UNIVERSIDAD AUTÓNOMA METROPOLITANA
Casa abierta al tiempo
Unidad Iztapalapa

"Códigos constacíclicos sobre el anillo de Frobenius no de cadena $\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$ "

Tesis que presenta:

Juan Armando Velazco Velazco

Matrícula: 2193801760, correo-e: oczalevaj@gmail.com

Para obtener el grado de
Doctor en Ciencias (Matemáticas)

Asesor de tesis: Dr. Horacio Tapia Recillas

Sinodales:

Presidente: Doctor Horacio Tapia Recillas

Secretario: Doctor Mario Pineda Ruelas

Vocal: Doctor Manuel González Sarabia

Vocal: Doctor José Noé Gutierrez Herrera

Vocal: Doctor Eliseo Sarmiento Rosales

División de Ciencias Básicas e Ingeniería

Ciudad de México, 5 de agosto de 2024

A mi madre y a mi abuela, por su enorme cariño, su constante esfuerzo y sus muchas enseñanzas

Resumen

Una clase importante de códigos lineales son los códigos γ-constacíclicos definidos sobre un anillo, donde γ es una unidad en el alfabeto del código. Los códigos constacíclicos son una generalización de los códigos cíclicos y han despertado el interés de algunos grupos de investigación. En el presente trabajo, dado un número primo p y un entero $n > 0$ no divisible por p, se describen códigos γ-constacíclicos de longitud n definidos sobre el anillo de Frobenius finito, local, conmutativo, con identidad y no de cadena $\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$, donde $u^2 = 0$ y $k > 1$. La descripción algebraica que se propone de estos códigos se da a partir del Teorema Chino del Residuo y la teoría de elementos idempotentes, motivo por el cual se pide que p y n sean primos relativos, $\text{mcd}(p, n) = 1$, para tener así una condición de separabilidad que será útil en el estudio de la familia de ideales del anillo cociente,

$$\mathcal{R}_k[x]/\langle x^n - \gamma \rangle, \text{ con } \gamma \text{ una unidad del anillo } \mathcal{R}_k.$$

Se presentan en este trabajo, resultados que podría ser posible extender a otros anillos con propiedades algebraicas similares, de cadena o no de cadena, para estudiar códigos cíclicos y constacíclicos sobre dichos anillos a partir de esta propuesta de descripción de los mismos. También son presentados ejemplos de aplicación del trabajo desarrollado, para algunos valores específicos de p y k.

Agradecimientos

La presente tesis ha sido producto no sólo de mi esfuerzo, sino también del de mi familia, a la cual agradezco profundamente por su apoyo incondicional en todo momento; en especial a mi madre, es ella la primer persona a quién quiero agradecer.

En lo que respecta a lo académico, agradezco en primer lugar al doctor Horacio Tapia Recillas, por mostrarme que la dedicación y esfuerzo rinden frutos. Su disciplina y entrega para con el trabajo matemático han sido fundamentales para llevar a cabo este proyecto. Gracias, doctor. También quiero dar mi agradecimiento a la doctora Shirley Bromberg Silverstein (UAM - I) y a los doctores Mario Pineda Ruelas (UAM - I) y Rafael del Río Castillo (IIMAS-UNAM); profesores que me transmitieron saberes y puntos de vista que me dieron, y permitieron, el gusto por la investigación matemática. Sus enseñanzas las llevo presentes en mi día a día.

Deseo aprovechar este espacio para mencionar a esas personas que se han mantenido cerca de mí a lo largo de todos estos años, apoyándome de diversas formas, pero en particular, con su invaluable amistad y cariño: querida Rossy, mis estimados Mike Huerta, Marcos, (mi buen) Luis, Gustavo (¡primo!), Fer, Félix (dondequiera que estés, amigo), Felipe, Cando y Bart: gracias amigos, por acompañarme en este bello, aunque también duro camino que es el aprender algo de matemáticas.

Finalmente, doy gracias al Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCYT), por el apoyo número 764803 que me fue otorgado para llevar a cabo mis estudios de doctorado.

Índice general

Introducción

La teoría de códigos detectores-correctores de errores se inicia formalmente con los trabajos "A Mathematical Theory of Communication"de Claude E. Shannon, (1948) y "Error Detecting and Error Correcting Codes"de Richard W. Hamming (1950). A grandes rasgos, el objetivo principal de la teoría es el estudio y elaboración de métodos para la transmisión y almacenamiento confiable y eficiente de información en medios susceptibles de presentar ruido. Denotando por E al emisor, R al receptor, de manera esquemática tenemos,

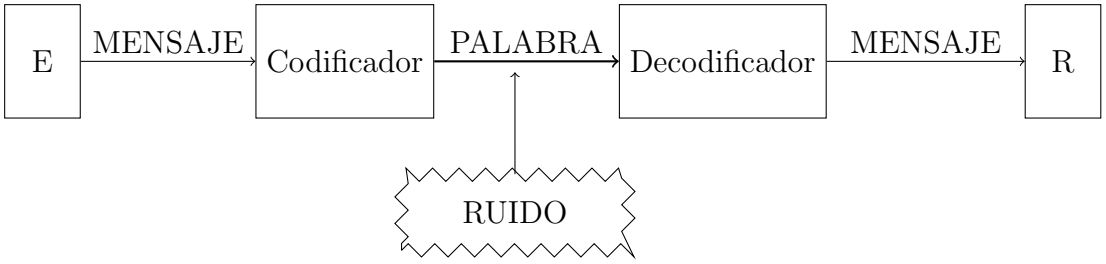


Figura 1: Problema fundamental de la teoría de códigos detectores-correctores de errores

Hoy en día, desde el punto de vista matemático, la investigación de la teoría de códigos se realiza mediante una fuerte interrelación entre varias áreas de las matemáticas, como lo son el álgebra, la teoría de números, las matemáticas discretas, la combinatoria y teoría de diseños, la geometría, la geometría algebraica y la probabilidad sólo por mencionar las ramas más conocidas. Desde el punto de vista de las aplicaciones, el estudio de códigos de diversa naturaleza, en particular los lineales, tiene un impacto directo en nuestro día a día con las implementaciones realizadas desde varios campos de la ingeniería para el manejo y transmisión de volúmenes de información, así como su procesamiento: comunicaciones satelitales e inalámbricas, telefonía celular y difusión (*broadcasting*) así como diversos dispositivos de almacenamiento son algunos contextos en los que la teoría de códigos tiene aplicaciones.

Existen varios tipos de códigos. Los más estudiados han sido los códigos lineales definidos sobre campos finitos $\mathbb{F}_q$, ya que ocupan un lugar preponderante en las aplicaciones. Usados para resolver problemas de ingeniería, se ha dado su descripción algebraica como subespacios vectoriales de un $\mathbb{F}_q$-espacio vectorial, donde $\mathbb{F}_q$ es un campo finito de $q = p^m$ elementos, p un primo y $m > 0$ un entero. Dada la naturaleza electrónica de la transmisión y almacenamiento de la información, los primeros modelos de estudio involucraron

sucesiones de ceros y unos; por ello, los matemáticos usaron y desarrollaron métodos algebraicos sobre el alfabeto de los números binarios, el campo finito $\mathbb{F}_2$, para estudiar a los códigos y, posteriormente, extendieron esa teoría a casos en los que el alfabeto es algún campo finito $\mathbb{F}_q$ arbitrario.

En la segunda mitad del siglo XX, en la década de los 70, se publicaron un par de artículos de I. Blake, [1] y [2], en los que el alfabeto para representar a la información es cambiado por un anillo finito, conmutativo con identidad y, casi veinte años después, se publican los trabajos de A. Hammons, V. Kummar, A. Calderbank et al, ([3]), V. Pless y Z. Qian ([4]) y J. Wood ([5]) que dan lugar a una intensa investigación sobre códigos que tienen como alfabeto anillos finitos, profundizando las técnicas de la teoría algebraica de códigos o teoría de códigos algebraicos, considerada ya una rama de las matemáticas puras ([6]).

En los últimos 20 años se ha desarrollado mucha investigación sobre códigos lineales cuyo alfabeto sea un anillo de Frobenius finito, conmutativo con identidad. Tales investigaciones han girado en torno a la descripción de códigos cíclicos, y sus generalizaciones, definidos sobre anillos de Frobenius finitos de cadena (ver, por ejemplo, [7], [8]). En los últimos años se ha despertado el interés de varios grupos de investigación por la descripción de códigos cíclicos y constacíclicos definidos sobre anillos finitos de Frobenius, no de cadena, conmutativos con identidad, como lo son trabajos presentados en [9], [10] y, en particular en nuestro país el llevado a cabo, por ejemplo, por [11]. Cabe mencionar, que el inicio del estudio de códigos constacíclicos se dio a partir de investigaciones realizadas sobre códigos negacíclicos llevados a cabo por E. Berlekamp en 1966 ([12]), definiendo éstos códigos sobre campos finitos, y el de J. Wolfmann en 1999 ([13]) quién los definió sobre el anillo $\mathbb{Z}_4$.

El presente trabajo de investigación, versa sobre la descripción de códigos lineales de tipo constacíclico con las siguientes características: dado un número primo p y una longitud n no divisible por p, se estudian códigos constacíclicos definidos sobre el anillo de Frobenius finito, local, conmutativo, con identidad, no de cadena

$$\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$$

donde se satisface que $u^2 = 0$ y $\mathbb{Z}_{p^k}$ es el anillo de enteros modulo p^k. Es importante hacer mención de que la investigación en sus inicios partió del estudio de códigos cíclicos para el caso en el que $p = 2$, es decir, el alfabeto era $\mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$, con la longitud de tales códigos impar (ver [14] y [15]). Se observó que los resultados obtenidos podían extenderse para un p arbitrario y en el contexto de códigos constacíclicos. Del trabajo [15]) y lo desarrollado en la presente tesis se da el apéndice B, en el cuál se obtienen los códigos cíclicos de longitud $n = 7$ para el anillo $\mathcal{R}_2 = \mathbb{Z}_4 + u\mathbb{Z}_4$. Investigaciones relacionadas y previas llevadas a cabo por otros grupos de investigación, con un enfoque centrado en códigos lineales y cíclicos de longitud n impar sobre el anillo $\mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$, antecediendo el presente trabajo, son los artículos de B. Yildiz y S. Karadeniz ([9]), B. Yildiz y N. Aydin ([16]) así como el realizado por R. Bandi y M. Bhaintwal ([17]). Nótese también que en J. Gao, F. Fu et al ([18]), se presentó una descripción de códigos cíclicos de longitud n sobre el anillo $\mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$, $u^2 = 0$, donde p y n son primos relativos.

Nuestro punto de vista al realizar el presente estudio difiere de los trabajos mencionados al final del párrafo anterior: la metodología usada en la presente investigación fue partir de las propiedades algebraicas del anillo finito $\mathcal{R}_k$, con particular énfasis en su conjunto de ideales, a partir de lo cual se estudian a los códigos constacíclicos de longitud n, con n y p primos relativos, y que, desde el punto de vista algebraico, son ideales del anillo cociente

$$\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - \gamma \rangle, \gamma \in \mathcal{U}(\mathcal{R}_k),$$

donde $\mathcal{U}(\mathcal{R}_k)$ denota al grupo de unidades de $\mathcal{R}_k$. Una vez obtenida una descripción de estos códigos constacíclicos, se procede a ampliarla a partir de elementos idempotentes del anillo $\mathcal{R}_{k,n}$.

El manuscrito está organizado de la siguiente manera: en el Capítulo 1 se presentan las definiciones, conceptos y resultados matemáticos necesarios para el desarrollo del presente estudio, así como el contexto necesario de la teoría de códigos lineales sobre anillos finitos en el que se desarrolla la investigación. En el Capítulo 2 se hace un estudio de la estructura del anillo $\mathcal{R}_k$, su conjunto de ideales, así como sus propiedades algebraicas. El Capítulo 3 es la parte central de la presente tesis. En ese capítulo se muestra un estudio de la estructura algebraica de códigos constacíclicos definidos sobre el anillo $\mathcal{R}_k$ usando de forma combinada el Teorema Chino del Residuo y la teoría de elementos idempotentes, en nuestro contexto, el cuál es el de los anillos finitos, locales, conmutativos y con identidad.

Capítulo 1

Preliminares

En el presente capítulo se dan definiciones, conceptos y resultados generales de la teoría de códigos, del álgebra conmutativa y teoría de anillos necesarios para llevar a cabo nuestra investigación. Las principales referencias son [19] o [20] para aspectos generales sobre álgebra conmutativa usados en el presente trabajo. Para los tópicos relacionados específicamente con anillos finitos, el lector puede consultar [21] o [22]. Para profundizar en los temas relacionados con la teoría de códigos se recomienda [23] y, desde luego, el texto clásico [24] para códigos lineales y cíclicos sobre campos finitos. En particular, para códigos lineales definidos sobre anillos finitos de Frobenius, el lector podría consultar el relativamente reciente texto [6].

1.1. Anillos locales finitos de Frobenius

Por un anillo $(\mathcal{R}, +, \cdot)$, denotado sólo por $\mathcal{R}$, entenderemos siempre anillo conmutativo con identidad, $1 \in \mathcal{R}$, a menos que se indique otra cosa. Si I es un ideal de un anillo $\mathcal{R}$, la conmutatividad nos asegura que todos los ideales son bilaterales.

Definición. Un anillo $\mathcal{R}$ conmutativo con un único ideal máximo $\mathfrak{m}$ se dice que es **local**. El anillo cociente $\mathcal{R}/\mathfrak{m}$ es el **campo residual** de $\mathcal{R}$. Toda esta información estará abreviada en la terna $(\mathcal{R}, \mathfrak{m}, \mathcal{R}/\mathfrak{m})$. Si $\mathcal{R}$ es finito, tenemos que $\mathcal{R}/\mathfrak{m} = \mathbb{F}_q$ es un campo finito, con $q = p^m$ para p un primo y $m > 0$. En tal caso escribiremos la terna $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_q)$ para indicarlo.

Dado un conjunto no vacío $S \subseteq \mathcal{R}$, el **ideal generado** por S, denotado $\langle S \rangle$, está dado por $\langle S \rangle = \{\sum_{i=1}^{m} r_i s_i \mid r_i \in \mathcal{R}, s_i \in S, m \in \mathbb{N}\}$. En el caso en que $S = \{s_1, s_2, \ldots, s_n\}$, es decir si S es finito, escribiremos $\langle S \rangle = \langle s_1, s_2, \ldots, s_n \rangle$.

Definición. Sea $\mathcal{R}$ un anillo.

- Sea $\mathcal{L}$ el conjunto de ideales de $\mathcal{R}$ y considere la relación de orden $\preceq$ en $\mathcal{L}$ inducida por la inclusión de conjuntos. Si $(\mathcal{L}, \preceq)$ es un orden total se dirá que el anillo es **de cadena**. Diremos que $\mathcal{R}$ es **no de cadena** si $(\mathcal{L}, \preceq)$ no es un orden total.

- Si $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_q)$ es finito y local, existe un entero $t \geq 1$ tal que $\mathfrak{m}^t = \langle 0 \rangle$ y $\mathfrak{m}^{t-1} \neq \langle 0 \rangle$. Tal t recibe el nombre de **índice de nilpotencia** del ideal $\mathfrak{m}$.

El anillo de polinomios en la indeterminada x con coeficientes en $\mathcal{R}$ es denotado por $\mathcal{R}[x]$. Dado un anillo local $(\mathcal{R}, \mathfrak{m}, \mathcal{R}/\mathfrak{m})$ tenemos el mapeo o **función reducción módulo** $\mathfrak{m}$ $\bar{}$: $\mathcal{R} \longrightarrow \mathcal{R}/\mathfrak{m}$ dada por $\overline{r} = r + \mathfrak{m}$. Tal función $\bar{}$ se extiende de manera natural a $\mathcal{R}[x] \longrightarrow (\mathcal{R}/\mathfrak{m})[x]$ haciendo $f(x) \mapsto \overline{f}(x)$ donde $\overline{f}(x) = \overline{a}_0 + \overline{a}_1 x + \ldots + \overline{a}_{n-1} x^{n-1}$. Escribiremos $f \in \mathcal{R}[x]$ en lugar de $f(x)$ a menos que el contexto no sea claro.

Definición. Sea $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_q)$ un anillo finito, local, conmutativo con identidad. Sean $f, g \in \mathcal{R}[x]$.

(1) $f \in \mathcal{R}[x]$ es **regular** si no es un divisor de cero en $\mathcal{R}[x]$.

(2) Se dirá que $f \in \mathcal{R}[x]$ es **básico irreducible** si $\overline{f}$ es irreducible en $\mathbb{F}_q[x]$.

(3) f y g son **primos relativos** (o **coprimos**) si $\langle f \rangle + \langle g \rangle = \mathcal{R}[x]$.

(4) Un polinomio f es primario si el ideal generado por él, $\langle f \rangle \neq \langle 1 \rangle$, es primario, esto es, $gh \in \langle f \rangle$ implica que $g \in \langle f \rangle$ o $h^m \in \langle f \rangle$ para algún $m > 0$.

Recordemos que, dados f y g polinomios en $\mathcal{R}[x]$, se dice que f es un **divisor** de g si $\langle g \rangle \subseteq \langle f \rangle$; y que f será un **divisor propio** de g si se tiene la inclusión propia $\langle g \rangle \subset \langle f \rangle$. En particular, para $g \in \mathcal{R}[x]$ regular, se tiene la equivalencia siguiente: f es divisor propio de g en $\mathcal{R}[x]$ si y sólo si $\overline{f}$ es divisor propio de $\overline{g}$ en $(\mathcal{R}/\mathfrak{m})[x]$.

El lema de Hensel generalizado, que se enuncia a continuación, garantiza que dada una factorización como producto de polinomios primos relativos por pares sobre $\mathbb{F}_q[x]$ esta se levanta como una factorización de polinomios primos relativos por pares sobre $\mathcal{R}[x]$, con $\mathcal{R}$ un anillo local.

Teorema 1.1. *[Lema de Hensel, [21], XIII.4] Sea $f \in \mathcal{R}[x]$, con $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_q)$ anillo finito, local, conmutativo con identidad; tal que*

$$\overline{f} = \overline{g}_1 \overline{g}_2 \cdots \overline{g}_m \in \mathbb{F}_q[x],$$

donde $\overline{g}_1, \ldots, \overline{g}_m$ son primos relativos por pares. Entonces, existen $g_1, g_2, \ldots, g_m \in \mathcal{R}[x]$ tales que

(a) $g_1, g_2, \ldots, g_m$ son primos relativos por pares,

(b) $g_i + \mathfrak{m} = \overline{g}_i$, $1 \leq i \leq m$;

(c) $f = g_1 g_2 \cdots g_m$.

Con respecto a los polinomios regulares sobre un anillo finito $(\mathcal{R}, \mathfrak{m}, \mathcal{R}/\mathfrak{m})$ local y su factorización, serán necesarios los siguientes resultados.

Teorema 1.2. *[Teorema XIII.7, [21]] Sea $f \in \mathcal{R}[x]$ un polinomio regular, con $(\mathcal{R}, \mathfrak{m}, \mathcal{R}/\mathfrak{m})$ local y finito. Se cumple lo siguiente:*

(i) Si $\overline{f}$ es irreducible, entonces f es irreducible.

(ii) Si f es irreducible, entonces $\overline{f} = \delta g^l$, donde $\delta \in \mathcal{R}/\mathfrak{m} \setminus \{0\}$, $l > 0$ entero y $g \in (\mathcal{R}/\mathfrak{m})[x]$ es mónico irreducible.

(iii) Si $\overline{f}$ tiene raíces distintas en la cerradura algebraica de $\mathcal{R}/\mathfrak{m}$, entonces f es irreducible si y sólo si $\overline{f}$ es irreducible.

Demostración. Para el apartado (i), suponga que $f \in \mathcal{R}[x]$ no es irreducible, entonces, sin pérdida de generalidad, asuma que $f = gh$ para ciertos $f, g \in \mathcal{R}[x]$ y por lo tanto $\overline{f} = \overline{g}\overline{h}$, de donde $\overline{g}$ ó $\overline{h}$ es una unidad. Suponga que $\overline{g}$ es una unidad, es decir, $\overline{g} \in \mathcal{R}/\mathfrak{m} \setminus \{0\}$. Dado que $g = a_0 + a_1x + \ldots + a_mx^m \in \mathcal{R}[x]$, se tiene entonces que $\overline{g} = \overline{a}_0$ y por lo tanto $g = a_0 + r(x)$ con $r(x)$ nilpotente y $a_0 \in \mathcal{U}(\mathcal{R})$, es decir, g es una unidad en $\mathcal{R}[x]$. Para probar (ii), suponga que $\overline{f} = \delta \prod_{i=1}^m g_i^{l_i}$, con $\delta \in \mathcal{R}/\mathfrak{m} \setminus \{0\}$ y los g_i polinomios mónicos, irreducibles y coprimos por pares. Por el Lema de Hensel, Teorema 1.1, y de la irreducibilidad de f en $\mathcal{R}[x]$ se deduce que $m = 1$ y por lo tanto es posible escribir $\delta \prod_{i=1}^m g_i^{l_i} = \delta g^l$. La parte (iii) es una consecuencia de (i) y (ii), con las hipótesis dadas.□

La demostración del siguiente resultado viene dada en [21].

Teorema 1.3. *(Teorema XIII.11, [21]) Sea $f \in \mathcal{R}[x]$ un polinomio regular, con $(\mathcal{R}, \mathfrak{m}, \mathcal{R}/\mathfrak{m})$ anillo finito y local. Entonces,*

(i) $f = \delta \prod_{i=1}^m g_i$, con $\delta \in \mathcal{U}(\mathcal{R}[x])$ y $g_i \in \mathcal{R}[x]$ polinomios regulares, primarios y primos relativos por pares.

(ii) Si $f = \delta \prod_{i=1}^l g_i = \beta \prod_{i=1}^m h_i$, con $\delta, \beta \in \mathcal{U}(\mathcal{R})$ y con g_i, $i = 1, \ldots, l$; h_j, $j = 1, \ldots, m$ son polinomios primarios, primos relativos por pares, entonces $m = n$ y, después de un reordenamiento de índices, $\langle g_i \rangle = \langle h_i \rangle$, $1 \leq i \leq m$.

Dado un ideal I de un anillo $\mathcal{R}$, no es difícil comprobar que dado el conjunto

$$I[x] = \{f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathcal{R}[x] \mid a_i \in I\},$$

este es un ideal de $\mathcal{R}[x]$.

Definición. Sea $\mathcal{R}$ un anillo conmutativo con identidad. Se define el **espectro máximo** de $\mathcal{R}$ por

$$\text{Specm}(\mathcal{R}) = \{\mathfrak{m} \subset \mathcal{R} \mid \mathfrak{m} \text{ es ideal máximo}\},$$

y el **radical de Jacobson** de $\mathcal{R}$, denotado por $\text{Rad}(\mathcal{R})$, como

$$\text{Rad}(\mathcal{R}) = \bigcap_{\mathfrak{m} \in \text{Specm}(\mathcal{R})} \mathfrak{m}.$$

Los elementos de $\mathrm{Rad}(\mathcal{R})$ son caracterizados de la siguiente manera:

Proposición 1.4. *[ver [19], Proposición 1.9] Dado un anillo conmutativo con identidad $\mathcal{R}$ se tiene que $r \in \mathrm{Rad}(\mathcal{R})$ si y sólo si $1 - rs$ es una unidad en $\mathcal{R}$ para toda $s \in \mathcal{R}$.*

Dado un anillo finito, local, conmutativo con identidad $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_q)$ y su anillo de polinomios $\mathcal{R}[x]$, del hecho que $\mathrm{Rad}(\mathcal{R}) = \mathfrak{m}$ tendremos que $\mathfrak{m}[x]$ es el ideal formado por los elementos nilpotentes de $\mathcal{R}[x]$.

Lema 1.5. *Sean $f, g \in \mathcal{R}[x]$, $\mathcal{R}$ un anillo finito, local y conmutativo $(\mathcal{R}, \mathfrak{m}, \mathcal{R}/\mathfrak{m})$. Entonces, f y g son primos relativos (o coprimos) en $\mathcal{R}[x]$ si y sólo si $\overline{f}$ y $\overline{g}$ son primos relativos en $\mathbb{F}_q[x]$.*

Demostración. Sean $f, g \in \mathcal{R}[x]$ y suponga que $\overline{f}, \overline{g}$ son primos relativos. Entonces existe $\overline{\lambda}_f, \overline{\lambda}_g \in \mathbb{F}_q[x]$ tales que $\overline{\lambda}_f \overline{f} + \overline{\lambda}_g \overline{g} = 1$, de donde en $\mathcal{R}[x]$, $\lambda_f f + \lambda_g g = 1 + r$ con $r \in \mathfrak{m}[x]$. Dado que $\mathcal{R}$ es local, $1 + r$ es una unidad en $\mathcal{R}[x]$ y por lo tanto,

$$(1 + r)^{-1} \lambda_f f + (1 + r)^{-1} \lambda_g g = 1.$$

La implicación recíproca se sigue de las definiciones. □

Del Teorema 1.3, en un anillo finito, conmutativo y local $\mathcal{R}$ la factorización de un polinomio regular es, en general, dada por factores (polinomios) regulares.

Proposición 1.6. *Sea $f \in \mathcal{R}[x]$ un polinomio mónico regular, donde $(\mathcal{R}, \mathfrak{m}, \mathcal{R}/\mathfrak{m})$ es un anillo finito, conmutativo y local. Suponga que en $(\mathcal{R}/\mathfrak{m})[x]$ se tiene que $\overline{f} = \prod_{i=1}^{m} \overline{g}_i$ con los $\overline{g}_i$ polinomios distintos, mónicos e irreducibles. Entonces f admite una factorización única como producto de polinomios distintos, mónicos, básicos irreducibles y primos relativos por pares.*

Demostración. Dado que, en $(\mathcal{R}/\mathfrak{m})[x]$ se tiene que $\overline{f} = \prod_{i=1}^{m} \overline{g}_i$ con los $\overline{g}_i$ polinomios distintos, mónicos e irreducibles, del Lema generalizado de Hensel, 1.1, tenemos que esta factorización es levantada a

$$f = \prod_{i}^{m} g_i$$

con cada g_i tal que $g_i + \mathfrak{m} = \overline{g}_i$ y con g_i coprimo con g_j si $i \neq j$. Por el Teorema 1.2, cada g_i es básico irreducible, i. e., irreducible. Como cada uno de los g_i es preimagen de un correspondiente $\overline{g}_i \neq 0$, estos son regulares en $\mathcal{R}[x]$ y se tiene que,

$$f = \prod_{i}^{m} g_i,$$

es una descomposición factorial de f en polinomios regulares, primarios y coprimos por pares. Del Teorema 1.3, tal descomposición es única. □

1.1.1. Anillos de Frobenius finitos

Recordemos que dado un anillo $\mathcal{R}$, no necesariamente conmutativo, se denota por ${}_{\mathcal{R}}M$ a un $\mathcal{R}$-módulo izquierdo y que, análogamente, $M_{\mathcal{R}}$ denota a un $\mathcal{R}$-módulo derecho. Si el anillo $\mathcal{R}$ es finito, conmutativo con identidad se dice que un $\mathcal{R}$-módulo (izquierdo) M es **simple** si y sólo si se tiene el isomorfismo $M \cong \mathcal{R}/\mathfrak{m}$, como $\mathcal{R}$-módulos, para algún ideal máximo $\mathfrak{m}$ de $\mathcal{R}$ o, equivalentemente, si los únicos submódulos de M son los triviales. Un ideal I de un anillo $\mathcal{R}$ es **irreducible** si visto como un $\mathcal{R}$-módulo es simple.

Definición. Dado un anillo $\mathcal{R}$, se define el **zoclo** de $\mathcal{R}$, denotado $\mathrm{Soc}(\mathcal{R})$, como el ideal generado por la suma de los ideales irreducibles de $\mathcal{R}$.

Existen varias definiciones equivalentes de cuando un anillo es de Frobenius (ver por ejemplo [25], §16, capítulo 6). En lo que respecta a este trabajo usaremos la siguiente, que se puede consultar en [5].

Definición. Un anillo finito, no necesariamente conmutativo, con identidad $\mathcal{R}$ es **de Frobenius** si satisface

- ${}_{\mathcal{R}}(\mathcal{R}/\operatorname{Rad}(\mathcal{R})) \cong \mathrm{Soc}({}_{\mathcal{R}}\mathcal{R})$,
- $(\mathcal{R}/\operatorname{Rad}(\mathcal{R}))_{\mathcal{R}} \cong \mathrm{Soc}(\mathcal{R}_{\mathcal{R}})$,

como $\mathcal{R}$-módulos.

Nótese que en el caso en el que $\mathcal{R}$ sea conmutativo basta verificar sólo una de las condiciones.

Proposición 1.7. *Sea $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_q)$ un anillo finito, local, conmutativo con identidad. $\mathcal{R}$ es de Frobenius si y sólo si $\mathrm{Soc}(\mathcal{R})$ es un $\mathcal{R}$-módulo simple.*

Demostración. Si $\mathcal{R}$ es de Frobenius, entonces $\mathrm{Soc}(\mathcal{R}) \cong \mathcal{R}/\operatorname{Rad}(\mathcal{R}) = \mathcal{R}/\mathfrak{m}$ es simple como $\mathcal{R}$-módulo. Recíprocamente, si $\mathrm{Soc}(\mathcal{R})$ es un $\mathcal{R}$-módulo simple, entonces $\mathrm{Soc}(\mathcal{R}) \cong \mathcal{R}/\mathfrak{m}$ para algún ideal máximo $\mathfrak{m}$ y como $\mathcal{R}$ es local se tiene que $\mathrm{Soc}(\mathcal{R}) \cong \mathcal{R}/\operatorname{Rad}(\mathcal{R})$.□

1.2. El Teorema Chino del Residuo

En esta sección, dada la importancia del mismo para el presente trabajo, se muestra a manera de recordatorio un breve estudio del Teorema chino del residuo (abreviado como TCR).

En general, dado un anillo $\mathcal{R}$ conmutativo con identidad, dos ideales $\mathfrak{a}_1, \mathfrak{a}_2$ de $\mathcal{R}$ se dicen **coprimos** si ocurre que $\mathfrak{a}_1 + \mathfrak{a}_2 = \mathcal{R}$. En general, para ideales $\mathfrak{a}, \mathfrak{b}$ de un anillo conmutativo con identidad $\mathcal{R}$ se tiene de las definiciones que $\mathfrak{a} \cap \mathfrak{b} \supseteq \mathfrak{ab}$ donde $\mathfrak{ab}$ denota el producto de ideales, esto es, el ideal generado (sumas finitas) por todos los productos ab con $a \in \mathfrak{a}, b \in \mathfrak{b}$. Si $\mathfrak{a}$ y $\mathfrak{b}$ son coprimos, entonces $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$ ya que existen $a \in \mathfrak{a}$ y $b \in \mathfrak{b}$ tales que $a + b = 1$ y por lo tanto, para $c \in \mathfrak{a} \cap \mathfrak{b}$ tenemos que $c = ca + cb \in \mathfrak{ab}$. Dados dos elementos $r, s \in \mathcal{R}$ y un ideal $\mathfrak{a}$ de $\mathcal{R}$ se dirá que $r \equiv s \mod \mathfrak{a}$ si $r - s \in \mathfrak{a}$.

Lema 1.8. *Sea $\mathcal{R}$ un anillo conmutativo con identidad y $\mathfrak{a}_1, \mathfrak{a}_2$ ideales coprimos de $\mathcal{R}$. Dados $r_1, r_2 \in \mathcal{R}$, entonces existe un r en $\mathcal{R}$ tal que*

$$\begin{aligned} r &\equiv r_1 \quad \text{mód} \quad \mathfrak{a}_1 \\ r &\equiv r_2 \quad \text{mód} \quad \mathfrak{a}_2. \end{aligned}$$

Demostración. Como $\mathfrak{a}_1 + \mathfrak{a}_2 = \langle 1 \rangle$, existen $a_i \in \mathfrak{a}_i$, $i = 1, 2$ tales que $a_1 + a_2 = 1$ de ahí que

$$\begin{aligned} a_1 r_1 + a_2 r_1 &= r_1 \\ a_1 r_2 + a_2 r_2 &= r_2 \end{aligned}$$

y por lo tanto, no es dificil ver que el elemento de $\mathcal{R}$ definido por $r = a_1 r_2 + a_2 r_1$ satisface las condiciones pedidas. □

Corolario 1.9. *Sean $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ ideales coprimos por pares de un anillo conmutativo con identidad $\mathcal{R}$. Dados $r_1, r_2, r_3 \in \mathcal{R}$, existe $r \in \mathcal{R}$ tal que $r \equiv r_i \mod \mathfrak{a}_i$ con $i = 1, 2, 3$.*

Demostración. De las hipótesis, existen $a_{j1} \in \mathfrak{a}_1$, $a_j \in \mathfrak{a}_j$ con $j = 2, 3$ tales que

$$a_{21} + a_2 = 1, \ a_{31} + a_3 = 1 \text{ lo que implica } (a_{21} + a_2)(a_{31} + a_3) = 1,$$

es decir,

$$a_{21}a_{31} + a_{21}a_3 + a_2 a_{31} + a_2 a_3 = 1, \text{ de donde } \mathfrak{a}_1 + \mathfrak{a}_2\mathfrak{a}_3 = \mathcal{R}.$$

Por el Lema 1.8, existe un $x_1 \in \mathcal{R}$ tal que $x_1 \equiv 1 \mod \mathfrak{a}_1$ mientras que $x_1 \equiv 0 \mod \mathfrak{a}_2\mathfrak{a}_3$. Note que si $x_1 \equiv 0 \mod \mathfrak{a}_2\mathfrak{a}_3$, entonces $x_1 \in \mathfrak{a}_2 \cap \mathfrak{a}_3$. El mismo argumento garantiza existen $x_j \in \mathcal{R}$ tal que $x_j \equiv 1 \mod \mathfrak{a}_j$ y $x_j \equiv 0 \mod \prod_{i \neq j} \mathfrak{a}_i$, $j = 2, 3$. Entonces

$$r = r_1 x_1 + r_2 x_2 + r_3 x_3$$

satisface lo solicitado. □

Con las ideas anteriores, la demostración del resultado principal de esta sección se sigue fácilmente.

Teorema 1.10 (Teorema Chino del Residuo). *Sean $\mathcal{R}$ un anillo conmutativo con identidad y $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ ideales de $\mathcal{R}$ coprimos por pares, esto es, $\mathfrak{a}_i + \mathfrak{a}_j = \mathcal{R}$ para todo $i \neq j$. Si $r_1, r_2, \ldots, r_m$ son elementos de $\mathcal{R}$ entonces existe un elemento $r \in \mathcal{R}$ tal que $r \equiv r_i \mod \mathfrak{a}_i$ para $i = 1, 2, \ldots, m$.*

Demostración. Usando el Lema 1.8, para cada $i = 1, \ldots, m$ existe un $x_i \in \mathcal{R}$ tal que $x_i \equiv 1$ mód $\mathfrak{a}_i$ y $x_i \equiv 0 \mod \prod_{j \neq i} \mathfrak{a}_j$, pues para cada $i = 1, \ldots, m$, se tiene que $\mathfrak{a}_i + \prod_{j \neq i} \mathfrak{a}_j = \mathcal{R}$ ya que existen elementos a_{ji}, a_j tales que

$$a_{ji} + a_j = 1, \ \text{ con } a_{ji} \in \mathfrak{a}_i, a_j \in \mathfrak{a}_j, j \neq i,$$

lo que implica, por una aplicación sucesiva de la ley distributiva, que para cada $i = 1, 2, \ldots, m$ fijo se tiene que $\prod_{j \neq i}(a_{ji} + a_j) = A_i + A_j = 1$ con $A_i \in \mathfrak{a}_i$, $A_j \in \prod_{j \neq i} \mathfrak{a}_j$. Sea

$$r = r_1 x_1 + r_2 x_2 + \ldots + r_m x_m,$$

por construcción $r \equiv r_i \mod \mathfrak{a}_i$. □

Como una consecuencia directa del Teorema 1.10 se tiene el siguiente corolario, el cual será de utilidad para la descripción de códigos constacíclicos.

Corolario 1.11. *Sean* $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ *ideales coprimos por pares de un anillo conmutativo con identidad* $\mathcal{R}$*. Sea*

$$\Phi : \mathcal{R} \longrightarrow \prod_{i=1}^{m} \mathcal{R}/\mathfrak{a}_i = \bigoplus_{i=1}^{m} \mathcal{R}/\mathfrak{a}_i$$

la función inducida por el mapeo canónico $\mathcal{R} \longrightarrow \mathcal{R}/\mathfrak{a}_i$ *para cada factor. Entonces* Φ *es una sobreyección de anillos con núcleo* $\ker \Phi = \prod_{i=1}^{m} \mathfrak{a}_i$*. Se tiene así un isomorfismo*

$$\mathcal{R}/\prod_{i=1}^{m} \mathfrak{a}_i \cong \bigoplus_{i=1}^{m} \mathcal{R}/\mathfrak{a}_i$$

de anillos.

Demostración. Considere

$$(r_1 + \mathfrak{a}_1, r_2 + \mathfrak{a}_2, \ldots, r_m + \mathfrak{a}_m) \in \bigoplus_{i=1}^{m} \mathcal{R}/\mathfrak{a}_i.$$

Por el Teorema 1.10, existe un $r \in \mathcal{R}$ tal que $r \equiv r_i \mod \mathfrak{a}_i$, por lo que Φ es sobreyectiva. Note que $r \in \ker \Phi$ si y sólo si $r \in \bigcap_{i=1}^{m} \mathfrak{a}_i$. Del primer Teorema de isomorfismo para anillos se sigue la última afirmación. □

Como un ligero abuso de la notación, se denotará también por Φ al isomorfismo $\mathcal{R}/\prod_{i=1}^{m} \mathfrak{a}_i \longrightarrow \bigoplus_{i=1}^{m} \mathcal{R}/\mathfrak{a}_i$ del Corolario 1.11 y está definido por

$$r + \prod_{i=1}^{m} \mathfrak{a}_i \mapsto (r + \mathfrak{a}_1, r + \mathfrak{a}_2, \ldots, r + \mathfrak{a}_m).$$

1.3. Elementos idempotentes en anillos locales finitos

En esta sección se brindan las definiciones y resultados necesarios relacionados con elementos idempotentes en un anillo. Mayor detalle se puede encontrar en el Capítulo VII de la referencia [21] en lo que a anillos finitos se refiere, o bien, en un contexto mucho más general, el Capítulo 7 de la referencia [26], secciones 21 y 22.

Desde el punto de vista de la teoría algebraica de códigos, se han usado idempotentes para realizar descripciones de los llamados códigos cíclicos minimales definidos sobre campos finitos. Ver por ejemplo el texto [23]. En lo que respecta a códigos cíclicos definidos sobre anillos finitos, se han utilizado elementos idempotentes en las investigaciones [4] y [7].

Definición. Sea $\mathcal{R}$ un anillo conmutativo con identidad. Se dice que $e \in \mathcal{R}$ es **idempotente** si $e^2 = e$. Si $e \neq 1, 0$, se dice que e es **no trivial**. Se denotará por $E(\mathcal{R})$ al conjunto de elementos idempotentes del anillo $\mathcal{R}$. Dados $e, f \in E(\mathcal{R})$, si $ef = 0$, se dirá que los elementos e, f son **ortogonales** entre sí. Un elemento idempotente no cero $e \in E(\mathcal{R})$ es **primitivo** si $e = f + g$, con $f, g \in E(\mathcal{R})$ ortogonales entre sí, entonces $e = 0$ ó $f = 0$. Un conjunto de elementos idempotentes $\{e_1, e_2, \ldots, e_l\} \subset E(\mathcal{R})$ tales que

$$e_1 + e_2 + \ldots + e_l = 1$$

recibe el nombre de **conjunto completo** de elementos idempotentes. Si cada uno de los elementos del conjunto anterior satisfacen que son primitivos y ortogonales entre sí por pares, se dirá que se tiene un **conjunto completo de elementos idempotentes primitivos ortogonales por pares**.

En ocasiones, se escribirá correspondientemente idempotente (idempotentes) para referirse a un elemento idempotente (elementos idempotentes).

Proposición 1.12. *Sea $\mathcal{R}$ un anillo conmutativo con identidad. Suponga que*

$$E = \{e_1, e_2, \ldots, e_l\} \subset E(\mathcal{R}),$$

es un conjunto completo de elementos idempotentes primitivos ortogonales por pares. Entonces, E es único.

Demostración. Suponga que existe algún otro conjunto completo de idempotentes primitivos ortogonales por pares $F = \{f_1, f_2, \ldots, f_m\} \subset E(\mathcal{R})$ con $l \leq m$. Del hecho de ser E y F conjuntos completos de idempotentes tenemos que

$$e_i = e_i \sum_{j=1}^{m} f_j,$$

pero, por hipótesis, cada $e_i \in E$ es primitivo y de la ortogonalidad por pares de los f_i se deduce que $e_i = e_i f_j$ para algún $j \in \{1, \ldots, m\}$. De manera similar tenemos que, para tal j, $f_j = e_l f_j$. Se afirma que $e_i = e_l$. Si $l \neq i$, entonces $e_i = e_i f_j = e_i(e_l f_j) = 0$, lo que no es posible dado que e_i es primitivo, por lo tanto $e_i = e_l$, de donde $e_i = e_i f_j = f_j$. Esto argumento prueba también que $l = m$. □

Recordemos que un anillo $\mathcal{R}$ conmutativo con identidad es descomponible si existe una familia finita de anillos conmutativos con identidad $\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_l$ no triviales y tales que $\mathcal{R}_i \subset \mathcal{R}$ para cada $1 \leq i \leq l$ como ideales y de tal modo que $\mathcal{R} \cong \bigoplus_{i=1}^{l} \mathcal{R}_i$. Un anillo es indescomponible si no es descomponible. Es conocido, además, que dado un elemento idempotente $e \in \mathcal{R}$, se tiene la descomposición

$$\mathcal{R} = e\mathcal{R} \oplus (1 - e)\mathcal{R},$$

donde $1 - e$ es el idempotente complementario de e (capítulo 7, sección 21 ver [26]).

Proposición 1.13. *Sea $\mathcal{R}$ un anillo conmutativo con identidad. Suponga que $E(\mathcal{R}) \supset \{0,1\}$ y sea $e \in E(\mathcal{R}) \setminus \{0,1\}$. Entonces $e\mathcal{R} = \langle e \rangle$ es un anillo indescomponible si y sólo si e es elemento idempotente primitivo.*

Demostración. Suponga que $e \in \mathcal{R}$ es elemento idempotente primitivo. Que $e\mathcal{R} = \langle e \rangle$ es un anillo se deriva de las propiedades de ser un ideal, más aún, para cualquier $r \in \mathcal{R}$ se cumple que $e(er) = e^2r = er$ por lo que e es la identidad en $e\mathcal{R}$. Si $e\mathcal{R} = f(e\mathcal{R}) \oplus (e-f)e\mathcal{R}$, para $f \in E(e\mathcal{R})$, por ser e primitivo se debe tener que $f = 0$ o $e - f = 0$ y por lo tanto el anillo $e\mathcal{R}$ es indescomponible.

Si se supone ahora que el anillo $e\mathcal{R}$ es indescomponible, se afirma que su conjunto de idempotentes $E(e\mathcal{R}) = \{e, 0\}$. Suponga que $e = f + g$ con $f, g \in E(\mathcal{R})$ idempotentes ortogonales entre sí. Es claro que entonces $e = ef + eg \in e\mathcal{R}$ con ef y eg idempotentes ortogonales entre sí. Por otra parte, para un $h \in E(e\mathcal{R})$ con $h \neq e, 0$ se cumple que $e\mathcal{R} = h(e\mathcal{R}) \oplus (e-h)(e\mathcal{R})$ que contradice la hipótesis de ser $e\mathcal{R}$ indescomponible. Así pues, $f = 0$ ó $g = 0$ y por lo tanto e es elemento idempotente primitivo. □

1.4. Códigos lineales y constacíclicos sobre anillos

1.4.1. Códigos lineales sobre campos finitos

Los códigos detectores-correctores de errores, como su nombre indica, ayudan a detectar y corregir problemas que surgen durante la transmisión y recepción de información a través de un canal susceptible de presentar ruido ([23]). Dada la naturaleza de la transmisión y almacenamiento de la información a través de medios electrónicos, en un inicio se trabajó sobre el campo binario $\mathbb{F}_2$, extendiéndose después las ideas a campos finitos $\mathbb{F}_q$. Los códigos pueden ser lineales o no lineales.

Dado que el presente trabajo trata sobre una subfamilia de códigos lineales, se procede a dar las definiciones necesarias para establecer el contexto adecuado. Con la finalidad de fijar ideas, recordemos la definición de código lineal sobre un campo finito y algunos otros términos relacionados.

Definición. Sea $\mathbb{F}_q$ un campo finito con q elementos, $q = p^m$ para un número primo p y un entero $m > 0$. Un subespacio $\mathcal{C}$ de dimensión k del $\mathbb{F}_q$-espacio vectorial $\mathbb{F}_q^n$ es un **código lineal** de longitud n y dimensión k. El campo base $\mathbb{F}_q$ recibe el nombre de **alfabeto** del código. Una **palabra de código**, o simplemente **palabra**, es un vector $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$.

Dado un conjunto X se define $\bar{d} : X \times X \longrightarrow \mathbb{R}$ por

$$\bar{d}(x,y) = \begin{cases} 1 & \text{si } x \neq y \\ 0 & \text{si } x = y \end{cases}$$

No es difícil probar que la función $\bar{d}$ es una métrica, más aún, en realidad es la **métrica discreta** definida en X.

Definición. Sea $(n,k)-\mathcal{C}$ un código lineal sobre $\mathbb{F}_q$.

- Se define la **distancia de Hamming** entre dos palabras $\mathbf{x},\mathbf{y}\in\mathcal{C}$, denotada por $d_H(\mathbf{x},\mathbf{y})$, como el número de coordenadas en que difieren. Ello se puede escribir en términos de la métrica discreta definida en $\mathbb{F}_q$. Esto es, si $\mathbf{x}=(x_0,x_1,\ldots,x_{n-1})$, $\mathbf{y}=(y_1,y_2,\ldots,y_{n-1})\in\mathbb{F}_q^n$, entonces

$$d_H(\mathbf{x},\mathbf{y})=\sum_{j=0}^{n-1}\bar{d}(x_j,y_j)$$

- Se define el **peso de Hamming** de una palabra, $\mathbf{x}\in\mathcal{C}$, denotado por $w_H(\mathbf{x})$, como el número de coordenadas no nulas de la misma o bien $w_H(\mathbf{x})=d_H(\mathbf{x},0)$.

De lo anterior, se cumple que $d_H(\mathbf{x},\mathbf{y})=w(\mathbf{x}-\mathbf{y})$.

Ejemplo 1. Si $\mathbf{x}=(1,0,0,1,1,0)$, y $\mathbf{y}=(1,0,0,0,1,0)$

$$d_H(\mathbf{x},\mathbf{y})=1,$$

mientras que

$$w_H(\mathbf{x})=3.$$

De las definiciones se sigue de forma directa la siguiente proposición.

Proposición 1.14. *La distancia de Hamming es una métrica en* $\mathbb{F}_q^n$.

Definición. La **distancia mínima**, d, de un código $\mathcal{C}$ se define como

$$d=\min_{\mathbf{x}\neq\mathbf{y}}\{d_H(\mathbf{x},\mathbf{y})\mid\mathbf{x},\mathbf{y}\in\mathcal{C}\}=\min_{\mathbf{x}\neq\mathbf{y}}\{w(\mathbf{x}-\mathbf{y})\mid\mathbf{x},\mathbf{y}\in\mathcal{C}\}=\min\{w(\mathbf{x})\mid\mathbf{x}\in\mathcal{C}\setminus\{\mathbf{0}\}$$

Cuando son definidos sobre campos finitos, los códigos lineales tienen parámetros que los distinguen. Dado un código lineal $\mathcal{C}$, este tendrá los siguientes parámetros: Su longitud n, su dimensión k, su eficiencia $R=\frac{k}{n}$ y su distancia mínima d. Para indicar tales parámetros de manera abreviada se escribe usualmente $(n,k,d)-\mathcal{C}$ ó, si no se conoce el parámetro d, $(n,k)-\mathcal{C}$ para un código lineal $\mathcal{C}$ de longitud n y dimensión k definido sobre un campo finito $\mathbb{F}_q$.

Finalmente, recordemos que en el espacio vectorial $\mathbb{F}_q^n$ se define el producto interno usual $\bullet:\mathbb{F}_q^n\times\mathbb{F}_q^n\longrightarrow\mathbb{F}_q$, es decir, dados $\mathbf{x}=(x_0,x_1,\ldots,x_{n-1}),\mathbf{y}=(y_0,y_1,\ldots,y_{n-1})$, entonces $\mathbf{x}\bullet\mathbf{y}=\sum_{i=0}^{n-1}x_iy_i$. Bajo este producto interno, dado un código lineal $\mathcal{C}\subset\mathbb{F}_q^n$ se define el código dual $\mathcal{C}^\perp$ de $\mathcal{C}$ por

$$\mathcal{C}^\perp=\{\mathbf{x}\in\mathbb{F}_q^n\mid\mathbf{x}\bullet\mathbf{c}=0\text{ para todo }\mathbf{c}\in\mathcal{C}\}.$$

1.4.2. Códigos lineales sobre anillos finitos

El estudio de códigos definidos sobre anillos finitos cobró notoriedad con los artículos realizados por Ian F. Blake en la década de los 70 (ver [1] y [2]). Alrededor de veinte años después, los trabajos seminales de A. R. Hammons, P. V. Kumar, A. R. Calderbank y N. J. A. Sloane y P. Solé en [3] así como el de V. S. Pless y Z. Qian en [4] hicieron énfasis en la estructura de los códigos lineales y cíclicos sobre el anillo $\mathbb{Z}_4$. En la misma dirección, un par de años más tarde, pero generalizando el estudio de códigos cíclicos sobre el anillo de enteros $\mathbb{Z}_{p^m}$, con p un número primo y $m \leq 1$, se tiene la investigación de P. Kanwar y S. R. López-Permouth ([7]). Tales investigaciones se extendieron a un contexto más general y para el año 2004, S. López-Permouth y H. Q. Dinh muestran un estudio de códigos cíclicos y negacíclicos sobre anillos finitos de cadena ([28]). Cabe mencionar en este punto, que en México se han realizado contribuciones relacionadas con códigos cíclicos y constacíclicos definidos sobre anillos finitos, conmutativos con identidad. El lector puede consultar, sólo por mencionar algunas de estas investigaciones, el artículo publicado por H. Tapia-Recillas y G. Vega ([29]) que versa en particular sobre códigos constacíclicos definidos sobre el anillo de cadena $\mathbb{Z}_{2^k}$, o recientemente, el trabajo llevado a cabo por C. A. Castillo-Guillén, C. Rentería Márquez y H. Tapia-Recillas [11] en el que se estudian códigos constacíclicos definidos sobre algunos anillos finitos y locales que son no de cadena.

De todo ese trabajo se tiene que cuando el alfabeto es ahora un anillo $\mathcal{R}$, usualmente conmutativo y finito, la noción de espacio vectorial para un código lineal es cambiada por la de un $\mathcal{R}$-módulo.

Definición. Sea $\mathcal{R}$ un anillo finito. Un **código** $\mathcal{C}$ es un subconjunto de $\mathcal{R}^n$. Se dirá que $\mathcal{C}$ es un **código lineal** de longitud n sobre el alfabeto $\mathcal{R}$ si $\mathcal{C}$ es un submódulo de $\mathcal{R}^n$.

A diferencia de los códigos lineales definidos sobre campos finitos, en un código lineal $\mathcal{C}$ definido sobre un anillo finito no necesariamente se tiene un parámetro análogo al de dimensión dado que un módulo no necesariamente tiene una base en el mismo sentido que en el de los espacios vectoriales. Por otro lado, es posible definir la distancia y peso de Hamming. d_H y w_H de igual forma como en el caso de códigos sobre campos finitos, pero es posible que estos sean sustituidos por otras definiciones de distancias u otros pesos, dependiendo fuertemente la elección del anillo y la información que se desea obtener a partir de tales definiciones; ver, por ejemplo, [16] o [9], donde el peso de Hamming es sustituido por el peso de Lee.

El problema que se aborda en esta investigación, el cual es la descripción de códigos constacíclicos a partir de ideales, no está relacionado directamente con tales conceptos por lo que no se profundiza en las correspondientes definiciones, sin embargo, se hace mención de los mismos por las perspectivas de trabajos posteriores que se podrían derivar en algún momento dado, las cuales serán mencionadas más adelante.

Dado $\mathcal{R}$ un anillo finito, conmutativo, con identidad; considere el $\mathcal{R}$-módulo $\mathcal{R}^n$ y sea $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{R}^n$. Se tiene una función $\mathcal{P} : \mathcal{R}^n \longrightarrow \mathcal{R}[x]$ dada por

$$(c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \ldots + c_{n-1} x^{n-1},$$

llamada la **representación polinomial** de los elementos $\mathbf{c} \in \mathcal{R}^n$ en $\mathcal{R}[x]$.

Definición. Sea $\mathcal{C} \subset \mathcal{R}^n$ un código lineal definido sobre el anillo $\mathcal{R}$. Dada una unidad $\gamma \in \mathcal{U}(\mathcal{R})$, se dirá que $\mathcal{C}$ es un código **constacíclico** (o γ-**constacíclico** si se quiere hacer énfasis en la unidad γ) si ocurre que

$$(\gamma c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C} \text{ siempre que } (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}.$$

Observación 1. En el caso particular en el que $\gamma = 1$, el código $\mathcal{C}$ recibe el nombre de **cíclico**; mientras que si $\gamma = -1$ se dirá que $\mathcal{C}$ es **negacíclico**.

Así, se tiene que los códigos constacíclicos son una generalización de los de tipo cíclico. Nótese que mediante la representación polinomial $\mathcal{P}$ definida líneas arriba, los elementos de $\mathcal{R}^n$ son interpretados como polinomios de grado no mayor a $n-1$, en particular, en el caso de un código constacíclico, $\mathcal{C} \subset \mathcal{R}^n$, se tiene la siguiente proposición.

Proposición 1.15. *Sean $\mathcal{R}$ un anillo conmutativo con identidad, $\gamma \in \mathcal{U}(\mathcal{R})$. Mediante la representación polinomial*

$$\mathcal{P} : \mathcal{R}^n \longrightarrow \mathcal{R}[x]/\langle x^n - \gamma \rangle$$

se tiene una correspondencia biyectiva entre los códigos constacíclicos de $\mathcal{R}^n$ y los ideales del anillo cociente $\mathcal{R}[x]/\langle x^n - \gamma \rangle$.

Demostración. Es claro que $\mathcal{P}$ es un isomorfismo de $\mathcal{R}$-módulos. Sea $\mathcal{C} \subset \mathcal{R}^n$ un código γ-constacíclico. Dado $\mathbf{c} \in \mathcal{C}$, se tiene que $\mathcal{P}(\mathbf{c}) = c(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$, de donde,

$$xc(x) = c_0 x + c_1 x^2 + \ldots + c_{n-1}x^n = \gamma c_{n-1} + c_0 x + c_1 x^2 + \ldots + c_{n-1}x^{n-1},$$

que tiene asociada al elemento $(\gamma c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. A partir de la observación anterior, para probar que $\mathcal{P}(\mathcal{C})$ es un ideal, considere $r(x) = \mathcal{P}(\mathbf{r})$, con $\mathbf{r} = (r_0, r_1, \ldots, r_{n-1}) \in \mathcal{R}^n$ y $\mathbf{c} \in \mathcal{C}$, entonces

$$c(x)r(x) = r_0 c(x) + r_1 xc(x) + \ldots + r_{n-1}x^{n-1}c(x),$$

y del hecho de ser $\mathcal{C}$ lineal y de que $\mathcal{P}^{-1}(x^i c(x)) \in \mathcal{C}$ para $1 \leq i \leq n-1$ se tiene que $\mathcal{P}^{-1}(c(x)r(x)) \in \mathcal{C}$, así pues $\mathcal{P}(\mathcal{C})$ es un ideal de $\mathcal{R}[x]/\langle x^n - \gamma \rangle$.

Sea $\mathcal{I}$ un ideal propio del anillo cociente $\mathcal{R}[x]/\langle x^n - \gamma \rangle$, el cuál en particular es un $\mathcal{R}$-submódulo y por ser $\mathcal{P}$ un isomorfismo de módulos se tiene que $\mathcal{P}^{-1}(\mathcal{I}) = \mathcal{C} \subset \mathcal{R}^n$ es un $\mathcal{R}$-submódulo. En $\mathcal{R}[x]/\langle x^n - \gamma \rangle$ se cumple que $x^n = \gamma$ y por lo tanto, dado $c(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \in \mathcal{I}$ se tiene que

$$xc(x) = \gamma c_{n-1} + c_0 x + c_1 x^2 + \ldots + c_{n-2}x^{n-1} \in \mathcal{I},$$

pero ello implica que $\mathcal{P}^{-1}(\gamma c_{n-1} + c_0 x + c_1 x^2 + \ldots + c_{n-2}x^{n-1}) = (\gamma c_{n-1}, c_0, \ldots . c_{n-2}) \in \mathcal{C}$, teniendo así que

$$(\gamma c_{n-1}, c_0, \ldots . c_{n-2}) \in \mathcal{C} \text{ siempre que } (c_0, c_1, \ldots . c_{n-1}) \in \mathcal{C}. \qquad \square$$

De la proposición anterior, dados un anillo $\mathcal{R}$, una longitud n, con $n > 0$ entero, y $\gamma \in \mathcal{U}(\mathcal{R})$, identificaremos a un código γ-constacíclico $\mathcal{C}$ de $\mathcal{R}^n$ con un ideal $\mathcal{P}(\mathcal{C})$ de $\mathcal{R}[x]/\langle x^n - \gamma \rangle$ haciendo referencia únicamente al código γ-constacíclico $\mathcal{C}$. Dicho de otro modo, dar la descripción de todos los ideales de

$$\mathcal{R}[x]/\langle x^n - \gamma \rangle$$

es dar la descripción de todos los códigos γ-constacíclicos de longitud n definidos sobre $\mathcal{R}$. Parte de esa descripción consiste en decir si, por ejemplo, la estructura de ideales de $\mathcal{R}[x]/\langle x^n - \gamma \rangle$ es o no de ideales principales. En nuestro caso, parte del objetivo de este trabajo de investigación es determinar la estructura de ideales del anillo cociente

$$\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - \gamma \rangle,$$

donde $\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$, $u^2 = 0$, γ es una unidad en $\mathcal{R}_k$ y la longitud $n > 0$ del código es tal que el primo p y n no tienen factores en común.

Capítulo 2

El anillo $\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$

En este capítulo inicia el trabajo de investigación que motiva este escrito. Se realiza un estudio de las propiedades algebraicas del anillo $\mathcal{R}_k$ que será el alfabeto para los códigos constacíclicos de nuestro interés, así como el respectivo conjunto de ideales, centrándonos, dadas la conmutatividad del anillo, en los ideales principales.

Dado un número primo p, se define el anillo $\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$, por

$$\mathcal{R}_k = \{a + bu \mid a, b \in \mathbb{Z}_{p^k}, u^2 = 0\},$$

donde $\mathbb{Z}_{p^k}$ es el anillo de enteros módulo p^k, es decir,

$$\mathbb{Z}_{p^k} = \{0, 1, \ldots, p^k - 1\}$$

tomando como representantes de clase al sistema completo de residuos. El anillo $\mathcal{R}_k$ tiene así las operaciones naturales de suma y producto, esto es, dados $a + bu, c + du \in \mathcal{R}_k$ tenemos

$$(a + bu) + (c + du) = (a + c) + (b + d)u,$$

y

$$(a + bu)(c + du) = ac + (ad + bc)u.$$

Casos particulares de este anillo con $p = 2$, $k = 2$, esto es $\mathcal{R}_2 = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$, han aparecido en artículos relativamente recientes; uno de estos trabajos es el artículo [10], donde se plantea el uso de anillos de Frobenius y no de cadena como alfabeto para códigos definidos sobre anillos. Entre los anillos de orden 16 estudiados aparece $\mathcal{R}_2$ (ver la Proposición 3.5 de ese artículo). Otra investigación que usa como alfabeto a $\mathcal{R}_2$ es [9], trabajo en el que se estudia a códigos lineales sobre ese anillo y las identidades de MacWilliams. También, en una dirección ligeramente distinta, estudiando códigos cíclicos sobre ese anillo, se tienen las investigaciones [16] y [17]. Con los parámetros $p = 2$, $k = 3$, esto es $\mathcal{R}_3 = \mathbb{Z}_8 + u\mathbb{Z}_8$ con $u^2 = 0$, se mostró un estudio de códigos lineales sobre $\mathcal{R}_3$ en [30]. Por otra parte, algunos resultados sobre códigos cíclicos y sus respectivos generadores fueron presentados en [18] para el anillo $\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$, $u^2 = 0$.

Recordemos, de la Sección 1.1, que el zoclo de un anillo $\mathcal{R}$, denotado por $\mathrm{Soc}(\mathcal{R})$, es el ideal generado por la suma de los ideales irreducibles de $\mathcal{R}$ y que un anillo finito, local, conmutativo y con identidad es de Frobenius si su zoclo es un $\mathcal{R}$-módulo simple (ver Proposición 1.7). El anillo $\mathcal{R}_k$ tiene las siguientes propiedades:

Proposición 2.1. *Sea* $\mathcal{R}_k = \{a + bu \mid a, b \in \mathbb{Z}_{p^k}, k > 1, u^2 = 0\}$. *Entonces*

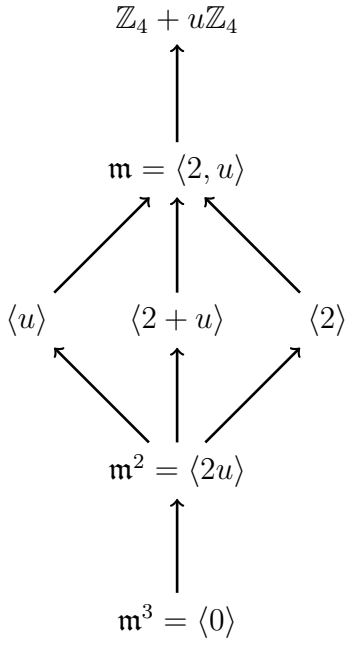
1. *El anillo* $\mathcal{R}_k$ *tiene cardinalidad* p^{2k} *y es isomorfo con el anillo cociente* $\mathbb{Z}_{p^k}[X]/\langle X^2\rangle$.
2. *El grupo de unidades está dado por* $\mathcal{U}(\mathcal{R}_k) = \{a + bu \mid a \in \mathcal{U}(\mathbb{Z}_{p^k})\}$ *con*
$$|\mathcal{U}(\mathcal{R}_k)| = p^{2k-1}(p-1).$$
3. *El anillo* $\mathcal{R}_k$ *es local, con ideal máximo* $\mathfrak{m} = \langle p, u\rangle$, *cuyo índice de nilpotencia es* $t = k + 1$.
4. *El anillo* $(\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}, \mathfrak{m} = \langle p, u\rangle, \mathcal{R}_k/\mathfrak{m} \cong \mathbb{F}_p)$ *es de Frobenius, no de cadena, con* $\mathrm{Soc}(\mathcal{R}_k) = \langle p^{k-1}u\rangle$.

Demostración. Las dos primeras partes de la proposición son cálculos directos de las definiciones. El conjunto de no unidades de $\mathcal{R}_k$ forma un ideal $\mathfrak{m}$ de lo que se concluye que es máximo. Cada elemento del ideal es de la forma $pa + bu$, $a, b \in \mathbb{Z}_{p^k}$, lo que implica que $\mathfrak{m} = \langle p, u\rangle$. En el conjunto de ideales tenemos a los elementos $\langle p^j\rangle$, $j = 1, 2, \ldots, k-1$, y $\langle u\rangle$ los cuales no son comparables con el orden inducido por la inclusión y por tanto $\mathcal{R}_k$ es no de cadena. Finalmente, nótese que $\mathfrak{m}^k = \langle p^{k-1}u\rangle = \{0, p^{k-1}u, 2p^{k-1}u, \ldots, (p-1)p^{k-1}u\}$ es el único ideal irreducible de $\mathcal{R}_k$ y por definición se tiene que $\mathrm{Soc}(\mathcal{R}_k) = \langle p^{k-1}u\rangle$. □

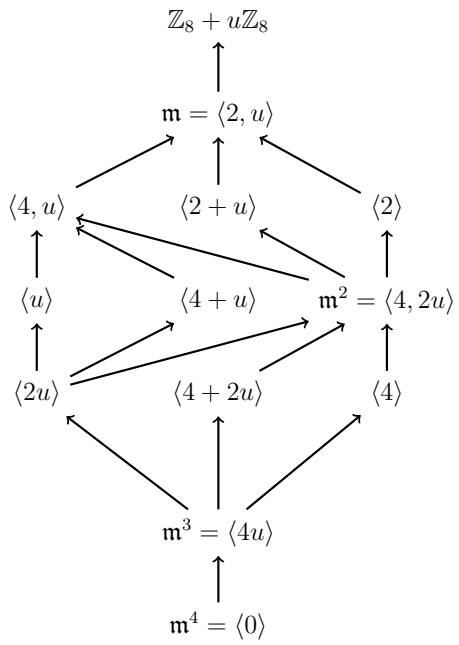
Ejemplo 2. Consideremos el caso $p = 2$. Si $k = 2$ se tiene el anillo $\mathcal{R}_2 = \mathbb{Z}_4 + u\mathbb{Z}_4$, con $u^2 = 0$. Su conjunto de ideales $\mathcal{L}_2$ consta de los siguientes elementos:

$$\mathcal{L}_2 = \{\langle 0\rangle, \langle 2u\rangle, \langle 2\rangle, \langle u\rangle, \langle 2 + u\rangle, \langle 2, u\rangle, \langle 1\rangle\}.$$

De la Proposición 2.1, $|\mathcal{R}_2| = 16$ y $\mathcal{U}(\mathcal{R}_2) = \{1 + au, 3 + au \mid a \in \mathbb{Z}_4\}$. Su diagrama de ideales es mostrado en el apartado (a) de la siguiente figura



(a) Ideales de $\mathcal{R}_2$



(b) Ideales de $\mathcal{R}_3$

Análogamente, para $k = 3$: el anillo $\mathcal{R}_3 = \mathbb{Z}_8 + u\mathbb{Z}_8$ está dado por

$$\mathcal{R}_3 = \{a + bu \mid a, b \in \mathbb{Z}_8, u^2 = 0\}.$$

Tenemos que $|\mathcal{R}_3| = 64$ y

$$\mathcal{U}(\mathcal{R}_3) = \{a + bu \mid a = 1, 3, 5, 7, b \in \mathbb{Z}_8\}.$$

Su conjunto de ideales, $\mathcal{L}_3$, de $\mathcal{R}_3$ está dado por

$$\mathcal{L}_3 = \{\langle 0\rangle, \langle 4u\rangle, \langle 2\rangle, \langle u\rangle, \langle 2u\rangle, \langle 4\rangle, \langle 4+u\rangle, \langle 4+2u\rangle, \langle 2+u\rangle, \langle 4, 2u\rangle, \langle 4, u\rangle, \langle 2, u\rangle, \langle 1\rangle\}$$

De la Proposición 2.1, $\mathfrak{m} = \langle 2, u\rangle$ y $\mathrm{Soc}(\mathcal{R}_3) = \mathfrak{m}^3 = \langle 4u\rangle$. Su diagrama de ideales es mostrado en la figura (b).

2.1. El conjunto de ideales de $\mathcal{R}_k$

Procedemos a estudiar el conjunto de ideales del anillo $\mathcal{R}_k$. A partir de la Proposición 2.1 sabemos que $\mathcal{R}_k$ tiene ideal máximo $\mathfrak{m} = \langle p, u\rangle$, por lo tanto cualquier ideal propio del anillo tendrá a lo más dos generadores.

2.1.1. Ideales principales de $\mathcal{R}_k$

El anillo $\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$ tal que $u^2 = 0$ es un anillo finito conmutativo con identidad y artiniano por lo tanto se cumple que si se tienen dos ideales principales $\langle r\rangle$, $\langle s\rangle$ tales que $\langle r\rangle = \langle s\rangle$ entonces r y s son elementos asociados en $\mathcal{R}_k$.

Primero se hará una observación de carácter elemental, pero que nos ayuda a estudiar el número de ideales principales del anillo $\mathcal{R}_k$.

Lema 2.2. *Sea I un ideal principal de $\mathcal{R}_k$. Entonces*

$$I = \langle p^d + \nu u \rangle,$$

para algún $\nu \in \{0, 1, 2, \ldots, p^d - 1\}$ y $1 \leq d \leq k$.

Demostración. Sea $I = \langle p^d\alpha + \beta u\rangle$. Sin pérdida de generalidad, es posible suponer $\alpha \in \mathcal{U}(\mathbb{Z}_{p^k})$. Se tienen dos casos: Si $\beta \in \mathcal{U}(\mathcal{R}_k)$, es sencillo ver que $I = \langle p^d + \alpha^{-1}\beta u\rangle$. Por otra parte, si $\beta \notin \mathcal{U}(\mathcal{R})$, entonces $\beta = p^j\gamma$ para alguna $\gamma \in \mathcal{U}(\mathbb{Z}_{p^k})$, i. e., $I = \langle p^d\alpha + p^j\gamma u\rangle$. Si $d < j$ es suficiente notar que $(\alpha + p^{j-d}\gamma u) \in \mathcal{U}(\mathcal{R})$ para obtener que $I = \langle p^d\rangle$. En el caso que $j < d$ se tiene que $\alpha^{-1}(p^d\alpha + p^j\gamma u) = p^d + p^j\alpha^{-1}\gamma u$, y así $I = \langle p^d + \alpha^{-1}\beta u\rangle$. Se ha probado, pues, que

$$I = \langle p^d + \alpha^{-1}\beta u\rangle \text{ ó } I = \langle p^d\rangle.$$

Resta ver que existe un $\nu \in \{0, 1, 2, \ldots, p^d - 1\}$ tal que $I = \langle p^d + \nu u\rangle$. Así, suponga que $\alpha^{-1}\beta \notin \{1, 2, \ldots, p^d - 1\}$. Es posible escribir $\alpha^{-1}\beta = p^d m + \nu$, donde $m \in \mathbb{Z}_{p^k}$, y $\nu \in \{0, 1, 2, \ldots, p^d - 1\}$. De ahí que

$$p^d + \alpha^{-1}\beta u = p^d + (p^d m + \nu)u = p^d(1 + mu) + \nu u,$$

y dado que $1 + mu \in \mathcal{U}(\mathcal{R})$ se tiene entonces que $(1 + mu)^{-1} = 1 + (p^k - m)u$, por lo tanto

$$(1 + mu)^{-1}(p^d(1 + mu) + \nu u) = (1 + (p^k - m)u)(p^d(1 + mu) + \nu u) = p^d + \nu u,$$

de donde $\langle p^d + \alpha^{-1}\beta u\rangle = \langle p^d + \nu u\rangle$, $\nu \in \{1, 2, \ldots, p^d - 1\}$. □

De lo anterior, consideramos al grupo de unidades $\mathcal{U}(\mathcal{R}_k)$ de $\mathcal{R}_k$ para hacer uso de algo de teoría de grupos y así obtener información sobre el número de ideales principales del anillo. Para tales fines recordemos lo siguiente: una acción (izquierda) de un grupo Γ en un conjunto $Y \neq \emptyset$ es una función $\star : \Gamma \times Y \longrightarrow Y$ que satisface

(a1) $e \star y = y$ para todo $y \in Y$, e el elemento neutro del grupo Γ.

(a2) Dados $\gamma_1, \gamma_2 \in \Gamma$ tenemos que

$$\gamma_2 \star (\gamma_1 \star y) = (\gamma_2 \cdot \gamma_1) \star y,$$

para todo $y \in Y$.

Dado un grupo Γ y una acción (izquierda) en un conjunto Y diremos que Y es un Γ-conjunto o que Γ actúa en Y. De manera por completo análoga es posible definir acciones derechas, pero para nuestros propósitos basta con la definición y aplicaciones de las acciones izquierdas.

Dado un grupo Γ y un Γ-conjunto Y, considere un $\gamma \in \Gamma$. Se define el conjunto de puntos fijos de Y bajo la acción de $\gamma \in \Gamma$, denotado Y^γ como

$$Y^\gamma = \{y \in Y \mid \gamma \star y = y\}.$$

Por otra parte, dados dos elementos $y_1, y_2 \in Y$, se dirá que y_2 es Γ-equivalente con y_1 si existe un $\gamma \in \Gamma$ tal que $\gamma \star y_1 = y_2$. Lo anterior induce una relación $\sim$ en Y que resulta ser de equivalencia, teniéndose así una partición de Y en clases donde, para cada $y \in Y$, su clase $[y]$ estará dada por

$$[y] = \{\gamma \star y \mid \gamma \in \Gamma\}.$$

Cada una de estas clases recibe el nombre de órbita de $y \in Y$ bajo la acción de Γ en Y.

En este contexto, recordemos el Lema de Frobenius-Burnside.

Teorema 2.3 (Lema de Frobenius-Burnside, [31]). *Sea Γ un grupo y $Y \neq \emptyset$ un Γ conjunto. Si N denota al número de órbitas de Y bajo la acción de Γ, entonces*

$$N = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} |Y^\gamma|.$$

En el caso particular del anillo $\mathcal{R}_k$, como se había mencionado al inicio de la Sección, consideremos $\Gamma = \mathcal{U}(\mathcal{R}_k)$ como grupo, y hagamos actuar $\star : \Gamma \times \mathcal{R}_k \longrightarrow \mathcal{R}_k$ por traslación, esto es,

$$\gamma \star r = \gamma r.$$

Entonces, por una aplicación directa del Lema de Frobenius-Burnside, calculamos el número de ideales principales de $\mathcal{R}_k$ de la siguiente manera.

Teorema 2.4. *Sean $\gamma \in \Gamma$ y $X^\gamma = \{x \in \mathcal{R}_k \mid \gamma \cdot x = x\}$ el conjunto fijo de γ bajo la acción de grupo dada. Entonces, el número N_{p^k} de ideales principales I de $\mathcal{R}_k$ tales que*

$$I = \langle p^d + \nu u \rangle,\ 1 \leq d \leq k, \nu \in \{0, 1, \ldots, p^d - 1\} \text{ ó } I = \langle p^d u \rangle$$

es

$$N_{p^k} = \frac{1}{p^{2k-1}(p-1)} \sum_{\gamma \in \Gamma} |X^\gamma|.$$

Ejemplo 3. Sea $p = 2$ y considere el anillo $\mathcal{R}_3 = \mathbb{Z}_8 + u\mathbb{Z}_8$ del ejemplo 2. Para cada $\gamma \in \mathcal{U}(\mathcal{R}_3)$, usando un programa hecho en el software SageMath ([32]), se tiene la siguiente tabla, a partir de la cual se realiza el conteo de ideales principales,

γ	$\lvert X^\gamma\rvert$	γ	$\lvert X^\gamma\rvert$	γ	$\lvert X^\gamma\rvert$	γ	$\lvert X^\gamma\rvert$
1	64	$1+5u$	8	$3+6u$	4	$5+7u$	8
3	4	$1+6u$	16	$3+7u$	4	$7+u$	4
5	16	$1+7u$	8	$5+u$	8	$7+2u$	4
7	4	$3+u$	4	$5+2u$	16	$7+3u$	4
$1+u$	8	$3+2u$	4	$5+3u$	8	$7+4u$	4
$1+2u$	16	$3+3u$	4	$5+4u$	16	$7+5u$	4
$1+3u$	8	$3+4u$	4	$5+5u$	8	$7+6u$	4
$1+4u$	32	$3+5u$	4	$5+6u$	16	$7+7u$	4

Cuadro 2.1: Cardinalidades del conjunto fijo X^γ de la unidad $\gamma \in \mathcal{U}(\mathcal{R}_3)$

donde $X^\gamma = \{x \in X \mid \gamma \cdot x = x\}$. Así $\sum_{\gamma\in\Gamma}|X^\gamma| = 320$; por el Teorema 2.4 se tienen

$$N_8 = \frac{1}{2^5}\sum_{\gamma\in\Gamma}|X^\gamma| = \frac{320}{32} = 10$$

ideales principales. Nótese que los ideales triviales $\langle 0\rangle$ y $\langle 1\rangle$ están siendo considerados en el conteo.

Se realizaron cálculos similares para los anillos $\mathbb{Z}_{16}+u\mathbb{Z}_{16}$, $\mathbb{Z}_{81}+u\mathbb{Z}_{81}$ y $\mathbb{Z}_{625}+u\mathbb{Z}_{625}$ obteniendo

p^k	2^4	3^4	5^4
N_{p^k}	15	25	49

Cuadro 2.2: Número de ideales principales N_{p^k} de los anillos $\mathcal{R}_k$ con parámetros $p = 3, 4, 5$ y $k = 4$

2.1.2. Ideales con dos generadores

Debido a que el ideal máximo de $\mathcal{R}_k$ es $\mathfrak{m} = \langle p, u\rangle$, se tiene que ninguno de los ideales del anillo $\mathcal{R}_k$ será generado por más de dos elementos. La cantidad de ideales del anillo aumenta conforme k lo hace por lo que los esfuerzos se dirigen hacia determinar criterios simples para descartar ideales con dos generadores duplicados. No es complicado probar a partir de las definiciones que, dados α_1 y α_2 elementos de $\mathcal{R}_k\backslash\mathcal{U}(\mathcal{R}_k)$, se tendrá que $\langle\alpha_1, \alpha_2\rangle$ es un ideal con dos generadores si $\alpha_i \notin \langle\alpha_j\rangle$ para $i \neq j$, $i, j \in \{1, 2\}$. Consecuentemente, se tiene la siguiente

Proposición 2.5. *El anillo $\mathcal{R}_k$ tiene al menos los siguientes ideales generados por 2 elementos*

$$\langle p^d, u\rangle, \langle p^d, pu\rangle, \langle p^d, p^2u\rangle, \ldots, \langle p^d, p^{d-1}u\rangle$$

para $1 \leq d \leq k-1$.

Con el objetivo de facilitar la tarea para calcular los ideales, algunos criterios para descartar ideales duplicados en $\mathcal{R}_k$ son los siguientes.

Proposición 2.6. *Sea $I = \langle p^d + \nu u, p^d + \rho u\rangle$ un ideal generado por dos elementos. Si $\nu \not\equiv \rho \mod p$, entonces*

$$I = \langle p^d, u\rangle.$$

Demostración. De la hipótesis $\nu \not\equiv \rho \mod p$ se tiene que $\nu - \rho$ es una unidad en $\mathbb{Z}_{p^k}$ y por ende en $\mathcal{R}_k$, de donde

$$(p^d + \nu u) - (p^d + \rho u) = (\nu - \rho)u \in I$$

y por lo tanto $u \in I$. De esto se sigue fácilmente que $p^d \in I$ y por lo tanto $\langle p^d, u\rangle \subseteq I$. La otra contención se sigue de las definiciones. □

Con una idea similar en los cálculos de la prueba, se puede probar la siguiente proposición.

Proposición 2.7. *Si $I = \langle p^d + p^l\alpha u, p^d + p^m\beta u\rangle$ con $\alpha, \beta \in \mathcal{U}(\mathbb{Z}_{p^k})$ es un ideal de $\mathcal{R}_k$ con dos generadores y $m \leq l$, entonces, $I = \langle p^d, p^m u\rangle$ si y sólo si $p^m u \in I$.*

Cabe señalar que es posible plantear algunos criterios similares para descartar ideales con dos generadores, los cuales se obtienen a partir de los resultados iniciales dados al inicio de esta sección. A continuación se muestran los conjuntos de ideales para los anillos $\mathcal{R}_3 = \mathbb{Z}_{27} + u\mathbb{Z}_{27}$, $p = 3$, y $\mathcal{R}_4 = \mathbb{Z}_{16} + u\mathbb{Z}_{16}$ con $p = 2$. Los cálculos fueron programados con el software SageMath.

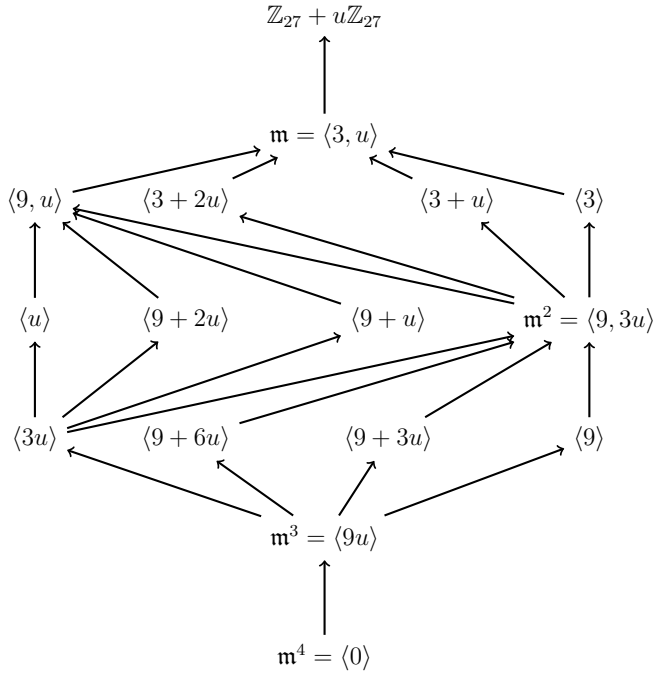


Figura 2.2: Ideales de $\mathcal{R}_3 = \mathbb{Z}_{27} + u\mathbb{Z}_{27}$

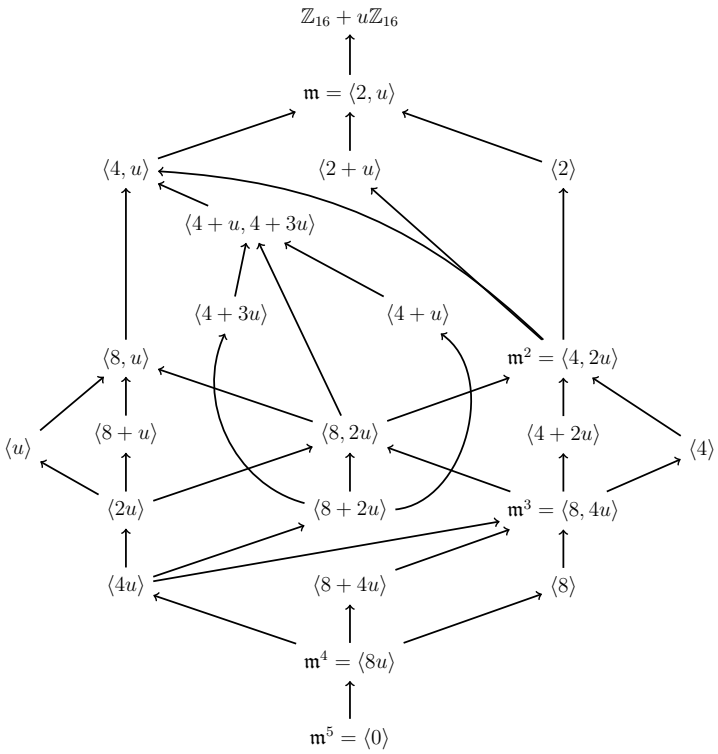


Figura 2.3: Ideales de $\mathcal{R}_4 = \mathbb{Z}_{16} + u\mathbb{Z}_{16}$

En el apéndice A se dan los generadores de los ideales para cuando el primo es $p = 2$, teniendo así los anillos $\mathcal{R}_k$ para $k = 2, 3, 4, 5, 6, 7$.

Capítulo 3

Códigos constacíclicos sobre $\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$

En el presente capítulo se desarrolla la parte central de este trabajo, esto es, dado un primo p, el estudio de los códigos constacíclicos de longitud n, con n y p primos relativos, definidos sobre el anillo $\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$, $u^2 = 0$. Se obtiene la descripción de los mismos y se proporcionan ejemplos computacionales para ilustrar las aplicaciones del desarrollo teórico.

3.1. Códigos constacíclicos sobre $\mathcal{R}_k$

Recordemos que un código lineal de longitud n definido sobre un anillo finito conmutativo con identidad $\mathcal{R}$ es un $\mathcal{R}$-submódulo $\mathcal{C} \subset \mathcal{R}^n$. Dada una unidad $\gamma \in \mathcal{U}(\mathcal{R})$, un código lineal $\mathcal{C}$ se dirá **constacíclico** o (γ-constacíclico si se quiere enfatizar la respectiva unidad) si, dada una palabra $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \subset \mathcal{R}^n$, entonces $(\gamma c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$.

Dado un anillo conmutativo con identidad $\mathcal{R}$ y una unidad del mismo, $\gamma \in \mathcal{U}(\mathcal{R})$, de la representación polinomial $\mathcal{P} : \mathcal{R}^n \longrightarrow \mathcal{R}[x]$ dada por

$$(c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$$

se induce un isomorfismo entre $\mathcal{R}^n$ y el anillo cociente $\mathcal{R}[x]/\langle x^n - \gamma \rangle$, de lo cual se tiene una correspondencia biyectiva entre los códigos γ-constacíclicos y los ideales del anillo cociente $\mathcal{R}[x]/\langle x^n - \gamma \rangle$. No está de más mencionar que los elementos de este último anillo son tratados como polinomios de grado menor que n.

De lo dicho líneas arriba, la discusión siguiente se desarrollará al considerar un número primo p y un entero positivo n tal que $\text{mcd}(p, n) = 1$; el anillo $\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$, donde $u^2 = 0$ y $k > 1$ es un entero. Así, dada una unidad $\gamma \in \mathcal{U}(\mathcal{R}_k)$, nuestro objetivo es estudiar los ideales del anillo $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - \gamma \rangle$.

3.1.1. Resultados básicos

Dado un polinomio mónico básico irreducible $f \in \mathcal{R}_k[x]$, se considera el anillo cociente

$$\mathcal{R}_{k,f} = \mathcal{R}_k[x]/\langle f \rangle.$$

Se estudia la estructura del mismo con la finalidad de ver cómo se relaciona su estructura de ideales con la correspondiente estructura de ideales del anillo $\mathcal{R}_k$. Con tal notación se establece el siguiente lema.

Lema 3.1. *Sean $f \in \mathcal{R}_k[x]$ un polinomio mónico básico irreducible y $\mathcal{R}_{k,f} = \mathcal{R}_k[x]/\langle f \rangle$. Dado $g \in \mathcal{R}_k[x]$, se tiene que $g + \langle f \rangle \in \mathcal{U}(\mathcal{R}_{k,f})$ si y sólo si g es primo relativo con f en $\mathcal{R}_k[x]$.*

Demostración. Suponga que $f, g \in \mathcal{R}_k[x]$ son primos relativos. Por definición, $\langle g \rangle + \langle f \rangle = \langle 1 \rangle$ en $\mathcal{R}_k[x]$ implica que existen $h_0, h_1 \in \mathcal{R}_k[x]$ tales que $h_0 g + h_1 f = 1$ de donde, en $\mathcal{R}_{k,f}$, $h_0 g + \langle f \rangle = 1 + \langle f \rangle$ y así $g + \langle f \rangle \in \mathcal{U}(\mathcal{R}_{k,f})$. Recíprocamente, suponga que se tiene $g + \langle f \rangle \in \mathcal{U}(\mathcal{R}_{k,f})$. Por definición, existe un $h + \langle f \rangle$ en $\mathcal{R}_{k,f}$ tal que $(g + \langle f \rangle)(h + \langle f \rangle) = 1 + \langle f \rangle$. Entonces existen F_0, F_1 en $\mathcal{R}_k[x]$ tales que $gh + fF_0 = 1 + fF_1$ de donde $\langle g \rangle + \langle f \rangle = \langle 1 \rangle$ en $\mathcal{R}_k[x]$. □

Corolario 3.2. *Con la notación como en el Lema 3.1, si $f, h \in \mathcal{R}_k[x]$ no son primos relativos en $\mathcal{R}_k[x]$, entonces $(1 + h) + \langle f \rangle \in \mathcal{U}(\mathcal{R}_{k,f})$.*

Demostración. Si $h \in \mathfrak{m}[x] \subset \mathcal{R}_k[x]$ el resultado es inmediato: $(1 + h) + \langle f \rangle \in \mathcal{U}(\mathcal{R}_{k,f})$ ya que $1 + \langle f \rangle$ es una unidad y $h + \langle f \rangle$ es nilpotente. Supóngase, pues, que $h \notin \mathfrak{m}[x]$. Por hipótesis $\overline{h}$ y $\overline{f}$ no son primos relativos en $\mathbb{F}_p[x]$ lo que significa, dado que $\overline{f}$ es irreducible, que $\overline{h} = \overline{h}_0 \overline{f}$ para algún $\overline{h}_0 \in \mathbb{F}_p[x]$. Así

$$\overline{1 + h} - \overline{h}_0 \overline{f} = 1 + \overline{h}_0 \overline{f} - \overline{h}_0 \overline{f} = 1 \in \mathbb{F}_p[x]$$

y por el Lema 1.5 se tiene que $1 + h$ y f son coprimos en $\mathcal{R}_k[x]$. El resultado se sigue ahora por el Lema 3.1. □

Proposición 3.3. *Sea $f \in \mathcal{R}_k[x]$ un polinomio mónico básico irreducible. Entonces, $\mathcal{R}_{k,f}$ es un anillo local.*

Demostración. Se mostrará que el conjunto de no unidades $\mathfrak{M}$ de $\mathcal{R}_{k,f}$ es un ideal. Para probar tal afirmación basta con mostrar que $\mathfrak{M}$ es cerrado bajo la adición. Así pues, sean $g + \langle f \rangle, h + \langle f \rangle$ no unidades. Por el Lema 3.1 g y h no son, respectivamente, primos relativos en $\mathcal{R}_k[x]$ con f. Suponga, sin pérdida de generalidad, que $(g + h) + \langle f \rangle = 1 + \langle f \rangle$. Esto implica que $g + \langle f \rangle = (1 - h) + \langle f \rangle$ lo que nos conduce a un absurdo: por un lado $g + \langle f \rangle$ es una no unidad de $\mathcal{R}_{k,f}$ y por el otro, en $\mathcal{R}_k[x]$, se tiene que $\langle 1 - h \rangle + \langle f \rangle = \langle 1 \rangle$ debido a que, bajo el mapeo reducción, $\overline{1 - h}$ y $\overline{f}$ son primos relativos en $\mathbb{F}_2[x]$, y usando el Lema 1.5 se tiene que $(1 - h) + \langle f \rangle \in \mathcal{U}(\mathcal{R}_{k,f})$. Así, tenemos que las no unidades de $\mathcal{R}_{k,f}$ forman un ideal y por lo tanto $\mathcal{R}_{k,f}$ es un anillo local. □

Proposición 3.4. *Sean $f \in \mathcal{R}_k[x]$ un polinomio mónico, básico, irreducible y $\mathcal{R}_{k,f} = \mathcal{R}_k[x]/\langle f\rangle$. Entonces, cualquier ideal $\mathcal{I}$ de $\mathcal{R}_{k,f}$ tiene la forma*

$$\mathcal{I} = I\mathcal{R}_{k,f},$$

donde $I\mathcal{R}_{k,f}$ denota la extensión del ideal I de $\mathcal{R}_k$ al anillo $\mathcal{R}_{k,f}$.

Demostración. De la Proposición 3.3 se tiene que el conjunto de no unidades $\mathfrak{M}$ es el ideal máximo de $\mathcal{R}_{k,f}$, de lo cuál se sigue que $\mathfrak{m}\mathcal{R}_{k,f} \subseteq \mathfrak{M}$. Sea $g + \langle f\rangle$ un elemento no cero de $\mathfrak{M}$. Existen $h \in \mathcal{R}_k[x]$ y $r \in \mathfrak{m}[x]$ tales que $g = hf + r$ de donde $g + \langle f\rangle = r + \langle f\rangle$ y así $\mathfrak{M} \subseteq \mathfrak{m}\mathcal{R}_{k,f}$.
Sea $\mathcal{I} \subset \mathfrak{M}$ un ideal y considere $g + \langle f\rangle \in \mathcal{I}$. Sea $J = \pi^{-1}(\mathcal{I})$, donde π es el mapeo canónico $\mathcal{R}_k[x] \longrightarrow \mathcal{R}_{k,f}$. El conjunto J es un ideal propio de $\mathcal{R}_k[x]$. Existe un ideal I de $\mathcal{R}_k$ tal que $J = \langle f, I[x]\rangle$ donde $I[x] \subseteq \mathfrak{m}[x]$. Dado que existe un $r \in \pi^{-1}(g + \langle f\rangle) \subset J$ y como $\pi(\pi^{-1}(g + \langle f\rangle)) \subset \pi(\pi^{-1}(\mathcal{I})) = \pi(J) = I\mathcal{R}_{k,f}$ se tiene que $\pi(r) = g + \langle f\rangle \in I\mathcal{R}_{k,f}$, por lo tanto $\mathcal{I} \subseteq I\mathcal{R}_{k,f}$. La otra inclusión se sigue del hecho de que si $h + \langle f\rangle \in I\mathcal{R}_{k,f}$, entonces $\pi^{-1}(h + \langle f\rangle) \subset J = \pi^{-1}(\mathcal{I})$. □

Sea $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - \gamma\rangle$. Lo siguiente es consecuencia directa del Teorema Chino del Residuo 1.10.

Teorema 3.5. *Sean $\gamma \in \mathcal{U}(\mathcal{R}_k)$, p un primo y $n > 0$ un entero tal que $\mathrm{mcd}(p, n) = 1$. Suponga que $x^n - \gamma = \prod_{i=1}^{m} f_i$, donde los polinomios f_i son distintos, mónicos, básicos irreducibles y coprimos por pares en $\mathcal{R}_k[x]$. Entonces,*

$$\mathcal{R}_{k,n} \cong \bigoplus_{i=1}^{m} \mathcal{R}_{k,f_i},$$

donde $\mathcal{R}_{k,f_i} = \mathcal{R}_k[x]/\langle f_i\rangle$. En particular, cualquier ideal I of $\mathcal{R}_{k,n}$ es tal que

$$I \cong \bigoplus_{i=1}^{m} I_i\mathcal{R}_{k,f_i},$$

donde I_i es un ideal de $\mathcal{R}_k$.

Como una consecuencia inmediata del Teorema 3.5 se tiene lo siguiente.

Corolario 3.6. *Dado un primo p, n un entero tal que $\mathrm{mcd}(p, n) = 1$ y $x^n - \gamma = \prod_{i=1}^{m} f_i$ como en el Teorema 3.5.*

1. *El anillo $\mathcal{R}_{k,n}$ no es de ideales principales.*
2. *Sea $\mathcal{L}_k$ el conjunto de ideales del anillo $\mathcal{R}_k$ (incluyendo el ideal trivial $\langle 1\rangle$) y m el número de factores de $x^n - \gamma$ en $\mathcal{R}_k[x]$. Entonces el anillo $\mathcal{R}_{k,n}$ tiene $|\mathcal{L}_k|^m$ ideales.*
3. *El anillo $\mathcal{R}_{k,n}$ es semilocal. Más aún, $\mathcal{R}_{k,n}$ tiene exactamente m ideales máximos.*

Demostración. Con la notación anterior, para la primera afirmación considere el ideal $I = \mathfrak{m}\mathcal{R}_{k,f_1} \bigoplus_{i=2}^{m} \langle f_i \rangle$. Se sigue del Teorema 3.5 que dado que el ideal $\mathfrak{m}\mathcal{R}_{k,f_1} \bigoplus_{i=2}^{m} \langle f_i \rangle$ tiene al menos dos generadores, su preimagen bajo el isomorfismo dado por 3.5 es un ideal con al menos dos generadores. La segunda afirmación es una consecuencia directa del principio multiplicativo del conteo. La tercera afirmación se sigue del hecho que los ideales $\mathfrak{M}_j$ con forma

$$\mathfrak{M}_j = (\langle 1 + \langle f_1 \rangle \rangle, \ldots, \langle p + \langle f_j \rangle, u + \langle f_j \rangle \rangle, \ldots, \langle 1 + \langle f_m \rangle \rangle)$$

son máximos para cada $1 \leq j \leq m$. Más aún,

$$\left(\bigoplus_{i=1}^{m} \mathcal{R}_{k,f_i} \right) / \mathfrak{M}_j \cong \mathbb{F}_{p^{\deg f_j}},$$

y por lo tanto su preimagen bajo el isomorfismo del Teorema 3.5 debe ser un ideal máximo. □

Recordemos que el anillo $\mathcal{R}_k$ es local con ideal máximo $\mathfrak{m} = \langle p, u \rangle$ y campo residual $\mathbb{F}_p$. Si $f \in \mathcal{R}_k[x]$ su imagen bajo la función reducción módulo $\mathfrak{m}$ a $\mathbb{F}_p[x]$ es denotada por $\overline{f}$. Se tiene lo siguiente:

Proposición 3.7. *Sean γ una unidad del anillo $\mathcal{R}_k$, $x^n - \gamma = \prod_{i=1}^{m} f_i$ donde n es un entero no divisible por p y los f_i's son polinomios distintos, mónicos, básicos irreducibles y primos relativos por pares en $\mathcal{R}_k[x]$. Sea $\overline{x^n - \gamma} = \Pi_{i=1}^{m} \overline{f_i}$ como producto correspondiente de factores irreducibles en $\mathbb{F}_p[x]$. Entonces, un ideal principal distinto de cero $\mathcal{C} = \langle f + \langle x^n - \gamma \rangle \rangle \subseteq \mathcal{R}_{k,n}$ es trivial si y sólo si $\operatorname{mcd}(\overline{f}, \overline{x^n - \gamma}) = 1$ en $\mathbb{F}_p[x]$.*

Demostración. Si $\operatorname{mcd}(\overline{f}, \overline{x^n - \gamma}) = 1$, entonces $\operatorname{mcd}(\overline{f}, \overline{f_i}) = 1$ para todo i y del Lema 1.5 se tiene que $\langle f \rangle + \langle f_i \rangle = \langle 1 \rangle$ en $\mathcal{R}_k[x]$. El Teorema 3.5 y el Lema 3.1 implican

$$\langle f + \langle x^n - \gamma \rangle \rangle \cong \oplus_{i=1}^{m} \langle 1 + \langle f_i \rangle \rangle = \bigoplus_{i=1}^{m} \mathcal{R}_{k,f_i}.$$

Recíprocamente, suponga $\mathcal{C} = \langle f + \langle x^n - \gamma \rangle \rangle$ es un ideal no cero y trivial $\mathcal{R}_{k,n}$. Entonces, existe $h + \langle x^n - \gamma \rangle$ tal que $fh + \langle x^n - \gamma \rangle = 1 + \langle x^n - \gamma \rangle$ de donde $fh \equiv 1 \mod \langle f_i \rangle$, $i = 1, \ldots, m$, y por la Proposición 3.1 f y f_i son primos relativos en $\mathcal{R}_k[x]$. Aplicando directamente el Lema 1.5 tendremos que $\operatorname{mcd}(\overline{f}, \overline{x^n - \gamma}) = 1$ en $\mathbb{F}_p[x]$. □

3.2. Descripción de códigos constacíclicos mediante elementos idempotentes

En esta sección se presenta la descripción de códigos constacíclicos definidos sobre el anillo $\mathcal{R}_k$ por medio de elementos idempotentes del anillo

$$\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - \gamma \rangle, \gamma \in \mathcal{U}(\mathcal{R}_k).$$

Recordemos que, dados un primo p y un entero n no divisible por p, es posible descomponer al polinomio $x^n-\gamma$, en $\mathcal{R}_k[x]$, como producto de polinomios mónicos básicos irreducibles coprimos por pares, esto es, $x^n-\gamma=\prod_{i=1}^m f_i$ y de la aplicación del Teorema Chino del Residuo (3.5), se tiene el isomorfismo de anillos $\mathcal{R}_{k,n}\cong\bigoplus_{i=1}^m\mathcal{R}_{k,f_i}$ donde para cada i,

$$\mathcal{R}_{k,f_i}=\mathcal{R}_k[x]/\langle f_i\rangle.$$

En $\bigoplus_{i=1}^m\mathcal{R}_{k,f_i}$ se tiene un conjunto completo de elementos idempotentes primitivos y ortogonales por pares $\{\mathbf{e}_1,\mathbf{e}_2,\ldots,\mathbf{e}_m\}$ donde $\mathbf{e}_i=(0,\ldots,1+\langle f_i\rangle,\ldots,0)$, elemento que tiene coordenadas cero en todas las posiciones $j\neq i$. Del Corolario 1.11, tenemos el isomorfismo $\Phi:\mathcal{R}_{k,n}\longrightarrow\bigoplus_{i=1}^m\mathcal{R}_{k,f_i}$ dado por

$$\Phi(c+\langle x^n-\gamma\rangle)=(c_1+\langle f_1\rangle,c_2+\langle f_2\rangle,\ldots,c_m+\langle f_m\rangle),$$

donde $c\equiv c_i\mod\langle f_i\rangle$ para $i=1,2,\ldots,m$. La situación descrita puede verse en el siguiente diagrama, donde los isomorfismos son los dados del Teorema Chino del Residuo 3.5, es decir Φ, y en las flechas verticales tenemos las correspondientes funciones reducción.

$$\begin{array}{ccc}\mathcal{R}_k[x]/\langle x^n-\gamma\rangle & \xrightarrow{\Phi} & \bigoplus_{i=1}^m\mathcal{R}_k[x]/\langle f_i\rangle \\ \downarrow & & \downarrow \\ \mathbb{F}_p[x]/\langle\overline{x^n+\gamma}\rangle & \xrightarrow[\cong]{} & \bigoplus_{i=1}^m\mathbb{F}_p[x]/\langle\overline{f}_i\rangle.\end{array}$$

Para los propósitos de este trabajo, será necesario determinar el isomorfismo inverso de Φ, lo cual hacemos a partir de las consideraciones siguientes. Dado $x^n-\gamma=\prod_{i=1}^m f_i$ en $\mathcal{R}_k[x]$ como producto de básicos irreducibles coprimos por pares, sea $F_i=\overline{f}_i$ para $i=1,2,\ldots,m$. Así, para la correspondiente reducción se tiene la expresión $\overline{x^n-\gamma}=\prod_{i=1}^m F_i$ como producto de polinomios irreducibles, primos, relativos por pares en $\mathbb{F}_p[x]$. Definamos $\hat{F}_i=\prod_{j\neq i}F_j$, entonces $\mathrm{mcd}(\hat{F}_1,\hat{F}_2,\ldots,\hat{F}_m)=1$ y del Lema 1.5, en $\mathcal{R}_k[x]$, los correspondientes $\hat{f}_1,\ldots,\hat{f}_m$ donde $\hat{f}_i=\prod_{j\neq i}f_j$, son primos relativos; por lo que existe, para $i=1,2,\ldots,m$, $\hat{\lambda}_i\in\mathcal{R}_k[x]$ tal que

$$\hat{\lambda}_1\hat{f}_1+\hat{\lambda}_2\hat{f}_2+\ldots+\hat{\lambda}_m\hat{f}_m=1.$$

Observe que $\sum_{j=1}^m\hat{\lambda}_j\hat{f}_j\equiv\hat{\lambda}_i\hat{f}_i\equiv 1\mod\langle f_i\rangle$, $i=1,2,...,m$. Así, la función ϕ definida de $\bigoplus_{i=1}^m\mathcal{R}_{k,f_i}$ a $\mathcal{R}_{k,n}$ como

$$\phi(c_1+\langle f_1\rangle,c_2+\langle f_2\rangle,\ldots,c_m+\langle f_m\rangle)=\sum_{i=1}^m\hat{\lambda}_i\hat{f}_ic_i+\langle x^n-\gamma\rangle,$$

es el isomorfismo inverso de Φ definido líneas arriba.

Proposición 3.8. *Sea $\mathcal{R}_k=\mathbb{Z}_{p^k}+u\mathbb{Z}_{p^k}$, con $u^2=0$, p primo y n un entero primo relativo con p. Considere el polinomio $x^n-\gamma=\prod_{i=1}^m f_i$ como producto de polinomios f_i mónicos, básicos irreducibles y primos relativos por pares. Entonces, el conjunto*

$$E_{k,n}=\{\hat{e}_1,\hat{e}_2,...,\hat{e}_m\},$$

donde $\hat{e}_i = \hat{\lambda}_i \hat{f}_i + \langle x^n - \gamma \rangle$, $\hat{f}_i = \prod_{j \neq i} f_j$, *y los* $\hat{\lambda}_i$, $i = 1, 2, ..., m$, *definido anteriormente es un conjunto completo de elementos idempotentes primitivos ortogonales por pares del anillo* $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - \gamma \rangle$.

Demostración. Sea $\hat{e}_i = \phi(\mathbf{e}_i)$ donde $\mathbf{e}_i$ es el i-ésimo vector coordenado de $\bigoplus_{i=1}^m \mathcal{R}_{k,f_i}$ y $\phi = \Phi^{-1}$ el isomorfismo definido previamente. De la definición de ϕ se tiene que $\hat{e}_i = \hat{\lambda}_i \hat{f}_i + \langle x^n - \gamma \rangle$ es elemento idempotente. Para $i \neq j$ tenemos que

$$\hat{e}_i \hat{e}_j + \langle x^n - \gamma \rangle = 0,$$

ya que $\hat{f}_i \hat{f}_j = (x^n - \gamma) h(x)$ y por construcción de ϕ se tiene que

$$\hat{e}_1 + \hat{e}_2 + \ldots + \hat{e}_m = 1 + \langle x^n - \gamma \rangle. \qquad \square$$

Nótese en la exposición anterior lo siguiente: existe una versión del algoritmo de Euclides en $\mathcal{R}_k$ a partir del cuál los $\hat{\lambda}_i$ serían calculados (dados $f, g \in \mathcal{R}_k[x]$, con g regular, tal algoritmo existe, ver [21] ejercicio XIII.6). Cabe mencionar en este punto que para propósitos teóricos esto funciona bien, sin embargo, un poco más adelante se presentará un método para aplicar en la práctica: de las propiedades de $\mathcal{R}_k$ que se transfieren al anillo $\mathcal{R}_{k,n}$, es posible obtener el conjunto $E_{k,n}$ por medio de levantamiento de elementos idempotentes ([33]), esto dada la unicidad del conjunto completo de elementos idempotentes primitivos y ortogonales por pares $E_{k,n}$.

Obsérvese también que, si el conjunto completo de elementos idempotentes primitivos ortogonales por pares $E_{k,n}$ de $\mathcal{R}_{k,n}$ es dado, entonces el isomorfismo de anillos $\phi : \bigoplus_{i=1}^m \mathcal{R}_{k,f_i} \longrightarrow \mathcal{R}_{k,n}$ puede ser escrito en términos de esos elementos idempotentes como

$$\phi(c_1 + \langle f_1 \rangle, c_2 + \langle f_2 \rangle, ..., c_m + \langle f_m \rangle) = \sum_{i=1}^m c_i \hat{e}_i + \langle x^n - \gamma \rangle. \tag{3.1}$$

Con esta presentación de ϕ podemos establecer lo siguiente.

Corolario 3.9. *Dado un entero positivo* n *primo relativo con* p, *sea* $\mathcal{C}$ *un código constacíclico de longitud* n *definido sobre* $\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$. *Dado* $x^n - \gamma = \prod_{i=1}^m f_i$ *como producto de polinomios mónicos, básicos irreducibles y primos relativos por pares en* $\mathcal{R}_k[x]$, *se tiene que*

$$\mathcal{C} = \langle F + \langle x^n - \gamma \rangle, H + \langle x^n - \gamma \rangle \rangle.$$

Demostración. De la Proposición 3.4 y el Corolario 3.6 cualquier ideal $\mathcal{C}$ en $\mathcal{R}_{k,n}$ tiene a lo más dos generadores: para un ideal máximo

$$\mathfrak{M}_j = (\langle 1 + \langle f_1 \rangle \rangle, \ldots, \langle p + \langle f_j \rangle, u + \langle f_j \rangle \rangle, \ldots, \langle 1 + \langle f_m \rangle \rangle)$$

en $\bigoplus_{i=1}^m \mathcal{R}_{k,f_i}$. En $\mathcal{R}_{k,n}$ se tiene que,

$$\phi(\mathfrak{M}_j) = \langle p\hat{e}_j + \sum_{i \neq j}^m \hat{e}_i + \langle x^n - \gamma \rangle, u\hat{e}_j + \sum_{i \neq j}^m \hat{e}_i + \langle x^n - \gamma \rangle \rangle,$$

donde $\hat{e}_i \in E_{k,n}$, el conjunto completo de elementos idempotentes primitivos ortogonales por pares de $\mathcal{R}_{k,n}$. Dado un ideal no trivial $\bigoplus_{i=1}^{m} \mathcal{C}_i$ en $\bigoplus_{i=1}^{m} \mathcal{R}_{k,f_i}$ cada ideal $\mathcal{C}_i \subset \mathcal{R}_{k,f_i}$ tiene a lo más dos generadores. Sea

$$G = \{p^d + u\nu \in \mathcal{R}_k \mid 0 \leq d \leq k, \nu \in \{0, 1, \ldots, p^d - 1\}\} \cup \{p^d u \mid 1 \leq d \leq k-1\}$$

el conjunto de generadores de los ideales principales en $\mathcal{R}_k$. Entonces, de la Proposición 3.4, para cada $1 \leq j \leq m$ se tiene que

$$\mathcal{C}_j = \langle g_{jl_1} + \langle f_j \rangle, g_{jl_2} + \langle f_j \rangle \rangle,$$

para algún $g_{jl_1}, g_{jl_2} \in G$. Lo anterior implica que

$$\phi(\bigoplus_{j=1}^{m} \mathcal{C}_j) = \left\langle \sum_{j=1}^{m} g_{jl_1}\hat{e}_j + \langle x^n - \gamma \rangle, \sum_{j=1}^{m} g_{jl_2}\hat{e}_j + \langle x^n - \gamma \rangle \right\rangle,$$

Y el resultado se cumple al hacer $F = \sum_{j=1}^{m} g_{jl_1}\hat{e}_j$ y $H = \sum_{j=1}^{m} g_{jl_2}\hat{e}_j$. □

Corolario 3.10. *Un ideal $\mathcal{C} \subseteq \mathcal{R}_{k,n}$ es principal si y sólo si $\mathcal{C} \cong \oplus_{i=1}^{m} \mathcal{C}_i$ con cada $\mathcal{C}_i$ ideal principal en $\mathcal{R}_{k,f_i}$.*

Nótese que cuando el isomorfismo ϕ definido arriba es restringido a cada sumando de $\bigoplus_{i=1}^{m} \mathcal{R}_{k,f_i}$ se induce un isomorfismo de anillos ϕ_i entre $\mathcal{R}_{k,f_i}$ y el anillo $\hat{e}_i\mathcal{R}_{k,n} = \langle \hat{e}_i \rangle$, donde $\hat{e}_i \in E_{k,n}$. Más aún, se tiene $\mathcal{R}_{k,f_i} \cong \langle \hat{f}_i + \langle x^n - \gamma \rangle \rangle$ como anillos, donde $\phi_i(1 + \langle f_i \rangle) = \hat{e}_i + \langle x^n - \gamma \rangle$. Por lo tanto, de la Proposición 3.4, cada ideal $I_i\mathcal{R}_{k,f_i}$ es mapeado por medio de ϕ_i a un ideal $I_i\mathcal{R}_{k,n}\hat{e}_i = I_i\mathcal{R}_{k,n}(\hat{f}_i + \langle x^n - \gamma \rangle)$ en $\mathcal{R}_{k,n}$, y entonces todo ideal $\mathcal{C}$ de $\mathcal{R}_{k,n}$ es suma de ideales $I_i\mathcal{R}_{k,n}\hat{e}_i$, i.e., $\mathcal{C} = \sum_{i=1}^{m} I_i\mathcal{R}_{k,n}\hat{e}_i = \sum_{i=1}^{m} I_i\mathcal{R}_{k,n}(\hat{f}_i + \langle x^n - \gamma \rangle)$. Establecemos lo anterior formalmente en el siguiente corolario.

Corolario 3.11. *Considere el anillo $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - \gamma \rangle$, donde $\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$, $u^2 = 0$ y $n > 0$ un entero no divisible por p. Sea $x^n - \gamma = \prod_{i=1}^{m} f_i$ la presentación de $x^n - \gamma$ como producto de polinomios distintos, mónicos, básicos irreducibles y coprimos por pares en $\mathcal{R}_k[x]$ y sea $\mathcal{C}$ un ideal en $\mathcal{R}_{k,n}$. Entonces,*

$$\mathcal{C} = \sum_{i=1}^{m} I_i\mathcal{R}_{k,n}\hat{e}_i,$$

donde I_i es un ideal de $\mathcal{R}_{k,f_i}$ y $\hat{e}_i \in E_{k,n}$.

Con el objetivo de dar la descripción de un código constacíclico en términos de elementos idempotentes en $\mathcal{R}_{k,n}$ se enuncia el siguiente lema,

Lema 3.12. *Sea $\mathcal{C} = \langle f \rangle$ un ideal principal en un anillo conmutativo $\mathcal{R}$ con identidad y sea e un elemento idempotente no trivial en $\mathcal{C}$. Entonces,*

(a) $\mathcal{C} = \langle e \rangle$ *si y sólo si* $f = ef$. *En este caso,* $ec = c$ *para todo* $c \in \mathcal{C}$.

(b) El idempotente e *tal que* $\langle f \rangle = \langle e \rangle$ *es único.*

Demostración. Supongamos que $\mathcal{C} = \langle e \rangle$, con e un elemento idempotente. Entonces, $f = eg$ para algún $g \in \mathcal{R}$. De ahí que $ef = e(eg) = e^2 g = eg = f$. Note que esto implica en general que para cualquier $c \in \mathcal{C}$, con las hipótesis dadas, se tiene que $ec = c$. Recíprocamente, supóngase que existe un idempotente $e \in \mathcal{C}$ tal que $f = ef$. Con estas hipótesis resulta claro que $\langle f \rangle = \langle e \rangle$ ya que $\langle e \rangle \subseteq \langle f \rangle$ y $\langle e \rangle \supseteq \langle f \rangle$. Para la segunda afirmación suponga que $e' \in \mathcal{C}$ es otro idempotente tal que $\mathcal{C} = \langle e' \rangle$. Entonces, de la primer parte de la proposición se tiene que

$$e' = (e')e = e. \qquad \square$$

Dados un primo p y un entero $n > 0$ primo relativo con p, se tiene que $x^n - \gamma = \prod_{i=1}^{m} f_i$ como producto de polinomios distintos, mónicos, básicos irreducibles y primos relativos por pares en $\mathcal{R}_k[x]$. A partir de ese indizado, tenemos a los polinomios $\hat{f}_i = \prod_{j \neq i} f_j$, $i = 1, 2, \ldots, m$ y para cada uno de ellos hay asociado un elemento idempotente primitivo $\hat{e}_i \in E_{k,n}$ (Proposición 3.8). Con lo anterior, es posible dar el siguiente resultado.

Teorema 3.13. *Sean* $n > 0$ *un entero no divisible por* p, $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - \gamma \rangle$ *y* $x^n - \gamma = \prod_{i=1}^{m} f_i$ *la presentación de* $x^n - \gamma$ *como producto de polinomios distintos, mónicos, básicos irreducibles y primos relativos por pares en* $\mathcal{R}_k[x]$. *Considere un ideal principal no trivial* $\mathcal{C} = \langle f + \langle x^n - \gamma \rangle \rangle$ *de* $\mathcal{R}_{k,n}$ *y asuma que* $f = f_{j_1} f_{j_2} \cdots f_{j_s}$ *donde* $j_l \in M = \{1, 2, ..., m\}, l = 1, 2, ..., s$. *Entonces, existe un elemento idempotente* $e_f + \langle x^n - \gamma \rangle \in \mathcal{R}_{k,n}$ *tal que*

$$\mathcal{C} = \langle e_f + \langle x^n - \gamma \rangle \rangle,$$

y está dado por

$$e_f + \langle x^n - \gamma \rangle = \sum_i \hat{e}_i + \langle x^n - \gamma \rangle,$$

donde $i \in M \setminus \{j_1, j_2, ..., j_s\}$ *y* $\{\hat{e}_i + \langle x^n - \gamma \rangle\} \subseteq E_{k,n}$ *es el conjunto completo de idempotentes primitivos ortogonales por pares, dados en la Proposición 3.8.*

Demostración. Dado que $f = \prod_{l=1}^{s} f_{j_l}$, sea $\hat{f} = \prod_i f_i$ con $i \in M \setminus \{j_1, j_2, ..., j_s\}$. Así f y $\hat{f}$ son primos relativos y por lo tanto existen $\lambda, \hat{\lambda} \in \mathcal{R}_k[x]$ tales que $\lambda f + \hat{\lambda}\hat{f} = 1$. Sea $e_f + \langle x^n - \gamma \rangle = \lambda f + \langle x^n - \gamma \rangle \in \mathcal{R}_{k,n}$. De la definición resulta claro que este es un elemento idempotente. Observe que

$$\lambda f \equiv 1 \equiv \hat{\lambda}_i \hat{f}_i \mod \langle f_i \rangle, i \in M \setminus \{j_1, j_2, \ldots, j_s\},$$

y

$$\lambda f \equiv 0 \mod \langle f_{j_l} \rangle, l = 1, 2, \ldots, s.$$

Así,

$$f e_f + \langle x^n - \gamma \rangle = f(\lambda f) + \langle x^n - \gamma \rangle = f(1 - \hat{\lambda}\hat{f}) + \langle x^n - \gamma \rangle = f + \langle x^n - \gamma \rangle.$$

y del Lema 3.12 se sigue que $\langle f + \langle x^n - \gamma \rangle \rangle = \langle e_f + \langle x^n - \gamma \rangle \rangle$. $\square$

Corolario 3.14. *Con la notación previa, $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - \gamma\rangle$ tiene al menos 2^m elementos idempotentes, donde m es el número de factores básicos irreducibles y primos relativos por pares de $x^n - \gamma$ en $\mathcal{R}_k[x]$.*

Los elementos de $E_{k,n}$ nos permite expresar el isomorfismo $\phi : \bigoplus_{i=1}^{m} \mathcal{R}_{k,f_i} \longrightarrow \mathcal{R}_{k,n}$ de tal modo que podemos describir a un código constacíclico (ideal) $\mathcal{C} \subseteq \mathcal{R}_{k,n}$ a partir de los ideales $\mathcal{C}_i$, $i = 1, \ldots, m$, que lo conforman en $\bigoplus_{i=1}^{m} \mathcal{R}_{k,f_i}$. Ahora se procede a realizar el cálculo explícito de los elementos idempotentes del conjunto $E_{k,n}$.

Con el objetivo de calcular el conjunto completo de idempotentes primitivos ortogonales por pares se da el siguiente resultado, el cual es una adaptación del Teorema 3.2 presentado en el trabajo [8].

Proposición 3.15. *Sea $n > 0$ un entero no divisible por p, p un primo, y considere el anillo $R_n = \mathbb{F}_p[x]/\langle x^n - \gamma\rangle$. Sea $x^n - \gamma = \prod_{i=1}^{m} g_i$ la factorización de $x^n - \gamma$ como producto de polinomios distintos, mónicos, irreducibles y primos relativos por pares en $\mathbb{F}_p[x]$, y sea $\hat{g}_i = \prod_{j \neq i} g_j$. Entonces, el conjunto*

$$\{\hat{\theta}_1, ..., \hat{\theta}_m\}$$

con $\hat{\theta}_i = \Lambda_i \hat{g}_i + \langle x^n - \gamma\rangle, i = 1, 2, ..., m$, Λ_i tales que $\Lambda_i \hat{g}_i \equiv 1 \mod \langle g_i\rangle$ es un conjunto completo de idempotentes primitivos ortogonales por pares en R_n.

Demostración. Teorema 3.2, dado en la referencia [8]. □

La Proposición 3.15 usada en combinación con la siguiente proveerá de un método para determinar el conjunto completo de idempotentes primitivos ortogonales por pares, $E_{k,n}$ en la Proposición 3.8, del anillo $\mathcal{R}_{k,n}$. Recordemos que un levantamiento o *lifting* de un elemento idempotente se define del siguiente modo si I es un ideal de un anillo $\mathcal{R}$, un elemento idempotente $e \in \mathcal{R}$ es un levantamiento (lifting) de un elemento idempotente $x \in \mathcal{R}/I$ si $\overline{e} = x$, donde $\overline{\ } : \mathcal{R} \longrightarrow \mathcal{R}/I$ es la reducción módulo I.

Proposición 3.16. *([33], Proposición 4.1) Sean $\mathcal{R}$ un anillo conmutativo y N un ideal nilpotente de $\mathcal{R}$ con índice de nilpotencia $t \geq 2$. Sea $s > 1$ la característica del anillo cociente $\mathcal{R}/N$. Si e es un elemento idempotente de $\mathcal{R}/N$, entonces*

$$e^{s^{t-1}}$$

es un elemento idempotente del anillo $\mathcal{R}$. Más aún, si existe una colección de elementos idempotentes primitivos ortogonales por pares de $\mathcal{R}/N$ ésta levanta a un conjunto de elementos idempotentes de $\mathcal{R}$ con las mismas propiedades. Además, $|E(\mathcal{R})| = |E(\mathcal{R}/N)|$ donde $E(\mathcal{R})$ es el conjunto de elementos idempotentes de $\mathcal{R}$.

Ahora se procede a aplicar los dos resultados previos a nuestro anillo de interés. Recordemos que $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - \gamma\rangle$ y que $\mathfrak{m}_{k,n} = \mathfrak{m}\mathcal{R}_{k,n}$ es un ideal con índice de nilpotencia $t = k + 1$, dado que $\mathfrak{m}$ es el ideal máximo $\mathcal{R}_k$ (Proposición 2.1). Por otra parte, $\mathcal{R}_{k,n}/\mathfrak{m}_{k,n} = \mathbb{F}_p[x]/\langle \overline{x^n - \gamma}\rangle$ tiene característica $s = p$ y así, tenemos el siguiente resultado.

Teorema 3.17. *Con la notación como en las proposiciones 3.8 y 3.15; de la Proposición 3.16 se tiene que*

$$E_{k,n} = \{\hat{\theta}_1^{p^k}, \hat{\theta}_2^{p^k}, \ldots, \hat{\theta}_m^{p^k}\}$$

es el conjunto completo de elementos idempotentes primitivos y ortogonales por pares del anillo $\mathcal{R}_{k,n}$ obtenidos por levantamiento, donde los $\hat{\theta}_i \in R_n = \mathbb{F}_p[x]/\langle\overline{x^n - \gamma}\rangle$ con $i = 1, \ldots, m$; forman un conjunto completo de idempotentes primitivos y ortogonales por pares en el anillo R_n.

De los resultados 3.13 y 3.17 se tiene la siguiente proposición.

Proposición 3.18. *Sea $\mathcal{C} = \langle f + \langle x^n - \gamma\rangle, ug + \langle x^n - \gamma\rangle\rangle$ un ideal de $\mathcal{R}_{k,n}$ con dos generadores tales que f y g tienen factores en común con $x^n - \gamma$ en $\mathcal{R}_k[x]$. Entonces,*

$$\mathcal{C} = \langle e_f + \langle x^n - \gamma\rangle, ue_g + \langle x^n - \gamma\rangle\rangle,$$

donde $e_f + \langle x^n - \gamma\rangle$ y $e_g + \langle x^n - \gamma\rangle\rangle$ son los elementos idempotentes asociados a $f + \langle x^n - \gamma\rangle$ y $g + \langle x^n - \gamma\rangle$ respectivamente, en el sentido del Teorema 3.13.

3.3. Ejemplos

En la presente sección se dan ejemplos de códigos constacíclicos obtenidos a partir de la teoría desarrollada a lo largo de este capítulo. Todos los ejemplos han sido desarrollados con el software SageMath ([32]) para llevar a cabo la parte computacional.

Ejemplo 4. Sean $p = 2, k = 2, \gamma = 3$ y $n = 7$. Entonces, $\mathcal{R}_2 = \mathbb{Z}_4 + u\mathbb{Z}_4$ con $u^2 = 0$, y $\mathcal{R}_{2,7} = \mathcal{R}_2[x]/\langle x^7 - 3\rangle$. En $\mathcal{R}_2[x]$ se tiene que $x^7 - 3 = f_1 f_2 f_3$ donde $f_1 = x + 1, f_2 = x^3 + 2x^2 + x + 1$, y $f_3 = x^3 + x^2 + 2x + 1$. Con estos parámetros en el anillo $R_7 = \mathbb{F}_2[x]/\langle x^7 - 1\rangle$ se obtiene que $\overline{f}_1 = x + 1 + \langle x^7 - 1\rangle$, $\overline{f}_2 = x^3 + x + 1 + \langle x^7 - 1\rangle$, y $\overline{f}_3 = x^3 + x^2 + 1 + \langle x^7 - 1\rangle$, a partir de lo cual, el conjunto completo de idempotentes primitivos y ortogonales por pares es $\{\hat{\theta}_1, \hat{\theta}_2, \hat{\theta}_2\}$ con $\hat{\theta}_1 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 + \langle x^7 - 1\rangle$, $\hat{\theta}_2 = x^4 + x^2 + x + 1 + \langle x^7 - 1\rangle$ y $\hat{\theta}_3 = x^6 + x^5 + x^3 + 1 + \langle x^7 - 1\rangle$. Del Teorema 3.17, con parámetros $p = 2, k = 2$, se calcula el conjunto completo de elementos idempotentes primitivos y ortogonales por pares de $\mathcal{R}_{2,7}$ cuya existencia se señala en el Teorema 3.8: $E_{2,7} = \{\hat{e}_1, \hat{e}_2, \hat{e}_3\}$, con $\hat{e}_i = \hat{\theta}_i^4$, $i = 1, 2, 3$,

$$\begin{aligned}
\hat{\theta}_1^4 &= 3x^6 + x^5 + 3x^4 + x^3 + 3x^2 + x + 3 + \langle x^7 - 3\rangle, \\
\hat{\theta}_2^4 &= 2x^6 + 2x^5 + 3x^4 + 2x^3 + 3x^2 + x + 1 + \langle x^7 - 3\rangle, \\
\hat{\theta}_3^4 &= 3x^6 + x^5 + 2x^4 + x^3 + 2x^2 + 2x + 1 + \langle x^7 - 3\rangle.
\end{aligned}$$

Así, el conjunto de todos los elementos idempotentes del anillo $\mathcal{R}_{2,7}$, Corolario 3.14, es

$$E(\mathcal{R}_{2,7}) = \{1, 0, \hat{e}_1, \hat{e}_2, \hat{e}_3, e_4, e_5, e_6\},$$

donde $e_4 = \hat{e}_2 + \hat{e}_3 = x^6 + 3x^5 + x^4 + 3x^3 + x^2 + 3x + 2 + \langle x^7 - 3\rangle$, $e_5 = \hat{e}_1 + \hat{e}_3 = 2x^6 + 2x^5 + x^4 + 2x^3 + x^2 + 3x + \langle x^7 - 3\rangle$ y $e_6 = \hat{e}_1 + \hat{e}_2 = x^6 + 3x^5 + 2x^4 + 3x^3 + 2x^2 + 2x + \langle x^7 - 3\rangle$.

Ejemplo 5. Continuando con el ejemplo 4. Nuevamente, sean $p = 2, k = 2, n = 7$, pero ahora tomemos $\gamma = 3 + 2u$. Se tiene así que $\mathcal{R}_{2,7} = \mathcal{R}_2[x]/\langle x^7 - (3+2u)\rangle$. En $\mathcal{R}_2[x]$, factorizamos $x^7 - (3+2u) = f_1 f_2 f_3$ donde

$$f_1 = x - (3+2u),\ f_2 = x^3 + 2x^2 + x - (3+2u),\ f_3 = x^3 - (3+2u)x^2 + 2x - (3+2u)$$

los cuales son polinomios distintos, mónicos, básicos irreducibles y coprimos por pares, dado que, en $\mathbb{F}_2[x]$, se tiene que $\overline{x^7 - (3+2u)} = x^7 - 1 = \overline{f}_1\overline{f}_2\overline{f}_3$ como en el ejemplo 4, y por lo tanto, el anillo $R_7 = \mathbb{F}_2[x]/\langle x^7 - 1\rangle$ tiene el mismo conjunto completo de elementos idempotentes primitivos y ortogonales por pares. Del Teorema 3.17, el correspondiente conjunto completo de elementos idempotentes primitivos y ortogonales por pares de $\mathcal{R}_{2,7}$ está dado por $E_{2,7} = \{\hat{e}_1, \hat{e}_2, \hat{e}_3\} = \{\hat{\theta}_i^4,\ i = 1, 2, 3\}$, con

$$\begin{aligned}
\hat{\theta}_1^4 &= 3x^6 - (3+2u)x^5 + 3x^4 - (3+2u)x^3 + 3x^2 - (3+2u)x + 3 + \langle x^7 - (3+2u)\rangle,\\
\hat{\theta}_2^4 &= 2x^6 + 2x^5 + 3x^4 + 2x^3 + 3x^2 - (3+2u)x + 1 + \langle x^7 - (3+2u)\rangle,\\
\hat{\theta}_3^4 &= 3x^6 - (3+2u)x^5 + 2x^4 - (3+2u)x^3 + 2x^2 + 2x + 1 + \langle x^7 - (3+2u)\rangle.
\end{aligned}$$

Un código $(3+2u)$-constacíclico no trivial definido sobre $\mathcal{R}_2 = \mathbb{Z}_4 + u\mathbb{Z}_4$ es $\mathcal{C} = \phi(\oplus_i^3 \mathcal{C}_i)$ donde $\phi : \bigoplus_{i=1}^3 \mathcal{R}_{k,f_i} \longrightarrow \mathcal{R}_{2,7}$ es el isomorfismo definido en (3.1) y $\mathcal{C}_1 = \langle (2+u) + \langle f_1\rangle\rangle$, $\mathcal{C}_2 = \langle 1 + \langle f_2\rangle\rangle$ y $\mathcal{C}_3 = \langle 1 + \langle f_3\rangle\rangle$, así

$$\mathcal{C} = \langle (2+u)\hat{e}_1 + \hat{e}_2 + \hat{e}_3\rangle.$$

Ejemplo 6. En este ejemplo se ilustra el Teorema 3.13 aplicado al caso en el que la unidad $\gamma = 1$, es decir, cuando tenemos un código cíclico. Por simplificación notacional, omitimos la notación del tipo $f + \langle x^n - 1\rangle$ especificando de ser necesario el contexto en el cuál los elementos sean mencionados. Sea $\mathcal{R}_3 = \mathbb{Z}_8 + u\mathbb{Z}_8$, $u^2 = 0$ y considere el polinomio $x^{15} - 1 = f_1 f_2 f_3 f_4 f_5$ donde

$$f_1 = x + 7,\ f_2 = x^2 + x + 1,\ f_3 = x^4 + 4x^3 + 6x^2 + 3x + 1$$

$$f_4 = x^4 + 3x^3 + 6x^2 + 4x + 1,\ f_5 = x^4 + x^3 + x^2 + x + 1$$

en $\mathcal{R}_3[x]$. Sea $\{\hat{\theta}_1, \hat{\theta}_2, \hat{\theta}_3, \hat{\theta}_4, \hat{\theta}_5\}$ el conjunto completo de idempotentes primitivos, ortogonales por pares de $R_{15} = \mathbb{F}_2[x]/\langle x^{15} - 1\rangle$, en donde,

$$\begin{aligned}
\hat{\theta}_1 &= x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,\\
\hat{\theta}_2 &= x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x,\\
\hat{\theta}_3 &= x^{12} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x,\\
\hat{\theta}_4 &= x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^7 + x^6 + x^3,\\
\hat{\theta}_5 &= x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x.
\end{aligned}$$

Tomemos $k = 3$ para aplicar el Teorema 3.17 al conjunto de idempotentes anterior, así,

$$\{\hat{\theta}_1^8, \hat{\theta}_2^8, \hat{\theta}_3^8, \hat{\theta}_4^8, \hat{\theta}_5^8\} \subset \mathcal{R}_{3,15}.$$

El correspondiente conjunto completo de elementos idempotentes primitivos ortogonales por pares en $\mathcal{R}_{3,15} = \mathcal{R}_3[x]/\langle x^{15}-1\rangle$ está dado entonces por $E_{3,15} = \{\hat{e}_1, \hat{e}_2, \hat{e}_3, \hat{e}_4, \hat{e}_5\}$ con $\hat{e}_i = \hat{\theta}_i^8$, $i = 1, 2, \ldots, 5$. Específicamente,

$$\begin{aligned}
\hat{e}_1 &= 7(x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1),\\
\hat{e}_2 &= x^{14}+x^{13}+6x^{12}+x^{11}+x^{10}+6x^9+x^8+x^7+6x^6+x^5+x^4+6x^3+x^2+x+6,\\
\hat{e}_3 &= 4x^{14}+4x^{13}+x^{12}+4x^{11}+2x^{10}+x^9+3x^8+4x^7+x^6+2x^5+3x^4+x^3+3x^2+3x+4,\\
\hat{e}_4 &= 3x^{14}+3x^{13}+x^{12}+3x^{11}+2x^{10}+x^9+4x^8+3x^7+x^6+2x^5+4x^4+x^3+4x^2+4x+4,\\
\hat{e}_5 &= x^{14}+x^{13}+x^{12}+x^{11}+4x^{10}+x^9+x^8+x^7+x^6+4x^5+x^4+x^3+x^2+x+4.
\end{aligned}$$

Debido a que $f = f_2 f_3$ en $\mathcal{R}_3[x]$, con la notación como en el Teorema 3.13, se sigue que $\mathcal{C} = \langle f\rangle$ tiene como elemento idempotente generador a $e_f = \hat{e}_1 + \hat{e}_4 + \hat{e}_5$, i. e.,

$$e_f = 3x^{14}+3x^{13}+x^{12}+3x^{11}+5x^{10}+x^9+4x^8+3x^7+x^6+5x^5+4x^4+x^3+4x^2+4x+7.$$

Por supuesto, $f = fe_f$ y así $\langle f\rangle = \langle e_f\rangle$.

El siguiente ejemplo ilustra la Proposición 3.18.

Ejemplo 7. Sean $k = 2, n = 7, \gamma = 1$, tenemos $\mathcal{R}_2 = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$ y $\mathcal{R}_{2,7} = \mathcal{R}_2[x]/\langle x^7-1\rangle$. En $\mathcal{R}_2[x]$ se tiene la factorización $x^7-1 = f_1 f_2 f_3$ donde $f_1 = x+3$, $f_2 = x^3+2x^2+x+3$, $f_3 = x^3+3x^2+2x+3$. Se tiene así en $\mathbb{F}_2[x]$, $x^7-1 = \overline{f}_1\overline{f}_2\overline{f}_3$ con $\overline{f}_1 = x+1$, $\overline{f}_2 = x^3+x+1$, $\overline{f}_3 = x^3+x^2+1$. De lo anterior, el conjunto completo de elementos idempotentes primitivos ortogonales por pares de $\mathbb{F}_2[x]/\langle x^7-1\rangle$ es $\{\hat{\theta}_1, \hat{\theta}_2, \hat{\theta}_3\}$ donde

$$\hat{\theta}_1 = x^6+x^5+x^4+x^3+x^2+x+1,\ \hat{\theta}_2 = x^4+x^2+x+1, \hat{\theta}_3 = x^6+x^5+x^3+1.$$

Dado que el índice de nilpotencia del ideal máximo $\mathfrak{m} = \langle 2, u\rangle$ de $\mathcal{R}_2$ es $t = 3$ y la característica del anillo $\mathbb{F}_2[x]/\langle x^7-1\rangle$ es $s = 2$, del Teorema 3.17, obtenemos que $E_{2,7} = \{e_1, e_2, e_3\} = \{\hat{\theta}_1^4, \hat{\theta}_2^4, \hat{\theta}_3^4\}$ con

$$\begin{aligned}
\hat{\theta}_1^4 &= 3(x^6+x^5+x^4+x^3+x^2+x+1),\\
\hat{\theta}_2^4 &= 2x^6+2x^5+3x^4+2x^3+3x^2+3x+1,\\
\hat{\theta}_3^4 &= 3x^6+3x^5+2x^4+3x^3+2x^2+2x+1.
\end{aligned}$$

Con tal información, los elementos idempotentes generadores del ideal $\mathcal{C} = \langle 1+2x+x^2+3x^3, u(x-1)\rangle = \langle f, ug\rangle$ del anillo $\mathcal{R}_{2,7}$ se determinan a continuación: Observe que $f = 3f_3$, $g = f_1$ y de los Teoremas 3.13 y 3.18, $e_{f_3} = e_1 + e_2 = x^6+x^5+2x^4+x^3+2x^2+2x$, mientras que $e_g = x^6+x^5+x^4+x^3+x^2+x+2$. Así,

$$\langle f, ug\rangle = \langle e_f, ue_g\rangle.$$

Ejemplo 8. Sea $p = 5, k = 2, n = 6$ y tomemos $\gamma = 8$. Así $\mathcal{R}_2 = \mathbb{Z}_{25} + u\mathbb{Z}_{25}$ y $\mathcal{R}_{2,6} = \mathcal{R}_2[x]/\langle x^6-8\rangle$. En $\mathcal{R}_2[x]$ tenemos la factorización $x^6-8 = f_1 f_2 f_3$ donde $f_1 = x^2+23$,

$f_2 = x^2 + 12x + 23$, $f_3 = x^2 + 13x + 23$. Sea $F = f_2 f_3 + \langle x^6 - 8\rangle$ y $G = f_1 + \langle x^6 - 8\rangle$. Entonces,

$$\begin{aligned} F &= x^4 + 2x^2 + 4 + \langle x^6 - 8\rangle, \\ G &= x^2 + 23 + \langle x^6 - 8\rangle. \end{aligned}$$

En otras palabras, tenemos un código constacíclico no trivial sobre $\mathcal{R}_2$:

$$\mathcal{C} = \langle F, uG\rangle$$

Determinemos los idempotentes asociados a este código. Observemos que en $\mathbb{F}_5[x]$ la función reducción nos dice que

$$\overline{x^6 - 8} = x^6 + 2 = \overline{f}_1\overline{f}_2\overline{f}_3$$

donde $\overline{f}_1 = x^2 + 3$, $\overline{f}_2 = x^2 + 2x + 3$, $\overline{f}_3 = x^2 + 3x + 3$. De la Proposición 3.15, el conjunto completo de elementos idempotentes primitivos ortogonales por pares en $R_6 = \mathbb{F}_5[x]/\langle x^6 + 2\rangle$ es $\{\hat{\theta}_1 = 3x^4 + x^2 + 2 + \langle x^6 + 2\rangle, \hat{\theta}_2 = x^5 + x^4 + 2x^2 + x + 2 + \langle x^6 + 2\rangle, \hat{\theta}_3 = 4x^5 + x^4 + 2x^2 + 4x + 2 + \langle x^6 + 2\rangle\}$. Dado que el índice de nilpotencia del ideal máximo de $\mathcal{R}_2$ es $t = 3$ y tenemos $p = 5$, del Teorema 3.17, $E_{2,6} = \{\hat{e}_1, \hat{e}_2, \hat{e}_3\} = \{\hat{\theta}_1^{25}, \hat{\theta}_2^{25}, \hat{\theta}_3^{25}\}$ donde $\hat{e}_i = \hat{\theta}_i^{25}$, $i = 1, 2, 3$, y

$$\begin{aligned} \hat{\theta}_1^{25} &= 23x^4 + 21x^2 + 17 + \langle x^6 - 8\rangle, \\ \hat{\theta}_2^{25} &= 6x^5 + x^4 + 2x^2 + x + 17 + \langle x^6 - 8\rangle, \\ \hat{\theta}_3^{25} &= 19x^5 + x^4 + 2x^2 + 24x + 17 + \langle x^6 - 8\rangle. \end{aligned}$$

Con esta información, los idempotentes generadores del código constacíclico se calculan de la manera siguiente: Dado que $F = f_2 f_3$, $G = f_1$ en $\mathcal{R}_2[x]$; del Teorema 3.13 se obtiene que $e_F = \hat{e}_1 = 23x^4 + 21x^2 + 17 + \langle x^6 - 8\rangle$, y similarmente $e_G = \hat{e}_2 + \hat{e}_3 = 2x^4 + 4x^2 + 9 + \langle x^6 - 8\rangle$. Obsérvese que $e_F, e_G \in \mathcal{C}$, $e_F(F + \langle x^6 - 8\rangle) = F + \langle x^6 - 8\rangle$ y $e_G(uG + \langle x^6 - 8\rangle) = uG + \langle x^6 - 8\rangle$. Así,

$$\langle F, uG\rangle = \langle e_F, ue_G\rangle.$$

3.4. Conclusiones y perspectivas

A continuación se presentan conclusiones del trabajo realizado, así como el planteamiento de posibles investigaciones futuras a partir del mismo.

3.4.1. Conclusiones

En el presente trabajo se ha planteado una metodología para, dado un primo p, llevar a cabo la descripción de códigos γ-constacíclicos de longitud n no divisible por p, con $\gamma \in \mathcal{U}(\mathcal{R}_k)$, y

$$\mathcal{R}_k = \mathbb{Z}_{p^k} + \mathbb{Z}_{p^k}, \text{ con } u^2 = 0,$$

es el anillo alfabeto. Esto se hace a partir de la descripción de los ideales del anillo cociente $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - \gamma\rangle$ obtenidos desde un producto directo de anillos locales del $\mathcal{R}_k[x]/\langle f\rangle$ con $f \in \mathcal{R}_k[x]$ básico irreducible. Dado un anillo de Frobenius finito, local, conmutativo con identidad $\mathcal{R}$, en el caso en el que el grado de $p(x) = x^n - \gamma \in \mathcal{R}[x]$ es primo relativo con la característica del campo residual $\mathcal{R}/\mathfrak{m}$, la metodología previa consultada consiste, a grandes rasgos, en estudiar los factores de $p(x)$ y, a partir de ello, describir a los ideales del anillo cociente $\mathcal{R}[x]/\langle x^n - \gamma\rangle$. Es de notar, que los generadores de muchos de esos ideales quedan expresados en términos de los factores de $p(x)$, o bien, guardan una estrecha relación con los mismos a partir de otras consideraciones sobre el anillo alfabeto (ver, por ejemplo, [7], [16], [17], [34]).

En nuestro caso, dado $x^n - \gamma = \prod_i^m f_i \in \mathcal{R}_k[x]$ como producto de polinomios f_i distintos, básicos irreducibles y primos relativos por pares;

- Estudiamos propiedades algebraicas y el conjunto de ideales, con énfasis en los ideales principales, del anillo $\mathcal{R}_k$.

- A partir de esas propiedades, se cuenta con criterios computacionales (a nivel de implementación), para facilitar la obtención el conjunto de ideales del anillo $\mathcal{R}_k$, de hecho, con el Teorema 2.4 se pueden contar los ideales principales de $\mathcal{R}_k$.

- La estructura de ideales del anillo $\mathcal{R}_k$ es transferida al anillo local $\mathcal{R}_k[x]/\langle f\rangle$, con $f \in \mathcal{R}_k[x]$ básico irreducible (Proposición 3.4 y Lemas 3.1 y 3.3).

- A partir de producto directo de anillos locales $\mathcal{R}_{k,f_i} = \mathcal{R}_k[x]/\langle f_i\rangle$ se determina una familia completa de elementos idempotentes primitivos y ortogonales por pares en $\mathcal{R}_{k,n}$ (Proposición 3.8). Para esto se utiliza, como sustento teórico, el Teorema Chino del Residuo (1.10) y el isomorfismo 3.1, dado en la Sección 3.2.

- Con lo anterior, dado cualquier ideal en el producto directo $\bigoplus_{i=1}^m \mathcal{R}_{k,f_i}$ se pueden obtener los generadores (o generador) del correspondiente ideal en el anillo $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - \gamma\rangle$.

- En contraparte, en el anillo $\mathcal{R}_{k,n}$ se tiene la Proposición 3.7 que nos ayuda a descartar ideales distintos de cero triviales, permitiendo construir códigos γ-constacíclicos a partir de la factorización en básicos irreducibles coprimos por pares de $x^n - \gamma$ en $\mathcal{R}_k[x]$ y, con el Teorema 3.13, se construye el idempotente asociado a dicho ideal, esto a partir del conjunto completo de idempotentes primitivos ortogonales por pares de $\mathcal{R}_{k,n}$.

- En adición a lo anterior, se presenta el cálculo de la familia completa de elementos idempotentes primitivos y ortogonales por pares (Teorema 3.17) por medio de levantamientos del anillo $\mathbb{F}_2[x]/\langle\overline{x^n - \gamma}\rangle$ a el anillo $\mathcal{R}_{k,n}$, usando herramientas desarrolladas previamente por grupos de investigación a los que el director de la presente tesis pertenece ([33]).

- Se proporcionan ejemplos que ilustran los resultados centrales del presente trabajo.

- Se aprovecha este espacio para mencionar que surgieron dos investigaciones derivadas de este trabajo, ya publicadas, relacionadas con anillos de matrices ([35] y [36]).

3.4.2. Perspectivas

Del presente trabajo de investigación se originan las siguientes posibles direcciones de trabajo posterior.

- La metodología presentada para describir códigos constacíclicos ¿es posible extenderla a otros anillos con propiedades algebraicas similares? y de ser así, ¿para cuáles anillos específicamente? Nótese que en la descripción de ideales mediante la familia completa de idempotentes primitivos y ortogonales por pares no interviene la propiedad del anillo de ser de cadena o no de cadena. Un ejemplo de anillo finito, local y conmutativo con identidad de cadena lo sería $\mathbb{F}_p + u\mathbb{F}_p$, con $u^2 = 0$.

- Lo desarrollado, se cumple en particular para el caso $p = 2, k > 1$. En este caso particular, se observa que la cardinalidad del grupo de unidades es $2^{2k-1} = \frac{|\mathcal{R}_k|}{2}$. En ese contexto, la reducción de $x^n - \gamma$ a $\mathbb{F}_2[x]$ nos dice que estudiar códigos constacíclicos en ese anillo guarda relación con códigos cíclicos y negacíclicos sobre $\mathbb{F}_2$ ¿existen códigos duales y autoduales no triviales sobre $\mathcal{R}_k$? de existir ¿cuál es su caracterización y cómo estudiar estos códigos duales y autoduales a partir de la familia completa de elementos idempotentes primitivos y ortogonales por pares?

- Desde luego, dado un número primo p, la pregunta natural al tener el anillo $\mathcal{R}_k = \mathbb{Z}_{p^k} + u\mathbb{Z}_{p^k}$ es ¿cómo describir códigos γ-constacíclicos cuya longitud n no sea un primo relativo con p?

Apéndice A

Algunos conjuntos de ideales del anillo $\mathcal{R}_k$, con $p = 2$

En el presente apéndice se dan las familias de ideales para $p = 2$ y valores pequeños de k. Los cálculos fueron hechos por medio de programas realizados en SageMath ([32]).

$\langle u \rangle$	$\langle 0 \rangle$	
$\langle 2u \rangle$	$\langle 2 \rangle$ $\langle 2+u \rangle$	$\langle 2, u \rangle$

$\langle u \rangle$	$\langle 0 \rangle$	
$\langle 2u \rangle$	$\langle 2 \rangle$ $\langle 2+u \rangle$	$\langle 2, u \rangle$
$\langle 4u \rangle$	$\langle 4 \rangle$ $\langle 4+u \rangle$ $\langle 4+2u \rangle$	$\langle 4, u \rangle$ $\langle 4, 2u \rangle$

Cuadro A.1: Conjunto de ideales de los anillos $\mathcal{R}_2 = \mathbb{Z}_4 + u\mathbb{Z}_4$ (tabla izquierda) y $\mathcal{R}_3 = \mathbb{Z}_8 + u\mathbb{Z}_8$, $u^2 = 0$ (tabla derecha).

$\langle u \rangle$	$\langle 0 \rangle$	
$\langle 2u \rangle$	$\langle 2 \rangle$ $\langle 2+u \rangle$	$\langle 2, u \rangle$
$\langle 4u \rangle$	$\langle 4 \rangle$ $\langle 4+u \rangle$ $\langle 4+2u \rangle$ $\langle 4+3u \rangle$	$\langle 4, u \rangle$ $\langle 4, 2u \rangle$ $\langle 4+u, 4+3u \rangle$
$\langle 8u \rangle$	$\langle 8 \rangle$ $\langle 8+u \rangle$ $\langle 8+2u \rangle$ $\langle 8+4u \rangle$	$\langle 8, u \rangle$ $\langle 8, 2u \rangle$ $\langle 8, 4u \rangle$

Cuadro A.2: Conjunto de ideales del anillo $\mathcal{R}_4 = \mathbb{Z}_{16} + u\mathbb{Z}_{16}$, $u^2 = 0$.

$\langle u\rangle$	$\langle 0\rangle$	
$\langle 2u\rangle$	$\langle 2\rangle$ $\langle 2+u\rangle$	$\langle 2,u\rangle$
$\langle 4u\rangle$	$\langle 4\rangle$ $\langle 4+u\rangle$ $\langle 4+2u\rangle$ $\langle 4+3u\rangle$	$\langle 4,u\rangle$ $\langle 4,2u\rangle$ $\langle 4+u,4+3u\rangle$
$\langle 8u\rangle$	$\langle 8\rangle$ $\langle 8+u\rangle$ $\langle 8+2u\rangle$ $\langle 8+3u\rangle$ $\langle 8+4u\rangle$ $\langle 8+6u\rangle$	$\langle 8,u\rangle$ $\langle 8,2u\rangle$ $\langle 8,4u\rangle$ $\langle 8+u,8+3u\rangle$ $\langle 8+2u,8+6u\rangle$
$\langle 16u\rangle$	$\langle 16\rangle$ $\langle 16+u\rangle$ $\langle 16+2u\rangle$ $\langle 16+4u\rangle$ $\langle 16+8u\rangle$	$\langle 16,u\rangle$ $\langle 16,2u\rangle$ $\langle 16,4u\rangle$ $\langle 16,8u\rangle$

$\langle u\rangle$	$\langle 0\rangle$	
$\langle 2u\rangle$	$\langle 2\rangle$ $\langle 2+u\rangle$	$\langle 2,u\rangle$
$\langle 4u\rangle$	$\langle 4\rangle$ $\langle 4+u\rangle$ $\langle 4+2u\rangle$ $\langle 4+3u\rangle$	$\langle 4,u\rangle$ $\langle 4,2u\rangle$ $\langle 4+u,4+3u\rangle$
$\langle 8u\rangle$	$\langle 8\rangle$ $\langle 8+u\rangle$ $\langle 8+2u\rangle$ $\langle 8+3u\rangle$ $\langle 8+4u\rangle$ $\langle 8+5u\rangle$ $\langle 8+6u\rangle$ $\langle 8+7u\rangle$	$\langle 8,u\rangle$ $\langle 8,2u\rangle$ $\langle 8,4u\rangle$ $\langle 8+u,8+3u\rangle$ $\langle 8+u,8+5u\rangle$ $\langle 8+2u,8+6u\rangle$ $\langle 8+3u,8+7u\rangle$
$\langle 16u\rangle$	$\langle 16\rangle$ $\langle 16+u\rangle$ $\langle 16+2u\rangle$ $\langle 16+3u\rangle$ $\langle 16+4u\rangle$ $\langle 16+6u\rangle$ $\langle 16+8u\rangle$ $\langle 16+12u\rangle$	$\langle 16,u\rangle$ $\langle 16,2u\rangle$ $\langle 16,4u\rangle$ $\langle 16,8u\rangle$ $\langle 16+u,16+3u\rangle$ $\langle 16+2u,16+6u\rangle$ $\langle 16+4u,16+12u\rangle$
$\langle 32u\rangle$	$\langle 32\rangle$ $\langle 32+u\rangle$ $\langle 32+2u\rangle$ $\langle 32+4u\rangle$ $\langle 32+8u\rangle$ $\langle 32+16u\rangle$	$\langle 32,u\rangle$ $\langle 32,2u\rangle$ $\langle 32,4u\rangle$ $\langle 32,8u\rangle$ $\langle 32,16u\rangle$

Cuadro A.3: Conjunto de ideales del anillo $\mathcal{R}_5 = \mathbb{Z}_{32} + u\mathbb{Z}_{32}$ (izquierda) y $\mathcal{R}_6 = \mathbb{Z}_{64} + u\mathbb{Z}_{64}$ (derecha), con $u^2 = 0$.

$\langle u \rangle$	$\langle 0 \rangle$	
$\langle 2u \rangle$	$\langle 2 \rangle$	$\langle 2, u \rangle$
	$\langle 2+u \rangle$	
$\langle 4u \rangle$	$\langle 4 \rangle$	$\langle 4, u \rangle$
	$\langle 4+u \rangle$	$\langle 4, 2u \rangle$
	$\langle 4+2u \rangle$	$\langle 4+u, 4+3u \rangle$
	$\langle 4+3u \rangle$	
$\langle 8u \rangle$	$\langle 8 \rangle$	$\langle 8, u \rangle$
	$\langle 8+u \rangle$	$\langle 8, 2u \rangle$
	$\langle 8+2u \rangle$	$\langle 8, 4u \rangle$
	$\langle 8+3u \rangle$	$\langle 8+u, 8+3u \rangle$
	$\langle 8+4u \rangle$	$\langle 8+u, 8+5u \rangle$
	$\langle 8+5u \rangle$	$\langle 8+2u, 8+6u \rangle$
	$\langle 8+6u \rangle$	$\langle 8+3u, 8+7u \rangle$
	$\langle 8+7u \rangle$	
$\langle 16u \rangle$	$\langle 16 \rangle$	$\langle 16, u \rangle$
	$\langle 16+u \rangle$	$\langle 16, 2u \rangle$
	$\langle 16+2u \rangle$	$\langle 16, 4u \rangle$
	$\langle 16+3u \rangle$	$\langle 16, 8u \rangle$
	$\langle 16+4u \rangle$	$\langle 16+u, 16+3u \rangle$
	$\langle 16+5u \rangle$	$\langle 16+u, 16+5u \rangle$
	$\langle 16+6u \rangle$	$\langle 16+2u, 16+6u \rangle$
	$\langle 16+7u \rangle$	$\langle 16+2u, 16+10u \rangle$
	$\langle 16+8u \rangle$	$\langle 16+6u, 16+14u \rangle$
	$\langle 16+10u \rangle$	$\langle 16+4u, 16+12u \rangle$
	$\langle 16+12u \rangle$	$\langle 16+3u, 16+7u \rangle$
	$\langle 16+14u \rangle$	

$\langle 32u \rangle$	$\langle 32 \rangle$	$\langle 32, u \rangle$
	$\langle 32+u \rangle$	$\langle 32, 2u \rangle$
	$\langle 32+2u \rangle$	$\langle 32, 4u \rangle$
	$\langle 32+3u \rangle$	$\langle 32, 8u \rangle$
	$\langle 32+4u \rangle$	$\langle 32, 16u \rangle$
	$\langle 32+6u \rangle$	$\langle 32+u, 32+3u \rangle$
	$\langle 32+8u \rangle$	$\langle 32+2u, 32+6u \rangle$
	$\langle 32+12u \rangle$	$\langle 32+4u, 32+12u \rangle$
	$\langle 32+16u \rangle$	$\langle 32+8u, 32+24u \rangle$
	$\langle 32+14u \rangle$	
$\langle 64u \rangle$	$\langle 64 \rangle$	$\langle 64, u \rangle$
	$\langle 64+u \rangle$	$\langle 64, 2u \rangle$
	$\langle 64+2u \rangle$	$\langle 64, 4u \rangle$
	$\langle 64+4u \rangle$	$\langle 64, 8u \rangle$
	$\langle 64+8u \rangle$	$\langle 64, 16u \rangle$
	$\langle 64+16u \rangle$	$\langle 64, 32u \rangle$
	$\langle 64+32u \rangle$	

Cuadro A.4: Conjunto de ideales del anillo $\mathcal{R}_7 = \mathbb{Z}_{128} + u\mathbb{Z}_{128}$, $u^2 = 0$

Apéndice B

Aplicación: Códigos cíclicos de longitud $n = 7$ sobre $\mathcal{R}_2 = \mathbb{Z}_4 + u\mathbb{Z}_4$

A manera de aplicación de lo desarrollado en el presente trabajo de tesis, se presenta la determinación de códigos cíclicos de longitud $n = 7$ definidos sobre el anillo $\mathcal{R}_2$ para el caso $p = 2$, es decir, con el anillo alfabeto dado por

$$\mathcal{R}_2 = \mathbb{Z}_4 + u\mathbb{Z}_4,\ u^2 = 0.$$

Este es un anillo finito, local, conmutativo con identidad y no de cadena (Proposición 2.1). Es un anillo de Frobenius con ideal máximo $\mathfrak{m} = \langle 2, u\rangle$ cuyo índice de nilpotencia es $t = 3$, su zoclo $\mathrm{Soc}(\mathcal{R}_2) = \langle 2u\rangle$ y campo residual $\mathbb{F}_2$ con característica 2. En el apéndice *A* se tiene que su conjunto de ideales está dado por

$$\mathcal{L}_2 = \{\langle 0\rangle, \langle 2u\rangle, \langle 2\rangle, \langle 2+u\rangle, \langle u\rangle, \langle 2, u\rangle, \langle 1\rangle\}.$$

Sea $x^7 - 1 = f_1 f_2 f_3$ con $f_1 = x+3$, $f_2 = x^3+2x^2+x+3$ y $f_3 = x^3+3x^2+2x+3$. Cada uno de los f_i es básico irreducible y la correspondiente reducción para cada $i = 1, 2, 3$ es $\overline{f}_1 = x+1$, $\overline{f}_2 = x^3+x+1$ y $\overline{f}_3 = x^3+x^2+1$ en $\mathbb{F}_2[x]$, así $\overline{x^n - 1} = x^7 + 1 = \overline{f}_1\overline{f}_2\overline{f}_3$.

Nuestro objetivo es describir los ideales del anillo cociente

$$\mathcal{R}_{2,7} = \mathcal{R}_2[x]/\langle x^7 - 1\rangle.$$

Con tal fin, se define en el anillo $\mathbb{F}_2[x]$,

$$\hat{F}_1 = \overline{f}_2\overline{f}_3, \hat{F}_2 = \overline{f}_1\overline{f}_3, \hat{F}_3 = \overline{f}_1\overline{f}_2$$

y mediante el algoritmo de Euclides en $\mathbb{F}_2[x]$, obtenemos en $\mathbb{F}_2[x]/\langle x^7+1\rangle$ un conjunto completo de elementos idempotentes primitivos y ortogonales por pares,

$$\begin{aligned}
\hat{\theta}_1 &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 + \langle x^7 + 1\rangle,\\
\hat{\theta}_2 &= x^4 + x^2 + x + 1 + \langle x^7 + 1\rangle,\\
\hat{\theta}_3 &= x^6 + x^5 + x^3 + 1 + \langle x^7 + 1\rangle.
\end{aligned}$$

Dado que el índice de nilpotencia del ideal máximo $\mathfrak{m}$ de $\mathcal{R}_2$ es $t = 3$ y la característica del anillo $\mathbb{F}_2[x]/\langle x^7 - 1\rangle$ es $s = 2$, del Teorema 3.17, obtenemos que el conjunto completo de elementos idempotentes primitivos y ortogonales por pares de la Proposición 3.8, en $\mathcal{R}_{2,7} = \mathcal{R}_2[x]/\langle x^7 - 1\rangle$, es dado por $E_{2,7} = \{\hat{e}_1, \hat{e}_2, \hat{e}_3\} = \{\hat{\theta}_1^4, \hat{\theta}_2^4, \hat{\theta}_3^4\}$, donde

$$\begin{aligned}
\hat{\theta}_1^4 &= 3(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) + \langle x^7 - 1\rangle, \\
\hat{\theta}_2^4 &= 2x^6 + 2x^5 + 3x^4 + 2x^3 + 3x^2 + 3x + 1 + \langle x^7 - 1\rangle, \\
\hat{\theta}_3^4 &= 3x^6 + 3x^5 + 2x^4 + 3x^3 + 2x^2 + 2x + 1.
\end{aligned}$$

Como consecuencia del Teorema Chino del Residuo, 3.5, al considerar la reducción del polinomio $x^n - 1$, así como las reducciones de sus correspondientes factores, tenemos el diagrama

$$\begin{array}{ccc}
\mathcal{R}_2[x]/\langle x^n - 1\rangle & \xrightarrow{\cong} & \bigoplus_{i=1}^m \mathcal{R}_2[x]/\langle f_i\rangle \\
\downarrow & & \downarrow \\
\mathbb{F}_2[x]/\langle \overline{x^n + 1}\rangle & \xrightarrow[\cong]{} & \bigoplus_{i=1}^m \mathbb{F}_2[x]/\langle \overline{f}_i\rangle.
\end{array}$$

De ahí que el isomorfismo $\Phi : \mathcal{R}_{2,7} \longrightarrow \bigoplus_{i=1}^3 \mathcal{R}_2[x]/\langle f_i\rangle$ dado por

$$\Phi(f + \langle x^7 - 1\rangle) = (f + \langle f_1\rangle, f + \langle f_2\rangle, f + \langle f_3\rangle)$$

tiene como isomorfismo inverso a $\phi : \bigoplus_{i=1}^3 \mathcal{R}_2[x]/\langle f_i\rangle \longrightarrow \mathcal{R}_{2,7}$,

$$\phi(r_1 + \langle f_1\rangle, r_2 + \langle f_2\rangle, r_3 + \langle f_3\rangle) = \sum_{i=1}^{3} r_i\hat{e}_i + \langle x^7 - 1\rangle.$$

Un hecho inmediato a partir de lo anterior es que

$$\mathcal{R}_{2,7} = \langle \hat{e}_1 + \hat{e}_2 + \hat{e}_3\rangle.$$

Del Corolario 3.6, $\mathcal{R}_{2,7}$ es un anillo semilocal con 3 ideales máximos $\mathfrak{m}_i$, $i = 1, 2, 3$ cada uno con dos generadores. Ellos son determinados vía el isomorfismo ϕ:

$$\begin{aligned}
\mathfrak{m}_1 &= \langle 2\hat{e}_1 + e_2 + e_3 + \langle x^7 - 1\rangle, ue_1 + e_2 + e_3 + \langle x^7 - 1\rangle\rangle, \\
\mathfrak{m}_2 &= \langle \hat{e}_1 + 2e_2 + e_3 + \langle x^7 - 1\rangle, e_1 + ue_2 + e_3 + \langle x^7 - 1\rangle\rangle, \\
\mathfrak{m}_3 &= \langle \hat{e}_1 + e_2 + 2e_3 + \langle x^7 - 1\rangle, e_1 + e_2 + ue_3 + \langle x^7 - 1\rangle\rangle,
\end{aligned}$$

En el artículo [34] se presenta una tabla con códigos cíclicos no triviales definidos sobre $\mathcal{R}_2$, obtenidos mediante un enfoque de estudio distinto al presentado en este trabajo de tesis. En la siguiente tabla se muestran los ideales propios del anillo cociente $\mathcal{R}_{2,7}$ obtenidos desde nuestra perpectiva del cómo describir a los ideales de $\mathcal{R}_{2,7}$.

Cuadro B.1: Ideales del anillo $\mathcal{R}_{2,7}$

$\langle 0\rangle$	$\langle 2u\hat{e}_3\rangle$
$\langle 2\hat{e}_3\rangle$	$\langle (2+u)\hat{e}_3\rangle$
$\langle u\hat{e}_3\rangle$	$\langle \langle 2,u\rangle \hat{e}_3\rangle$
$\langle \hat{e}_3\rangle$	$\langle 2u\hat{e}_2\rangle$
$\langle 2u\hat{e}_2+2u\hat{e}_3\rangle$	$\langle 2u\hat{e}_2+2\hat{e}_3\rangle$
$\langle 2u\hat{e}_2+(2+u)\hat{e}_3\rangle$	$\langle 2u\hat{e}_2+u\hat{e}_3\rangle$
$\langle 2u\hat{e}_2+\langle 2,u\rangle \hat{e}_3\rangle$	$\langle 2u\hat{e}_2+\hat{e}_3\rangle$
$\langle 2\hat{e}_2\rangle$	$\langle 2\hat{e}_2+2u\hat{e}_3\rangle$
$\langle 2\hat{e}_2+2\hat{e}_3\rangle$	$\langle 2\hat{e}_2+(2+u)\hat{e}_3\rangle$
$\langle 2\hat{e}_2+u\hat{e}_3\rangle$	$\langle 2\hat{e}_2+\langle 2,u\rangle \hat{e}_3\rangle$
$\langle 2\hat{e}_2+\hat{e}_3\rangle$	$\langle (2+u)\hat{e}_2\rangle$
$\langle (2+u)\hat{e}_2+2u\hat{e}_3\rangle$	$\langle (2+u)\hat{e}_2+2\hat{e}_3\rangle$
$\langle (2+u)\hat{e}_2+(2+u)\hat{e}_3\rangle$	$\langle (2+u)\hat{e}_2+u\hat{e}_3\rangle$
$\langle (2+u)\hat{e}_2+\langle 2,u\rangle \hat{e}_3\rangle$	$\langle (2+u)\hat{e}_2+\hat{e}_3\rangle$
$\langle u\hat{e}_2\rangle$	$\langle u\hat{e}_2+2u\hat{e}_3\rangle$
$\langle u\hat{e}_2+2\hat{e}_3\rangle$	$\langle u\hat{e}_2+(2+u)\hat{e}_3\rangle$
$\langle u\hat{e}_2+u\hat{e}_3\rangle$	$\langle u\hat{e}_2+\langle 2,u\rangle \hat{e}_3\rangle$
$\langle u\hat{e}_2+\hat{e}_3\rangle$	$\langle \langle 2,u\rangle \hat{e}_2\rangle$
$\langle (2,u)\hat{e}_2+2u\hat{e}_3\rangle$	$\langle \langle 2,u\rangle \hat{e}_2+2\hat{e}_3\rangle$
$\langle \langle 2,u\rangle \hat{e}_2+(2+u)\hat{e}_3\rangle$	$\langle \langle 2,u\rangle \hat{e}_2+u\hat{e}_3\rangle$
$\langle \langle 2,u\rangle \hat{e}_2+\langle 2,u\rangle \hat{e}_3\rangle$	$\langle \langle 2,u\rangle \hat{e}_2+\hat{e}_3\rangle$
$\langle \hat{e}_2\rangle$	$\langle \hat{e}_2+2u\hat{e}_3\rangle$
$\langle \hat{e}_2+2\hat{e}_3\rangle$	$\langle \hat{e}_2+(2+u)\hat{e}_3\rangle$
$\langle \hat{e}_2+u\hat{e}_3\rangle$	$\langle \hat{e}_2+\langle 2,u\rangle \hat{e}_3\rangle$
$\langle \hat{e}_2+\hat{e}_3\rangle$	$\langle 2u\hat{e}_1\rangle$
$\langle 2u\hat{e}_1+2u\hat{e}_3\rangle$	$\langle 2u\hat{e}_1+2\hat{e}_3\rangle$
$\langle 2u\hat{e}_1+(2+u)\hat{e}_3\rangle$	$\langle 2u\hat{e}_1+u\hat{e}_3\rangle$
$\langle 2u\hat{e}_1+\langle 2,u\rangle \hat{e}_3\rangle$	$\langle 2u\hat{e}_1+\hat{e}_3\rangle$
$\langle 2u\hat{e}_1+2u\hat{e}_2\rangle$	$\langle 2u\hat{e}_1+2u\hat{e}_2+2u\hat{e}_3\rangle$
$\langle 2u\hat{e}_1+2u\hat{e}_2+2\hat{e}_3\rangle$	$\langle 2u\hat{e}_1+2u\hat{e}_2+(2+u)\hat{e}_3\rangle$
$\langle 2u\hat{e}_1+2u\hat{e}_2+u\hat{e}_3\rangle$	$\langle 2u\hat{e}_1+2u\hat{e}_2+\langle 2,u\rangle \hat{e}_3\rangle$
$\langle 2u\hat{e}_1+2u\hat{e}_2+\hat{e}_3\rangle$	$\langle 2u\hat{e}_1+2\hat{e}_2\rangle$
$\langle 2u\hat{e}_1+2\hat{e}_2+2u\hat{e}_3\rangle$	$\langle 2u\hat{e}_1+2\hat{e}_2+2\hat{e}_3\rangle$
$\langle 2u\hat{e}_1+2\hat{e}_2+(2+u)\hat{e}_3\rangle$	$\langle 2u\hat{e}_1+2\hat{e}_2+u\hat{e}_3\rangle$
$\langle 2u\hat{e}_1+2\hat{e}_2+\langle 2,u\rangle \hat{e}_3\rangle$	$\langle 2u\hat{e}_1+2\hat{e}_2+\hat{e}_3\rangle$
$\langle 2u\hat{e}_1+(2+u)\hat{e}_2\rangle$	$\langle 2u\hat{e}_1+(2+u)\hat{e}_2+2u\hat{e}_3\rangle$
$\langle 2u\hat{e}_1+(2+u)\hat{e}_2+2\hat{e}_3\rangle$	$\langle 2u\hat{e}_1+(2+u)\hat{e}_2+(2+u)\hat{e}_3\rangle$
$\langle 2u\hat{e}_1+(2+u)\hat{e}_2+u\hat{e}_3\rangle$	$\langle 2u\hat{e}_1+(2+u)\hat{e}_2+(2,u)\hat{e}_3\rangle$
$\langle 2u\hat{e}_1+(2+u)\hat{e}_2+\hat{e}_3\rangle$	$\langle 2u\hat{e}_1+u\hat{e}_2\rangle$
$\langle 2u\hat{e}_1+u\hat{e}_2+2u\hat{e}_3\rangle$	$\langle 2u\hat{e}_1+u\hat{e}_2+2\hat{e}_3\rangle$

$\langle 2u\hat{e}_1 + u\hat{e}_2 + (2+u)\hat{e}_3\rangle$	$\langle 2u\hat{e}_1 + u\hat{e}_2 + u\hat{e}_3\rangle$
$\langle 2u\hat{e}_1 + u\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$	$\langle 2u\hat{e}_1 + u\hat{e}_2 + \hat{e}_3\rangle$
$\langle 2u\hat{e}_1 + \langle 2,u\rangle\hat{e}_2\rangle$	$\langle 2u\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + 2u\hat{e}_3\rangle$
$\langle 2u\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + 2\hat{e}_3\rangle$	$\langle 2u\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + (2+u)\hat{e}_3\rangle$
$\langle 2u\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + u\hat{e}_3\rangle$	$\langle 2u\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$
$\langle 2u\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + \hat{e}_3\rangle$	$\langle 2u\hat{e}_1 + \hat{e}_2\rangle$
$\langle 2u\hat{e}_1 + \hat{e}_2 + 2u\hat{e}_3\rangle$	$\langle 2u\hat{e}_1 + \hat{e}_2 + 2\hat{e}_3\rangle$
$\langle 2u\hat{e}_1 + \hat{e}_2 + (2+u)\hat{e}_3\rangle$	$\langle 2u\hat{e}_1 + \hat{e}_2 + u\hat{e}_3\rangle$
$\langle 2u\hat{e}_1 + \hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$	$\langle 2u\hat{e}_1 + \hat{e}_2 + \hat{e}_3\rangle$
$\langle 2\hat{e}_1\rangle$	$\langle 2\hat{e}_1 + 2u\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + 2\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + (2+u)\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + u\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + \langle 2,u\rangle\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + \hat{e}_3\rangle$	$\langle 2\hat{e}_1 + 2u\hat{e}_2\rangle$
$\langle 2\hat{e}_1 + 2u\hat{e}_2 + 2u\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + 2u\hat{e}_2 + 2\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + 2u\hat{e}_2 + (2+u)\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + 2u\hat{e}_2 + u\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + 2u\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + 2u\hat{e}_2 + \hat{e}_3\rangle$
$\langle 2\hat{e}_1 + 2\hat{e}_2\rangle$	$\langle 2\hat{e}_1 + 2\hat{e}_2 + 2u\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + 2\hat{e}_2 + 2\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + 2\hat{e}_2 + (2+u)\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + 2\hat{e}_2 + u\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + 2\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + 2\hat{e}_2 + \hat{e}_3\rangle$	$\langle 2\hat{e}_1 + (2+u)\hat{e}_2\rangle$
$\langle 2\hat{e}_1 + (2+u)\hat{e}_2 + 2u\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + (2+u)\hat{e}_2 + 2\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + (2+u)\hat{e}_2 + (2+u)\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + (2+u)\hat{e}_2 + u\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + (2+u)\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + (2+u)\hat{e}_2 + \hat{e}_3\rangle$
$\langle 2\hat{e}_1 + u\hat{e}_2\rangle$	$\langle 2\hat{e}_1 + u\hat{e}_2 + 2u\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + u\hat{e}_2 + 2\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + u\hat{e}_2 + (2+u)\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + u\hat{e}_2 + u\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + u\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + u\hat{e}_2 + \hat{e}_3\rangle$	$\langle 2\hat{e}_1 + \langle 2,u\rangle\hat{e}_2\rangle$
$\langle 2\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + 2u\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + 2\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + (2+u)\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + u\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + \hat{e}_3\rangle$
$\langle 2\hat{e}_1 + \hat{e}_2\rangle$	$\langle 2\hat{e}_1 + \hat{e}_2 + 2u\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + \hat{e}_2 + 2\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + \hat{e}_2 + (2+u)\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + \hat{e}_2 + u\hat{e}_3\rangle$	$\langle 2\hat{e}_1 + \hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$
$\langle 2\hat{e}_1 + \hat{e}_2 + \hat{e}_3\rangle$	$\langle (2+u)\hat{e}_1\rangle$
$\langle (2+u)\hat{e}_1 + 2u\hat{e}_3\rangle$	$\langle (2+u)\hat{e}_1 + 2\hat{e}_3\rangle$
$\langle (2+u)\hat{e}_1 + (2+u)\hat{e}_3\rangle$	$\langle (2+u)\hat{e}_1 + u\hat{e}_3\rangle$
$\langle (2+u)\hat{e}_1 + \langle 2,u\rangle\hat{e}_3\rangle$	$\langle (2+u)\hat{e}_1 + \hat{e}_3\rangle$
$\langle (2+u)\hat{e}_1 + 2u\hat{e}_2\rangle$	$\langle (2+u)\hat{e}_1 + 2u\hat{e}_2 + 2u\hat{e}_3\rangle$
$\langle (2+u)\hat{e}_1 + 2u\hat{e}_2 + 2\hat{e}_3\rangle$	$\langle (2+u)\hat{e}_1 + 2u\hat{e}_2 + (2+u)\hat{e}_3\rangle$
$\langle (2+u)\hat{e}_1 + 2u\hat{e}_2 + u\hat{e}_3\rangle$	$\langle (2+u)\hat{e}_1 + 2u\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$
$\langle (2+u)\hat{e}_1 + 2u\hat{e}_2 + \hat{e}_3\rangle$	$\langle (2+u)\hat{e}_1 + 2\hat{e}_2\rangle$

$\langle(2+u)\hat{e}_1+2\hat{e}_2+2u\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+2\hat{e}_2+2\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+2\hat{e}_2+(2+u)\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+2\hat{e}_2+u\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+2\hat{e}_2+\langle 2,u\rangle\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+2\hat{e}_2+\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+(2+u)\hat{e}_2\rangle$	$\langle(2+u)\hat{e}_1+(2+u)\hat{e}_2+2u\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+(2+u)\hat{e}_2+2\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+(2+u)\hat{e}_2+(2+u)\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+(2+u)\hat{e}_2+u\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+(2+u)\hat{e}_2+\langle 2,u\rangle\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+(2+u)\hat{e}_2+\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+u\hat{e}_2\rangle$
$\langle(2+u)\hat{e}_1+u\hat{e}_2+2u\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+u\hat{e}_2+2\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+u\hat{e}_2+(2+u)\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+u\hat{e}_2+u\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+u\hat{e}_2+\langle 2,u\rangle\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+u\hat{e}_2+\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+\langle 2,u\rangle\hat{e}_2\rangle$	$\langle(2+u)\hat{e}_1+\langle 2,u\rangle\hat{e}_2+2u\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+\langle 2,u\rangle\hat{e}_2+2\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+\langle 2,u\rangle\hat{e}_2+(2+u)\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+\langle 2,u\rangle\hat{e}_2+u\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+\langle 2,u\rangle\hat{e}_2+\langle 2,u\rangle\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+\langle 2,u\rangle\hat{e}_2+\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+\hat{e}_2\rangle$
$\langle(2+u)\hat{e}_1+\hat{e}_2+2u\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+\hat{e}_2+2\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+\hat{e}_2+(2+u)\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+\hat{e}_2+u\hat{e}_3\rangle$
$\langle(2+u)\hat{e}_1+\hat{e}_2+\langle 2,u\rangle\hat{e}_3\rangle$	$\langle(2+u)\hat{e}_1+\hat{e}_2+\hat{e}_3\rangle$
$\langle u\hat{e}_1\rangle$	$\langle u\hat{e}_1+2u\hat{e}_3\rangle$
$\langle u\hat{e}_1+2\hat{e}_3\rangle$	$\langle u\hat{e}_1+(2+u)\hat{e}_3\rangle$
$\langle u\hat{e}_1+u\hat{e}_3\rangle$	$\langle u\hat{e}_1+\langle 2,u\rangle\hat{e}_3\rangle$
$\langle u\hat{e}_1+\hat{e}_3\rangle$	$\langle u\hat{e}_1+2u\hat{e}_2\rangle$
$\langle u\hat{e}_1+2u\hat{e}_2+2u\hat{e}_3\rangle$	$\langle u\hat{e}_1+2u\hat{e}_2+2\hat{e}_3\rangle$
$\langle u\hat{e}_1+2u\hat{e}_2+(2+u)\hat{e}_3\rangle$	$\langle u\hat{e}_1+2u\hat{e}_2+u\hat{e}_3\rangle$
$\langle u\hat{e}_1+2u\hat{e}_2+\langle 2,u\rangle\hat{e}_3\rangle$	$\langle u\hat{e}_1+2u\hat{e}_2+\hat{e}_3\rangle$
$\langle u\hat{e}_1+2\hat{e}_2\rangle$	$\langle u\hat{e}_1+2\hat{e}_2+2u\hat{e}_3\rangle$
$\langle u\hat{e}_1+2\hat{e}_2+2\hat{e}_3\rangle$	$\langle u\hat{e}_1+2\hat{e}_2+(2+u)\hat{e}_3\rangle$
$\langle u\hat{e}_1+2\hat{e}_2+u\hat{e}_3\rangle$	$\langle u\hat{e}_1+2\hat{e}_2+\langle 2,u\rangle\hat{e}_3\rangle$
$\langle u\hat{e}_1+2\hat{e}_2+\hat{e}_3\rangle$	$\langle u\hat{e}_1+(2+u)\hat{e}_2\rangle$
$\langle u\hat{e}_1+(2+u)\hat{e}_2+2u\hat{e}_3\rangle$	$\langle u\hat{e}_1+(2+u)\hat{e}_2+2\hat{e}_3\rangle$
$\langle u\hat{e}_1+(2+u)\hat{e}_2+(2+u)\hat{e}_3\rangle$	$\langle u\hat{e}_1+(2+u)\hat{e}_2+u\hat{e}_3\rangle$
$\langle u\hat{e}_1+(2+u)\hat{e}_2+\langle 2,u\rangle\hat{e}_3\rangle$	$\langle u\hat{e}_1+(2+u)\hat{e}_2+\hat{e}_3\rangle$
$\langle u\hat{e}_1+u\hat{e}_2\rangle$	$\langle u\hat{e}_1+u\hat{e}_2+2u\hat{e}_3\rangle$
$\langle u\hat{e}_1+u\hat{e}_2+2\hat{e}_3\rangle$	$\langle u\hat{e}_1+u\hat{e}_2+(2+u)\hat{e}_3\rangle$
$\langle u\hat{e}_1+u\hat{e}_2+u\hat{e}_3\rangle$	$\langle u\hat{e}_1+u\hat{e}_2+\langle 2,u\rangle\hat{e}_3\rangle$
$\langle u\hat{e}_1+u\hat{e}_2+\hat{e}_3\rangle$	$\langle u\hat{e}_1+\langle 2,u\rangle\hat{e}_2\rangle$
$\langle u\hat{e}_1+\langle 2,u\rangle\hat{e}_2+2u\hat{e}_3\rangle$	$\langle u\hat{e}_1+\langle 2,u\rangle\hat{e}_2+2\hat{e}_3\rangle$
$\langle u\hat{e}_1+\langle 2,u\rangle\hat{e}_2+(2+u)\hat{e}_3\rangle$	$\langle u\hat{e}_1+\langle 2,u\rangle\hat{e}_2+u\hat{e}_3\rangle$
$\langle u\hat{e}_1+\langle 2,u\rangle\hat{e}_2+(2,u)\hat{e}_3\rangle$	$\langle u\hat{e}_1+\langle 2,u\rangle\hat{e}_2+\hat{e}_3\rangle$
$\langle u\hat{e}_1+\hat{e}_2\rangle$	$\langle u\hat{e}_1+\hat{e}_2+2u\hat{e}_3\rangle$
$\langle u\hat{e}_1+\hat{e}_2+2\hat{e}_3\rangle$	$\langle u\hat{e}_1+\hat{e}_2+(2+u)\hat{e}_3\rangle$
$\langle u\hat{e}_1+\hat{e}_2+u\hat{e}_3\rangle$	$\langle u\hat{e}_1+\hat{e}_2+\langle 2,u\rangle\hat{e}_3\rangle$

$\langle u\hat{e}_1 + \hat{e}_2 + \hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + 2u\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + 2\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + (2+u)\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + u\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + \langle 2,u\rangle\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + \hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + 2u\hat{e}_2\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + 2u\hat{e}_2 + 2u\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + 2u\hat{e}_2 + 2\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + 2u\hat{e}_2 + (2+u)\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + 2u\hat{e}_2 + u\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + 2u\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + 2u\hat{e}_2 + \hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + 2\hat{e}_2\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + 2\hat{e}_2 + 2u\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + 2\hat{e}_2 + 2\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + 2\hat{e}_2 + (2+u)\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + 2\hat{e}_2 + u\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + 2\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + 2\hat{e}_2 + \hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + (2+u)\hat{e}_2\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + (2+u)\hat{e}_2 + 2u\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + (2+u)\hat{e}_2 + 2\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + (2+u)\hat{e}_2 + (2+u)\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + (2+u)\hat{e}_2 + u\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + (2+u)\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + (2+u)\hat{e}_2 + \hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + u\hat{e}_2\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + u\hat{e}_2 + 2u\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + u\hat{e}_2 + 2\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + u\hat{e}_2 + (2+u)\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + u\hat{e}_2 + u\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + u\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + u\hat{e}_2 + \hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + \langle 2,u\rangle\hat{e}_2\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + 2u\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + 2\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + (2+u)\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + u\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + \langle 2,u\rangle\hat{e}_2 + \hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + \hat{e}_2 + 0\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + \hat{e}_2 + 2u\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + \hat{e}_2 + 2\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + \hat{e}_2 + (2+u)\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + \hat{e}_2 + u\hat{e}_3\rangle$
$\langle\langle 2,u\rangle\hat{e}_1 + \hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$	$\langle\langle 2,u\rangle\hat{e}_1 + \hat{e}_2 + \hat{e}_3\rangle$
$\langle\hat{e}_1\rangle$	$\langle\hat{e}_1 + 2u\hat{e}_3\rangle$
$\langle\hat{e}_1 + 2\hat{e}_3\rangle$	$\langle\hat{e}_1 + (2+u)\hat{e}_3\rangle$
$\langle\hat{e}_1 + u\hat{e}_3\rangle$	$\langle\hat{e}_1 + \langle 2,u\rangle\hat{e}_3\rangle$
$\langle\hat{e}_1 + \hat{e}_3\rangle$	$\langle\hat{e}_1 + 2u\hat{e}_2\rangle$
$\langle\hat{e}_1 + 2u\hat{e}_2 + 2u\hat{e}_3\rangle$	$\langle\hat{e}_1 + 2u\hat{e}_2 + 2\hat{e}_3\rangle$
$\langle\hat{e}_1 + 2u\hat{e}_2 + (2+u)\hat{e}_3\rangle$	$\langle\hat{e}_1 + 2u\hat{e}_2 + u\hat{e}_3\rangle$
$\langle\hat{e}_1 + 2u\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$	$\langle\hat{e}_1 + 2u\hat{e}_2 + \hat{e}_3\rangle$
$\langle\hat{e}_1 + 2\hat{e}_2\rangle$	$\langle\hat{e}_1 + 2\hat{e}_2 + 2u\hat{e}_3\rangle$
$\langle\hat{e}_1 + 2\hat{e}_2 + 2\hat{e}_3\rangle$	$\langle\hat{e}_1 + 2\hat{e}_2 + (2+u)\hat{e}_3\rangle$
$\langle\hat{e}_1 + 2\hat{e}_2 + u\hat{e}_3\rangle$	$\langle\hat{e}_1 + 2\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$
$\langle\hat{e}_1 + 2\hat{e}_2 + \hat{e}_3\rangle$	$\langle\hat{e}_1 + (2+u)\hat{e}_2\rangle$
$\langle\hat{e}_1 + (2+u)\hat{e}_2 + 2u\hat{e}_3\rangle$	$\langle\hat{e}_1 + (2+u)\hat{e}_2 + 2\hat{e}_3\rangle$
$\langle\hat{e}_1 + (2+u)\hat{e}_2 + (2+u)\hat{e}_3\rangle$	$\langle\hat{e}_1 + (2+u)\hat{e}_2 + u\hat{e}_3\rangle$
$\langle\hat{e}_1 + (2+u)\hat{e}_2 + \langle 2,u\rangle\hat{e}_3\rangle$	$\langle\hat{e}_1 + (2+u)\hat{e}_2 + \hat{e}_3\rangle$
$\langle\hat{e}_1 + u\hat{e}_2\rangle$	$\langle\hat{e}_1 + u\hat{e}_2 + 2u\hat{e}_3\rangle$
$\langle\hat{e}_1 + u\hat{e}_2 + 2\hat{e}_3\rangle$	$\langle\hat{e}_1 + u\hat{e}_2 + (2+u)\hat{e}_3\rangle$

$\langle \hat{e}_1 + u\hat{e}_2 + u\hat{e}_3 \rangle$	$\langle \hat{e}_1 + u\hat{e}_2 + \langle 2, u \rangle \hat{e}_3 \rangle$
$\langle \hat{e}_1 + u\hat{e}_2 + \hat{e}_3 \rangle$	$\langle \hat{e}_1 + \langle 2, u \rangle \hat{e}_2 \rangle$
$\langle \hat{e}_1 + \langle 2, u \rangle \hat{e}_2 + 2u\hat{e}_3 \rangle$	$\langle \hat{e}_1 + \langle 2, u \rangle \hat{e}_2 + 2\hat{e}_3 \rangle$
$\langle \hat{e}_1 + \langle 2, u \rangle \hat{e}_2 + (2+u)\hat{e}_3 \rangle$	$\langle \hat{e}_1 + \langle 2, u \rangle \hat{e}_2 + u\hat{e}_3 \rangle$
$\langle \hat{e}_1 + \langle 2, u \rangle \hat{e}_2 + \langle 2, u \rangle \hat{e}_3 \rangle$	$\langle \hat{e}_1 + \langle 2, u \rangle \hat{e}_2 + \hat{e}_3 \rangle$
$\langle \hat{e}_1 + \hat{e}_2 \rangle$	$\langle \hat{e}_1 + \hat{e}_2 + 2u\hat{e}_3 \rangle$
$\langle \hat{e}_1 + \hat{e}_2 + 2\hat{e}_3 \rangle$	$\langle \hat{e}_1 + \hat{e}_2 + (2+u)\hat{e}_3 \rangle$
$\langle \hat{e}_1 + \hat{e}_2 + u\hat{e}_3 \rangle$	$\langle \hat{e}_1 + \hat{e}_2 + \langle 2, u \rangle \hat{e}_3 \rangle$

Apéndice C

Código fuente para calcular ideales de $\mathcal{R}_k = \mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$

En el presente apéndice se incluye el código fuente para obtener el conjunto de ideales del anillo $\mathcal{R}_k = \mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$. El programa se realizó originalmente en SageMath 9.2 y ha sido probado y mejorado en las versiones 9.3 y 10.0 ([32]). Se proporciona el código tal y como aparece en el correspondiente notebook de Sage.

Se parte de las definición de ideal en anillos conmutativos y se toman en cuenta las consideraciones sobre $\mathcal{R}_k$ dadas en el capítulo 2. El programa también devuelve, aunque no en una forma optimizada, las contenciones entre ideales, lo que permitiría al usuario construir diagramas como el mostrado en la figura 2.3.

Se recomiendan valores pequeños de k ya que los ideales se van almacenando en la memoria principal para ser analizados como conjuntos. Con modificaciones mínimas, el programa también podría calcular el conjunto de ideales para $p > 2$ aunque, dado el número de elementos que se tendría en tal caso, el proceso puede ser muy tardado.

Código fuente para calcular el conjunto de ideales del anillo $\mathcal{R}_k = \mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$

[ ]:
```
reset() #Free resources
```

[ ]:
```
from datetime import datetime
print("Starting at:")
datetime.now().strftime('%Y-%m-%d %H:%M:%S') #Hora de inicio
```

[ ]:
```
k = 4 #exponent for 2
p = 2 #Prime for build F_p, this value must be p=2 DON'T CHANGE IT!
polyDeg = 15 #Degree of X^n - 1
modulo = p**k
ringZMod2k = IntegerModRing(modulo) #Ring of integers mod 2^k
R.<x> = PolynomialRing(ringZMod2k) #Polynomial ring in x associated to ringZMod2k
polynomial = x^2 #Polynomial for calculating the quotient ring S.<u>
I = R.ideal(polynomial) #Construction of ideal I=<polynomial>
S.<u> = R.quotient_ring(I) #Quotient ring, polynomial forms in u
listOfRingSElements = list(S) #The elements of the quotien ring S.<u>
#Auxiliar variable for storage the units of the ring ringZMod2k
listOfRingZMod2kUnits = []
#Auxiliar variable for storage the non units of the ring ringZMod2k
listOfRingZmod2kNonUnits = []

listOfRingZMod2kUnits.append(listOfRingSElements[1]) #Add to the list the identity: 1
listOfRingZmod2kNonUnits.append(listOfRingSElements[0]) #Add to the list the first non unit: 0

for j in range(2,modulo):
    if GCD(j,modulo) == 1:
        listOfRingZMod2kUnits.append(listOfRingSElements[j])
    else:
        listOfRingZmod2kNonUnits.append(listOfRingSElements[j])

listOfRingZMod2kElements = list(ringZMod2k) #We put in a list the elements of the ring ringZMod2k
listOfRingSUnits = [] #For the units of th ring  S.<u>
listOfRingSNonUnits = [] #For the non units of th ring  S.<u>
#listOfRingSNonUnits.append(listOfRingSElements[0]) #Agregamos el cero

for i in range(len(listOfRingZMod2kUnits)):
    listOfRingSUnits.append(listOfRingZMod2kUnits[i])

for i in range(len(listOfRingZmod2kNonUnits)):
    listOfRingSNonUnits.append(listOfRingZmod2kNonUnits[i])

nZeroElemOfRingZMod2k = [] #Auxiliar variable for build the units of the ring S.<u>
for i in range(1, modulo):
    nZeroElemOfRingZMod2k.append(listOfRingZMod2kElements[i]),
    #print(nZeroElemOfRingZMod2k)

for unitOfZMod2k in listOfRingZMod2kUnits:
    for element in nZeroElemOfRingZMod2k:
        listOfRingSUnits.append(u*element + unitOfZMod2k)

for nonUnitOfZMod2k in listOfRingZmod2kNonUnits:
```

```
    for element in nZeroElemOfRingZMod2k:
        listOfRingSNonUnits.append(u*element + nonUnitOfZMod2k)
```

[ ]:
```
numOfIdealsOfRingS = (k**2) + k
listOfIdealsOfS = [] #Variable for storage the lattice of ideals of the ring S.<u>
for j in range(0,numOfIdealsOfRingS):
    listOfIdealsOfS.append([])
listOfGeneratorsOfIdeals = []
```

Ideals with form $\langle 2^j, 2^{j-1}u\rangle$ $j = 1, 2, \ldots, k+1$

[ ]:
```
for i in range(0,k+1):
    primeToPowerJ = listOfRingSElements[2]**(k-(i-1))
    primeToPowerJm1u = (listOfRingSElements[2]**(k-i))*u
    listOfGeneratorsOfIdeals.append(set([primeToPowerJ,primeToPowerJm1u]))
    print("=-==-==-==-==-==-==-==-==-==-=")
    print("Ideal with generators:", primeToPowerJ, ",",primeToPowerJm1u)
    for a in range(len(listOfRingZMod2kElements)):
        for b in range(len(listOfRingZMod2kElements)):
            newElement = primeToPowerJ*listOfRingZMod2kElements[a] +␣
↪primeToPowerJm1u*listOfRingZMod2kElements[b]
            if newElement not in listOfIdealsOfS[i]:
                listOfIdealsOfS[i].append(newElement)
    print("Ideal with cardinality:",len(listOfIdealsOfS[i]), " at index of listOfIdealsOfS ", i)
idxA = k+1
#print(idxA)
```

Ideals with form $\langle 2^j + 2^{j-1}u\rangle$ $j = 1, 2, \ldots, k-1$

[ ]:
```
for i in range(2,k+1):
    primeToPowerJ = listOfRingSElements[2]**(k-(i-1))
    primeToPowerJm1u = (listOfRingSElements[2]**(k-i))*u
    auxSUM = primeToPowerJ + primeToPowerJm1u
    listOfGeneratorsOfIdeals.append(set([auxSUM]))
    print("=-==-==-==-==-==-==-==-==-==-=")
    print("Ideal with generator:",auxSUM)
    for a in range(len(listOfRingSElements)):
        newElement = auxSUM*listOfRingSElements[a]
        if newElement not in listOfIdealsOfS[idxA]:
            listOfIdealsOfS[idxA].append(newElement)
    print("Ideal with cardinality:",len(listOfIdealsOfS[idxA]), " at index of listOfIdealsOfS ", idxA)
    idxA = idxA + 1
    #print(idxA)
```

Ideals with form $\langle 2^{j-1}u\rangle$ $j = 1, 2, \ldots, k-1$

[ ]:
```
for i in range(1,k):
    primeToPowerJm1u = (listOfRingSElements[2]**(i-1))*u
    print("=-==-==-==-==-==-==-==-==-==-=")
    print("Ideal with generator:",primeToPowerJm1u)
    listOfGeneratorsOfIdeals.append(set([primeToPowerJm1u]))
    for a in range(len(listOfRingSElements)):
        newElement = primeToPowerJm1u*listOfRingSElements[a]
        if newElement not in listOfIdealsOfS[idxA]:
            listOfIdealsOfS[idxA].append(newElement)
    print("Ideal with cardinality:",len(listOfIdealsOfS[idxA])," at index of listOfIdealsOfS ", idxA)
    idxA = idxA + 1
    #print(idxA)
```

Ideals with form $\langle 2^{j-1}\rangle$, $j = 1, 2, \ldots, k-1$.

[ ]:
```
for i in range(1,k):
    primeToPowerJ = (listOfRingSElements[2]**(i))
    print("=-==-==-==-==-==-==-==-==-==-=")
    print("Ideal with generator:",primeToPowerJ)
    listOfGeneratorsOfIdeals.append(set([primeToPowerJ]))
    for a in range(len(listOfRingSElements)):
        newElement = primeToPowerJ*listOfRingSElements[a]
```

```
        if newElement not in listOfIdealsOfS[idxA]:
            listOfIdealsOfS[idxA].append(newElement)
    print("Ideal with cardinality:",len(listOfIdealsOfS[idxA])," at index of listOfIdealsOfS ", idxA)
    idxA = idxA + 1
    #print(idxA)
```

Ideals with form $\langle 2^{j+1}, 2^{l-1}u\rangle$ $j = i$, $l \leq i$ and $i = 1, 2, \ldots, k-2$

[ ]:
```
#idxA=0 #This is auxiliar for ONLY RUN THE NEXT TWO CELLs, IT MUST BE COMMENTED
```

[ ]:
```
for i in range(1,k-1):#k-1 for the index take the value k-2
    primeToPowerJ = listOfRingSElements[2]**(i+1)
    for l in range(1,i+1):
        primeToPowerJm1u = (listOfRingSElements[2]**(l-1))*u
        print("=-=-=-=-=-=-=-=-=-=-=-=-=-=")
        print("Ideal with generators:",primeToPowerJ,",", primeToPowerJm1u)
        listOfGeneratorsOfIdeals.append(set([primeToPowerJ,primeToPowerJm1u]))
        for a in range(len(listOfRingZMod2kElements)):
            for b in range(len(listOfRingZMod2kElements)):
                newElement = primeToPowerJ*listOfRingZMod2kElements[a] +␣
↪primeToPowerJm1u*listOfRingZMod2kElements[b]
                if newElement not in listOfIdealsOfS[idxA]:
                    listOfIdealsOfS[idxA].append(newElement)
        print("Ideal with cardinality:",len(listOfIdealsOfS[idxA])," at index of listOfIdealsOfS ", idxA)
        idxA = idxA+1
        #print(idxA)
```

Ideals with form $\langle 2^{j+1} + 2^{l-1}u\rangle$ $j = i$, $l \leq i$ and $i = 1, 2, \ldots, k-2$

[ ]:
```
for i in range(1,k-1):#k-1 for the index take the value k-2
    primeToPowerJ = listOfRingSElements[2]**(i+1)
    for l in range(1,i+1):
        primeToPowerJm1u = (listOfRingSElements[2]**(l-1))*u
        auxSum = primeToPowerJ + primeToPowerJm1u
        print("=-=-=-=-=-=-=-=-=-=-=-=-=-=")
        print("Ideal with generator:",auxSum)
        listOfGeneratorsOfIdeals.append(set([auxSum]))
        for a in range(len(listOfRingSElements)):
            newElement = auxSum*listOfRingSElements[a]
            if newElement not in listOfIdealsOfS[idxA]:
                listOfIdealsOfS[idxA].append(newElement)
        print("Ideal with cardinality:",len(listOfIdealsOfS[idxA])," at index of listOfIdealsOfS ", idxA)
        idxA = idxA+1
        #print(idxA)
```

[ ]:
```
#Select all content and Press CTRL + / for comment or uncomment the content of a cell
listOfIdealsOfSAsSets = []
for i in range(numOfIdealsOfRingS):
    listOfIdealsOfSAsSets.append(set(listOfIdealsOfS[i]))
```

[ ]:
```
len(listOfIdealsOfSAsSets)
```

[ ]:
```
#We liberate the space in memory for the list listOfIdealsOfS
listOfIdealsOfS = []
```

[ ]:
```
for i in range(2, k-1):#k-1 for the proccess runs until k-2
    powOfGen2 = listOfRingZmod2kNonUnits[1]**(i)
    indexMiddleList = 2**(i)
    auxListZ2d = listOfRingZMod2kElements[1:indexMiddleList]
    for j in range(len(auxListZ2d)):
        listAuxForIdeal = []
        genOfnotJointIdeal = auxListZ2d[j]*u + powOfGen2
        auxSetOfGen = set([genOfnotJointIdeal])
        if auxSetOfGen not in listOfGeneratorsOfIdeals:
            for a in range(len(listOfRingSElements)):
                newElement = genOfnotJointIdeal*listOfRingSElements[a]
```

```
                if newElement not in listAuxForIdeal:
                    listAuxForIdeal.append(newElement)
            setAux = set(listAuxForIdeal)
            if setAux not in listOfIdealsOfSAsSets:
                listOfGeneratorsOfIdeals.append(set([genOfnotJointIdeal]))
                print("=-==-==-==-==-==-==-==-=")
                print("*Ideal with generator ",genOfnotJointIdeal," added at position: ",␣
↪len(listOfIdealsOfSAsSets)-1, "cardinality: ", len(listAuxForIdeal))
                listOfIdealsOfSAsSets.append(setAux)
            else:
                print("The ideal with generator ",genOfnotJointIdeal,"already exists, at index: ",␣
↪listOfIdealsOfSAsSets.index(setAux))
        else:
            print("The ideal with generators ", auxSetOfGen, "has been already calculated" )
#
print("Now, the cardinality of the Lattice is: ", len(listOfIdealsOfSAsSets))
listAuxForIdeal = [] #Empty the content of this variable
```

[ ]:
```
# ####For the lemmas the 2-generated ideals
indexMiddleList = 2^(k-1)
auxListZ2d = listOfRingZMod2kElements[1:indexMiddleList]
for a in range(2, k-1):#k-1 for the proccess runs until k-2
    firstPartOfGen1 = listOfRingZmod2kNonUnits[1]**(a)
    for b in range(len(auxListZ2d)):
        if int(auxListZ2d[b]) < 2**(a):
            genOfNotJointIdealA = auxListZ2d[b]*u + firstPartOfGen1
            #print(genOfNotJointIdealA)
            for c in range(a,a+1):
                firstPartOfGen2 = listOfRingZmod2kNonUnits[1]**(c)
                for d in range(len(auxListZ2d)):
                    if int(auxListZ2d[d]) < 2**(c) and ((int(auxListZ2d[d]) - int(auxListZ2d[b])) % 2 == 0):
                        genOfNotJointIdealB = auxListZ2d[d]*u + firstPartOfGen2
                        print("=-==-==-==-==-==-==-==-=")
                        print("Ideal with generators: ", genOfNotJointIdealA, genOfNotJointIdealB)
                        auxSetOfGen = set([genOfNotJointIdealA, genOfNotJointIdealB])
                        if auxSetOfGen not in listOfGeneratorsOfIdeals:
                            listAuxForIdeal = []
                            listAuxForIdeal_1 = []
                            listAuxForIdeal_2 = []
                            print("Calculating the first ideal with generator ", genOfNotJointIdealA)
                            for i in range(len(listOfRingSElements)):
                                newElement_1 = genOfNotJointIdealA*listOfRingSElements[i]
                                if newElement_1 not in listAuxForIdeal_1:
                                    listAuxForIdeal_1.append(newElement_1)
                            print("Ideal with generator ", genOfNotJointIdealA, "has been calculated")
                            print("Calculating the second ideal with generator ", genOfNotJointIdealB)
                            for i in range(len(listOfRingSElements)):
                                newElement_2 = genOfNotJointIdealB*listOfRingSElements[i]
                                if newElement_2 not in listAuxForIdeal_2:
                                    listAuxForIdeal_2.append(newElement_2)
                            print("Ideal with generator ", genOfNotJointIdealB, "has been calculated")
                            for i in range(len(listAuxForIdeal_1)):
                                for j in range(len(listAuxForIdeal_2)):
                                    newElement = listAuxForIdeal_1[i] + listAuxForIdeal_2[j]
                                    if newElement not in listAuxForIdeal:
                                        listAuxForIdeal.append(newElement)
                            print("Analyzing ideal...")
                            setA = set(listAuxForIdeal)
                            if setA not in listOfIdealsOfSAsSets:
                                listOfGeneratorsOfIdeals.append(set([genOfNotJointIdealA,␣
↪genOfNotJointIdealB]))
                                listOfIdealsOfSAsSets.append(setA)
                                print("***NEW ideal found REVIEW at index: ", listOfIdealsOfSAsSets.
↪index(setA), "cardinality: ", len(setA))
                            else:
                                print("The ideal already exists, at index: ", listOfIdealsOfSAsSets.
↪index(setA))
```

```
                        else:
                            print("The ideal with generators ", auxSetOfGen, "has been already calculated" )
print("Now, the cardinality of the Lattice is: ", len(listOfIdealsOfSAsSets))
listAuxForIdeal = [] #Empty the content of this variable
```

[ ]:
```
for i in range(1, len(listOfIdealsOfSAsSets)):
    for j in range(len(listOfIdealsOfSAsSets)):
            if i!=j and listOfIdealsOfSAsSets[i].issubset(listOfIdealsOfSAsSets[j]):
                print("====================")
                print("I_"+str(i)+" is a subset of I_"+str(j))
    print("******************************")
```

[ ]:
```
for i in range(len(listOfGeneratorsOfIdeals)):
    print("Ideal with generator(s): ",listOfGeneratorsOfIdeals[i], "at index: ", i)
print("=-==-==-==-==-==-==-=")
print("Total of ideals counting trivials: ", len(listOfGeneratorsOfIdeals) + 1)
print("=-==-==-==-==-==-==-=")
```

[ ]:
```
print("Proccess finished at:")
datetime.now().strftime('%Y-%m-%d %H:%M:%S') #Hora de finalizacion
```

Bibliografía

[1] I. F. Blake, "Codes over certain rings," *Information and Control*, vol. 20, pp. 396–404, 1972.

[2] I. F. Blake, "Codes over integer residue rings," *Information and Control*, vol. 29, pp. 295–300, 1975.

[3] A. R. Hammons, 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 Transactions on Information Theory*, vol. 40, pp. 301–319, march 1994.

[4] V. S. Pless and Z. Qian, "Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$," *IEEE Transactions on Information Theory*, vol. 42, pp. 1594–1600, september 1996.

[5] J. A. Wood, "Duality for modules over finite rings and applications to coding theory," *American Journal of Mathematics*, vol. 121, pp. 555–575, june 1999.

[6] S. T. Dougherty, *Algebraic Coding Theory over Finite Commutative Rings*. Springer International Publishing AG, 1 ed., 2017.

[7] P. Kanwar and S. López-Permouth, "Cyclic codes over the integers modulo p^m," *Finite Fields and Their Applications*, vol. 3, pp. 334–352, 1997.

[8] M. Charkani and J. Kabore, "Primitive idempotents and constacyclic codes over finite chain rings," *Gulf Journal of Mathematics*, vol. 8, no. 2, pp. 55–67, 2020. Retrieved from https://gjom.org/index.php/gjom/article/view/434.

[9] B. Yildiz and S. Karadeniz, "Linear codes over $\mathbb{Z}_4+u\mathbb{Z}_4$: MacWilliams identities, projections, and formally self-dual codes," *Finite Fields and Their Applications*, vol. 27, pp. 24–40, May 2014.

[10] E. Martínez-Moro and S. Szabo, "On codes over local Frobenius non-chain rings of order 16," *Contemporary Mathematics*, vol. 634, pp. 227–241, 2015.

[11] C. A. Castillo-Guillén, C. Rentería-Márquez, and H. Tapia-Recillas, "Constacyclic codes over finite local Frobenius non-chain rings with nilpotency index 3," *Finite Fields and Their Applications*, vol. 43, pp. 1–21, 2017.

[12] E. R. Berlekamp, "Negacyclic codes for the Lee metric," tech. rep., North Carolina State University. Dept. of Statistics, 1966.

[13] J. Wolfmann, "Correspondence-negacyclic and cyclic codes over $\mathbb{Z}_4$," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2527–2531, 1999.

[14] J. Diaz-Vargas, C. J. Rubio-Barrios, H. Tapia-Recillas, and J. A. Velazco-Velazco, "Linear Codes over the Ring $R_m = \mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$," *International Journal of Algebra*, vol. 15, no. 4, pp. 215–219, 2021. https://doi.org/10.12988/ija.2021.91568.

[15] H. Tapia-Recillas and J. A. Velazco-Velazco, "Cyclic Codes over the ring $\mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$," *São Paulo Journal of Mathematical Sciences*, vol. 18, pp. 14–27, may 2024. https://doi.org/10.1007/s40863-024-00412-z.

[16] B. Yildiz and N. Aydin, "On cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and their $\mathbb{Z}_4$-images," *International Journal of Information and Coding Theory*, vol. 2, pp. 226–237, december 2014.

[17] R. Bandi and M. Bhaintwal, "Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$," *Conference: IWSDA'15*, September 2015. The seventh International Workshop on Signal Design and its Applications in Communications, Bengaluru, India.

[18] J. Gao, F. Fu, L. Xiao, and R. Bandi, "Some results on cyclic codes over $\mathbb{Z}_q + u\mathbb{Z}_q$," *Discrete Mathematics, Algorithms and Applications*, vol. 7, no. 4, 2015.

[19] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[20] S. Lang, *Algebra*, vol. 211 of *Graduate Text in Mathematics*. Springer New York, NY, 3 ed., 2012. Originally published by Addison-Wesley, 1993.

[21] B. R. McDonald, *Finite Rings with Identity*. No. 28 in Pure and Applied mathematics, Marcel Dekker Inc., 1974.

[22] G. Bini and F. Flamini, *Finite commutative Rings and their Applications*. Springer Science+Bussines Media, 1 ed., 2002.

[23] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 1 ed., 2003.

[24] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*. Elsevier/North-Holland, 1 ed., 1977.

[25] T. Y. Lam, *Lectures on Modules and Rings*, vol. 189 of *Graduated Texts in Mathematics*. Springer Verlag New York, Inc., 1999.

[26] T. Y. Lam, *A First Course in Noncommutative Rings*, vol. 131 of *Graduated Texts in Mathematics*. Springer Verlag New York, Inc., 1991.

[27] R. Lidl and H. Niederreiter, *Finite Fields*. Encyclopedia of Mathematics and its applications, Cambridge University Press, 2nd ed., 1996.

[28] H. Q. Dinh and S. R. López-Permouth, "Cyclic and negacyclic codes over finite chain rings," *IEEE Transactions on Information Theory*, vol. 50, no. 8, pp. 1728–1744, 2004. https://doi.org/10.1109/TIT.2004.831789.

[29] H. Tapia-Recillas and G. Vega, "Some constacyclic codes over $\mathbb{Z}_{2^k}$ and binary quasi-cyclic codes," *Discrete Applied Mathematics*, vol. 128, no. 1, pp. 305–316, 2003. International Workshop on Coding and Cryptography (WCC2001).

[30] W. LI, M. Yue, Z. Huang, and Z. LI, "Linear codes over the ring $\mathbb{Z}_8 + u\mathbb{Z}_8$," in *2018 International Conference on Information, Electronic and Communication Engineering*, pp. 311–315, DEStech Publications, Inc., october 2018.

[31] J. J. Rotman, *An introduction to the Theory of Groups*, vol. 148 of *Graduated Texts in Mathematics*. New York: Springer New York, NY, 1994.

[32] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 10.0)*, 2023. `https://www.sagemath.org`.

[33] F. D. Melo-Hernández, C. A. Hernández-Melo, and H. Tapia-Recillas, "On idempotents of a class of commutative rings," *Communications in Algebra*, vol. 48, pp. 4013–4026, 2020.

[34] R. Bandi and M. Bhaintwal, "A note on cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$," *Discrete Mathematics, Algorithms and Applications*, vol. 08, no. 01, p. 1650017, 2016. https://doi.org/10.1142/S1793830916500178.

[35] H. Tapia-Recillas and J. A. Velazco-Velazco, "Vector-circulant matrices and codes over rings," *Mixba'al Revista Metropolitana de Matemáticas*, vol. 13, no. 1, pp. 95–98, 2022. www.doi.org/10.24275/uami/dcbi/mix/v13n1/hotav.

[36] H. Tapia-Recillas and J. A. Velazco-Velazco, "Vector-circulant matrices and codes over rings," *Gulf Journal of Mathematics*, vol. 15, no. 2, pp. 160–165, 2023. https://doi.org/10.56947/gjom.v15i2.1412.

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

ACTA DE DISERTACIÓN PÚBLICA

No. 00090
Matrícula: 2193801760

Códigos constacíclicos sobre el anillo de Frobenius no de cadena $R_x=Z_{pk}+uZ_{pk}$

En la Ciudad de México, se presentaron a las 11:00 horas del día 5 del mes de agosto del año 2024 en la Unidad Iztapalapa de la Universidad Autónoma Metropolitana, los suscritos miembros del jurado:

DR. HORACIO TAPIA RECILLAS
DR. MANUEL GONZALEZ SARABIA
DR. JOSE NOE GUTIERREZ HERRERA
DR. ELISEO SARMIENTO ROSALES
DR. MARIO PINEDA RUELAS

Bajo la Presidencia del primero y con carácter de Secretario el último, se reunieron a la presentación de la Disertación Pública cuya denominación aparece al margen, para la obtención del grado de:

DOCTOR EN CIENCIAS (MATEMÁTICAS)

DE: JUAN ARMANDO VELAZCO VELAZCO

y de acuerdo con el artículo 78 fracción IV del Reglamento de Estudios Superiores de la Universidad Autónoma Metropolitana, los miembros del jurado resolvieron:

Aprobar

Acto continuo, el presidente del jurado comunicó al interesado el resultado de la evaluación y, en caso aprobatorio, le fue tomada la protesta.

JUAN ARMANDO VELAZCO VELAZCO
ALUMNO

REVISÓ

MTRA. ROSALIA SERRANO DE LA PAZ
DIRECTORA DE SISTEMAS ESCOLARES

DIRECTOR DE LA DIVISIÓN DE CBI

Roman Linares Romero
DR. ROMAN LINARES ROMERO

PRESIDENTE

DR. HORACIO TAPIA RECILLAS

VOCAL

DR. MANUEL GONZALEZ SARABIA

VOCAL

DR. JOSE NOE GUTIERREZ HERRERA

VOCAL

DR. ELISEO SARMIENTO ROSALES

SECRETARIO

DR. MARIO PINEDA RUELAS