \varphi_1(h+\langle f_j\rangle) = \varphi_1(g+\langle f_j\rangle) \end{aligned}$$

De esto se tiene que φ_1 está bien definida y es inyectiva.

Por otro lado,

$$\begin{aligned} \varphi_1((h+\langle f_j\rangle)+(g+\langle f_j\rangle)) &= \varphi_1((h+g)+\langle f_j\rangle) \\ &= (h+g)\hat{f}_j+\langle x^n-1\rangle \\ &= (h\hat{f}_j+\langle x^n-1\rangle)+(g\hat{f}_j+\langle x^n-1\rangle) \\ &= \varphi_1(h+\langle f_j\rangle)+\varphi_1(g+\langle f_j\rangle), \end{aligned}$$

y

$$\begin{aligned} \varphi_1((h+\langle f_j\rangle)(g+\langle f_j\rangle)) &= \varphi_1((hg)+\langle f_j\rangle) \\ &= (hg)e_j+\langle x^n-1\rangle \\ &= (hg)e_j^2+\langle x^n-1\rangle \\ &= (he_j+\langle x^n-1\rangle)(ge_j+\langle x^n-1\rangle) \\ &= \varphi_1(h+\langle f_j\rangle)\varphi_1(g+\langle f_j\rangle). \end{aligned}$$

Por lo que φ_1 es un homomorfismo de anillos, ahora sea $g+\langle x^n-1\rangle$ un elemento de $\langle e_j+\langle x^n-1\rangle\rangle$ entonces $g+\langle x^n-1\rangle = e_j k+\langle x^n-1\rangle$ para algún $k+\langle x^n-1\rangle$ en $\mathcal{R}_n$ donde k es un polinomio con coeficientes en $\mathbb{Z}_4$, luego, $k+\langle f_j\rangle$ es un elemento de I_j tal que

$$\varphi_1(k+\langle f_j\rangle) = e_j k+\langle x^n-1\rangle = g+\langle x^n-1\rangle$$

de ahí que φ_1 es sobreyectiva.

Por tanto cuando $I_j=\langle 1+\langle f_j\rangle\rangle$ es isomorfo a $\langle\hat{f}_j+\langle x^n-1\rangle\rangle$ el cual es un ideal de $\mathcal{R}_n$.

ii) Cuando $I_j=\langle 2+\langle f_j\rangle\rangle$, tenemos que cualquier elemento de I_j es de la forma $2k+\langle f_j\rangle$ donde $k+\langle f_j\rangle$ es un elemento de $\frac{\mathbb{Z}_4[x]}{\langle f_j\rangle}$, por lo que definimos, de manera muy similar a como lo hicimos en i), la siguiente función

$$\begin{aligned} \varphi_2 : I_j &\to \langle 2e_j+\langle x^n-1\rangle\rangle \\ 2h+\langle f_j\rangle &\mapsto 2he_j+\langle x^n-1\rangle \end{aligned}$$

la cual está bien definida y es inyectiva puesto que, si $2h+\langle f_j\rangle$, $2g+\langle f_j\rangle$ en I_j se tiene lo siguiente

$$\begin{aligned} 2h+\langle f_j\rangle = 2g+\langle f_j\rangle &\Leftrightarrow 2(h-g) = f_j k \text{ para algún } k\in\mathbb{Z}_4[x] \\ &\Leftrightarrow 2(h-g)e_j = e_j f_j k \\ &\Leftrightarrow 2(h-g)e_j = a_j\hat{f}_j f_j k \\ &\Leftrightarrow 2he_j - 2ge_j = a_j(x^n-1)k \text{ para algún } k\in\mathbb{Z}_4[x] \\ &\Leftrightarrow 2he_j+\langle x^n-1\rangle = 2ge_j+\langle x^n-1\rangle \\ &\Leftrightarrow \varphi_2(2h+\langle f_j\rangle) = \varphi_2(2g+\langle f_j\rangle) \end{aligned}$$

Además se tiene que φ_2 es un homomorfismo de anillos y la prueba de esto es como en el inciso i), para ver la sobreyectividad tomamos un elemento $g+\langle x^n-1\rangle$ en $\langle 2\hat{f}_j+\langle x^n-1\rangle\rangle$, por lo que existe $k+\langle x^n-1\rangle \in \mathcal{R}_n$ tal que $g+\langle x^n-1\rangle = 2e_jk+\langle x^n-1\rangle$ luego, como k es un elemento de $\mathbb{Z}_4[x]$ entonces $2k+\langle f_j\rangle$ está en I_j y se sigue que

$$\varphi_2(2k+\langle f_j\rangle) = g+\langle x^n-1\rangle$$

Por lo que, siempre que $I_j = \langle 2+\langle f_j\rangle\rangle$, I_j es isomorfo al ideal de $\mathcal{R}_n$, $\langle 2\hat{f}_j+\langle x^n-1\rangle\rangle$

iii) Por último consideramos el caso cuando $I_j = \langle 0+\langle f_j\rangle\rangle = \langle f_j\rangle$, notemos que para todo elemento $h+\langle f_j\rangle$ en $\langle 0+\langle f_j\rangle\rangle$ se cumple que $h = kf_j$ para algún $k \in \mathbb{Z}_[x]$ por lo que $he_j = ha_j\hat{f}_j = ka_jf_j\hat{f}_j \in \langle x^n-1\rangle$. Definimos la función

$$\begin{aligned} \varphi_3 : I_j &\to \langle 0+\langle x^n-1\rangle\rangle \\ hf_j+\langle f_j\rangle &\mapsto hf_je_j+\langle x^n-1\rangle \end{aligned}$$

Podemos ver que φ_3 está bien definida y es inyectiva, pues dados $hf_j+\langle f_j\rangle, gf_j+\langle f_j\rangle \in I_j$ se tiene que

$$\begin{aligned} hf_j+\langle f_j\rangle = gf_j+\langle f_j\rangle &\Leftrightarrow hf_j-gf_j = kf_j \text{ para algún } k\in\mathbb{Z}_4[x] \\ &\Leftrightarrow hf_je_j-gf_je_j = kf_je_j \\ &\Leftrightarrow hf_je_j-gf_je_j = kf_j\hat{f}_ja_j \\ &\Leftrightarrow hf_je_j-gf_je_j = ka_j(x^n-1) \text{ para algún } k\in\mathbb{Z}_4[x] \\ &\Leftrightarrow hf_je_j+\langle x^n-1\rangle = gf_je_j+\langle x^n-1\rangle \\ &\Leftrightarrow \varphi_3(hf_j+\langle f_j\rangle) = \varphi_3(gf_j+\langle f_j\rangle) \end{aligned}$$

además es homomorfismo de anillos y sobreyectiva ya que $0+\langle x^n-1\rangle = a_jf_j\hat{f}_j+\langle x^n-1\rangle$ y $\varphi_3(f_j+\langle f_j\rangle) = a_j\hat{f}_jf_j+\langle x^n-1\rangle$.

Así, si $I_j = \langle 0+\langle f_j\rangle\rangle = \langle f_j\rangle$ entonces I_j es isomorfo a $\langle 0+\langle x^n-1\rangle\rangle$

Por lo tanto, como a cada ideal I_j se le puede identificar con un ideal de $\mathcal{R}_n$, entonces cada ideal I de $\mathcal{R}_n$ es la suma de ideales de la forma $\langle \hat{f}_i+\langle x^n-1\rangle\rangle$ y $\langle 2\hat{f}_j+\langle x^n-1\rangle\rangle$.

□

Corolario 3.1. *El número de códigos cíclicos sobre $\mathbb{Z}_4$ de longitud n es, 3^r, donde r es el número de factores polinomiales básicos irreducibles de x^n-1*

Demostración. Tenemos que $\mathcal{C}$ es un código cíclico de $\mathcal{R}_n$, si $\mathcal{C}$ es un ideal de $\mathcal{R}_n$ y por el teorema previo tenemos que

$$\mathcal{C} \simeq I_1 \oplus I_2 \oplus \cdots \oplus I_r$$

donde cada I_j es un ideal del anillo $\frac{\mathbb{Z}_4[x]}{\langle f_j\rangle}$, y como cada ideal I_j puede ser $\langle 0+\langle f_j\rangle\rangle$, $\langle 1+\langle f_j\rangle\rangle$ ó $\langle 2+\langle f_j\rangle\rangle$ entonces por el principio multiplicativo, existen 3^r ideales distintos en $\mathcal{R}_n$.

□

A partir de ahora denotaremos a el ideal $\langle x^n-1\rangle$ por I, es decir, $I = \langle x^n-1\rangle$.

Teorema 3.2. *Supongamos que $\mathcal{C}$ es un $\mathbb{Z}_4$—código cíclio de longitud n, donde n no es par. Entonces existen F_0, F_1 y F_2 polinomios únicos, mónicos y coprimos por parejas (posiblemente alguno igual a 1) tales que $F_0F_1F_2 = x^n-1$ y $\mathcal{C}$ es generado por $\{\hat{F}_1+I, 2\hat{F}_2+I\}$, es decir, $\mathcal{C} = \langle \hat{F}_1+I, 2\hat{F}_2+I\rangle$.*

Demostración. Sabemos que x^n-1 tiene una única factorización en $\mathbb{Z}_4[x]$, digamos, $x^n-1 = f_1f_2\cdots f_r$ donde los f_i son polinomios básicos irreducibles y coprimos por pares, además como x^n-1 es mónico los f_i también pueden escogerse mónicos.

Para cada $i,j \in \{1,2,\ldots,r\}$ definimos $\hat{f}_i = \prod_{j\neq i} f_j$.

Es importante mencionar que a partir de este momento estaremos trabajando sobre el anillo $\mathcal{R}_n$ a menos que se indique lo contrario, por lo que, para fines prácticos, en la demostración, a las clases residuales de $\mathcal{R}_n$ las denotaremos únicamente por el representante, es decir, $g+\langle x^n+1\rangle = g$.

Como $\mathcal{C}$ es ideal de $\mathcal{R}_n$ entonces por el Teorema 3.1, $\mathcal{C}$ es suma de ideales del tipo $\langle 2^j \hat{f}_i \rangle$ donde $j = 0, 1, 2$.

Reordenando, si fuese necesario, podemos suponer que $\mathcal{C}$ es la suma de

$$\langle \hat{f}_{k_1+1} \rangle, \langle \hat{f}_{k_1+2} \rangle, \ldots, \langle \hat{f}_{k_1+k_2} \rangle, \langle 2\hat{f}_{k_1+k_2+1} \rangle, \ldots, \langle 2\hat{f}_{k_1+k_2+k_3} \rangle$$

donde $k_1 + k_2 + k_3 = r$

Sea $k_0 = 0$, para $i \in 0, 1, 2$, definimos en $\mathbb{Z}_4[x]$

$$F_i = \begin{cases} 1 & \text{si } k_{i+1} = 0 \\ f_{k_0+\cdots+k_i+1} f_{k_0+\cdots+k_i+2} \cdots f_{k_0+\cdots+k_{i+1}} & \text{si } k_{i+1} \neq 0 \end{cases}$$

y $\hat{F}_i = \prod_{j \neq i} F_j$ con $j \in \{0, 1, 2\}$.

Así,

$$\begin{aligned} F_0 &= \begin{cases} 1 & \text{si } k_1 = 0 \\ f_1 f_2 \cdots f_{k_1} & \text{si } k_1 \neq 0 \end{cases} \\ F_1 &= \begin{cases} 1 & \text{si } k_2 = 0 \\ f_{k_1+1} f_{k_1+2} \cdots f_{k_1+k_2} & \text{si } k_2 \neq 0 \end{cases} \\ F_2 &= \begin{cases} 1 & \text{si } k_3 = 0 \\ f_{k_1+k_2+1} f_{k_1+k_2+2} \cdots f_{k_1+k_2+k_3} & \text{si } k_3 \neq 0 \end{cases} \end{aligned}$$

Sean

$$\mathcal{C} = \langle \hat{f}_{k_1+1} \rangle + \langle \hat{f}_{k_1+2} \rangle + \cdots + \langle \hat{f}_{k_1+k_2} \rangle + \langle 2\hat{f}_{k_1+k_2+1} \rangle + \cdots + \langle 2\hat{f}_r \rangle \quad \text{y} \quad \mathcal{C}_1 = \langle \hat{F}_1, 2\hat{F}_2 \rangle$$

Veamos que $\mathcal{C} = \mathcal{C}_1$

$\subseteq$] Probemos

i) Para cada l_1, con $1 \leqslant l_1 \leqslant k_2$: $\langle \hat{f}_{k_1+l_1} \rangle \subseteq \langle \hat{F}_1 \rangle$,

ii) Para cada l_2, con $1 \leqslant l_2 \leqslant k_3$: $\langle 2\hat{f}_{k_1+k_2+l_2} \rangle \subseteq \langle 2\hat{F}_2 \rangle$.

Para el caso i), sean $l_1 \in \{1, 2, \ldots, k_2\}$ y $u \in \langle \hat{f}_{k_1+l_1} \rangle$, entonces existe $h \in \mathcal{R}_n$ tal que $u = h\hat{f}_{k_1+l_1} = hf_1 f_2 \cdots f_{k_1+l_1-1} f_{k_1+l_1+1} \cdots f_r$

$$\begin{aligned} &\Rightarrow \quad u = h(f_1 f_2 \cdots f_{k_1})(f_{k_1+1} \cdots f_{k_1+l_1-1} f_{k_1+l_1+1} \cdots f_{k_1+k_2})(f_{k_1+k_2+1} \cdots f_r) \\ &\Rightarrow \quad u = (F_0 F_2)(h(f_{k_1+1} \cdots f_{k_1+l_1-1} f_{k_1+l_1+1} \cdots f_{k_1+k_2})) \\ &\Rightarrow \quad u \in \langle \hat{F}_1 \rangle \end{aligned}$$

de ahí que i) se cumple y como $\langle \hat{F}_1 \rangle$ es un ideal de $\mathcal{R}_n$ se sigue que

$$\langle \hat{f}_{k_1+1} \rangle + \langle \hat{f}_{k_1+2} \rangle + \cdots + \langle \hat{f}_{k_1+k_2} \rangle \subseteq \langle \hat{F}_1 \rangle.$$

Para ii), de manera similar al caso previo tomamos $l_2 \in \{1, 2, \ldots, k_3\}$ y $v \in \langle 2\hat{f}_{k_1+k_2+l_2} \rangle$, entonces existe $g \in \mathcal{R}_n$ tal que $v = 2g\hat{f}_{k_1+k_2+l_2} = 2gf_1 f_2 \cdots f_{k_1} f_{k_1+1} \cdots f_{k_1+k_2} \cdots f_{k_1+k_2+l_2-1} f_{k_1+k_2+l_2+1} \cdots \cdots f_r$

$$\begin{aligned} &\Rightarrow \quad v = 2g(f_1 f_2 \cdots f_{k_1})(f_{k_1+1} \cdots f_{k_1+k_2})(f_{k_1+k_2+1} \cdots f_{k_1+k_2+l_2-1} f_{k_1+k_2+l_2+1} \cdots f_r) \\ &\Rightarrow \quad v = 2(F_0 F_1)(h(f_{k_1+k_2+1} \cdots f_{k_1+k_2+l_2-1} f_{k_1+k_2+l_2+1} \cdots f_r)) \\ &\Rightarrow \quad v \in \langle 2\hat{F}_2 \rangle \end{aligned}$$

de ahí que ii) se cumple y como $\langle 2\hat{F}_2 \rangle$ es un ideal de $\mathcal{R}_n$ se sigue que

$$\langle 2\hat{f}_{k_1+k_2+1} \rangle + \cdots + \langle 2\hat{f}_r \rangle \subseteq \langle 2\hat{F}_2 \rangle.$$

Por lo tanto,

$$\mathcal{C} = \langle \hat{f}_{k_1+1} \rangle + \langle \hat{f}_{k_1+2} \rangle + \cdots + \langle \hat{f}_{k_1+k_2} \rangle + \langle 2\hat{f}_{k_1+k_2+1} \rangle + \cdots + \langle 2\hat{f}_r \rangle \subseteq \langle \hat{F}_1, 2\hat{F}_2 \rangle = \mathcal{C}_1.$$

$\supseteq$] Ahora probemos que $\mathcal{C}_1 \subseteq \mathcal{C}$, para ello probaremos lo siguiente

i) $\langle \hat{F}_1 \rangle \subseteq \sum_{l_1=1}^{k_2} \langle \hat{f}_{k_1+l_1} \rangle$,

ii) $\langle 2\hat{F}_2 \rangle \subseteq \sum_{l_2=1}^{k_3} \langle 2\hat{f}_{k_1+k_2+l_2} \rangle$.

En el caso i) notemos que

$$\begin{aligned}\sum_{l_1=1}^{k_2} \hat{f}_{k_1+l_1} &= \hat{f}_{k_1+1} + \hat{f}_{k_1+2} + \cdots + \hat{f}_{k_1+k_2} \\ &= (f_1 \cdots f_{k_1} f_{k_1+2} \cdots f_r) + (f_1 \cdots f_{k_1+1} f_{k_1+3} \cdots f_r) + \cdots + \\ &\quad + (f_1 \cdots f_{k_1+k_2-1} f_{k_1+k_2+1} \cdots f_r) \\ &= (f_1 \cdots f_{k_1})(f_{k_1+k_2+1} \cdots f_r)[(f_{k_1+2} \cdots f_{k_1+k_2}) + (f_{k_1+1} f_{k_1+3} \cdots f_{k_1+k_2}) + \cdots + \\ &\quad + (f_{k_1+1} \cdots f_{k_1+k_2-1})]\end{aligned}$$

Definimos $\check{f}_{k_1+l_1} = f_{k_1+1} f_{k_1+2} \cdots f_{k_1+l_1-1} f_{k_1+l_1+1} \cdots f_{k_1+k_2}$ para cada $l_1 \in \{1, 2, \ldots, k_2\}$, entonces, de la última igualdad se obtinen lo siguiente

$$\sum_{l_1=1}^{k_2} \hat{f}_{k_1+l_1} = (f_1 \cdots f_{k_1})(\check{f}_{k_1+1} + \check{f}_{k_1+2} + \cdots + \check{f}_{k_1+k_2})(f_{k_1+k_2+1} \cdots f_r).$$

Afirmación. $\mathrm{mcd}(\check{f}_{k_1+1}, \check{f}_{k_1+2}, \ldots, \check{f}_{k_1+k_2}) = 1$ en $\mathbb{Z}_4[x]$.

Sea $g \in \mathbb{Z}_4[x]$ tal que para cada $l_1 \in \{1, 2, \ldots, k_2\}$, g divide a $\check{f}_{k_1+l_1}$ y sea $q \in \{1, 2, \ldots, k_2\}$ entonces g divide a $\check{f}_{k_1+q}$ por lo que existe al menos un elemento, i, en $\{1, 2, \ldots, k_2\}$ distinto de q tal que f_{k_1+i} es divisible por g, esto ya que los $f_{k_1+l_1}$ son coprimos por pares, pero $g|\check{f}_{k_1+i}$ por lo que para algún $j \in \{1, 2, \ldots, k_2\}$ con $j \neq i$ se cumple que $g|f_{k_1+j}$ y como f_{k_1+i} y $f_{k_1+j})$ son coprimos entonces $g|1$, de ahí que $g = 1$, lo que queríamos probar.

De la afirmación se sigue que, para cada $l_1 \in \{1, 2, \ldots, k_2\}$ existe $u_{k_1+l_1}$ en $\mathbb{Z}_4[x]$ tal que

$$\sum_{l_1=1}^{k_2} u_{k_1+l_1} \check{f}_{k_1+l_1} = 1$$

Entonces

$$\begin{aligned}\sum_{l_1=1}^{k_2} u_{k_1+l_1} \hat{f}_{k_1+l_1} &= (f_1 \cdots f_{k_1})(\sum_{l_1=1}^{k_2} u_{k_1+l_1} \check{f}_{k_1+l_1})(f_{k_1+k_2+1} \cdots f_r) \\ &= (f_1 \cdots f_{k_1})(f_{k_1+k_2+1} \cdots f_r) \\ &= F_0 F_2\end{aligned}$$

y como para cada $l_1 \in \{1, 2, \ldots, k_2\}$ se cumple que $u_{k_1+l_1} \hat{f}_{k_1+l_1} \in \langle \hat{f}_{k_1+l_1} \rangle$ entonces $\hat{F}_1 \in \sum_{l_1=1}^{k_2} \langle \hat{f}_{k_1+l_1} \rangle$, así $\langle \hat{F}_1 \rangle \subseteq \sum_{l_1=1}^{k_2} \langle \hat{f}_{k_1+l_1} \rangle$.

Por otro lado, para ii) tenemos que

$$\begin{aligned}\sum_{l_2=1}^{k_3} 2\hat{f}_{k_1+k_2+l_2} &= 2\hat{f}_{k_1+k_2+1} + 2\hat{f}_{k_1+k_2+2} + \cdots + 2\hat{f}_{k_1+k_2+k_3} \\ &= 2(f_1 \cdots f_{k_1+k_2} f_{k_1+k_2+2} \cdots f_r) + 2(f_1 \cdots f_{k_1+k_2+1} f_{k_1+k_2+3} \cdots f_r) + \cdots + \\ &\quad + 2(f_1 \cdots f_{k_1+k_2+k_3-1}) \\ &= 2(f_1 \cdots f_{k_1})(f_{k_1+1} \cdots f_{k_1+k_2})[(f_{k_1+k_2+2} \cdots f_r) + (f_{k_1+k_2+1} f_{k_1+k_2+3} \cdots f_r) + \\ &\quad + \cdots + (f_{k_1+k_2+1} \cdots f_{r-1})]\end{aligned}$$

Para cada $l_2 \in \{1,2,\ldots,k_3\}$ definimos $\check{f}_{k_1+k_2+l_2} = f_{k_1+k_2+1} f_{k_1+k_2+2} \cdots f_{k_1+k_2+l_2-1} f_{k_1+k_2+l_2+1} \cdots f_{k_1+k_2+k_3}$ así,

$$\sum_{l_2=1}^{k_3} 2\hat{f}_{k_1+k_2+l_2} = 2(f_1 \cdots f_{k_1})(f_{k_1+1} \cdots f_{k_1+k_2})(\check{f}_{k_1+k_2+1} + \check{f}_{k_1+k_2+2} + \cdots + \check{f}_{k_1+k_2+k_3})$$

De manera análoga a como se afirmó en i), tenemos que $mcd(\check{f}_{k_1+k_2+1}, \check{f}_{k_1+k_2+2}, \ldots, \check{f}_{k_1+k_2+k_3}) = 1$ en $\mathbb{Z}_4[x]$ y la prueba de esto se remite al mismo argumento usado en i), por lo que para cada $l_2 \in \{1,2,\ldots,k_3\}$ existe $\nu_{k_1+k_2+l_2}$ en $\mathbb{Z}_4[x]$ tal que

$$\sum_{l_2=1}^{k_3} \nu_{k_1+k_2+l_2} \check{f}_{k_1+k_2+l_2} = 1$$

luego

$$\begin{aligned} \sum_{l_2=1}^{k_3} 2\nu_{k_1+k_2+l_2} \hat{f}_{k_1+k_2+l_2} &= 2(f_1 \cdots f_{k_1})(f_{k_1+1} \cdots f_{k_1+k_2})(\sum_{l_2=1}^{k_3} \nu_{k_1+k_2+l_2} \check{f}_{k_1+k_2+l_2}) \\ &= 2F_0F_1 \end{aligned}$$

y ya que para cada $l_2 \in \{1,2,\ldots,k_3\}$ se cumple que $2\nu_{k_1+k_2+l_2} \hat{f}_{k_1+k_2+l_2} \in \langle 2\hat{f}_{k_1+k_2+l_2} \rangle$, entonces $\langle 2\hat{F}_2 \rangle \subseteq \sum_{l_2=1}^{k_3} \langle 2\hat{f}_{k_1+k_2+l_2} \rangle$.

Por lo tanto,

$$\mathcal{C}_1 = \langle \hat{F}_1, 2\hat{F}_2 \rangle \subseteq \langle \hat{f}_{k_1+1} \rangle + \langle \hat{f}_{k_1+2} \rangle + \cdots + \langle \hat{f}_{k_1+k_2} \rangle + \langle 2\hat{f}_{k_1+k_2+1} \rangle + \cdots + \langle 2\hat{f}_r \rangle = \mathcal{C}.$$

□

Como mencionamos al principio de este capítulo, $\mathcal{C}$ es un código cíclico sobre $\mathbb{Z}_4$ si es un $\mathbb{Z}_4-$submódulo cerrado bajo corrimiento cíclico. En la siguiente proposición veremos cual es la cardinalidad de $\mathcal{C}$.

Proposición 3.2. *Sea $\mathcal{C}$ como en el teorema previo, entonces $|\mathcal{C}| = 4^{grad(F_1)} 2^{grad(F_2)}$ y si*

i) $F_2 = 1$, $\mathcal{C} = \langle F_0 + I \rangle$ *y* $|\mathcal{C}| = 4^{n-grad(F_0)}$

ii) $F_1 = 1$, $\mathcal{C} = \langle 2F_0 + I \rangle$ *y* $|\mathcal{C}| = 2^{n-grad(F_0)}$

Demostración. Sean F_0, F_1 y F_2 polinomios únicos, mónicos y coprimos por parejas tales que $F_0F_1F_2 = x^n - 1$ donde $grad(F_0) = t$, $grad(F_1) = r$, $grad(F_2) = s$ y $\mathcal{C} = \langle \hat{F}_1 + I, 2\hat{F}_2 + I \rangle$. Recordemos que $\langle \hat{F}_1 + I \rangle$ y $\langle 2\hat{F}_2 + I \rangle$ son $\mathbb{Z}_4-$submódulos y con esto en mente probemos los siguiente

a) $|\langle \hat{F}_1 + I \rangle| = 4^{grad(F_1)}$

b) $|\langle 2\hat{F}_2 + I \rangle| = 2^{grad(F_2)}$

a) Notemos que $grad(\hat{F}_1) = grad(F_0F_2) = grad(F_0) + grad(F_2) = t + s = n - r$ esto ya que $t + r + s = n$, por lo que, $n - grad(\hat{F}_1) = r$

Como $\langle \hat{F}_1 + I \rangle = \{(g + I)(\hat{F}_1 + I) : g + I \in \mathcal{R}_n\}$, mostremos que es suficiente restringir al polinomio g a polinomios de grado menor que $n - (n - r) = r$. Sea $g + I \in \langle \hat{F}_1 + I \rangle$ entonces $g + I = (h + I)(\hat{F}_1 + I)$ para algún $h + I \in \mathcal{R}_n$ con $h = h_0 + h_1x + \cdots + h_dx^d$. Supongamos que $d = grad(h) \geqslant r$, por lo que existe $k \geqslant 0$ tal que $d = r + k$. Definimos el polinomio

$$q_1 = h - h_dx^{d-r}F_1$$

como F_1 es mónico entonces el polinomio q_1 tiene grado menor que d, multiplicando por $\hat{F}_1$ tenemos lo siguiente

$$\begin{aligned} & q_1\hat{F}_1 = h\hat{F}_1 - h_dx^{d-r}F_1\hat{F}_1 \\ \Rightarrow \quad & q_1\hat{F}_1 = h\hat{F}_1 - h_dx^{d-r}(x^n - 1) \\ \Rightarrow \quad & q_1\hat{F}_1 - h\hat{F}_1 \in \langle x^n - 1 \rangle = I \\ \Rightarrow \quad & q_1\hat{F}_1 + I = h\hat{F}_1 + I \\ \Rightarrow \quad & g + I = q_1\hat{F}_1 + I \end{aligned}$$

Si $j = grad(q_1) \geqslant r$ volvemos a aplicar el procedimiento de arriba y definimos $q_2 = q_1 - q_{1_j} x^{j-r} F_1$, donde $grad(q_2) < grad(q_1)$ y después de multiplicar por $\hat{F}_1$ tenemos que $g + I = q_2\hat{F}_1 + I$ y si nuevamente se tiene que $grad(q_2) \geqslant r$ entonces procedemos de manera análoga a como lo hicimos antes, en general, será necesario realizar esto a lo más $k+1$ veces para poder obtener un polinomio q tal que $grad(q) < r$ y $g + I = q\hat{F}_1 + I$, por lo que $g + I$ se puede ver como el producto de $\hat{F}_1 + I$ con $q + I$ donde q es un polinomio de grado menor que r, lo que queríamos probar. Ahora en bien, sea $q(x) = q_0 + q_1 x + \cdots + q_{r-1}x^{r-1}$ un polinomio en $\mathbb{Z}_4[x]$, tenemos que cada $q_i \in \mathbb{Z}_4[x]$, por lo que, por el principio multiplicativo $q(x)$ se puede escribir de 4^r formas distintas, de ahí que el conjunto $\langle \hat{F}_1 + I\rangle = \{(g + I)(\hat{F}_1 + I) : g + I \in \mathcal{R}_n\}$, tiene 4^r elementos distintos. Así $|\langle \hat{F}_1 + I\rangle| = 4^r = 4^{grad(F_1)}$

b) Ya que $\langle 2\hat{F}_2 + I\rangle = \{(g+I)(2\hat{F}_2 + I) \colon g + I \in \mathcal{R}_n\}$, podemos ver que se puede restringir al polinomio g a polinomios de grado menor que s y la prueba de esto es igual a la que se realizó en el inciso b) cuando restringimos g a polinomios de grado menor que r, solo se debe tener presente que ahora trabajamos con los polinomios $\hat{F}_2$ y F_2 cuyos grados son $n - s$ y s respectivamente. sea $g \in \mathbb{Z}_4[x]$ un polinomio de grado menor que s, tenemos que los coeficientes del polinomio $2g$ serán 0 ó 2, ya que en $\mathbb{Z}_4$ $2 \cdot 1 = 2 = 2 \cdots 3$ y $2 \cdot 0 = 0 = 2 \cdot 2$ luego, el número de polinomios de la forma $2g$, donde $grad(g) < s$, en $\mathbb{Z}_4[x]$ es de 2^s, esto por el principio multiplicativo, por lo que $|\langle 2\hat{F}_2 + I\rangle| = 2^s = 2^{g}rad(F_2)$.

Afirmación. $\langle \hat{F}_1 + I\rangle \cap \langle 2\hat{F}_2 + I\rangle = \langle 0 + I\rangle$.

Sabemos que $0 + I \in \langle \hat{F}_1 + I\rangle$ y $0 + I \in \langle 2\hat{F}_2 + I\rangle$ por lo que $\langle 0 + I\rangle \subseteq \langle \hat{F}_1 + I\rangle \cap \langle 2\hat{F}_2 + I\rangle$. Sea $a + I \in \langle \hat{F}_1 + I\rangle \cap \langle 2\hat{F}_2 + I\rangle$ entonces existen $h_1 + I, h_2 + I \in \mathcal{R}_n$ con $grad(h_1) < r$ y $grad(h_2) < s$ tales que $a + I = (h_1 + I)(\hat{F}_1 + I)$ y $a + I = (h_2 + I)(2\hat{f}_2 + I)$, igualando ambos lados tenemos, $h_1\hat{F}_1 + I = 2h_2\hat{F}_2 + I$ lo cual nos dice que $h_1F_0F_2 - 2h_2F_0F_1 \in I = \langle x^n - 1\rangle$ pero como $grad(h_1F_0F_2) < n$ y $grad(2h_2F_0F_1) < n$ entonces $grad(h_1F_0F_2 - 2h_2F_0F_1) < n$ por lo que $h_1F_0F_2 - 2h_2F_0F_1 = 0$, luego:

$$h_1F_0F_2 = 2h_2F_0F_1 \tag{7}$$

así que $F_2|2h_2F_0F_1$, y ya que F_0, F_1 y F_2 son coprimos por pares, entonces F_0F_1 y F_2 son coprimos y como además F_2 no divide a 2 pues $F_2 \neq 1$, así tenemos que $F_2|h_2$, es decir, exite $k \in \mathbb{Z}_4[x]$ tal que $h_2 = kF_2$, sustituyendo esto en (7) tenemos que $h_1F_0F_2 = 2kF_2F_0F_1 = 2k(x^n - 1)$, así que $h_1F_0F_2 \in I$, luego $h_1\hat{F}_1 + I = 0 + I$, es decir $a + I = 0 + I$. Por lo que $\langle \hat{F}_1 + I\rangle \cap \langle 2\hat{F}_2 + I\rangle = \langle 0 + I\rangle$.

De la afirmación se sigue que

$$\mathcal{C} = \langle \hat{F}_1 + I\rangle \oplus \langle 2\hat{F}_2 + I\rangle.$$

Por lo tanto

$$|\mathcal{C}| = |\langle \hat{F}_1 + I\rangle||\langle 2\hat{F}_2 + I\rangle| = 4^{grad(F_1)}2^{grad(F_2)}.$$

i) Si $F_2 = 1$, entonces $x^n - 1 = F_0F_1$ de ahí que $\mathcal{C} = \langle \hat{F}_1 + I, 2\hat{F}_2 + I\rangle = \langle F_0 + I\rangle + \langle 2F_0F_1 + I\rangle = \langle F_0 + I\rangle$ y $|\mathcal{C}| = 4^{n-grad(\hat{F}_1)} = 4^{n-grad(F_0)}$,

ii) Si $F_1 = 1$, entonces $x^n - 1 = F_0F_2$ por lo que $\mathcal{C} = \langle \hat{F}_1 + I, 2\hat{F}_2 + I\rangle = \langle F_0F_2 + I\rangle + \langle 2F_0 + I\rangle = \langle 2F_0 + I\rangle$ y así $|\mathcal{C}| = 2^{n-grad(\hat{F}_2)} = 2^{n-grad(F_0)}$.

□

3.2 CÓDIGO DUAL

Ahora hablaremos del código dual de un $\mathbb{Z}_4$-código cíclico, para ello necesitamos definir el producto interno en $\mathbb{Z}_4^n$. Sean $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ y $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$ en $\mathbb{Z}_4^n$, definimos

$$\mathbf{a} \cdot \mathbf{b} = a_0b_0 + a_1b_1 + \cdots + a_{n-1}b_{n-1} \quad (\text{mód } 4)$$

En la Definición 2.8 se habló del código dual de un código sobre un campo finito, para un $\mathbb{Z}_4$-código cíclico la definición es la misma con la observación de que ahora estamos sobre $\mathbb{Z}_4$, es decir,

$$\mathcal{C}^{\perp} = \{\mathbf{u} \in \mathbb{Z}_4^n : \mathbf{u} \cdot \mathbf{v} = 0 \text{ para todo } \mathbf{v} \in \mathcal{C}\} \tag{8}$$

Nuestro mayor interés es poder conocer la forma del polinomio generador del código dual.

Definition 3.1. *Sea* $f(x) = f_0 + f_1x + \cdots + f_dx^d$ *un polinomio en* $\mathbb{Z}_4[x]$ *con* $f_d \neq 0$*, definimos el polinomio recíproco de* $f(x)$ *como*

$$f^*(x) = \pm x^d f(x^{-1}) = \pm(a_0x^d + a_1x^{d-1} + \cdots + a_{d-1}x + a_d)$$

El siguiente lema enuncia dos propiedades importantes del polinomio recíproco que nos serán de gran utilidad en la prueba del Teorema 3.4.

Lema 3.4. *Sean* $f(x) = a_0 + a_1x + \cdots + a_sx^s$ *y* $g(x) = b_0 + b_1x + \cdots + b_tx^t$ *polinomios en* $\mathbb{Z}_4[x]$ *con* $s \geqslant t$*, entonces*

i) $(f^*)^*(x) = f(x)$,

ii) $(f(x)g(x))^* = f^*(x)g^*(x)$,

iii) $(f(x) + g(x))^* = f^*(x) + g^*(x)x^r$ *para algún* $r \geqslant 0$.

Demostración. i) Tenemos que $f^*(x) = \pm x^s f(x^{-1}) = \pm(a_0x^s + a_1x^{s-1} + \cdots + a_{s-1}x + a_s)$ luego

$$\begin{aligned}(f^*)^*(x) &= \pm x^s f^*(x^{-1}) \\ &= \pm x^s(\pm(a_0x^{-s} + a_1x^{-(s-1)} + \cdots + a_{s-1}x^{-1} + a_s)) \\ &= a_0 + a_1x + \cdots + a_{s-1}x^{s-1} + a_sx^s \\ &= f(x).\end{aligned}$$

ii) Tenemos que

$$(f(x)g(x))^* = \pm x^{s+t}f(x^{-1})g(x^{-1}) = (\pm x^s f(x^{-1}))(\pm x^t g(x^{-1})) = f^*(x)g^*(x).$$

iii) Como $s \geqslant t$ entonces existe un $r \geqslant 0$ tal que $t + r = s$ y como $grad(f(x) + g(x)) = s = t + r$, entonces

$$\begin{aligned}(f(x) + g(x))^* &= \pm x^s(f(x^{-1}) + g(x^{-1})) \\ &= \pm x^s f(x^{-1}) + (\pm x^{t+r}g(x^{-1})) \\ &= f^*(x) + (\pm x^t g(x^{-1}))x^r \\ &= f^*(x) + x^r g^*(x)\end{aligned}$$

lo que queríamos probar.

□

Obsérvese que $grad(f(x)) = grad(f^*(x))$.

Teorema 3.3. *Sean* $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ *y* $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$ *vectores en* $\mathbb{Z}_4^n$ *con polinomios asociados* $a(x)$ *y* $b(x)$*. Entonces* $\mathbf{a}$ *es ortogonal a* $\mathbf{b}$ *y a todos sus corrimientos cíclicos si y sólo si,* $a(x)b^*(x) = 0$ *en* $\mathcal{R}_n$.

Demostración. Tenemos que $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ y $b^*(x) = b_{n-1} + b_{n-2}x + \cdots + b_1x^{n-2} + b_0x^{n-1}$. Realizemos el producto de $a(x)b^*(x)$ en $\mathcal{R}_n$, recordando que aquí $x^n = 1$. Así

$$
\begin{aligned}
0 &= a(x)b^*(x)\\
&= (a_0 + a_1x + \cdots + a_{n-1}x^{n-1})b^*(x)\\
&= a_0b^*(x) + a_1xb^*(x) + \cdots + a_{n-1}x^{n-1}b^*(x)\\
&= a_0b_{n-1} + a_0b_{n-2}x + \cdots + a_0b_1x^{n-2} + a_0b_0x^{n-1} +\\
&\quad + a_1b_{n-1}x + a_1b_{n-2}x^2 + \cdots + a_1b_1x^{n-1} + a_1b_0x^n +\\
&\quad + \cdots +\\
&\quad + a_{n-1}b_{n-1}x^{n-1} + a_{n-1}b_{n-2}x^n + \cdots + a_{n-1}b_1x^{2n-3} + a_{n-1}b_0x^{2n-2}\\
&= a_0b_{n-1} + a_0b_{n-2}x + \cdots + a_0b_0x^{n-1} +\\
&\quad a_1b_0 + a_1b_{n-1}x + a_1b_{n-2}x^2 + \cdots + a_1b_1x^{n-1} +\\
&\quad + \cdots +\\
&\quad + a_{n-1}b_{n-2} + a_{n-1}b_{n-3}x + \cdots + a_{n-1}b_{n-1}x^{n-1}\\
&= (a_0b_{n-1} + a_1b_0 + \cdots + a_{n-1}b_{n-2}) +\\
&\quad (a_0b_{n-2} + a_1b_{n-1} + \cdots + a_{n-1}b_{n-3})x +\\
&\quad + \cdots +\\
&\quad (a_0b_0 + a_1b_1 + \cdots + a_{n-1}b_{n-1})x^{n-1}\\
\iff 0 &= a_0b_{n-1} + a_1b_0 + \cdots + a_{n-1}b_{n-2}\\
0 &= a_0b_{n-2} + a_1b_{n-1} + \cdots + a_{n-1}b_{n-3}\\
&\vdots\\
0 &= a_0b_0 + a_1b_1 + \cdots + a_{n-1}b_{n-1}\\
\iff 0 &= (a_0, a_1, \ldots, a_{n-1}) \cdot (b_{n-1}, b_0, \ldots, b_{n-2})\\
0 &= (a_0, a_1, \ldots, a_{n-1}) \cdot (b_{n-2}, b_{n-1}, \ldots, b_{n-3})\\
&\vdots\\
0 &= (a_0, a_1, \ldots, a_{n-1}) \cdot (b_0, b_1, \ldots, b_{n-1})\\
\iff &\quad \mathbf{a} \text{ es ortogonal a } \mathbf{b} \text{ y a todos sus corrimientos cíclicos.}
\end{aligned}
$$

□

Observación 3.2. *Del teorema anterior y de (8), se tiene que*

$$\mathcal{C}^\perp = \{b(x) + I \in \mathcal{R}_n | a(x)b^*(x) + I = 0 + I \text{ para cada } a(x) + I \in \mathcal{C}\}. \tag{9}$$

El siguiente teorema nos muestra como es el dual de un código cíclico $\mathcal{C}$ sobre $\mathbb{Z}_4$.

Teorema 3.4. *Sea* $\mathcal{C} = \langle \hat{F}_1 + I, 2\hat{F}_2 + I\rangle$ *un* $\mathbb{Z}_4$*-código cíclico de longitud impar* n*, donde* F_0*,* F_1 *y* F_2 *son polinomios mónicos y coprimos por pares tales que* $F_0F_1F_2 = x^n - 1$ *y* $|\mathcal{C}| = 4^{grad(F_1)}2^{grad(F_2)}$*. Entonces*

$$\mathcal{C}^\perp = \langle F_1^*F_2^* + I, 2F_0^*F_1^* + I\rangle \text{ y } |\mathcal{C}^\perp| = 4^{grad(F_0)}2^{grad(F_2)}$$

Si $F_2 = 1$*, entonces* $\mathcal{C} = \langle F_0 + I\rangle$ *y* $\mathcal{C}^\perp = \langle F_1^* + I\rangle$.
Si $F_1 = 1$*, entonces* $\mathcal{C} = \langle 2F_0 + I\rangle$ *y* $\mathcal{C}^\perp = \langle F_2^* + I, 2F_0^* + I\rangle$.

Demostración. Sea $g = F_1^*F_2^*$, entonces, por el Lema 3.4 $g^* = (F_1^*F_2^*)^* = (F_1^*)^*(F_2^*)^* = F_1F_2$. Luego

$$\hat{F}_1g^* = (F_0F_2)(F_1F_2) = (F_0F_1F_2)F_2 = (x^n - 1)F_2 = 0 \text{ en } \mathcal{R}_n \tag{10}$$

y

$$2\hat{F}_2g^* = (2F_0F_1)(F_1F_2) = (F_0F_1F_2)2F_1 = (x^n - 1)2F_1 = 0 \text{ en } \mathcal{R}_n \tag{11}$$

Sean $a + I \in \mathcal{C}$, entonces $a + I = (k_1\hat{F}_1 + I) + (2k_2\hat{F}_2 + I)$ para algunos $k_1 + I, k_2 + I \in \mathcal{R}_n$ y $q + I \in \langle F_1^*F_2^* + I\rangle$ se tiene que existe $k_3 + I \in \mathcal{R}_n$ tal que $q + I = k_3F_1^*F_2^* + I$, luego $q - k_3F_1^*F_2^* \in I = \langle x^n - 1\rangle$, es decir, existe $k_4 \in \mathbb{Z}_4[x]$ tal que $q - k_3F_1^*F_2^* = k_4(x^n - 1)$, luego pasamos sumando a q ó $-k_3F_1^*F_2^*$,

dependiendo de cual tenga grado mayor o igual al grado de $k_4(x^n-1)$, sin pérdida de generalidad supongamos que $-k_3F_1^*F_2^*$ es de grado mayor o igual a $k_4(x^n-1)$, entonces $q = k_3F_1^*F_2^* + k_4(x^n-1)$, luego por iii) del Lema 3.4, existe un $r \geqslant 0$ tal que $q^* = k_3^*F_1F_2 + x^rk_4^*(x^n-1)^* = k_3^*g^* - x^rk_4^*(x^n-1)$ puesto que $(x^n-1)^* = -(x^n-1)$, así $q^* - k_3^*g^* = -x^rk_4^*(x^n-1)$, por tanto $q^* + I = k_3^*g^* + I$. Luego

$$\begin{aligned}(a+I)(q^*+I) &= ((k_1\hat{F}_1+I)+(2k_2\hat{F}_2+I))(k_3^*g^*+I)\\ &= (k_1\hat{F}_1+I)(k_3^*g^*+I)+(2k_2\hat{F}_2+I)(k_3^*g^*+I)\\ &= (k_1k_3^*\hat{F}_1g^*+I)+(k_2k_3^*2\hat{F}_2g^*+I)\\ &= 0+I\end{aligned}$$

esto último por (10) y (11). Luego, por la Observación 3.2 se sigue que $q+I \in \mathcal{C}^\perp$, de ahí que

$$\langle F_1^*F_2^*+I\rangle \subseteq \mathcal{C}^\perp.$$

Por otro lado, sea $h = 2F_0^*F_1^*$, entonces $h^* = 2F_0F_1$ y tenemos lo siguiente

$$\hat{F}_1h^* = (F_0F_2)(2F_0F_1) = 2F_0(x^n-1) = 0 \text{ en } \mathcal{R}_n \tag{12}$$

y

$$2\hat{F}_2h^* = 2(F_0F_1)(2F_0F_1) = 4(F_0F_1)(F_0F_1) = 0 \text{ en } \mathcal{R}_n \tag{13}$$

Sean $b+I \in \mathcal{C}$ y $p+I \in \langle 2F_0^*F_1^*+I\rangle$ entonces existen $k_1+I, k_2+I, k_3+I \in \mathcal{R}_n$ tales que $a+I = (k_1\hat{F}_1+I)+(2k_2\hat{F}_2+I)$ y $p+I = 2k_3F_0^*F_1^*+I$. Notemos que, haciendo el mismo procedimiento que hicimos antes, $p^*+I = 2k_3^*F_0F_1+I = 2k_3^*h^*+I$. Entonces

$$\begin{aligned}(b+I)(p^*+I) &= ((k_1\hat{F}_1+I)+(2k_2\hat{F}_2+I))(2k_3^*h^*+I)\\ &= (k_1\hat{F}_1+I)(2k_3^*h^*+I)+(2k_2\hat{F}_2+I)(2k_3^*h^*+I)\\ &= (2k_1k_3^*\hat{F}_1h^*+I)+(4k_2k_3^*\hat{F}_2h^*+I)\\ &= 0+I\end{aligned}$$

esto último por (12) y (13). Así, por la Observación 3.2 se tiene que $p+I \in \mathcal{C}^\perp$, por lo tanto

$$\langle 2F_0^*F_1^*+I\rangle \subseteq \mathcal{C}^\perp.$$

Veamos que $\langle F_1^*F_2^*+I, 2F_0^*F_1^*+I\rangle \subseteq \mathcal{C}^\perp$.

Sean $t+I \in \langle F_1^*F_2^*+I, 2F_0^*F_1^*+I\rangle$ y $c+I \in \mathcal{C}$ entonces existen $q+I \in \langle F_1^*F_2^*+I\rangle$ y $p+I \in \langle 2F_0^*F_1^*+I\rangle$ tales que $t+I = (q+I)+(p+I) = (q+p)+I$ y sin pérdida de generalidad supongamos que $grad(q) \geqslant grad(p)$, así, por el inciso iii) del Lema 3.4 tenemos que $(q+p)^* = q^*+x^rp^*$ para algún $r \geqslant 0$, luego

$$\begin{aligned}((q+p)^*+I)(c+I) &= (q^*+x^rp^*+I)(c+I)\\ &= ((q^*+I)+(x^rp^*+I))(c+I)\\ &= (q^*c+I)+(x^rp^*c+I)\\ &= 0+I\end{aligned}$$

donde la última igualdad se da ya que $\langle F_1^*F_2^*+I\rangle \subseteq \mathcal{C}^\perp$ y $\langle 2F_0^*F_1^*+I\rangle \subseteq \mathcal{C}^\perp$. Así $t+I \in \mathcal{C}$, por lo que

$$\langle F_1^*F_2^*+I, 2F_0^*F_1^*+I\rangle \subseteq \mathcal{C}^\perp. \tag{14}$$

Ya que $F_0^*F_1^*F_2^* = 1-x^n = -(x^n-1)$ entonces de manera análoga a como se hizo en la Proposición 3.2, se puede ver que

- $|\langle F_1^*F_2^*+I\rangle| = 4^{grad(F_0)}$
- $|\langle 2F_0^*F_1^*+I\rangle| = 2^{grad(F_2)}$

De ahí que

$$|\langle F_1^* F_2^* + I, 2F_0^* F_1^* + I\rangle| = 4^{grad(F_0)} 2^{grad(F_2)}. \tag{15}$$

Como todo código cíclico de longitud n sobre un anillo $\mathbb{Z}_{p^a}$ tiene una matriz generadora "estándar" y de manera análoga su código dual, luego por las propiedades de dichas matrices, se cumple que $|\mathcal{C}||\mathcal{C}^\perp| = p^{an}$ (cf [CS95]) en este caso, nosotros tenemos que $p = 2$ y $a = 2$, y por Proposición 3.2 $|\mathcal{C}| = 4^{grad(F_1)} 2^{grad(F_2)} = 2^{2grad(F_1)+grad(F_2)}$ por lo que $|\mathcal{C}^\perp| = \frac{2^{2n}}{|\mathcal{C}|} = 2^{2n} 2^{-2grad(F_1)-grad(F_2)}$, pero $n = grad(F_0) + grad(F_1) + grad(F_2)$, así $2^{2n-2grad(F_1)-grad(F_2)}$ pero $2grad(F_0) + 2grad(F_1) + 2grad(F_2) - 2grad(F_1) - grad(F_2) = 2grad(F_0) + grad(F_2)$, así

$$|\mathcal{C}^\perp| = 2^{2grad(F_0)+grad(F_2)} = 4^{grad(F_0)} 2^{grad(F_2)}$$

pero por (15) tenemos que

$$|\mathcal{C}^\perp| = |\langle F_1^* F_2^* + I, 2F_0^* F_1^* + I\rangle|. \tag{16}$$

Por lo tanto, por (14) y (16), se sigue que

$$\mathcal{C}^\perp = \langle F_1^* F_2^* + I, 2F_0^* F_1^* + I\rangle.$$

Si $F_2 = 1$, entonces $F_2^* = 1$, y así $\langle 2F_0^* F_1^* + I\rangle \subseteq \langle F_1^* + I\rangle$ por lo que $\langle F_1^* F_2^* + I, 2F_0^* F_1^* + I\rangle = \langle F_1^* + I\rangle$, es decir, $\mathcal{C}^\perp = \langle F_1^* + I\rangle$.

Si $F_1 = 1$, entonces $F_1^* = 1$, luego, $\mathcal{C}^\perp = \langle F_2^* + I, 2F_0^* + I\rangle$.

□

3.3 GENERADORES IDEMPOTENTES

Definición 3.2. *Un idempotente en $\mathbb{Z}_4[x]$ es un polinomio $e(x)$ tal que*

$$e^2(x) \equiv e(x) \pmod{x^n - 1}$$

Observación 3.3. *Cada polinomio en $\mathbb{F}_2[x]$ se puede ver como un polinomio en $\mathbb{Z}_4[x]$.*

Teorema 3.5. *Sea $\mathcal{C}$ un $\mathbb{Z}_4$−código cíclico de longitud impar n.*

i) Si $\mathcal{C} = \langle f + I\rangle$, donde $fg = x^n - 1$ para algún $g \in \mathbb{Z}_4[x]$, entonces $\mathcal{C}$ tiene un idempotente generador en $\mathbb{Z}_4[x]$.

ii) Si $\mathcal{C} = \langle 2f + I\rangle$ y f divide a $x^n - 1$ entonces $\mathcal{C} = \langle 2e + I\rangle$ donde e es un generador binario idempotente de $\langle \mu(f) + I\rangle$.

iii) Si $\mathcal{C} = \langle fh + I, 2fg + I\rangle$ donde $fgh = x^n - 1$, entonces $\mathcal{C} = \langle e + I, 2v + I\rangle$ donde e es un idempotente en $\mathbb{Z}_4[x]$; v es un idempotente en $\mathbb{F}_2[x]$.

Demostración. i) Como f y g son coprimos entonces existen $u, v \in \mathbb{Z}_4[x]$ tales que $1 = fu + gv$. Sea $e = fu$, entonces $e = 1 - gv$ y $e^2 = e - gve$, sustituyendo e tenemos que $e^2 = e - gv(fu)$ y así $e^2 = e - uv(x^n - 1)$, por lo que $e^2 - e \in \langle x^n - 1\rangle$, y por tanto $e^2 \equiv e \pmod{x^n - 1}$, por lo que e es idempotente en $\mathbb{Z}_4[x]$.

Ahora, tenemos que en $\mathcal{R}_n$, $e = fu$, por lo que $e + I \in \langle f + I\rangle$. Veamos que $f + I \in \langle e + I\rangle$.

Como $e = 1 - gv$ entonces $fe = f - fgv$ y como $fg = x^n - 1$ se sigue que $f - fgv - f = (x^n - 1)v$, así $f - fgv \equiv f \pmod{x^n - 1}$

$$\begin{aligned}
&\Rightarrow \quad fe \equiv f \pmod{x^n - 1}\\
&\Rightarrow \quad fe - f \in \langle x^n - 1\rangle = I\\
&\Rightarrow \quad fe + I = f + I\\
&\Rightarrow \quad (f + I)(e + I) = f + I\\
&\Rightarrow \quad f + I \in \langle e + I\rangle.
\end{aligned}$$

Por lo tanto $\langle f + I\rangle = \langle e + I\rangle$.

ii) Probemos que $2f(x) = 2\bar{\mu}(f(x)) = \bar{f}(x)$ donde $\bar{\mu}$ es como se definió en (5). Sea $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_sx^s \in \mathbb{Z}_4[x]$, tenemos que los $a_i \in \mathbb{Z}_4$, luego $2f(x) = 2a_0 + 2a_1x + 2a_2x^2 + \cdots + 2a_sx^s$ y observemos lo siguiente

$$\begin{array}{llllll} a_i = 0 & \Rightarrow & 2a_i = 0 & y & \mu(a_i) = 0 & \Rightarrow & 2\mu(a_i) = 0 = 2a_i \\ a_i = 1 & \Rightarrow & 2a_i = 2 & y & \mu(a_i) = 1 & \Rightarrow & 2\mu(a_i) = 2 = 2a_i \\ a_i = 2 & \Rightarrow & 2a_i = 0 & y & \mu(a_i) = 0 & \Rightarrow & 2\mu(a_i) = 0 = 2a_i \\ a_i = 3 & \Rightarrow & 2a_i = 2 & y & \mu(a_i) = 1 & \Rightarrow & 2\mu(a_i) = 2 = 2a_i \end{array}$$

donde μ es como se defininió en (4). Así

$$2a_0 + 2a_1x + 2a_2x^2 + \cdots + 2a_sx^s = 2\mu(a_0) + 2\mu(a_1)x + 2\mu(a_2)x^2 + \cdots + 2\mu(a_s)x^s.$$

Por lo que $2f(x) = 2\bar{f}(x)$ y como $\bar{f}(x) \in \mathbb{F}_2[x]$ tenemos que por Teorema 2.10 $\langle \bar{f}(x) + I\rangle$ contiene un único idempotente $e(x)$, tal que $\langle \bar{f}(x) + I\rangle = \langle e(x) + I\rangle$, luego $\langle 2\bar{f}(x) + I\rangle = \langle 2e(x) + I\rangle$ en $\dfrac{\mathbb{Z}_4[x]}{\langle x^n - 1\rangle}$ y así $\langle 2f(x) + I\rangle = \langle 2e(x) + I\rangle$.

iii) De i) tenemos que $\langle fh + I\rangle = \langle e + I\rangle$ con e un idempotente en $\mathbb{Z}_4[x]$ y por ii) tenemos que $\langle 2fg + I\rangle = \langle 2v + I\rangle$ donde v es un idempotente en $\mathbb{F}_2[x]$. Por lo tanto

$$\langle fh + I, 2fg + I\rangle = \langle e + I, 2v + I\rangle.$$

□

El siguiente teorema nos permite conocer el generador idempontente del código dual $\mathcal{C}^\perp$, cuando conocemos el generador idempotente del código cíclico $\mathcal{C}$.

Observación 3.4. *Tenemos que* x *y* $x^n - 1$ *son coprimos en* $\mathbb{Z}_4[x]$*, por lo que existen* $a(x), b(x) \in \mathbb{Z}_4[x]$ *tales que*

$$a(x)x + b(x)(x^n - 1) = 1$$

pero entonces

$$a(x)x - 1 = -b(x)(x^n - 1)$$

por lo que

$$a(x)x \equiv 1 \pmod{x^n - 1}$$

De ahí que $a(x)$ *es el inverso de* x *en* $\mathcal{R}_n$ *y denotamos a* $a(x)$ *por* x^{-1}.

Teorema 3.6. *Si un código cíclico sobre* $\mathbb{Z}_4$*,* $\mathcal{C}$*, tiene el generador idempotente* $e(x)$*, entonces* $\mathcal{C}^\perp$ *tiene el generador idempotente* $1 - e(x^{-1})$.

Demostración. Sabemos que $\mathcal{C}$ tiene un polinomio generador en $\mathcal{R}_n$, dígamos que $\mathcal{C} = \langle g(x) + I\rangle$, donde $g(x)$ divide a $x^n - 1$ y además como ya vimos en el Teorema 3.2 $g(x)$ es producto de básicos irreducibles y coprimos por pares, además, existe $h(x) \in \mathbb{Z}_4[x]$ tal que $g(x)h(x) = x^n - 1$ $g(x)$, $h(x)$ son coprimos, es decir $\langle g(x)\rangle + \langle h(x)\rangle = \langle 1\rangle$, por lo que existen $s(x), t(x) \in \mathbb{Z}_4[x]$ tales que

$$1 = s(x)g(x) + t(x)h(x) \tag{17}$$

Sean $e_1(x) = s(x)g(x)$ y $e_2(x) = t(x)h(x)$, podemos ver que $e_1(x)$ y $e_2(x)$ son idempotentes de manera análoga a como lo hicimos en el inciso i) del Teorema 3.5 y por este mismo teorema se tiene que $\langle g(x) + I\rangle = \langle e_1(x) + I\rangle$ y $\langle h(x) + I\rangle = \langle e_2(x) + I\rangle$. Como $e(x)$ es el generador idempotente de $\mathcal{C}$ en $\mathcal{R}_n$ entonces $e_1(x) = e(x)$, luego, sustituyendo en (17) tenemos que

$$1 = e(x) + e_2(x)$$

por lo que $e_2(x) = 1 - e(x)$. Por otro lado como $\langle h(x) + I\rangle = \langle e_2(x) + I\rangle$ entonces $e_2(x) = t(x)h(x)$ y $h(x) = k(x)e_2(x)$, esto en $\mathcal{R}_n$, luego $e_2(x^{-1}) = t(x^{-1})h(x^{-1})$ y $h(x^{-1}) = k(x^{-1})e_2(x^{-1})$, por lo que $\langle h(x^{-1}) + I\rangle = \langle e_2(x^{-1}) + I\rangle$

Por el Teorema 3.4 tenemos que $\mathcal{C}^{\perp} = \langle h^*(x) + I \rangle$ donde $h^*(x) = \pm x^{grad(h)} h(x^{-1})$, además por la observación anterior tenemos que $x^{-1} = x^{n-1}$ puesto que $x^{n-1}x \equiv 1 \pmod{x^n - 1}$. Sea $h(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_r x^r$ entonces

$$\begin{aligned} h(x^{-1}) &= h_0 + h_1 x^{-1} + h_2 x^{-2} + \cdots + h_r x^{-r} \\ &\text{y} \\ h(x^{n-1}) &= h_0 + h_1 x^{n-1} + h_2 (x^{n-1})^2 + \cdots + h_r (x^{n-1})^r \\ &= h_0 + h_1 x^{n-1} + h_2 x^{2(n-1)} + \cdots + h_r x^{r(n-1)} \\ &= h_0 + h_1 x^{-1} + h_2 x^{-2} + \cdots + h_r x^{-r} \end{aligned}$$

esto último haciendo reducción módulo $x^n - 1$, por lo que efectivamente $h(x^{-1}) = h(x^{n-1})$, luego

$$\begin{aligned} h^*(x) &= \pm x^r h(x^{-1}) \\ &= \pm x^r h(x^{n-1}) \end{aligned}$$

y además

$$\begin{aligned} \pm x^{n-r} h^*(x) &= \pm x^{n-r} (\pm x^r h(x^{-1}) \\ &= x^{n-r+r} h(x^{n-1}) \\ &= x^n h(x^{n-1}) \\ &= h(x^{n-1}) \text{ (en } \mathcal{R}_n) \end{aligned}$$

por lo que $\langle h^*(x) + I \rangle = \langle h(x^{-1}) + I \rangle$ y así $\mathcal{C}^{\perp} = \langle h(x^{-1}) + I \rangle = \langle e_2(x^{-1}) + I \rangle$ y como $e_2(x^{-1}) = 1 - e(x^{-1})$ entonces

$$\mathcal{C}^{\perp} = \langle (1 - e(x^{-1})) + I \rangle.$$

□

Teorema 3.7. *Sean $\mathcal{C}_1$ y $\mathcal{C}_2$ códigos cíclicos sobre $\mathbb{Z}_4$, con generadores idempotentes e_1 y e_2 en $\mathcal{R}_n$, entonces $\mathcal{C}_1 \cap \mathcal{C}_2$ tiene el generador idempotente $e_1 e_2$ y $\mathcal{C}_1 + \mathcal{C}_2$ tiene el generador idempotente $e_1 + e_2 - e_1 e_2$.*

Demostración. Primero probemos que $e_1 e_2$ y $e_1 + e_2 - e_1 e_2$ son idempontentes es $\mathcal{R}_n$. Tenemos que

$$(e_1 e_2)^2 = e_1^2 e_2^2 \equiv e_1 e_2 \pmod{x^n - 1}$$

puesto que e_1 y e_2 son idempotentes, por lo que $e_1 e_2$ es idempotente. Por otro lado

$$\begin{aligned} (e_1 + e_2 - e_1 e_2)^2 &= e_1^2 + e_1 e_2 - e_1^2 e_2 + e_1 e_2 + e_2^2 - e_1 e_2^2 - e_1^2 e_2 - e_1 e_2^2 + e_1^2 e_2^2 \\ &= e_1^2 + e_2^2 + 2e_1 e_2 - 2e_1^2 e_2 - 2e_1 e_2^2 + e_1^2 e_2^2 \\ &\equiv e_1 + e_2 + 2e_1 e_2 - 2e_1 e_2 - 2e_1 e_2 + e_1 e_2 \pmod{x^n - 1} \\ &\equiv e_1 + e_2 - e_1 e_2 \pmod{x^n - 1} \end{aligned}$$

por lo que $e_1 + e_2 - e_1 e_2$ es idempotente en $\mathcal{R}_n$

i) Veamos que $\mathcal{C}_1 \cap \mathcal{C}_2 = \langle e_1 e_2 + I \rangle$ donde $I = \langle x^n - 1 \rangle$.

   $\supseteq]$ Como $e_1 + I \in \mathcal{C}_1$ entonces $e_1 e_2 + I \in \mathcal{C}_1$, y de manera análoga tenemos que $e_1 e_2 + I \in \mathcal{C}_2$ por lo que $\langle e_1 e_2 + I \rangle \subseteq \mathcal{C}_1 \cap \mathcal{C}_2$.

   $\subseteq]$ Sea $c + I \in \mathcal{C}_1 \cap \mathcal{C}_2$, como $\langle e_1 + I \rangle = \mathcal{C}_1$ y $\langle e_2 + I \rangle = \mathcal{C}_2$ entonces $c + I = e_1 k_1 + I$ y $c + I = e_2 k_2 + I$ para algunos $k_1 + I, k_2 + I \in \mathcal{R}_n$, luego $e_1 k_1 + I = e_2 k_2 + I$, por lo que $e_2 e_1 k_1 + I = e_2 e_2 k_2 + I = e_2 k_2 + I$ puesto que $e_2^2 + I = e_2 + I$, así $e_1 e_2 k_1 + I = c + I$, por lo tanto $c + I \in \langle e_1 e_2 + I \rangle$.

   Así $\mathcal{C}_1 \cap \mathcal{C}_2 = \langle e_1 e_2 + I \rangle$.

ii) Probemos que $\mathcal{C}_1 + \mathcal{C}_2 = \langle (e_1 + e_2 - e_1 e_2) + I \rangle$

   Tenemos que $(e_1 + e_2 - e_1 e_2) + I = (e_1 + I) + ((1 - e_1) + I)(e_2 + I)$, donde $e_1 + I \in \mathcal{C}_1$ y $((1 - e_1) + I)(e_2 + I) \in \langle e_2 + I \rangle = \mathcal{C}_2$ por lo que $(e_1 + e_2 - e_1 e_2) + I \in \mathcal{C}_1 + \mathcal{C}_2$ y así, $\langle (e_1 + e_2 - e_1 e_2) + I \rangle \subseteq$

$\mathcal{C}_1 + \mathcal{C}_2$. Por otro lado, sea $c + I \in \mathcal{C}_1 + \mathcal{C}_2$, como $\langle e_1 + I\rangle = \mathcal{C}_1$ y $\langle e_2 + I\rangle = \mathcal{C}_2$ entonces existen $h_1 + I, h_2 + I \in \mathcal{R}_n$ tales que $c + I = (e_1h_1 + I) + (e_2h_2 + I) = (e_1h_1 + e_2h_2) + I$, luego

$$\begin{aligned}
(c+I)((e_1+e_2-e_1e_2)+I) &= (e_1h_1+e_2h_2+I)((e_1+e_2-e_1e_2)+I)\\
&= (e_1h_1+e_2h_2)(e_1+e_2-e_1e_2)+I\\
&= (e_1^2h_1+e_1e_2h_1-e_1^2e_2h_1+e_1e_2h_1+e_2^2h_2-e_1e_2^2h_2)+I\\
&= (e_1h_1+e_1e_2h_1-e_1e_2h_1+e_1e_2h_2+e_2h_2-e_1e_2h_2)+I\\
&\quad (\text{ya que } e_1 \text{ y } e_2 \text{ son idempotentes})\\
&= ((e_1+e_1e_2-e_1e_2)h_1+I)+((e_1e_2+e_2-e_1e_2)h_2+I)\\
&= (e_1h_1+I)+(e_2h_2+I)\\
&= c+I
\end{aligned}$$

de ahí que $c + I \in \langle(e_1 + e_2 - e_1e_2) + I\rangle$. Por lo tanto

$$\mathcal{C}_1 + \mathcal{C}_2 = \langle(e_1 + e_2 - e_1e_2) + I\rangle.$$

□

4 CÓDIGOS DE RESIDUOS CUADRÁTICOS SOBRE CAMPOS FINITOS

En este capítulo se mostrarán algunas propiedades importantes de los códigos de residuos cuadráticos de longitud prima p sobre un campo $\mathbb{F}_l$, donde l es otro primo, el cual es un residuo cudrático módulo p.

Definición 4.1. *Si m es un entero positivo, decimos que el entero a es un residuo cuadrático de m si $(a, m) = 1$ y la congruencia $x^2 \equiv a \pmod{m}$ tiene solución. Si la congruencia $x^2 \equiv a \pmod{m}$ no tiene solución, decimos que a es un residuo no cuadrático de m.*

Ejemplo 4.1. *Sea $m = 7$, tenemos que*

$$\begin{aligned} 1^2 &\equiv 1 \pmod{7} \\ 2^2 &\equiv 4 \pmod{7} \\ 3^2 &\equiv 2 \pmod{7} \\ 4^2 &\equiv 2 \pmod{7} \\ 5^2 &\equiv 4 \pmod{7} \\ 6^2 &\equiv 1 \pmod{7} \\ 7^2 &\equiv 0 \pmod{7} \end{aligned}$$

Por lo que los residuos cuadráticos de 7 son 1, 2 y 4, y los no residuos cuadráticos son 3, 5 y 6.

Ejemplo 4.2. *Sea $m = 11$, tenemos que*

$$\begin{aligned} 1^2 &\equiv 1 \pmod{11} \\ 2^2 &\equiv 4 \pmod{11} \\ 3^2 &\equiv 9 \pmod{11} \\ 4^2 &\equiv 5 \pmod{11} \\ 5^2 &\equiv 3 \pmod{11} \\ 6^2 &\equiv 3 \pmod{11} \\ 7^2 &\equiv 5 \pmod{11} \\ 8^2 &\equiv 9 \pmod{11} \\ 9^2 &\equiv 4 \pmod{11} \\ 10^2 &\equiv 1 \pmod{11} \\ 11^2 &\equiv 0 \pmod{11} \end{aligned}$$

Por lo que los residuos cuadráticos de 11 son 1, 3 4, 5 y 9 y los no residuos cuadráticos son 2, 6, 7, 8 y 10.

Teorema 4.1. *Si p es un primo impar entonces hay exactamente $\frac{p-1}{2}$ residuos cuadráticos de p, y $\frac{p-1}{2}$ residuos no cuadráticos de p, de entre los enteros $1, 2, \ldots, p-1$.*

Demostración. Podemos escribir los p elementos de $\mathbb{Z}_p$ como sigue:

$$-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-3}{2}, \frac{p-1}{2}$$

estamos haciendo uso del hecho de que $\mathbb{Z}_p \leftrightarrow \mathbb{F}_p = \{0, 1, \ldots, p-1\}$.

Ahora bien, en un campo la relación $a^2 - b^2 = (a+b)(a-b) = 0$ implica que $a = \pm b$. Así en un campo si dos cuadrados, a^2 y b^2 coinciden entonces $a = \pm b$. Esto nos dice que los cuadrados de los elementos

$$1, \ldots, \frac{p-3}{2}, \frac{p-1}{2} \in \mathbb{Z}_p^*$$

son distintos y hay $\frac{p-1}{2}$ de ellos distintos, luego también hay $\frac{p-1}{2}$ residuos no cuadráticos. □

Definición 4.2. *Cualquier elemento de $\mathbb{F}_p$ que genere el grupo multiplicativo $\mathbb{F}_q^*$ es llamado un elemento primitivo de $\mathbb{F}_p$.*

Ejemplo 4.3. *Tenemos que cuando* $p = 7$*, los elementos primitivos de* $\mathbb{F}_7$ *son* 3 *y* 5*, y cuando* $p = 11$*, los elementos primitivos de* $\mathbb{F}_{11}$ *son* 2, 6, 7 *y* 8*.*

Proposición 4.1. *Sea* $g \in \mathbb{F}_p$ *un elemento primitivo,* a *es un residuo cuadrático de* p *si y sólo si* $a = g^{2i}$ *para algún entero* i*.*

Demostración. Sea g un elemento primitivo de $\mathbb{F}_p$, es decir, $\mathbb{F}_p^* = \langle g \rangle$.

$\Rightarrow$] Sea a un residuo cuadrático de p, entonces $(a, p) = 1$ y existe un x tal que $x^2 \equiv a \pmod{p}$, podemos tomar x en $\{0, 1, 2 \ldots, p-1\}$, pero como $a \neq 0$ y $x \neq p$, entonces para que x sea solución de la congruencia x debe ser distinto de 0, por lo que $x \in \{1, 2 \ldots, p-1\}$, luego, podemos ver a x como un elemento de $\mathbb{F}_p^*$ y así, existe un entero i tal que $g^i = x$, luego $x^2 = (g^i)^2 = g^{2i}$, así, $g^{2i} \equiv a \pmod{p}$, por lo que, en $\mathbb{F}_p^*$, $a = g^{2i}$.

$\Leftarrow$] Supongamos que en $\mathbb{F}_p^*$, $a = g^{2i}$ para algún i en los enteros, luego, sea $x = g^i$, tenemos que $x^2 \equiv a \pmod{p}$, y además como $a \in \mathbb{F}_p^*$, entonces $(a, p) = 1$, por lo que a es un residuo cuadrático de p. □

Corolario 4.1. a *es un no residuo cuadrático de* q *si y sólo si* $a = g^{2i-1}$ *para algún entero* i*, donde* g *es un elemento primitivo de* $\mathbb{F}_p$*.*

Demostración. Por la proposición anterior tenemos que si a es un no residuo cuadrático de p entonces para todo entero j tenemos que $a \neq g^{2j}$ en $\mathbb{F}_p$ pero como $\langle g \rangle = \mathbb{F}_p^*$ entonces existe un entero k tal que $a \equiv g^k \pmod{p}$, y como k no es par, entonces $k = 2i - 1$ para algún entero i, es decir $a = g^{2i-1}$.

Por otro lado si $a = g^{2i-1}$ en $\mathbb{F}_p$, con i un entero, tenemos que a no es un residuo cuadrático, pero $(a, p) = 1$ puesto que $a \in \mathbb{F}_p^*$, por lo que a es un residuo no cuadrático de p. □

Observación 4.1. *Si* r *y* s *son residuos no cuadráticos de* p*, entonces existen* i, j *enteros tales que para* g *un elemento primitivo de* $\mathbb{F}_p$, $r = g^{2i-1}$ *y* $s = g^{2j-1}$ *y así* rs *es un residuo cuadrático puesto que* $rs = g^{2i-1}g^{2j-1} = g^{(2i-1)+(2j-1)} = g^{2(i-j-1)}$.

A partir de ahora denotaremos con Q al conjunto de todos los residuos cuadráticos módulo p y con N al conjunto de todos los no residuos cuadráticos módulo p. Así, si g es un elemento primitivo de $\mathbb{F}_p$, tenemos por la Proposición 4.1 y el Corolario 4.1 que

- $Q = \{g^{2i} : i \text{ es un entero}\}$,
- $N = \{g^{2j-1} : j \text{ es un entero}\}$,

además podemos ver que Q es un grupo cíclico generado por g^2 que tiene $\frac{p-1}{2}$ elementos.

Ahora, sea g un elemento primitivo de $\mathbb{F}_p$, tomemos un $l \in Q$ es decir $l = g^{2i}$ entonces tenemos lo siguiente:

i) para todo $q \in Q$, $lq \in Q$ puesto que $q = g^{2j}$ y así $lq = g^{2i}g^{2j} = g^{2(i+j)}$,

ii) para cada $n \in N$, $ln \in N$, esto ya que $n = g^{2k-1}$, luego $ln = g^{2i}g^{2k-1} = g^{2(i+k)-1}$.

Notemos que Q y N son disjuntos y además ambos son cerrados bajo la multiplicación por l.
A partir de ahora, l será un elemento en Q y además un primo.

Definición 4.3. *Las raíces de* $x^n - 1$ *en el campo de descomposición* $\mathbb{F}_{q^s}$ *son llamadas* n*–ésimas raíces de la unidad sobre* $\mathbb{F}_q$*.*

Definición 4.4. *Una* n*–ésima raíz de la unidad sobre* $\mathbb{F}_q$ *que genera el grupo cíclico formado por todas las* n*–ésimas raíces de la unidad es una* n*–ésima raíz de la unidad de orden* n *y es llamada una* n*–ésima raź primitiva de la unidad sobre* $\mathbb{F}_q$

Sea α una raíz p–ésima primitiva de la unidad en algún campo que contenga a $\mathbb{F}_l$. Definimos

$$q(x) = \prod_{r \in Q} (x - \alpha^r) \quad \text{y} \quad n(x) = \prod_{n \in N} (x - \alpha^n)$$

Proposición 4.2. *Los polinomios* $q(x)$ *y* $n(x)$ *tienen coeficientes en* $\mathbb{F}_l$.

Demostración. Notemos que $grad(q(x)) = |Q|$ y $grad(n(x)) = |N|$. Sea $q(x) = a_0 + a_1x + \cdots + a_sx^s$ donde $s = |Q|$ y los $a_i \in E$, con E un campo que contiene a $\mathbb{F}_l$. Elevamos cada coeficiente a_i a la potencia l, donde los a_i son sumas de productos de los α^r con $r \in Q$, y además como en un campo de característica l un primo, $(a+b)^l = a^l + b^l$, entonces

$$a_0^l + a_1^l x + \cdots + a_s^l x^s = \prod_{j\in Q}(x - \alpha^{lj})$$

por otro lado, recordemos que para cada $q \in Q$, $lq \in Q$, así

$$\prod_{j\in Q}(x - \alpha^{lj}) = \prod_{r\in Q}(x - \alpha^r) = q(x)$$

y así, tenemos que

$$a_0^l + a_1^l x + \cdots + a_s^l x^s = a_0 + a_1x + \cdots + a_sx^s$$

lo cual implica que para cada $i = 0, 1, \cdots, s$ $a_i^l = a_i$ y como para cualquier $c \in E$ tal que $c^l = c$, se sigue que $c \in \mathbb{F}_l$ (cf [Wano3]) entonces para cada i se cumple que $a_i \in \mathbb{F}_l$, por lo que $q(x) \in \mathbb{F}_l$.

Por otro lado, sea $n(x) = b_0 + b_1 + \cdots + b_tx^t$ donde $t = |N|$ y cada $b_i \in E$, con E un campo que contiene a $\mathbb{F}_l$, una vez mas elevando cada coeficiente de $n(x)$ a la potencia l, tenemos que

$$b_0^l + b_1^l x + \cdots + b_t^l x^t = \prod_{i\in N}(x - \alpha^{li})$$

esto ya que E es un campo de característica l por lo que $(a+b)^l = a^l + b^l$, como vimos antes para cada $m \in N$, $lm \in N$ por lo que

$$\prod_{i\in N}(x - \alpha^{li}) = \prod_{n\in Q}(x - \alpha^n) = n(x)$$

luego

$$b_0^l + b_1^l x + \cdots + b_t^l x^t = b_0 + b_1x + \cdots + b_tx^t$$

por lo que para cada $j = 0, 1 \ldots, t$, $b_j^l = b_j$ y como para cualquier $c \in E$ tal que $c^l = c$, se sigue que $c \in \mathbb{F}_l$ (cf [Wano3]) entonces para cada j se cumple que $b_j \in \mathbb{F}_l$, por lo que $n(x) \in \mathbb{F}_l$. □

Además notemos que para cada $r \in Q$, $q(\alpha^r) = 0$ y para cada $n \in N$, $n(\alpha^n) = 0$ y ya que α es una $p-$ésima raíz primitiva de la unidad sobre $\mathbb{F}_l$ entonces para cada $r \in Q$ y $n \in N$, tenemos que $(\alpha^r)^p - 1 = 0$ y $(\alpha^n)^p - 1 = 0$ por lo que $q(x)$ y $n(x)$ dividen a $x^p - 1$ y además, $q(x)$ y $n(x)$ son coprimos pues tienen raíces distintas. Por otro lado tenemos que $1^p - 1 = 0$ y 1 no es raíz de $q(x)$ y $n(x)$, por lo que $x - 1$ también divide a $x^p - 1$, y como $q(x)$, $n(x)$ y $x - 1$ tienen en total p raíces distintas de la unidad, entonces se sigue que

$$x^p - 1 = (x-1)q(x)n(x).$$

Sea $\mathcal{R}_p$ el anillo $\dfrac{\mathbb{F}_l[x]}{\langle x^p - 1\rangle}$.

Definición 4.5. *Los códigos de residuos cuadráticos* $\mathcal{Q}$, $\bar{\mathcal{Q}}$, $\mathcal{N}$ *y* $\bar{\mathcal{N}}$ *son códigos cíclicos de* $\mathbb{F}_l^p$, *es decir, son ideales del anillo* $\mathcal{R}_p$ *y sus polinomios generadores son*

$$q(x),\ \ (x-1)q(x),\ \ n(x),\ \ (x-1)n(x)$$

respectivamente. Algunas veces $\mathcal{Q}$ *y* $\mathcal{N}$ *son llamados códigos de residuos cuadráticos aumentados y,* $\bar{\mathcal{Q}}$ *y* $\bar{\mathcal{N}}$ *códigos de residuos cuadráticos reducidos.*

Observación 4.2. *Sea* $J = \langle x^p - 1\rangle$. *Como* $(x-1)q(x) + J \in \langle q(x) + J\rangle$ *entonces* $\bar{\mathcal{Q}} \subseteq \mathcal{Q}$ *y de la misma forma, ya que* $(x-1)n(x) + J \in \langle n(x) + J\rangle$ *entonces* $\bar{\mathcal{N}} \subseteq \mathcal{N}$.

Proposición 4.3. $\mathcal{Q}$ *y* $\mathcal{N}$ *tienen dimensión* $\frac{p+1}{2}$ *y* $\bar{\mathcal{Q}}$ *y* $\bar{\mathcal{N}}$ *tienen dimensión* $\frac{p-1}{2}$

Demostración. Como Q y N son códigos cíclicos, entonces por el inciso iii) del Teorema 2.6 tenemos que las dimensiones de Q y N son $p - grad(q(x))$ y $p - grad(n(x))$ respectivamente, pero el $grad(q(x)) = |Q|$ y $grad(n(x)) = |N|$ y por el Teorema 4.1 sabemos que $|Q| = \frac{p-1}{2} = |N|$, por lo que $p - \frac{p-1}{2} = \frac{2p-p+1}{2} = \frac{p+1}{2}$ y así la dimensión de Q y N es $\frac{p+1}{2}$.

Por otro lado, como $grad(q(x)) = \frac{p-1}{2} = grad(n(x))$ entonces el grado que $(x-1)q(x)$ y $(x-1)n(x)$ es $\frac{p-1}{2} + 1 = \frac{p+1}{2}$, luego, la dimensión de los códigos $\bar{Q}$ y $\bar{N}$ es $p - \frac{p+1}{2} = \frac{p-1}{2}$. □

A continuación se enunciarán algunos resultados que serán de gran utilidad más adelante para exhibir que los códigos Q y N son equivalentes.

Definición 4.6. *Un sistema completo de residuos módulo n es un conjunto de enteros tales que todo entero es congruentes módulo n a exactamente un entero del conjunto.*

El conjunto de enteros $\{0, 1, 2, \ldots, n-1\}$ es un sistema completo de residuos módulo n.

Lema 4.1. *Si $r_1, r_2, \ldots, r_n$ es un sistema completo de residuos módulo n y si a es un entero positivo tal que $(a, n) = 1$, entonces*

$$A = \{ar_1 + b,\ ar_2 + b, \ldots, ar_n + b\}$$

es un sistema completo de residuos módulo n.

Demostración. Sean $ar_i + b, ar_j + b \in A$, supongamos que $i \neq j$. Si $ar_i + b \equiv ar_j + b \pmod{n}$

$$\begin{aligned} &\Rightarrow \quad ar_i \equiv ar_j \pmod{n} \\ &\Rightarrow \quad r_i \equiv r_j \pmod{n} \text{ (ya que } (a, n) = 1) \end{aligned}$$

luego, sea $c \in \mathbb{Z}$ tal que $c \equiv r_i \pmod{n}$, entonces $c \equiv r_j \pmod{n}$, lo cual no puede ser posible puesto que $r_1, r_2 \ldots r_n$ son un sistema completo de residuos módulo n, por lo que $i = j$, así, para cuales quiera dos elementos distinto en A, estos no son congruentes módulo n. Como el conjunto de enteros A consiste de n enteros incongruentes módulo n y tenemos que para cada $i = 1, 2, \ldots, n$, $ar_i + b \equiv r_j \pmod{n}$ para algún $j = 1, 2, \ldots, n$ entonces, sea c un entero, tal que $c \equiv r_k \pmod{n}$ para un único $k \in \{1, 2, \ldots, n\}$ y como $r_k \equiv ar_j + b \pmod{n}$ para algún j, se sigue que $c \equiv ar_j + b \pmod{n}$ y además c es incongruente módulo n a cualquier otro elemento de A, por lo que A es un sistema completo de residuos módulo n. □

Lema 4.2. *Sean m y n dos enteros mayores que 1 y $mcd(m, n) = 1$. Entonces la función*

$$\begin{aligned} \chi_m : \frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle} &\longrightarrow \frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle} \\ a(x) + I &\longmapsto a(x^m) + I \end{aligned}$$

donde $I = \langle x^n - 1\rangle$, es una permutación de $\mathbb{F}_q^n$ cuando identificamos a $\mathbb{F}_q^n$ con $\frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle}$ a través de la función (3).

Demostración. Sea $f(x) = \sum_{i=0}^{n-1} f_i x^i$, tenemos que

$$\begin{aligned} \chi_m(f(x) + I) &= f(x^m) + I \\ &= f(x^m) \pmod{x^n - 1} \\ &= \sum_{i=0}^{n-1} f_i x^{(mi \pmod{n})}. \end{aligned}$$

Como $(m, n) = 1$ y $\{0, 1, 2, \ldots, n-1\}$ es un sistema completo de residuos módulo n, entonces, por el Lema 4.1 tenemos que para cada $i \in \{0, 1, 2, \ldots, n-1\}$, el conjunto

$$A_b = \{im + b : i = 0, 1, \ldots, n-1\}$$

es un sistema completo de residuos módulo n donde b es un entero, de ahí que si $b = 0$, entonces el conjunto

$$A_0 = \{0 \pmod{n}, 1m \pmod{n}, 2m \pmod{n}, \ldots, (p-1)m \pmod{n}\}$$

es un sistema completo de residuos, además, tenemos que para cada $a \in A_0$, $a \equiv i \pmod{n}$ para algún $i \in \{1, 2, \ldots, n\}$ que además es único.

Luego tenemos una permutación, pues a cada $i \in \{1, 2, \ldots, n\}$ lo manda a $mi \pmod{n}$ el cual es congruente módulo n con un único $j \in \{1, 2, \ldots, n\}$, es decir $i \mapsto j$ con $i, j \in \{1, 2, \ldots, n\}$, así, cuando tenemos el coeficiente f_i que acompaña a x^{mi}, tenemos que después de hacer la reducción módulo n, f_i será el coeficiente de x^j, para algún $j \in \{1, 2, \ldots, n\}$. Por lo tanto, χ_m es una permutación. □

Teorema 4.2. *Los códigos de residuos cuadráticos Q y N son equivalentes.*

Demostración. Por definición, $Q = \langle q(x) + J \rangle$ y $N = \langle n(x) + J \rangle$, donde $J = \langle x^p - 1 \rangle$. Escogemos un residuo no cuadrático, m, módulo p y consideramos la función

$$\begin{aligned} \chi_m : \frac{\mathbb{F}_l[x]}{\langle x^p - 1 \rangle} &\longrightarrow \frac{\mathbb{F}_l[x]}{\langle x^p - 1 \rangle} \\ a(x) + J &\longmapsto a(x^m) + J \end{aligned}$$

Como $(m, p) = 1$ entonces por el lema anterior tenemos que χ_m es una permutación, por lo que $\chi_m(Q)$ es un código equivalente de Q, esto por la Definición 2.5. Veamos que $\chi_m(Q) = N$. Probemos que $\chi_m(Q) \subseteq N$, para ello mostraremos que $\chi_m(q(x) + J) \in N$, es decir, que $n(x) = \prod_{t \in N} (x - \alpha^t)$ es un divisor de $\chi_m(q(x) + J) = \prod_{r \in Q} (x^m - \alpha^r)$ en $\mathcal{R}_p$.

Sea t un no residuo cuadrático, tenemos que por la Observación 4.1, tm es un no residuo cuadrático módulo p, por lo que α^{tm} es un raíz del polinomio $q(x)$ y así

$$0 = q(\alpha^{tm}) = q((\alpha^t)^m) = \chi_m(q(\alpha^t))$$

pero esto se cumple para cualquier $t \in N$, por lo que $n(x)$ es un divisor de $\chi_m(q(x))$ pues para cada $t \in N$, $n(\alpha^t) = 0$ y $n(x)$ no tiene raíces multiples, luego $\chi_m(q(x) + J) \in \langle n(x) + J \rangle = N$ y así $\chi_m(Q) \subseteq N$.

Por otro lado, como $|Q| = |\chi_m(Q)|$, donde $|Q| = l^{\frac{p+1}{2}}$ y además $|N| = l^{\frac{p+1}{2}}$ entonces $|\chi_m(Q)| = |N|$, por lo que $\chi_m(Q) = N$ y por lo tanto Q y N son equivalentes. □

Ejemplo 4.4. *Tomemos $p = 7$, del Ejemplo 4.1, se tiene que $Q = \{1, 2, 4\}$ y $N = \{3, 5, 6\}$, luego, tomamos $l \in Q$, y como l debe ser un primo, consideremos $l = 2$. Sea $\alpha \in \mathbb{F}_{2^3}$, con α una raíz primitiva 7−ésima de la unidad, tal que $\alpha^3 + \alpha + 1 = 0$, es decir α satisface al polinomio primitivo de grado 3, $x^3 + x + 1$, tenemos que $\alpha^3 = \alpha + 1$ y así teniendo presente que estamos trabajando sobre $\mathbb{F}_2$:*

$$\begin{array}{lllll} \alpha^4 = \alpha(1+\alpha) = \alpha + \alpha^2 & & & & \\ \alpha^5 = \alpha(\alpha+\alpha^2) = \alpha^2 + \alpha^3 & = & \alpha^2 + \alpha + 1 & & \\ \alpha^6 = \alpha(\alpha^2+\alpha+1) = \alpha + \alpha^2 + \alpha^3 & = & \alpha^2 + 1 & & \\ \alpha^7 = \alpha(\alpha^2+1) = \alpha^3 + \alpha & = & 1 & & \end{array}$$

ahora bien, hallemos los polinomios generadores de Q y N. Tenemos que

$$q(x) = \prod_{r \in Q} (x - \alpha^r) \text{ y } n(x) = \prod_{n \in N} (x - \alpha^n)$$

así,

$$q(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4) \text{ y } n(x) = (x - \alpha^3)(x - \alpha^5)(x - \alpha^6)$$

luego, desarrollando los productos y haciendo uso de las relaciones previas se sigue que

$$q(x) = x^3 + x + 1 \text{ y } n(x) = x^3 + x^2 + 1$$

luego, por el Ejemplo 2.2, podemos ver que el $[7, 4, 3]$-código lineal de Hamming es un código de residuos cuadráticos, y es equivalente al código Q. Nótese que si tomamos una raíz primitiva 7−ésima de la unidad distinta, $q(x)$ y $n(x)$ se intercambian, para ver esto, consideremos $\beta \in \mathbb{F}_{2^3}$, tal que β es una raíz primitiva 7−ésima de la unidad, y $\beta^3 + \beta^2 + 1 = 0$, luego $\beta^3 = \beta^2 + 1$ sobre $\mathbb{F}_2$, así

$$\begin{array}{lllll} \beta^4 = \beta(\beta^2+1) = \beta^3 + \beta & = & \beta^2 + \beta + 1 & & \\ \beta^5 = \beta(\beta^2+\beta+1) = \beta^3 + \beta^2 + \beta & = & \beta + 1 & & \\ \beta^6 = \beta(\beta+1) = \beta^2 + \beta & & & & \\ \beta^7 = \beta(\beta^2+\beta) = \beta^3 + \beta^2 & = & 1 & & \end{array}$$

por lo que

$$q(x) = \prod_{r \in Q} (x - \beta^r) = (x-\beta)(x-\beta^2)(x-\beta^4) = x^3 + x^2 + 1$$

y

$$n(x) = \prod_{n \in N} (x - \beta^n) = (x-\beta^3)(x-\beta^5)(x-\beta^6) = x^3 + x + 1$$

en efecto, se puede ver que cuando escogemos una raíz primitiva distinta los códigos se intercambian, pero por el Teorema 4.2 sabemos que Q y N son equivalentes.

En el siguiente ejemplo se habla sobre los dos códigos de Golay, dos códigos muy importantes, con propiedades muy interesantes, estos códigos son el $[23, 12, 7]$—código binario $\mathcal{G}_{23}$ y el $[11, 6, 5]$—código ternario $\mathcal{G}_{11}$

Ejemplo 4.5. *Los códigos $\mathcal{G}_{23}$ y $\mathcal{G}_{11}$ son códigos de residuos cuadráticos. Para $\mathcal{G}_{23}$ tenemos $p = 23$ y $l = 2$, donde, en efecto l es un residuo cuadrático módulo 23, puesto que $5^2 \equiv 2 \pmod{23}$, ahora, si nosotros tomamos una raíz primitiva 23—ésima de la unidad en alguna extensión de $\mathbb{F}_2$ podemos obtener alguno de los código de residuos cuadráticos, Q ó N, y haciendo los cálculos pertinentes se llega a que*

$$q(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1 \text{ y } n(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$$

y estos son divisores de $x^{23} - 1$, pues

$$x^{23} - 1 = (x-1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1).$$

Ahora bien, cuando consideramos al código $\mathcal{G}_{11}$, tenemos que $p = 11$ y por el Ejemplo 4.2 se sigue que, 3 es un residuo cuadrático módulo 11, así que tomando una raíz primitiva 11—ésima de la unidad en alguna extensión de $\mathbb{F}_3$, se obtienen los códigos de residuos cuadráticos Q y N, con generadores

$$q(x) = x^5 + x^4 - x^3 + x^2 - 1 \text{ y } n(x) = x^5 - x^3 + x^2 - x - 1$$

en efecto,

$$x^{11} - 1 = (x-1)(x^5 + x^4 - x^3 + x^2 - 1)(x^5 - x^3 + x^2 - x - 1).$$

Teorema 4.3. *Si d es la distancia mínima de $\mathcal{C}$ o N, entonces $d^2 \geqslant p$. Más aún si $p = 4k - 1$, entonces*

$$d^2 - d + 1 \geqslant p$$

Demostración. Sea $a(x) + J$ una palabra código de peso mínimo distinto de cero, d, en $\mathcal{C}$. Si n es un residuo no cuadrático, entonces $\chi_n(a(x) + J) = a(x^n) + J$ es una palabra código de peso mínimo en n, esto ya que los coeficientes distintos de cero de $a(x)$ seguirán siendo distintos de cero en $a(x^n)$, luego $(a(x) + J)(a(x^n) + J) \in \mathcal{C} \cap N$, es decir, es múltiplo de

$$\prod_{r \in Q} (x - \alpha^r) \prod_{n \in N} (x - \alpha^n) = \prod_{i=1}^{p-1} (x - \alpha^i)$$

puesto que Q y N son disjuntos y $Q \cup N$ son todos los enteros distintos de cero en $\mathbb{F}_p$, luego como $x^p - 1 = (x-1)q(x)n(x)$, entonces $x - 1$ divide a $x^p - 1$ y al hacer esta división nosotros tenemos que $x^p - 1 = (x-1)(\sum_{i=0}^{p-1} x^i)$, por lo que $n(x)q(x) = \sum_{i=0}^{p-1} x^i$ y así

$$\prod_{i=1}^{p-1} (x - \alpha^i) = \sum_{j=0}^{p-1} x^j$$

por lo que cualquier elemento de $\mathcal{C} \cap N$ tiene p coeficientes distintos de cero, y así, $(a(x) + J)(a(x^n) + J)$ tiene peso p. Como $a(x) + J$ tiene peso d, es decir, el polinomio $a(x)$ tiene d coeficientes distintos de cero, entonces $(a(x) + J)(a(x^n) + J)$ tiene a lo más, d^2 coeficientes distintos de cero, por lo que $d^2 \geqslant p$.

Si $p = 4k-1$, podemos ver a p como $p = 4(k-1)+4-1 = 4k_1+3$, y tenemos una propiedad que nos dice que si $p = 4m+3$ entonces -1 es un residuo no cuadrático módulo p (cf [MA78, Cap. 2]), luego tomemos $n = -1$, y sea $a(x) = a_0 + a_1x + \cdots + a_sx^s$ donde d coeficientes de $a(x)$ son distintos de cero, entonces $a(x^{-1}) = a_0 + a_1x^{-1} + \cdots + a_sx^{-s}$, donde d coeficientes son distintos de cero, notemos que al realizar el producto $a(x)a(x^{-1})$, tenemos lo siguiente $a_ix^ia_ix^{-i} = a_i^2x^0 = a_i^2$, esto para cada $i \in \{0,1,2,\ldots,s\}$ tal que $a_i \neq 0$ y como d coeficientes son distintos de cero entonces tendremos al menos d productos de la forma a_i^2 distintos de cero, que sumarlos, serán un elemento en $\mathbb{F}_l$, por lo que tendremos a lo más d^2-d+1 coeficientes distintos de cero en el producto $a(x)a(x^{-1})$, y como $a(x)a(x^{-1})+J \in \mathcal{C} \cap \mathcal{N}$ entonces $d^2-d+1 \geqslant p$. □

Con esto se termina una breve exposición de los códigos de residuos cuadráticos sobre campos finitos.

CONCLUSIONES

Se han estudiado los códigos cíclicos sobre campos finitos y sobre el anillo de Galois $\mathbb{Z}_4$, y a simple vista se puede ver que las diferencias son muchas y el trato que se le da a cada uno difiere por las propiedades que tienen los campos finitos y el anillo $\mathbb{Z}_4$, una de las diferencias más relevante es la forma en como son generados, pues bien, mientras que en los códigos cíclicos sobre campos finitos el polinomio generador es un divisor de $x^n - 1$, en los códigos cíclicos sobre $\mathbb{Z}_4$ el código no necesarimante es generado por un único polinomio, de manera general, el código es una suma directa de dos $\mathbb{Z}_4-$submódulos; otra gran diferencia es la estructura del código dual el cuál, cuando hablamos de códigos cíclicos sobre $\mathbb{Z}_4$, goza de unas propiedades muy peculiares, desde la forma en que este es generado hasta el generador idempotente que este puede poseer. En fin, ambos tipos de códigos son interesantes por su estructura, pero los códigos cíclicos sobre $\mathbb{Z}_4$ requieren de un cuidado mayor al ser estudiados. Y finalmente se abordaron las principales características de los códigos de residuos cuadráticos, notamos que dichos códigos se vuelven especiales por su construcción, la cual requiere de conocimiento sobre la teoría de números y sobre propiedades importantes de campos finitos.

BIBLIOGRAFÍA

[AM69] M. F. Atiyah and I. G. MacDonal, *Introduction to commutative algebra*, first edition ed., Addison-Wesley Publishing Company, Inc., 1969.

[CS95] A. R. Calderbank and N. J. A. Sloane, *Modular and p-adic cyclic codes*, Des., Codes and Cryptogr. **6** (1995), 21–35.

[DF04] D. S. Dummit and R. M. Foote, *Abstract algebra*, third edition ed., John Wiley and Sons, Inc., 2004.

[DLP04] H. Q. Dinh and S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory **50** (2004), no. 8, 1728–1744.

[GS99] M. Greferath and S. E. Schmidt, *Gray isometries for finite chain rings and a nonlinear ternary* $(36, 3^{12}, 15)$ *code*, IEEE Trans. Inform. Theory **45** (1999), 2522–2524.

[HP03] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003.

[Hun74] T. W. Hungerford, *Algebra*, Springer-Verlag, 1974.

[JKC+94] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of kerdock, preparata, goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319.

[Kas82] F. Kasch, *Modules and rings*, Academic Press., 1982.

[KLP97] P. Kanwar and S. R. López-Permouth, *Cyclic codes over the integers modulo* p^m, Finite Fields and Their Applications 3 (1997), no. 4, 334–352.

[LA14] C. A. López-Andrade, *Matemáticas y sus aplicaciones 4*, primera ed., ch. 1, pp. 5–33, Textos Científicos, Fomento Editorial de la Benemérita Universidad Autónoma de Puebla, México, 2014.

[LATR11] Carlos Alberto López-Andrade and Horacio Tapia-Recillas, *On the linearity and quasi-cyclicity of the gray image of codes over a galois ring*, Groups, Algebras and Applications, vol. CONM/537, AMS, 2011, pp. 255–268.

[LB02] S. Ling and J. T. Blackford, $\mathbb{Z}_{p^{k+1}}$*-linear codes*, IEEE Trans. Inform. Theory **48** (2002), no. 9, 2592–2605.

[MA78] F. J. MacWilliams and N. J. A.Sloane, *The theory of error-correcting codes*, The Netherlands: North Holland, 1978.

[McD74] B. R. McDonald, *Finite rings with identity*, Marcel Dekker Inc., 1974.

[McE04] R. J. McEliece, *The theory of information and coding*, second ed., Cambridge University Press, 2004.

[Ple89] V. Pless, *Introduction to the theory of error-correcting codes*, Wiley-Interscience, 1989.

[PQ96] V. S. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over* $\mathbb{Z}_4$, IEEE Trans. Inform. Theory **42** (1996), no. 5, 1594–1600.

[Ram17] A. R. García Ramírez, *Anillos de galois*, Tesis de Licenciatura, Benemérita Universidad Autónoma de Puebla, 2017.

[Rom92] S. Roman, *Coding and information theory*, first ed., Springer-Verlag, 1992.

[Rot03] J. J. Rotman, *Advanced modern algebra*, 2nd printing ed., Prentice Hall., 2003.

[Wan97] Z.-X. Wan, *Quaternary codes*, World Scientific Publishing Co. Pte. Ltd., 1997.

[Wan03] ———, *Lectures on finite fields and galois rings*, World Scientific Pub. Co. Inc., 2003.

[Wis91] R. Wisbauer, *Foundations of module and ring theory: A handbook for study and research*, first ed., Gordon and Breach Science Publishers Reading, 1991.

ÍNDICE ALFABÉTICO