IMÁGENES DE GRAY DE CÓDIGOS SOBRE ANILLOS DE GALOIS

TESIS QUE PRESENTA

CARLOS ALBERTO LÓPEZ ANDRADE

PARA OBTENER EL GRADO DE
DOCTOR EN CIENCIAS MATEMÁTICAS

ASESOR: DR. HORACIO TAPIA RECILLAS

UNIVERSIDAD AUTÓNOMA METROPOLITANA–IZTAPALAPA

http://www.izt.uam.mx/
Departamento de Matemáticas
Posgrado en Matemáticas
2011

Carlos Alberto López Andrade: *Imágenes de Gray de Códigos sobre Anillos de Galois,* Universidad Autónoma Metropolitana-Iztapalapa, © 2011.

SITIO WEB:
http://www.fcfm.buap.mx/fcfm/clopez

CORREO ELECTRÓNICO:
clopez@fcfm.buap.mx

A GRIS, SOFÍA Y SEBASTIÁN

AGRADECIMIENTOS

A Gris, mi amiga y amante, compañera en este viaje, por su generoso amor e infinita paciencia. Y a Sofía y Sebastián, mis amados hijos, por ser la alegría de mi vida.

A la Benemérita Universidad Autónoma de Puebla, a la Facultad de Ciencias de la Computación de la BUAP, a la Universidad Autónoma Metropolitana-Iztapalapa y al CONACYT, por su apoyo institucional.

A mi asesor, el Dr. Horacio Tapia Recillas, por su paciente colaboración en la dirección de este proyecto.

A mis amigos, por sus palabras de aliento.

INTRODUCCIÓN

El objeto principal de estudio en este trabajo es la imagen bajo el mapeo de Gray de códigos definidos sobre el anillo de Galois $GR(p^2, m)$.

En los años 90 el interés por los códigos lineales sobre los anillos finitos de enteros ([BSC95], [CS95], [PQ96], [CH97], [KLP97]) fué estimulado por los trabajos trascendentales de [Nec91] y [JKC+94]. En éste último trabajo se demuestra que los códigos binarios no-lineales de Kerdock y Preparata se describen como las imágenes bajo el mapeo de Gray de códigos lineales sobre el anillo $\mathbb{Z}_4$, de enteros módulo 4. El mapeo de Gray

$$\begin{aligned} \phi : \mathbb{Z}_4 &\rightarrow F_2 \times F_2 \\ 0 &\rightarrow (0,0) \\ 1 &\rightarrow (0,1) \\ 2 &\rightarrow (1,1) \\ 3 &\rightarrow (1,0) \end{aligned}$$

es una isometría con respecto a la métrica de Lee en $\mathbb{Z}_4$ y la métrica de Hamming en $F_2 \times F_2$, y es una herramienta esencial para la descripción de estos códigos. En [JKC+94] se dan condiciones necesarias y suficientes para que la imagen binaria de un código lineal sobre $\mathbb{Z}_4$ sea un código lineal, en [LB02] los autores obtienen el resultado correspondiente para códigos lineales sobre $\mathbb{Z}_{p^2}$, $p-$primo.

A finales del siglo pasado y principios del nuevo milenio el estudio de los códigos definidos sobre el anillo $\mathbb{Z}_{p^m}$ (donde p es un primo y m un entero positivo), y en general, de los códigos sobre anillos finitos de cadena incluyendo los anillos de Galois, se incrementó ([BU99], [GS99]), [NSM00], [DLP04], [KN01]).

Al mismo tiempo diversos investigadores se avocaron al estudio de la imagen bajo el mapeo de Gray de códigos definidos sobre el anillo $\mathbb{Z}_{p^m}$ ([Car98], [Wol99], [Wol01], [vv01], [TRV01], [LB02], [TRV03]).

J. Wolfmann en [Wol99] demuestra que la imagen de Gray de un código negacíclico lineal sobre $\mathbb{Z}_4$ es un código cíclico binario de distancia invariante (no necesariamente lineal) [Wol99, Teorema 3.5], y también demuestra que la imagen de Gray de un código cíclico lineal sobre $\mathbb{Z}_4$ de longitud impar es equivalente a un código cíclico binario (no necesariamente lineal) [Wol99, Teorema 3.9], para obtener éste último resultado utiliza la permutación de Nechaev.

H. Tapia-Recillas y G. Vega en [TRV01] generalizan el Teorema 3.5 y el Corolario 3.8 de [Wol99] para los códigos correspondientes sobre $\mathbb{Z}_{2^{k+1}}$.

S. Ling y J.T. Blackford prosiguen en esta línea; en [LB02] generalizan varios de los resultados de [Wol99], [Wol01] y [TRV01] para códigos sobre el anillo $\mathbb{Z}_{p^{k+1}}$, de enteros módulo p^{k+1}, donde p es un primo y $k \geqslant 1$ es un entero. En particular, demuestran que un código sobre $\mathbb{Z}_{p^{k+1}}$ es un código $(1-p^k)$-cíclico si y sólo si su imagen de Gray

es un código cuasi-cíclico sobre $\mathbb{Z}_p$ de índice p^{k-1} y de longitud $p^k n$, demuestran que la imagen de Gray de un código cíclico lineal sobre $\mathbb{Z}_{p^{k+1}}$ de longitud n primo relativo con p es equivalente a un código cuasi-cíclico (no necesariamente lineal) sobre $\mathbb{Z}_p$ y también dan condiciones necesarias y suficientes para que la imagen de Gray de un código lineal sobre $\mathbb{Z}_{p^2}$ sea lineal. Si $p = 2$ y $k = 1$ se recuperan [Wol99, Teorema 3.5], [Wol99, Teorema 3.9] y [JKC+94, Teorema 5] respectivamente.

En [Wol01] se determinan todos los códigos cíclicos lineales sobre $\mathbb{Z}_4$ de longitud impar cuya imagen de Gray son códigos lineales (o, equivalentemente, cuya imagen de Nechaev-Gray son códigos cíclicos lineales) o son códigos cíclicos lineales sobre F_2, dando condiciones sobre sus polinomios generadores. Este es un excelente artículo en el que se combinan las condiciones que caracterizan la estructura de los códigos cíclicos lineales sobre $\mathbb{Z}_4$ ([CS95], [PQ96], [KLP97]) con el mapeo de Gray y el mapeo de Nechaev-Gray (el mapeo de Gray seguido de la permutación de Nechaev). En particular, en [Wol01, Teorema 21], se demuestra que si $\mathcal{C}$ es un código cíclico lineal sobre $\mathbb{Z}_4$ de longitud n impar, Φ es el mapeo de Gray y $g(x) = 2d(x)$, donde $d(x)|x^n - 1$ en $\mathbb{Z}_4[x]$, es el polinomio generador de $\mathcal{C}$ entonces $\Phi(C)$ es el código binario cíclico lineal de longitud $2n$ generado por $\mu(d(x))(x^n - 1)$, donde $\mu(d(x))$ es la μ-reducción del polinomio $d(x)$. En [LB02, Teorema 4.13] se generaliza este teorema.

En ésta tesis se generalizan algunos de los resultados de [LB02] como los que se mencionan en los párrafos previos para los códigos correspondientes definidos sobre el anillo de Galois $\mathcal{R} = GR(p^2, m)$. Para tal propósito el artículo [GS99] es de particular importancia ya que en él los autores utilizan la isometría de Gray $\Phi : (\mathcal{R}^n, d_h) \to (F_q^{q^t n}, d_H)$, donde d_h y d_H denotan la distancia homogénea y la distancia de Hamming respectivamente, $q = p^m$ y $t \geqslant 1$, para construir códigos de longitud $q^t n$ sobre el alfabeto F_q, a partir de $\mathcal{R}$-códigos lineales de longitud n, donde $\mathcal{R}$ es un anillo finito de cadena de índice de nilpotencia $t + 1$, y en éste trabajo se usa una variante, salvo permutación, de ésta isometría, para construir códigos de longitud qn sobre el alfabeto F_q a partir de códigos sobre el anillo de Galois $GR(p^2, m)$ de longitud n, donde $GR(p^2, m)$ es un anillo finito de cadena de índice de nilpotencia 2 ($t = 1$).

Una herramienta fundamental para obtener los resultados deseados es el anillo de vectores de Witt de longitud 2, $\mathcal{W}_2(F_{p^m})$, el cuál es isomorfo al anillo de Galois $GR(p^2, m)$. En [AH98] se demuestra que el anillo de Galois $GR(p^n, m)$ es isomorfo al anillo de vectores de Witt de longitud n, $\mathcal{W}_n(F_{p^m})$. A partir de la suma y el producto entre los elementos del anillo de Witt $\mathcal{W}_2(F_{p^m})$, y el isomorfismo entre este anillo y el anillo de Galois $GR(p^2, m)$ se obtienen las componentes p-ádicas de la suma $a + b$ (Proposición 1.2) de $a, b \in GR(p^2, m)$, y en particular, la μ-reducción de las componentes p-ádicas del producto ηa (Lema 1.4) donde $a \in GR(p^2, m)$ es un elemento cualesquiera y $\eta = 1 + pN' \in GR(p^2, m)$ es una unidad principal, siendo N' un elemento del conjunto de Teichmüller del anillo de Galois, el conjunto de representantes del campo residual en $GR(p^2, m)$, tal que su μ-reducción es $n' \in \{1, \ldots, p-1\}$, i.e., $\mu(N') = n' \in \{1, \ldots, p-1\}$, donde $nn' \equiv 1 (\mod p)$.

El presente trabajo ha dado lugar a dos artículos de investigación [LATR08], [LATR11].

La tesis está organizada de la siguiente manera:

En el Capítulo 1 se proporcionan las definiciones y notación básica relacionadas con los campos finitos, anillos finitos de cadena y códigos definidos sobre éstos alfabetos.

También se aporta la Proposición 1.2 y el Lema 1.4 que son esenciales para establecer las Proposiciones 2.2 y 4.1, respectivamente.

En el Capítulo 2 introducimos la definición del mapeo de Gray en $\mathcal{R}^n$, siendo $\mathcal{R} = GR(p^2, m)$ el anillo de Galois, en la forma apropiada para nuestros propósitos y recordamos algunas de sus propiedades, también se establece la Proposición 2.2, ésta proposición nos lleva a obtener un importante teorema, en él se dan condiciones necesarias y suficientes para que la imagen de Gray de un $\mathcal{R}$-código lineal sea un código lineal sobre F_q [Teorema 2.2]. Tal teorema dice:

Teorema. *Sea $\mathcal{C}$ un $\mathcal{R}$-código lineal de longitud n y sea Φ el mapeo de Gray en $\mathcal{R}^n$. Entonces la imagen de Gray $\Phi(\mathcal{C})$ es un F_{p^m}-código lineal si y sólo si $p\Theta(\mathbf{A}, \mathbf{B}) \in \mathcal{C}$ para toda $\mathbf{A}, \mathbf{B} \in \mathcal{C}$.*

El Teorema 2.2 produce el resultado correspondiente que aparece en [JKC+94, Teorema 5] si $\mathcal{R} = \mathbb{Z}_4$ y nos da el mismo resultado que aparece en [LB02, Teorema 4.3] si $\mathcal{R} = \mathbb{Z}_{p^2}$.

En el Capítulo 3 se introducen los conceptos de código cuasi-cíclico de primer bloque de índice p^{m-1} y código $\hat{\gamma}$-cíclico sobre el anillo de Witt, $\mathcal{W}_2(F)$, también se introduce el concepto de código $\tilde{\tau}$-cuasi-cíclico sobre el campo finito F_q. Se estudia el mapeo de Gray definido sobre el anillo de Witt y la imagen de Gray de códigos, sin estructura lineal, definidos sobre este anillo con ciertas características sobre sus componentes. Se dan condiciones necesarias y suficientes para que la imagen de Gray de un código $\hat{\alpha}$-cíclico definido sobre el anillo de Witt sea cuasi-cíclico de primer bloque de índice p^{m-1} [Teorema 3.1] y también se dan condiciones necesarias y suficientes para que la imagen de Gray de un código $\hat{\gamma}$-cíclico de longitud n sobre $\mathcal{W}_2(F)$ sea un código $\tilde{\tau}$-cuasi-cíclico de longitud nq sobre F [Teorema 3.2]. La importancia de éste capítulo estriba en que el estudio del mismo sirvió de terreno de cultivo para la obtención de los resultados que se reportan en los capítulos 2 y 4.

En el Capítulo 4 se establece la Proposición 4.1, ésta proposición nos permite obtener un teorema que nos da condiciones necesarias y suficientes para que la imagen de Gray de un código $(1-p)$-cíclico definido sobre el anillo de Galois $GR(p^2, m)$ sea cuasi-cíclica [Teorema 4.1]. Este teorema dice:

Teorema. *Un $\mathcal{R}$-código $\mathcal{C}$ de longitud n es $\lambda = (1-p)$-cíclico si y sólo si su imagen de Gray $\Phi(\mathcal{C})$ es un código cuasi-cíclico sobre F_{p^m} de índice p^{m-1} y longitud np^m.*

Este resultado generaliza el que aparece en [Wol99] y [LB02].

También se establece la Proposición 4.3 que junto con la Proposición 4.2 y el Teorema 4.1 dan lugar a uno de los teoremas más relevantes de este trabajo, en él se dan condiciones necesarias y suficientes para la cuasi-ciclicidad no necesariamente lineal de la imagen de Gray de códigos cíclicos lineales sobre el anillo de Galois $GR(p^2, m)$ [Teorema 4.2]. Tal teorema dice:

Teorema. *Sea $\mathcal{C} \subseteq \mathcal{R}^n$ un código de longitud n primo relativo con p. Entonces el código $\mathcal{C}$ es cíclico lineal si y sólo si $\Pi^{\otimes p^{m-1}}(\Phi(\mathcal{C}))$ es un código cuasi-cíclico de índice p^{m-1} y longitud np^m sobre F.*

Este resultado generaliza el que aparece en [LB02] para códigos sobre el anillo $\mathbb{Z}_{p^2}$.

En el Capítulo 5 $\mathcal{R}$ denota un anillo finito de cadena de índice de nilpotencia 2 y π es el generador del ideal maximal $\mathcal{M}$ de $\mathcal{R}$. En la Proposición 5.1 se da la representación polinomial de $\Phi(A)$, donde $A \in \mathcal{R}^n$, y usando esta representación junto con el

Teorema 5.3 que caracteriza al polinomio generador de un $\mathcal{R}$-código cíclico lineal de longitud n primo relativo con la característica del campo residual da lugar a un teorema que establece la ciclicidad lineal de la imagen de Gray de una clase de $\mathcal{R}$-códigos cíclicos lineales [Teorema 5.4]. Este teorema dice:

Teorema. *Sea $\mathcal{C}$ un $\mathcal{R}$-código cíclico lineal de longitud n primo relativo con la característica del campo residual, generado por el polinomio $G(\xi) = \pi A(\xi)$ de grado r. Entonces $\Phi_{\mathcal{P}}(G(\xi)) = a(\xi)(\xi^n - 1)^{p^m - 1}$ donde $a(\xi) = \mu(A(\xi))$ y $\Phi_{\mathcal{P}}(G(\xi))$ divide a $\xi^{np^m} - 1$. Más aún, la imagen de Gray de $\mathcal{C}$, $\Phi(\mathcal{C})$, es un $[qn, n - r]$ código cíclico lineal sobre F_q.*

Este teorema generaliza parcialmente al que aparece en [LB02].

Cabe señalar que se esta preparando un artículo con los resultados de éste capítulo que será sometido a una revista para su publicación.

ÍNDICE GENERAL

1 PRELIMINARES

En éste capítulo, revisamos los fundamentos matemáticos necesarios que nos facilitarán una mejor comprensión de la tesis.

Tales fundamentos se dividen en tres temas: campos finitos, anillos finitos de cadena y códigos definidos sobre campos finitos y anillos finitos de cadena.

En la primera parte recordamos algunos conceptos básicos de los campos finitos F_{p^m}, en la segunda parte revisamos los anillos finitos de cadena (anillos de Galois y anillos de Witt): proporcionamos definiciones y propiedades acerca de los alfabetos sobre los cuales se definen nuestros códigos. En particular, se aportarán resultados relacionados con el anillo de Witt (anillo de Galois) que serán esenciales en la sección 2.1 y en los capítulos posteriores. En la parte final del capítulo recordamos algunos conceptos básicos de los códigos definidos sobre éstos alfabetos.

1.1 CAMPOS FINITOS

Los orígenes de los campos finitos se remontan a los siglos XVII y XVIII con los trabajos de Fermat (1601-1665), Euler (1707-1783), Lagrange (1736-1813) y Legendre (1752-1833), todos ellos trabajaron con campos finitos especiales, i.e., los llamados campos finitos primos, $\mathbb{Z}_p$, donde p es un primo. Se puede decir que la teoría general de los campos finitos comenzó con los trabajos de Carl Friedrich Gauss (1777-1855) y Evariste Galois (1811-1832). A finales del siglo XIX toda la estructura de los campos finitos era conocida. Pero en las últimas décadas adquirieron relevancia con el desarrollo de la computación, de la teoría de la información y de la seguridad informática.

A continuación se recordaran algunos conceptos fundamentales acerca de los campos finitos. Para los detalles se pueden consultar las siguientes referencias [LN97],[Wan03] y [MS77].

- $\mathbb{Z}_p = \mathbb{Z}/\langle p\rangle$, donde p es un primo, es un campo primo, el cual es denotado por F_p.
- Si $f(x) \in F_p[x]$ es un polinomio irreducible de grado m entonces $F_p[x]/\langle f(x)\rangle$ es un campo finito con p^m elementos, denotado por F_{p^m} ó $GF(p^m)$.
- En cualquier campo finito, el número de elementos es una potencia de un primo p y tal primo es la característica del campo.
- Si p es un primo y m es un entero positivo entonces existe un campo finito de orden p^m que es único salvo isomorfismo.
- Sean $q = p^m$, F_q un campo finito y a, b dos elementos cualesquiera de F_q entonces $(a+b)^p = a^p + b^p$. Más aún, $(a+b)^{p^m} = a^{p^m} + b^{p^m}$.

- El grupo multiplicativo de los elementos distintos de cero de F_q, denotado por F_q^*, es cíclico. Cualquier elemento generador de F_q^* es llamado un elemento primitivo.
- Todo subcampo de F_q tiene orden p^d, donde d es un divisor positivo de m. Recíprocamente, si $d|m$ entonces existe exactamente un subcampo de F_q de orden p^d.
- Un campo finito F_q es isomorfo al campo de descomposición de $x^q - x$ sobre F_p, donde $q = p^m$.
- Todo elemento $a \in F_q$ satisface $a^q = a$.
- F_{q^n} es un espacio vectorial de dimensión n sobre F_q.
- Una base de F_{q^n} sobre F_q tiene cardinalidad n y n es llamado el grado de F_{q^n} sobre F_q, lo cual es denotado por $[F_{q^n} : F_q] = n$.
- Sea $f(x)$ un polinomio mónico de grado n sobre F_q. Si $f(x)$ tiene un elemento primitivo de F_{q^n} como una de sus raíces, entonces $f(x)$ es llamado un polinomio primitivo de grado n sobre F_q.
- Si F_{p^m} se construye a partir de un polinomio primitivo irreducible $f(x)$ de grado m y ω es una raíz de $f(x)$ entonces $\{1, \omega, \omega^2, \ldots, \omega^{m-1}\}$ es una base de F_{p^m} sobre F_p.

1.2 ANILLOS FINITOS DE CADENA

Sea $\mathcal{R}$ un anillo conmutativo finito con identidad. Un ideal I de un anillo $\mathcal{R}$ es llamado *principal* si es generado por un solo elemento. Un anillo $\mathcal{R}$ es un anillo de ideales principales si todos sus ideales son principales. $\mathcal{R}$ es llamado local si $\mathcal{R}/\mathrm{rad}\,\mathcal{R}$ es un campo finito (o equivalentemente si $\mathcal{R}$ tiene un único ideal maximal). Un anillo $\mathcal{R}$ es de cadena si el conjunto de todos sus ideales es una cadena bajo la inclusión de conjuntos.

Para la clase de los anillos conmutativos finitos de cadena, se tienen las siguientes condiciones equivalentes (ver [DLP04]).

Proposición 1.1. *Para un anillo conmutativo finito $\mathcal{R}$ las siguientes condiciones son equivalentes:*

i) *$\mathcal{R}$ es un anillo local y el ideal maximal $\mathcal{M}$ de $\mathcal{R}$ es principal,*

ii) *$\mathcal{R}$ es un anillo local de ideales principales,*

iii) *$\mathcal{R}$ es un anillo de cadena.*

Sea $\mathcal{R}$ un anillo finito de cadena (AFC), π un generador fijo del ideal maximal $\mathcal{M}$ de $\mathcal{R}$ y sea t el índice de nilpotencia de π. Todos los ideales de $\mathcal{R}$ son principales de la forma (π^i) para $0 \leqslant i \leqslant t$. Los ideales de $\mathcal{R}$ forman la cadena

$$\mathcal{R} = \langle \pi^0 \rangle \supsetneq \langle \pi^1 \rangle \supsetneq \ldots \supsetneq \langle \pi^{t-1} \rangle \supsetneq \langle \pi^t \rangle = \langle 0 \rangle.$$

Sea $F = \mathcal{R}/\mathcal{M}$ el campo residual de $\mathcal{R}$, F es un campo finito isomorfo a F_{p^m} para algún primo p y $m \in \mathbb{N}$ y sea $\mu : \mathcal{R} \to F$, dado por $\mu(r) = r + \mathcal{M}$, el homomorfismo canónico de $\mathcal{R}$ sobre su campo residual. Este mapeo es extendido de la siguiente forma: $\mu : \mathcal{R}[x] \to F[x]$, mapea $r \to r + \mathcal{M}$ y a la variable x a x, para abreviar, llamamos a este mapeo μ-reducción.

Los siguientes resultados se encuentran en [NSM00].

Lema 1.1. *Para cualquier $r \in \mathcal{R} \setminus \{0\}$ hay un único entero i, $0 \leqslant i < t$ tal que $r = u\pi^i$, con u una unidad. La unidad u es única módulo π^{t-i}.*

Corolario 1.1. *Si $1 \leqslant i < j \leqslant t$ y $\pi^i c \in \pi^j\mathcal{R}$ entonces $c \in \pi^{j-i}\mathcal{R}$. En particular, si $\pi^i\mathcal{R} = 0$ entonces $c \in \pi^{t-i}\mathcal{R}$.*

Lema 1.2. *Sea $V \subseteq \mathcal{R}$ un conjunto de representantes para las clases de equivalencia de $\mathcal{R}$ bajo congruencia módulo $\mathcal{M}$. (Equivalentemente, se puede definir a V como el subconjunto maximal de $\mathcal{R}$ con la propiedad de que $\mu(r_1) \neq \mu(r_2)$ para todo $r_1, r_2 \in \mathcal{R}$, $r_1 \neq r_2$). Entonces:*

i) Para todo $r \in \mathcal{R}$ existen $r_0, \ldots, r_{t-1} \in V$ únicos tales que $r = \sum_{i=0}^{t-1} r_i\pi^i$;

ii) $|V| = |F|$;

iii) $|\pi^j\mathcal{R}| = |F|^{t-j}$ para $0 \leqslant j \leqslant t-1$.

En [dH01] se afirma que: todos los anillos conmutativos finitos de cadena pueden obtenerse a través de la siguiente construcción y también se refiere al lector a [McD74, págs. 307-308, 339-344] para las demostraciones de las afirmaciones en la construcción. Sea p un primo, $n, m > 0$ y $f \in \mathbb{Z}_{p^n}[x]$ un polinomio mónico de grado m cuya imagen en $\mathbb{Z}_p[x]$ es irreducible. Entonces $GR(p^n, m) = \mathbb{Z}_{p^n}[x]/(f)$ es un anillo cuya estructura depende sólo de p, n y m. $GR(p^n, m)$ es llamado un anillo de Galois de caracteristica p^n y rango m [Jan66, Rag69]. $GR(p^n, m)$ es un anillo local cuyo ideal maximal es $pGR(p^n, m)$. Todo anillo finito de cadena $\mathcal{R}$ es de la forma:

$$GR(p^n, m)[x]/(g, p^{n-1}x^l), \tag{1.1}$$

donde $g \in GR(p^n, m)[x]$ es un polinomio de Eisenstein de grado k, i.e., $g = x^k - p(a_{k-1}x^{k-1} + \cdots + a_0)$, $a_i \in GR(p^n, m)$ y a_0 es una unidad de $GR(p^n, m)$, $l = k$ cuando $n = 1$ y $1 \leqslant l \leqslant k$ cuando $n \geqslant 2$. Los enteros p, n, m, k, l son llamados los invariantes del anillo de cadena en (1.1) (cf. [CL73]).

Si $n = 1$, entonces los anillos de Galois en (1.1) son de la forma $GF(p^m)$ y $\mathcal{R} = GF(p^m)[x]/\langle x^k \rangle$.

A continuación enunciamos un par de ejemplos de anillos conmutativos finitos de cadena:

i) Anillos de Galois $GR(p^n, m)$ para algún primo p y enteros $n, m \geqslant 1$, si $m = 1$, $GR(p^n, 1) = \mathbb{Z}_{p^n}$ es el anillo de enteros módulo p^n y si $n = 1$, $GR(p, m) = F_{p^m}$ es el campo finito con p^m elementos.

ii) Anillo de clases residuales $GF(p)[\xi]/(w(\xi)^k)$ donde $w(\xi)$ es un polinomio irreducible sobre $GF(p)$ de grado m, con m y k enteros positivos (ver [US98]).

El grupo de unidades de un anillo conmutativo finito local es un objeto esencial en la estructura del anillo. En general, la estructura de tal grupo de unidades es difícil de determinar. Para anillos de Galois sus grupos de unidades son conocidos [McD74, págs. 322-323]. Para anillos de clases residuales se puede consultar [Cla77] y para los anillos finitos de cadena referimos al lector a [dH01].

Por la importancia en ésta tesis de los anillos de Galois y del anillo (truncado) de vectores de Witt, $\mathcal{W}_2(F)$, puntualizamos algunos aspectos de éstos en las subsecciones siguientes.

1.2.1 Anillos de Galois

La definición y propiedades básicas del anillo de Galois son recordadas en ésta subsección. Para más detalles referimos al lector a [McD74, XVI] y [Wan03, 14], (ver también [JKC+94],[BF02]).

Sea $\mathbb{Z}_{p^n}$ el anillo de enteros módulo p^n, donde p es un primo y n un entero positivo. Un polinomio irreducible $f(x) \in \mathbb{Z}_{p^n}[x]$ se dice *básico* si su reducción módulo p es irreducible.

El anillo de Galois $GR(p^n, m)$ está definido como:

$$GR(p^n, m) = \mathbb{Z}_{p^n}[x]/\langle f(x)\rangle$$

donde $f(x) \in \mathbb{Z}_{p^n}[x]$ es un polinomio monico, básico primitivo irreducible de grado m que divide a $x^{p^m-1} - 1$ y $\langle f(x)\rangle$ es el ideal de $\mathbb{Z}_{p^n}[x]$ generado por $f(x)$.

En la definición anterior se puede prescindir de la propiedad de que $f(x)$ sea primitivo irreducible y sólo pedir que sea básico irreducible (ver [McD74]), sin embargo, es muy útil, además considerar a $f(x)$ primitivo irreducible (ver [JKC+94], [Wan03]).

El anillo $\mathcal{R} = GR(p^n, m)$ es local con ideal maximal $\mathcal{M} = \langle p\rangle$ generado por p y campo residual $F = \mathcal{R}/\mathcal{M}$ isomorfo a F_{p^m}, el campo de Galois con p^m elementos. La cardinalidad de $\mathcal{R}$ es $|\mathcal{R}| = p^{nm}$, la característica de $\mathcal{R}$ es p^n y los elementos del ideal maximal $\mathcal{M}$ son los divisores de cero de $\mathcal{R}$. Cualquier ideal del anillo de Galois es de la forma $\langle p^i\rangle$ para $1 \leqslant i \leqslant n$ y hay una cadena de ideales:

$$\mathcal{R} = \langle 1\rangle \supset \langle p\rangle \supset \cdots \supset \langle p^n\rangle = \{0\}.$$

Sea $\mu : \mathcal{R} \longrightarrow F$, $\mu(\theta) = \overline{\theta}$ el mapeo canónico del anillo de Galois sobre su campo residual. Sea $\mathcal{T} \subset \mathcal{R}$, el conjunto de Teichmüller del anillo de Galois. Entonces cualquier $\beta \in \mathcal{R}$ tiene una única representación p-ádica (multiplicativa):

$$\beta = r_0(\beta) + r_1(\beta)p + \cdots + r_{n-1}(\beta)p^{n-1}$$

donde $r_i(\beta) \in \mathcal{T}$.

Si $\mathcal{R}^*$ denota el grupo de unidades de $\mathcal{R}$ entonces $\mathcal{R} = \mathcal{M} \cup \mathcal{R}^*$ y $\mathcal{R}^* = \mathcal{C} \times \mathcal{G}$ donde $\mathcal{C}$ es un grupo cíclico de orden $p^m - 1$ y $\mathcal{G}$ es un grupo de orden $p^{(n-1)m}$ (ver [McD74, Teorema XVI.9, pág. 322], [Wan03, Teorema 14.11, pág. 319]). Si $\omega \in \mathcal{R}$ es una raíz de $f(x)$ entonces el subgrupo $\mathcal{C}$ es generado por ω, su imagen $\bar{\omega} = \mu(\omega) \in F_{p^m}$ es una raíz del polinomio irreducible $\overline{f(x)} = \mu(f(x))$ y $F^*_{p^m} = F_{p^m} \setminus \{0\} = \langle\bar{\omega}\rangle$. Si $q = p^m$, el conjunto de Teichmüller puede tomarse como $\mathcal{T} = \{0, 1, \omega, \omega^2, ..., \omega^{q-2}\}$.

El anillo de Galois $\mathcal{R}$ tiene la estructura de un $(\mathbb{Z}_{p^n})$-módulo ([Wano3, págs. 311-313]):

$$\begin{aligned}\mathcal{R} &= \mathbb{Z}_{p^n}[\omega] \\ &= (\mathbb{Z}_{p^n}) + (\mathbb{Z}_{p^n})\,\omega + \cdots + (\mathbb{Z}_{p^n})\,\omega^{m-1}.\end{aligned}$$

Los elementos de $\mathcal{R} = \mathbb{Z}_{p^n}[\omega]$ se expresan unívocamente en la forma

$$a_0 + a_1\omega + \ldots + a_{m-1}\omega^{m-1},\ a_i \in \mathbb{Z}_{p^n}, (0 \leqslant i \leqslant m-1).$$

Tal expresión es llamada la representación aditiva de los elementos del anillo de Galois $\mathcal{R} = \mathbb{Z}_{p^n}[\omega]$.

Ejemplo 1.1. *Algunos anillos de Galois son:*

i) $GR(p, m) = GF(p, m) = F_{p^m}$, $GR(p^n, 1) = \mathbb{Z}_{p^n}$.

ii) *Sea* $f(x) = x^3 + x + 1 \in \mathbb{Z}_4[x]$ *un polinomio mónico básico irreducible sobre* $\mathbb{Z}_4$. *Entonces* $GR(2^2, 3) = \mathbb{Z}_4[x]/\langle f(x)\rangle$, *([McD74], pág.297).*

iii) *Sea* $g(x) = x^3 + 2x^2 + x - 1 \in \mathbb{Z}_4[x]$ *un polinomio mónico básico primitivo irreducible sobre* $\mathbb{Z}_4$. *Entonces* $GR(2^2, 3) = \mathbb{Z}_4[x]/\langle g(x)\rangle$, *([JKC+94], Sección III).*

iv) *Sea* $h(x) = x^2 + 4x + 8 \in \mathbb{Z}_9[x]$ *un polinomio mónico básico primitivo irreducible sobre* $\mathbb{Z}_9$. *Entonces* $GR(3^2, 2) = \mathbb{Z}_9[x]/\langle h(x)\rangle$, *([Wano3]).*

1.2.2 El Anillo de Witt $\mathcal{W}_2(F)$

Sea $\mathcal{R} = GR(p^2, m)$, el anillo de Galois de característica p^2. En ésta subsección la definición del anillo (truncado) de vectores de Witt, $\mathcal{W}_2(F)$, sobre el campo finito $F = F_{p^m}$ es enunciada y un isomorfismo entre el anillo de Galois $\mathcal{R}$ y $\mathcal{W}_2(F)$ es dado. La definición del anillo de vectores de Witt es más general (ver [Jac80, Ser62]) pero para los propósitos del presente trabajo sólo se considera $\mathcal{W}_2(F)$. La definición del anillo de Witt es independiente del anillo de Galois. Se dan algunas propiedades de este anillo o equivalentemente del anillo de Galois $\mathcal{R}$ que serán útiles en los capítulos posteriores para presentar los resultados sobre las imágenes de Gray de códigos definidos sobre el anillo $\mathcal{R}$.

Sea $(F, +, *) = (F_{p^m}, +, *)$ un campo finito con p^m elementos. El conjunto subyacente del anillo de Witt $\mathcal{W}_2(F)$ es justamente el producto cartesiano $F \times F$ y las operaciones "$+_w$", "$*_w$"son definidas de la siguiente manera:

$$(x_0, x_1) +_w (y_0, y_1) = (S_0(x_0, x_1, y_0, y_1), S_1(x_0, x_1, y_0, x_1))$$

donde

$$\begin{aligned}S_0(x_0, x_1, y_0, y_1) &= x_0 + y_0 \\ S_1(x_0, x_1, y_0, y_1) &= (x_1 + y_1) - h(x_0, y_0)\end{aligned}$$

con $h(x, y) = \frac{1}{p}((x + y)^p - x^p - y^p) \in \mathbb{Q}[x, y]$ y

$$(x_0, x_1) *_w (y_0, y_1) = (x_0 y_0, x_0^p y_1 + y_0^p x_1)$$

(para elementos $a, b \in F$ escribimos $a * b = ab$).

Si $F = \mathcal{R}/\mathcal{M}$ es el campo residual del anillo de Galois $\mathcal{R}$ es fácil ver que el mapeo

$$\psi : \mathcal{R} \longrightarrow \mathcal{W}_2(F),\ \hat{a} = \psi(a) = (a_0, a_1^p) \tag{1.2}$$

donde $a = \rho_0(a) + p\rho_1(a) \in \mathcal{R}$, $\rho_0(a), \rho_1(a) \in \mathcal{T}$ y $a_i := \overline{\rho_i(a)} = \mu(\rho_i(a))$, $i = 0, 1$, es un isomorfismo de anillos.

El mapeo inverso es:

$$\psi^{-1} : \mathcal{W}_2(F) \longrightarrow \mathcal{R},\ \psi^{-1}(b_0, b_1) = B_0 + pB_1^{1/p} \tag{1.3}$$

donde $B_0, B_1 \in \mathcal{T}$ son tales que $\overline{B}_i = b_i$ (la barra significa la imagen bajo el mapeo canónico μ). Si $\hat{a}, \hat{b}$ son elementos cualesquiera del anillo de Witt $\mathcal{W}_2(F)$ y si no se presenta confusión, los elementos $\hat{a} +_w \hat{b}$ y $\hat{a} *_w \hat{b}$ se denotarán por $\hat{a} + \hat{b}$ y $\hat{a}\hat{b}$ respectivamente.

En [AH98, Teorema 4 pág. 231-232] se demuestra que el anillo (truncado) de vectores de Witt $\mathcal{W}_n(F_{p^m})$ y el anillo de Galois $GR(p^n, m)$ son isomorfos.

El siguiente resultado será útil más adelante.

Proposición 1.2. *Sean* $a = \rho_0(a) + p\rho_1(a), b = \rho_0(b) + p\rho_1(b) \in \mathcal{R}$ *con* $\rho_i(a), \rho_i(b) \in \mathcal{T}$ *y* $\mu(\rho_i(a)) = r_i(a)$, $\mu(\rho_i(b)) = r_i(b)$ *para* $i = 0, 1$. *Sea* $a + b = \rho_0(a + b) + p\rho_1(a + b)$ *con* $\rho_i(a + b) \in \mathcal{T}$ *y* $\mu(\rho_i(a + b)) = r_i(a + b)$ *para* $i = 0, 1$. *Entonces*

$$\begin{aligned} r_0(a + b) &= r_0(a) + r_0(b) \\ r_1(a + b) &= [r_1(a)^p + r_1(b)^p - h(r_0(a), r_0(b))]^{1/p}. \end{aligned}$$

Demostración. Por el isomorfismo ψ entre el anillo de Galois $\mathcal{R} = GR(p^2, m)$ y el anillo de Witt $\mathcal{W}(F_{p^m})$ tenemos que

$$\begin{aligned} \psi(a) &= \hat{a} = (r_0(a), r_1(a)^p) \\ \psi(b) &= \hat{b} = (r_0(b), r_1(b)^p) \\ \psi(a + b) &= \widehat{a + b} = (r_0(a + b), r_1(a + b)^p). \end{aligned}$$

Como $\psi(a + b) = \psi(a) +_w \psi(b)$ y dado que

$$\begin{aligned} \psi(a) +_w \psi(b) &= (r_0(a), r_1(a)^p) +_w (r_0(b), r_1(b)^p) \\ &= (r_0(a) + r_0(b), r_1(a)^p + r_1(b)^p - h(r_0(a), r_0(b)) \end{aligned}$$

tenemos

$$\begin{aligned} r_0(a + b) &= r_0(a) + r_0(b), \\ r_1(a + b)^p &= r_1(a)^p + r_1(b)^p - h(r_0(a), r_0(b)). \end{aligned}$$

Por lo tanto, $r_0(a + b) = r_0(a) + r_0(b)$ y $r_1(a + b) = [r_1(a)^p + r_1(b)^p - h(r_0(a), r_0(b))]^{1/p}$. □

Sea $\mathcal{R} = GR(p^2, m)$ el anillo de Galois isomorfo a $\mathcal{W}_2(F)$, $\mathcal{T} = \langle\omega\rangle \cup \{0\} \subseteq \mathcal{R}$ el conjunto de Teichmüller, $\langle\overline{\omega}\rangle = F^* = F^*_{p^m}$ y sea $\widehat{\mathcal{T}} \subseteq \mathcal{W}_2(F)$ i.e., $\widehat{\mathcal{T}} = \psi(\mathcal{T}) = \{(0,0),(1,0),(\overline{\omega},0),(\overline{\omega}^2,0),\dots(\overline{\omega}^{p^m-2},0)\}$.

Sea η una unidad (principal) en $\mathcal{R}$ de manera que $\eta = 1 + pN'$ es la expansión p-ádica de η donde $N' \in \mathcal{T}$ es tal que $\mu(N') = n' \in \{1,\dots,p-1\}$.

Los dos lemas siguientes nos serán muy útiles para la demostración de resultados posteriores.

Lema 1.3. *Para cualesquiera* $\widehat{C}_1 = (\overline{\omega}^i, 0),\ \widehat{C}_2 = (\overline{\omega}^j, 0) \in \widehat{\mathcal{T}}$ *se tiene que*

$$\widehat{C}_1 + \widehat{C}_2 = \widehat{a} + \widehat{p}\,\widehat{b}$$

donde $\widehat{a}, \widehat{b} \in \widehat{\mathcal{T}}$ *son tales que* $\widehat{a} = (\overline{\omega}^i + \overline{\omega}^j, 0)$ *y* $\widehat{b} = (-h(\overline{\omega}^i, \overline{\omega}^j)^{1/p}, 0)$.

Demostración. Como

$$\begin{aligned}\widehat{C}_1 + \widehat{C}_2 &= (\overline{\omega}^i, 0) + (\overline{\omega}^j, 0)\\ &= (\overline{\omega}^i + \overline{\omega}^j, -h(\overline{\omega}^i, \overline{\omega}^j))\\ &= (\overline{\omega}^i + \overline{\omega}^j, 0) + (0,1)(-h(\overline{\omega}^i, \overline{\omega}^j)^{1/p}, 0)\end{aligned}$$

Entonces $\widehat{C}_1 + \widehat{C}_2 = (\overline{\omega}^i + \overline{\omega}^j, 0) + \widehat{p}(-h(\overline{\omega}^i, \overline{\omega}^j)^{1/p}, 0) = \widehat{a} + \widehat{p}\,\widehat{b}$ □

Observación 1.1. *Nótese que* $(-h(\overline{\omega}^i, \overline{\omega}^j)^{1/p})^p = -h(\overline{\omega}^i, \overline{\omega}^j)$ *en* F_{p^m} *para todo primo* p.

Lema 1.4. *Sea* $\eta = 1 + pN'$ *y sea* a *un elemento arbitrario de* $\mathcal{R}$ *cuya expansion* p*-ádica es* $a = \rho_0(a) + p\rho_1(a),\ \rho_0(a), \rho_1(a) \in \mathcal{T}$. *Entonces*

$$\eta a = \rho_0(\eta a) + p\rho_1(\eta a)$$

donde $\rho_0(\eta a), \rho_1(\eta a) \in \mathcal{T}$ *son tales que* $\rho_0(\eta a) = \rho_0(a)$. *Además* $r_0(\eta a) = \mu(\rho_0(\eta a)) = r_0(a)$ *y* $r_1(\eta a) = \mu(\rho_1(\eta a)) = r_1(a) + r_0(a)n'$.

Demostración. Si $\rho_0(a) = 0$ ó $\rho_1(a) = 0$ la afirmación del lema inmediatamente se sigue. Si $\rho_0(a) \neq 0 \neq \rho_1(a)$ y dado que $\rho_0(a) := a_0, \rho_1(a) := a_1, N' \in \mathcal{T}$ entonces $a_0 = \omega^j, a_1 = \omega^i, N' = \omega^k$ para algunos $i,j,k \in \{0,\dots,p^m-1\}$. Además, se tiene que, $\eta a = (1+pN')(a_0 + pa_1) = a_0 + p(a_1 + a_0N') = \rho_0(\eta a) + p\rho_1(\eta a)$, para algunos $\rho_1(\eta a) \in \mathcal{T}$ y $\rho_0(\eta a) = a_0 \in \mathcal{T}$, observese que $a_1 + a_0N'$ no necesariamente pertenece a $\mathcal{T}$, pero $p(a_1 + a_0N')$ visto en el anillo de Witt es $\widehat{p}(\widehat{a}_1 + \widehat{a}_0\widehat{N}')$, por el isomorfismo entre el anillo de Galois y el anillo de Witt, con $\widehat{a}_1, \widehat{a}_0, \widehat{N}' \in \widehat{\mathcal{T}}$ entonces $\widehat{a}_1 + \widehat{a}_0\widehat{N}' = (\overline{\omega}^i, 0) + (\overline{\omega}^j, 0)(\overline{\omega}^k, 0) = (\overline{\omega}^i, 0) + (\overline{\omega}^j\overline{\omega}^k, 0) = (\overline{\omega}^i + \overline{\omega}^j\overline{\omega}^k, 0) + \widehat{p}(-h(\overline{\omega}^i, \overline{\omega}^j\overline{\omega}^k)^{1/p}, 0)$, la última igualdad se sigue por el Lema 1.3, por consiguiente,

$$\begin{aligned}\widehat{p}(\widehat{a}_1 + \widehat{a}_0\widehat{N}') &= \widehat{p}\left[(\overline{\omega}^i + \overline{\omega}^j\overline{\omega}^k, 0) + \widehat{p}(-h(\overline{\omega}^i, \overline{\omega}^j\overline{\omega}^k)^{1/p}, 0)\right]\\ &= \widehat{p}(\overline{\omega}^i + \overline{\omega}^j\overline{\omega}^k, 0),\end{aligned}$$

i.e., $\widehat{p}(\widehat{a}_1 + \widehat{a}_0\widehat{N}') = \widehat{p}(\overline{\omega}^i + \overline{\omega}^j\overline{\omega}^k, 0)$ donde $(\overline{\omega}^i + \overline{\omega}^j\overline{\omega}^k, 0) \in \widehat{\mathcal{T}}$, de manera que, $(\overline{\omega}^i + \overline{\omega}^j\overline{\omega}^k, 0)$ corresponde a $\rho_1(\eta a) \in \mathcal{T}$ de tal forma que $r_1(\eta a) = \mu(\rho_1(\eta a)) = \overline{\omega}^i + \overline{\omega}^j\overline{\omega}^k = \mu(a_1) + \mu(a_0)\mu(N') = r_1(a) + r_0(a)n'$. □

1.3 CÓDIGOS DEFINIDOS SOBRE EL ALFABETO $\mathcal{A}$

Sea $\mathcal{A}$ un alfabeto finito y sea $\mathcal{A}^n$ el conjunto de n-adas de elementos de $\mathcal{A}$. Se dice que $\mathcal{C}$ es un *$\mathcal{A}$-código* de longitud n o que $\mathcal{C}$ es un código de longitud n sobre $\mathcal{A}$, si $\mathcal{C}$ es un subconjunto de $\mathcal{A}^n$. Un (n, M)- código $\mathcal{C}$ sobre $\mathcal{A}$ es un $\mathcal{A}$-código de longitud n y tamaño M. A los elementos de un $\mathcal{A}$-código $\mathcal{C}$ se les llama *palabras-código*.

Sea σ el corrimiento cíclico

$$\begin{aligned} \sigma : \mathcal{A}^n &\longrightarrow \mathcal{A}^n \\ (a_0, a_1, \ldots, a_{n-1}) &\longrightarrow (a_{n-1}, a_0, \ldots, a_{n-2}). \end{aligned} \tag{1.4}$$

El código $\mathcal{C} \subseteq \mathcal{A}^n$ es llamado un *$\mathcal{A}$-código cíclico* si $\sigma(\mathcal{C}) = \mathcal{C}$.

Si el alfabeto $\mathcal{A}$ es un campo finito F_{p^m}, $F_{p^m}^n$ es un espacio vectorial n-dimensional sobre F_{p^m}. Un subconjunto $\mathcal{C} \subseteq F_{p^m}^n$ es llamado un F_{p^m}-código lineal de longitud n si $\mathcal{C}$ es un subespacio vectorial de $F_{p^m}^n$. Un subconjunto $\mathcal{C} \subseteq F_{p^m}^n$ es llamado un $[n, k]$-código lineal de longitud n sobre F_{p^m} si $\mathcal{C}$ es un subespacio k-dimensional de $F_{p^m}^n$.

El peso de Hamming de un vector u, denotado por $wt_H(u)$, es el número de componentes distintas de cero, de ahí que, la distancia de Hamming entre dos vectores $u, v \in F_{p^m}^n$ está dada por $d_H(u, v) = wt(u - v)$.

Se dice que $\mathcal{C}$ es un F_{p^m}-código cíclico lineal si $\mathcal{C}$ es un F_{p^m}-código lineal y $\sigma(\mathcal{C}) = \mathcal{C}$.

Sea $\mathcal{A}_n = F_{p^m}[x]/\langle x^n - 1\rangle$ y

$$\begin{aligned} P : F_{p^m}^n &\longrightarrow \mathcal{A}_n, \\ (a_0, a_1, ..., a_{n-1}) &\longrightarrow a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle \end{aligned} \tag{1.5}$$

el mapeo representación polinomial de $F_{p^m}^n$ en el anillo $\mathcal{A}_n$.

Por medio de la representación polinomial las palabras-código pueden ser pensadas como polinomios.

$\mathcal{C}$ es un F_{p^m}-código cíclico lineal si y sólo si $P(\mathcal{C})$ es un ideal de $\mathcal{A}_n$ (cf. [MS77, Sec. 7.2]). $\mathcal{A}_n$ es un dominio de ideales principales, esto implica que, todo F_{p^m}-código cíclico lineal C tiene un único polinomio generador $g(x)$ (en el sentido de que $g(x)$ es un polinomio mónico de grado más pequeño en $P(\mathcal{C})$). Más aún, el polinomio generador $g(x)$ divide a $x^n - 1$ y el código cíclico lineal C tiene dimensión $k = n - grad(g(x))$. Además si $g(x) = g_0 + g_1 x + \cdots + g_r x^r$ entonces $g_0 \neq 0$ y $\mathcal{C}$ es generado (como un subespacio de $F_{p^m}^n$) por las filas de la matriz generadora [1]

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

(cf. [MS77, Sec 7.3]).

Si el alfabeto $\mathcal{A}$ es un anillo finito de cadena $\mathcal{R}$ y si se considera a $\mathcal{R}^n$ como un módulo sobre $\mathcal{R}$ en la forma usual, entonces un subconjunto $\mathcal{C} \subseteq \mathcal{R}^n$ es llamado un *$\mathcal{R}$-código lineal* de longitud n sobre $\mathcal{R}$ si $\mathcal{C}$ es un $\mathcal{R}$-submódulo de $\mathcal{R}^n$.

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

Se dice que $\mathcal{C}$ es un $\mathcal{R}$-código cíclico lineal si $\mathcal{C}$ es un $\mathcal{R}$-código lineal y $\sigma(\mathcal{C}) = \mathcal{C}$.

Con la notación anterior, reemplazando a F_{p^m} por $\mathcal{R}$, $\mathcal{C} \subseteq \mathcal{R}^n$ es un código cíclico lineal si y sólo si $P(\mathcal{C})$ es un ideal de $\mathcal{A}_n = \mathcal{R}[x]/\langle x^n - 1\rangle$

Ésta afirmación es la análoga del resultado conocido para los códigos cíclicos lineales sobre campos finitos mencionado previamente, la demostración es básicamente la misma que para el caso de campos.

En [DLP04] se caracteriza la estructura de los códigos cíclicos lineales de longitud n sobre un anillo finito de cadena $\mathcal{R}$ de índice de nilpotencia $t \geqslant 2$ siempre que n no sea divisible por la característica del campo residual F. En la sección 5.2 se mencionan un par de resultados en esa dirección.

Sea $\mathcal{R} = GR(p^2, m)$ el anillo de Galois, $\mathcal{M}$ su ideal maximal, $F = F_q$, $(q = p^m)$ el campo residual de $\mathcal{R}$ y $\mathcal{T}$ el conjunto Teichmüller de $\mathcal{R}$. Sea $\lambda = 1 - p = 1 + Tp$ una unidad (principal) del anillo de Galois $\mathcal{R} = GR(p^2, m)$ donde $T \in \mathcal{T}$ es tal que $\mu(T) = -1$.

Considérense los siguientes mapeos:

i) Sea $\lambda = 1 - p$. Entonces,

$$\begin{aligned} \nu_\lambda : \mathcal{R}^n &\longrightarrow \mathcal{R}^n, \\ (a_0, a_1, \ldots, a_{n-1}) &\longrightarrow (\lambda a_{n-1}, a_0, \ldots, a_{n-2}). \end{aligned}$$

ii) Para cualesquiera enteros positivos s y t sea

$$\begin{aligned} \sigma^{\otimes t} : F^{st} &\longrightarrow F^{st}, \\ (\mathbf{a}^{(1)}|\mathbf{a}^{(2)}|\cdots|\mathbf{a}^{(t)}) &\longrightarrow (\sigma(\mathbf{a}^{(1)})|\sigma(\mathbf{a}^{(2)})|\cdots|\sigma(\mathbf{a}^{(t)})) \end{aligned}$$

donde $\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(t)} \in F^s$ y $\sigma : F^s \longrightarrow F^s$ es el corrimiento cíclico usual. En particular, $\sigma^{\otimes 1} = \sigma$.

Un código $\mathcal{C} \subseteq \mathcal{R}^n$ es llamado λ-cíclico si $\nu_\lambda(\mathcal{C}) = \mathcal{C}$, mientras que un código $C \subseteq F^{st}$ que satisface $\sigma^{\otimes t}(C) = C$ es llamado cuasi-cíclico de índice t y longitud st.

A partir de este momento $\mathcal{R}$ es el anillo de Galois $GR(p^2, m)$ salvo que se diga otra cosa.

2 IMÁGENES DE GRAY LINEALES

En éste capítulo se dan condiciones necesarias y suficientes para que la imagen de Gray de un $\mathcal{R}$-código lineal sea un código lineal sobre F_{p^m}. Los resultados de éste capítulo están publicados en [LATR11].

2.1 EL MAPEO DE GRAY

Sea $\mathcal{R}$ el anillo de Galois $GR(p^2, m)$ de índice de nilpotencia 2, en ésta sección se introduce la definición del mapeo de Gray en $\mathcal{R}^n$ y algunas de sus propiedades básicas son recordadas.

Recordemos que si $X = (x_0, ..., x_{n-1})$ y $Y = (y_0, ..., y_{m-1})$ son elementos de $\mathcal{R}^n$ y $\mathcal{R}^m$ respectivamente, su producto de Kronecker está definido por:

$$X \otimes Y = (x_0Y, x_1Y, ..., x_{n-1}Y)$$

Obsérvese que $X \otimes Y$ tiene nm entradas. Este producto tiene varias propiedades incluyendo las siguientes:

$$\begin{aligned} X \otimes (Y + Z) &= X \otimes Y + X \otimes Z \\ (X + Y) \otimes Z &= X \otimes Z + Y \otimes Z \\ \alpha(X \otimes Y) &= (\alpha X) \otimes Y = X \otimes (\alpha Y) \\ (X_1, X_2) \otimes Y &= (X_1 \otimes Y, X_2 \otimes Y) \end{aligned}$$

donde $X, Y, Z, X_1, X_2 \in \mathcal{R}^n$ y $\alpha \in \mathcal{R}$.

Sea F el campo residual del anillo $\mathcal{R}$, sea $\mathbf{c_0} \in F^q$ el vector que enlista a todos los elementos de F y sea $\mathbf{c_1} = \mathbf{1_q} \in F^q$ el vector cuyas entradas son todas iguales a 1 de longitud $q = p^m$.

La notación siguiente se usará frecuentemente y se extenderá de manera análoga a los elementos $\mathbf{B}, \mathbf{A} + \mathbf{B}, \mathbf{A} + \mathbf{pB}$.

Sea $\mathbf{A} = (a_0, a_1, \ldots, a_{n-1})$ un elemento de $\mathcal{R}^n$, $a_i = \rho_0(a_i) + p\rho_1(a_i) \in \mathcal{R}$ la expansión p-ádica de a_i para cada $i = 0, \ldots, n-1$ y sea $\mu(\rho_k(a_i)) = r_i(a_i)$. Si $\rho_i(\mathbf{A}) = (\rho_i(a_0), \rho_i(a_1), \ldots, \rho_i(a_{n-1}))$ para $i = 0, 1$ entonces $\mathbf{A} = \rho_0(\mathbf{A}) + p\rho_1(\mathbf{A})$ y $r_i(\mathbf{A}) = (r_i(a_0), r_i(a_1), \ldots, r_i(a_{n-1}))$ para $i = 0, 1$.

El mapeo de Gray en $\mathcal{R}^n$ es definido (equivalentemente salvo permutación) como en ([GS99]) de la siguiente manera:

Definición 2.1. *El mapeo de Gray en $\mathcal{R}^n$ está dado por:*

$$\Phi : \mathcal{R}^n \longrightarrow F^{nq}, \ \Phi(\mathbf{A}) = \mathbf{c_0} \otimes r_0(\mathbf{A}) + \mathbf{c_1} \otimes r_1(\mathbf{A})$$

donde $\mathbf{A} = (a_0, ..., a_{n-1}) \in \mathcal{R}^n$ y " $\otimes$ " es el producto de Kronecker (expandido de derecha a izquierda).

El peso *homogéneo* en $\mathcal{R}$ es definido como (cf. [GS99], [HN99]):

$$wt_h(\gamma) = \begin{cases} (q-1), & \text{si } \gamma \in \mathcal{R} \setminus \langle p \rangle \\ q, & \text{si } \gamma \in \langle p \rangle \setminus \{0\} \\ 0, & \text{de otro modo} \end{cases}$$

donde $q = p^m$. El peso homogéneo en $\mathcal{R}^n$ está definido como:

$$wt_h(\mathbf{A}) = wt_h(a_0) + \cdots + wt_h(a_{n-1}).$$

El peso homogéneo en $\mathcal{R}^n$ induce una métrica, d_h, en $\mathcal{R}^n$. Sea d_H la métrica de Hamming en F^{nq}. Una de las principales propiedades del mapeo de Gray es el siguiente:

Teorema 2.1. *[GS99] El mapeo de Gray es una isometría inyectiva de* $(\mathcal{R}^n, d_h)$ *en* (F^{nq}, d_H).

El mapeo de Gray tiene otras propiedades incluyendo la siguiente cuya prueba básicamente se sigue de la definición de mapeo de Gray y de la Proposición 1.2.

Proposición 2.1. *Sean* $\mathbf{A} = \rho_0(\mathbf{A}) + p\rho_1(\mathbf{A})$ *y* $\mathbf{B} = \rho_0(\mathbf{B}) + p\rho_1(\mathbf{B})$ *elementos cualesquiera de* $\mathcal{R}^n$. *Entonces:*

$$\begin{aligned} \Phi(p\mathbf{B}) &= (r_0(\mathbf{B}), r_0(\mathbf{B}), \ldots, r_0(\mathbf{B})) \\ \Phi(\mathbf{A} + p\mathbf{B}) &= \Phi(\mathbf{A}) + \Phi(p\mathbf{B}), \end{aligned}$$

donde $\mu(\rho_0(\mathbf{B})) = r_0(\mathbf{B})$.

Demostración. Sean $\mathbf{A} = \rho_0(\mathbf{A}) + p\rho_1(\mathbf{A}), \mathbf{B} = \rho_0(\mathbf{B}) + p\rho_1(\mathbf{B}) \in \mathcal{R}^n$. Entonces $p\mathbf{B} = p\rho_0(\mathbf{B}) = \rho_0(p\mathbf{B}) + p\rho_1(p\mathbf{B})$ donde $\rho_0(p\mathbf{B}), \rho_1(p\mathbf{B}) \in \mathcal{T}^n$, así, $\rho_0(p\mathbf{B}) = 0$ y $\rho_1(p\mathbf{B}) = \rho_0(\mathbf{B})$, de ahí que, $r_0(p\mathbf{B}) = \mu(\rho_0(p\mathbf{B})) = 0$ y $r_1(p\mathbf{B}) = \mu(\rho_1(p\mathbf{B})) = r_0(\mathbf{B})$. Entonces

$$\begin{aligned} \Phi(p\mathbf{B}) &= \mathbf{c_0} \otimes r_0(p\mathbf{B}) + \mathbf{c_1} \otimes r_1(p\mathbf{B}) \\ &= \mathbf{c_1} \otimes r_0(\mathbf{B}) \\ &= (r_0(\mathbf{B}), r_0(\mathbf{B}), \ldots, r_0(\mathbf{B})) \end{aligned}$$

Ahora bien, sea $\mathbf{A} + p\mathbf{B} = \rho_0(\mathbf{A} + p\mathbf{B}) + p\rho_1(\mathbf{A} + p\mathbf{B})$ con $\rho_0(\mathbf{A} + p\mathbf{B}), \rho_1(\mathbf{A} + p\mathbf{B}) \in \mathcal{T}^n$ pero $r_0(\mathbf{A} + p\mathbf{B}) = \mu(\rho_0(\mathbf{A} + p\mathbf{B})) = r_0(\mathbf{A}) + r_0(p\mathbf{B}) = r_0(\mathbf{A})$, mientras que, $r_1(\mathbf{A} + p\mathbf{B}) = \mu(\rho_1(\mathbf{A} + p\mathbf{B})) = r_1(\mathbf{A}) + r_0(\mathbf{B})$ ya que

$$\begin{aligned} r_1(a_i + pb_i) &= [r_1(a_i)^p + r_1(pb_i)^p - h(r_0(a_i), r_0(pb_i))]^{1/p} \\ &= [r_1(a_i)^p + r_0(b_i)^p - h(r_0(a_i), 0)]^{1/p} \\ &= [r_1(a_i)^p + r_0(b_i)^p]^{1/p} \\ &= [(r_1(a_i) + r_0(b_i))^p]^{1/p} \\ &= r_1(a_i) + r_0(b_i) \end{aligned}$$

y

$$\begin{aligned} r_1(\mathbf{A} + p\mathbf{B}) &= (r_1(a_0 + pb_0), \ldots, r_1(a_i + pb_i), \ldots \\ &\quad \ldots, r_1(a_{n-1} + pb_{n-1})) \\ &= (r_1(a_0) + r_0(b_0), \ldots, r_1(a_i) + r_0(b_i), \ldots \\ &\quad \ldots, r_1(a_{n-1}) + r_0(b_{n-1})) \\ &= r_1(\mathbf{A}) + r_0(\mathbf{B}) \end{aligned}$$

Entonces

$$\begin{aligned}\Phi(\mathbf{A}+p\mathbf{B}) &= \mathbf{c_0}\otimes r_0(\mathbf{A}+p\mathbf{B})+\mathbf{c_1}\otimes r_1(\mathbf{A}+p\mathbf{B})\\ &= \mathbf{c_0}\otimes r_0(\mathbf{A})+\mathbf{c_1}\otimes (r_1(\mathbf{A})+r_0(\mathbf{B}))\\ &= (\mathbf{c_0}\otimes r_0(\mathbf{A})+\mathbf{c_1}\otimes r_1(\mathbf{A}))+\mathbf{c_1}\otimes r_0(\mathbf{B})\\ &= \Phi(\mathbf{A})+\Phi(p\mathbf{B})\end{aligned}$$

□

Como $GR(p^2,1)=\mathbb{Z}_{p^2}$, de la Proposición 2.1 se sigue la Proposición 2.1 de [LB02] para $k=1$.

Sean $\mathbf{A}=(a_0,a_1,\ldots,a_{n-1}),\mathbf{B}=(b_0,b_1,\ldots,b_{n-1})$ elementos de $\mathcal{R}^n$ y sea $a_i=\rho_0(a_i)+p\rho_1(a_i)\in\mathcal{R}$ la expansión p-ádica de a_i para cada i, $i=0,\ldots,n-1$ y $r_k(a_i)=\mu(\rho_k(a_i))$ para $k=0,1$. Sean $\rho_k(\mathbf{A})=(\rho_k(a_0),\rho_k(a_1),\ldots,\rho_k(a_{n-1}))$ y $r_k(\mathbf{A})=(r_k(a_0),r_k(a_1),\ldots\ldots,r_k(a_{n-1}))$ para $k=0,1$. Similarmente para $\mathbf{B}$, $\mathbf{A}+\mathbf{B}$ y $\mathbf{A}+\mathbf{pB}$.

Sean $\Theta(a_i,b_i)\in\mathcal{T}$ y $\theta(a_i,b_i)=\mu(\Theta(a_i,b_i))\in F_{p^m}$ tales que:

$$\theta(a_i,b_i)=r_1(a_i)+r_1(b_i)-[r_1(a_i)^p+r_1(b_i)^p-h(r_0(a_i),r_0(b_i))]^{\frac{1}{p}}.$$

Proposición 2.2. *Sea Φ el mapeo de Gray en $\mathcal{R}^n$ como se introduce en (2.1). Con la notación anterior para elementos cualesquiera $\mathbf{A}=(a_1,\ldots,a_{n-1}),\mathbf{B}=(b_1,\ldots,b_{n-1})\in\mathcal{R}^n$ se tiene que:*

$$\Phi(\mathbf{A})+\Phi(\mathbf{B})-\Phi(\mathbf{A}+\mathbf{B})=\Phi(p\Theta(\mathbf{A},\mathbf{B}) \tag{2.1}$$

donde

$$\begin{aligned}\Theta(\mathbf{A},\mathbf{B}) &= (\Theta(a_0,b_0),\ldots,\Theta(a_{n-1},b_{n-1}))\in\mathcal{T}^n,\\ \theta(\mathbf{A},\mathbf{B}) &= (\theta(a_0,b_0),\ldots,\theta(a_{n-1},b_{n-1}))\in F_{p^m}^n,\ y\\ \Phi(p\Theta(\mathbf{A},\mathbf{B}) &= (\theta(\mathbf{A},\mathbf{B}),\ldots,\theta(\mathbf{A},\mathbf{B})).\end{aligned}$$

Demostración. Sean $\mathbf{A},\mathbf{B}\in\mathcal{R}^n$, entonces

$$\begin{aligned}\Phi(\mathbf{A})+\Phi(\mathbf{B})-\Phi(\mathbf{A}+\mathbf{B}) &= \mathbf{c_0}\otimes r_0(\mathbf{A})+\mathbf{c_1}\otimes r_1(\mathbf{A})+\mathbf{c_0}\otimes r_0(\mathbf{B})\\ &\quad+\mathbf{c_1}\otimes r_1(\mathbf{B})-\mathbf{c_0}\otimes r_0(\mathbf{A}+\mathbf{B})-\mathbf{c_1}\otimes r_1(\mathbf{A}+\mathbf{B})\\ &= \mathbf{c_0}\otimes(r_0(\mathbf{A})+r_0(\mathbf{B}))+\mathbf{c_1}\otimes(r_1(\mathbf{A})+r_1(\mathbf{B}))\\ &\quad-\mathbf{c_0}\otimes(r_0(\mathbf{A})+r_0(\mathbf{B}))\\ &\quad-\mathbf{c_1}\otimes[r_1(\mathbf{A})^p+r_1(\mathbf{B})^p-h(r_0(\mathbf{A}),r_0(\mathbf{B}))]^{1/p}\\ &= \mathbf{c_1}\otimes(r_1(\mathbf{A})+r_1(\mathbf{B})\\ &\quad-[r_1(\mathbf{A})^p+r_1(\mathbf{B})^p-h(r_0(\mathbf{A}),r_0(\mathbf{B}))]^{1/p})\end{aligned}$$

donde

$$\begin{aligned}r_1(\mathbf{A})^p &:= (r_1(a_0)^p,r_1(a_1)^p,\ldots,r_1(a_{n-1})^p),\\ r_1(\mathbf{B})^p &:= (r_1(b_0)^p,r_1(b_1)^p,\ldots,r_1(b_{n-1})^p),\\ h(r_0(\mathbf{A}),r_0(\mathbf{B})) &:= (h(r_0(a_0),r_0(b_0)),\ldots,h(r_0(a_{n-1}),r_0(b_{n-1})))\end{aligned}$$

y

$$
\begin{aligned}
&[r_1(\mathbf{A})^p + r_1(\mathbf{B})^p - h(r_0(\mathbf{A}), r_0(\mathbf{B}))]^{1/p} \\
&:= ([r_1(a_0)^p + r_1(b_0)^p - h(r_0(a_0), r_0(b_0))]^{\frac{1}{p}}, \dots \\
&\dots, [r_1(a_{n-1})^p + r_1(b_{n-1})^p - h(r_0(a_{n-1}), r_0(b_{n-1}))]^{\frac{1}{p}}).
\end{aligned}
$$

De ahí que:

$$
\begin{aligned}
&r_1(\mathbf{A}) + r_1(\mathbf{B}) - [r_1(\mathbf{A})^p + r_1(\mathbf{B})^p - h(r_0(\mathbf{A}), r_0(\mathbf{B}))]^{1/p} \\
&= (\dots, r_1(a_i) + r_1(b_i) - [r_1(a_i)^p + r_1(b_i)^p - h(r_0(a_i), r_0(b_i))]^{\frac{1}{p}}, \dots) \\
&= (\dots, \theta(a_i, b_i), \dots) = \theta(\mathbf{A}, \mathbf{B})
\end{aligned}
$$

y por lo tanto

$$
\begin{aligned}
\Phi(\mathbf{A}) + \Phi(\mathbf{B}) - \Phi(\mathbf{A} + \mathbf{B}) &= \mathbf{c_1} \otimes \theta(\mathbf{A}, \mathbf{B}) \\
= (\theta(\mathbf{A}, \mathbf{B}), \dots, \theta(\mathbf{A}, \mathbf{B})) &= \Phi(p\Theta(\mathbf{A}, \mathbf{B})),
\end{aligned}
$$

con lo cual hemos demostrado la afirmación. □

2.2 IMAGEN DE GRAY LINEAL DE UN CÓDIGO LINEAL

Ahora enunciamos y demostramos uno de los resultados más relevantes de este estudio:

Teorema 2.2. *Sea $\mathcal{C}$ un $\mathcal{R}$-código lineal de longitud n y sea Φ el mapeo de Gray en $\mathcal{R}^n$. Entonces la imagen de Gray $\Phi(\mathcal{C})$ es un F_{p^m}-código lineal si y sólo si $p\Theta(\mathbf{A}, \mathbf{B}) \in \mathcal{C}$ para toda $\mathbf{A}, \mathbf{B} \in \mathcal{C}$.*

Demostración. Si $\mathbf{A}$, $\mathbf{B} \in \mathcal{R}^n$, se sigue a partir de la relación (2.1) y de la Proposición 2.1 que

$$\Phi(\mathbf{A}) + \Phi(\mathbf{B}) = \Phi(\mathbf{A} + \mathbf{B} + p\Theta(\mathbf{A}, \mathbf{B})). \tag{2.2}$$

Supongamos que $\Phi(\mathcal{C})$ es lineal. Entonces a partir de la relación (2.2) se sigue que $\mathbf{A} + \mathbf{B} + p\Theta(\mathbf{A}, \mathbf{B}) \in \mathcal{C}$ para cualquier $\mathbf{A}$, $\mathbf{B} \in \mathcal{C}$ y como $\mathcal{C}$ es lineal concluimos que $p\Theta(\mathbf{A}, \mathbf{B}) \in \mathcal{C}$. Recíprocamente, supongamos que $p\Theta(\mathbf{A}, \mathbf{B}) \in \mathcal{C}$ para cualquier $\mathbf{A}$, $\mathbf{B} \in \mathcal{C}$. Entoces a partir de la relación (2.2) y dado que $\mathcal{C}$ es $\mathcal{R}$-lineal, $\Phi(\mathbf{A}) + \Phi(\mathbf{B}) \in \Phi(\mathcal{C})$. Sea α cualquier elemento de $F_{p^m}^* = \langle \overline{\omega} \rangle$ y sea $\mathbf{D} \in \Phi(\mathcal{C})$ cualesquiera. Entonces $\alpha = \overline{\omega}^l$ para algún $l \in \{0, 1, \dots, p^m - 2\}$ y existe $\mathbf{A} = (a_0, \dots, a_j, \dots, a_{n-1}) \in \mathcal{C}$ tal que $\Phi(\mathbf{A}) = \mathbf{D}$. Entonces

$$
\begin{aligned}
\alpha\mathbf{D} &= \alpha\Phi(\mathbf{A}) = \alpha(\mathbf{c_0} \otimes r_0(\mathbf{A}) + \mathbf{c_1} \otimes r_1(\mathbf{A})) \\
&= \mathbf{c_0} \otimes \alpha r_0(\mathbf{A}) + \mathbf{c_1} \otimes \alpha r_1(\mathbf{A}))
\end{aligned}
$$

donde $\alpha r_i(\mathbf{A}) = (\alpha r_i(a_0), \dots, \alpha r_i(a_j), \dots, \alpha r_i(a_{n-1}))$ para $i = 0, 1$, y

$$\alpha r_i(a_j) = \overline{\omega}^l \mu(r_i(a_j)) = \mu(\omega^l \rho_i(a_j))$$

para $j = 0, 1, \ldots, n-1$ donde $\omega^l \rho_i(a_j) \in \mathcal{T}$. Sea $\mathbf{B} = (b_0, \ldots, b_j, \ldots, b_{n-1}) \in \mathcal{R}^n$ definido como $b_j = \omega^l \rho_0(a_j) + p\omega^l \rho_1(a_j)$ para $j = 0, 1, \ldots, n-1$. Entonces $\mathbf{B} = \omega^l \mathbf{A}$ y $\Phi(\mathbf{B}) = \alpha\Phi(\mathbf{A})$. Como $\mathcal{C}$ es $\mathcal{R}$-lineal y $\mathbf{A} \in \mathcal{C}$, $\omega^l \in \mathcal{T}$ se sigue que $\mathbf{B} \in \mathcal{C}$. Por consiguiente existe $\mathbf{B} \in \mathcal{C}$ tal que $\alpha\mathbf{D} = \Phi(\mathbf{B})$ implicando que $\alpha\mathbf{D} \in \Phi(\mathcal{C})$ para cualquier $\mathbf{D} \in \Phi(\mathcal{C})$ y cualquier $\alpha \in F_{p^m}$. Por lo tanto, $\Phi(\mathcal{C})$ es un F_{p^m}-código lineal. □

Observese que si $\mathcal{R} = \mathbb{Z}_4$ el Teorema 2.2 produce el resultado correspondiente que aparece en [JKC+94] y da el mismo resultado que aparece en [LB02] si $\mathcal{R} = \mathbb{Z}_{p^2}$.

3 IMÁGENES DE GRAY DE CÓDIGOS SOBRE EL ANILLO DE WITT

En éste capítulo, tomando en consideración que el anillo de Galois $\mathcal{R} = GR(p^2, m)$ y el anillo de Witt $\mathcal{W}_2(F)$ son isomorfos, la definición del mapeo de Gray sobre éste último anillo es recordada [TR06] con el objeto de dar condiciones necesarias y suficientes para que un código sobre el anillo de Witt sea $\hat{\alpha}$-cíclico en términos de su imagen de Gray además condiciones necesarias y suficientes para que un código sea $\hat{\gamma}$-cíclico también son dadas en términos de su imagen de Gray. Estos resultados generalizan algunos de los resultados que aparecen en [LB02] para códigos sobre el anillo $GR(p^2, 1) = \mathbb{Z}_{p^2}$. Los resultados presentados en éste capítulo están publicados en [LATR08].

Sea $\mathbf{c}_0 \in F^q$ el vector que enlista a todos los elementos de F, sea $\mathbf{1_q} = (1, 1, \ldots, 1) \in F^q$ el vector cuyas entradas son todas iguales a 1 de longitud $q = p^m$ y sea M la matriz de tamaño $2 \times q$ cuya primera fila es $\mathbf{c}_0$ y la segunda fila es $\mathbf{1_q}$. Entonces el mapeo de Gray en $\mathcal{W}_2(F)$ es definido por:

$$\widehat{\phi} : \mathcal{W}_2(F) \longrightarrow F^q, \ \widehat{\phi}(a_0, a_1) = (a_0, a_1)\mathbf{M}. \tag{3.1}$$

La relación del mapeo de Gray tal como se definió y el mapeo de Gray ϕ como se introduce en [GS99] es:

$$Im(\phi) = Im(\widehat{\phi} \circ \psi)$$

donde ψ es el isomorfismo entre el anillo de Galois $GR(p^2, m)$ y el anillo de Witt $\mathcal{W}_2(F)$ mencionado en la subsección 1.2.2.

A continuación el anillo de Galois $\mathcal{R} = GR(p^2, m)$ y el anillo de vectores de Witt $\mathcal{W}_2(F)$ así como los mapeos ϕ y $\widehat{\phi}$ serán utilizados libremente.

Para un entero positivo n, el mapeo de Gray es extendido coordenada-a-coordenada a $\mathcal{R}^n$ ó equivalentemente a $\mathcal{W}_2(F)^n$, i.e.,

$$\Phi(\mathbf{A}) = (\phi(A_0), \ldots, \phi(A_{n-1})) \in F^{nq} \tag{3.2}$$

donde $\mathbf{A} = (A_0, \ldots, A_{n-1}) \in \mathcal{R}^n$.

La definición (3.2) es equivalente salvo permutación a la dada en (2.1).

3.1 IMÁGENES DE GRAY CUASI-CÍCLICAS DE UNA CLASE DE $\mathcal{R}$-CÓDIGOS

En ésta sección vamos a expresar y enumerar los elementos del campo residual $F = F_{p^m}$ del anillo de Galois $\mathcal{R} = GR(p^2, m)$ (ó del anillo de Witt $\mathcal{W}_2(F)$) en la forma siguiente:

Para $i \in N$ tal que $0 \leqslant i \leqslant p^{m-1}$, considérese la representación de i en base p, i.e., $i = d_{i0} + d_{i1}p + \cdots + d_{i(m-2)}p^{m-2}$ donde $d_{is} \in \{0, \ldots, p-1\}$ para cada $s \in \{0, \ldots, m-2\}$ y sea $(i)_p = (d_{i0}, d_{i1}, \ldots, d_{i(m-2)})$.

Como el campo finito F es una extensión de grado m del campo base F_p sea $\Omega = \{1, \bar{\omega}, ..., \bar{\omega}^{m-1}\}$ una base de F sobre F_p. Para cada $j \in N$ tal que $0 \leqslant j \leqslant p-1$ sea

$$(j + (i)_p)\Omega = j + d_{i0}\bar{\omega} + d_{i1}\bar{\omega}^2 + \cdots + d_{i(m-2)}\bar{\omega}^{m-1}$$

y sea

$$\begin{aligned} \mathbf{B}_j \quad : \quad & (j + (0)_p)\Omega, (j + (1)_p)\Omega, \ldots \\ & \ldots, (j + (i)_p)\Omega, \ldots \\ & \ldots, (j + (p^{m-1} - 1)_p)\Omega. \end{aligned}$$

Entonces los elementos del campo finito F_{p^m} se pueden expresar y enumerar en la forma:

$$[B_0, B_1, ..., B_{p-1}]. \tag{3.3}$$

Sea M la matriz descrita anteriormente. Entonces la imagen de $(a_0, a_1) \in \mathcal{W}_2(F)$ bajo el mapeo de Gray, $\hat{\phi}(a_0, a_1) = (a_0, a_1)M$ (ver (3.1)), es el vector de longitud q:

$$(a_0\mathbf{B}_0 + a_1\mathbf{1}, \ldots, a_0\mathbf{B}_j + a_1\mathbf{1}, \ldots, a_0\mathbf{B}_{p-1} + a_1\mathbf{1})$$

donde

$$\begin{aligned} a_0\mathbf{B}_j + a_1\mathbf{1} : \\ & (j + (0)_p\Omega)a_0 + a_1, \ldots, (j + (i)_p\Omega)a_0 + a_1, \ldots, \\ & \ldots, (j + (p^{m-1} - 1)_p\Omega)a_0 + a_1 \end{aligned} \tag{3.4}$$

para $0 \leqslant j \leqslant p-1$.

Sea $\alpha = 1 + Tp$ una unidad (principal) del anillo de Galois $\mathcal{R} = GR(p^2, m)$ donde $T \in \mathcal{T}$ es tal que $\mu(\alpha) = -1$ y sea $\hat{\alpha} = (1, p-1)$ el elemento correspondiente en el anillo de Witt $\mathcal{W}_2(F)$. Sea σ el corrimiento cíclico usual, i.e., si $\mathbf{X} = (X_1, X_2, \ldots, X_q)$ entonces $\sigma(\mathbf{X}) = (X_q, X_1, \ldots, X_{q-1})$ y para cualquier entero positivo k, $0 \leqslant k < q$, σ^k significa corrimiento cíclico k lugares.

Con la notación anterior se tiene:

Lema 3.1. *Sea $\hat{\phi}$ el mapeo de Gray en $\mathcal{W}_2(F)$ y sea $\hat{\alpha}$ como se introdujo antes. Entonces para cualquier elemento $\hat{A} = (a_0, a_1) \in \mathcal{W}_2(F)$ tal que $a_0 \in F_p$ se tiene que*

$$\hat{\phi}\left(\hat{\alpha}\hat{A}\right) = \sigma^{p^{m-1}}\left(\hat{\phi}(\hat{A})\right).$$

Demostración. A partir del producto en el anillo de Witt y la definición del mapeo de Gray se sigue que

$$\begin{aligned} \hat{\phi}\left(\hat{\alpha}\hat{A}\right) &= (\ldots, a_0\mathbf{B}_j + ((p-1)a_0 + a_1)\mathbf{1}, \ldots) \\ &= (\ldots, (j + (p-1) + (i)_p\Omega)a_0 + a_1, \ldots,) \\ &= (a_0\mathbf{B}_{p-1} + a_1\mathbf{1}, \ldots, a_0\mathbf{B}_{j+(p-1)} + a_1\mathbf{1}, \ldots, a_0\mathbf{B}_{p-2} + a_1\mathbf{1}) \end{aligned}$$

(para $j \in \{0, 1, \ldots, p-1\}$, $j + (p-1)$ se toma módulo p y el producto $\hat{\alpha}\hat{A}$ se toma en el anillo de Witt).

Por otro lado,

$$\begin{aligned} \sigma^{p^{m-1}}\left(\hat{\phi}(\hat{A})\right) &= \sigma^{p^{m-1}}(a_0\mathbf{B}_0 + a_1\mathbf{1}, \ldots, a_0\mathbf{B}_j + a_1\mathbf{1}, \ldots, a_0\mathbf{B}_{p-1} + a_1\mathbf{1}) \\ &= (a_0\mathbf{B}_{p-1} + a_1\mathbf{1}, \ldots, a_0\mathbf{B}_{j-1} + a_1\mathbf{1}, \ldots, a_0\mathbf{B}_{p-2} + a_1\mathbf{1}) \end{aligned}$$

y la afirmación queda demostrada. □

Definimos los mapeos siguientes:

i) Sea $\hat{\alpha} = (1, p-1) \in \mathcal{W}_2(F)$ como se introdujo al inicio de ésta sección. Entonces,

$$\begin{aligned} \nu_{\hat{\alpha}} : \mathcal{W}_2(F)^n &\longrightarrow \mathcal{W}_2(F)^n, \\ (\hat{A}_0, \ldots, \hat{A}_{n-1}) &\longrightarrow (\hat{\alpha}\hat{A}_{n-1}, \ldots, \hat{A}_{n-2}). \end{aligned}$$

ii) Sea $F = F_q$, $(q = p^m)$, el campo residual del anillo de Galois $\mathcal{R}$ (ó anillo de Witt $\mathcal{W}_2(F)$) y σ el corrimiento cíclico usual. Para cualquier entero positivo n sea,

$$\tilde{\sigma} : F^{nq} \longrightarrow F^{nq},\ \tilde{\sigma}(\mathbf{X}) = (\sigma^{p^{m-1}}(\mathbf{X_{n-1}}), \mathbf{X_0}, \ldots, \mathbf{X_{n-2}})$$

i.e., la acción de $\tilde{\sigma}$ en $\mathbf{X} = (\mathbf{X}_0, \ldots, \mathbf{X}_{n-1})$, donde cada $\mathbf{X}_i \in F^q$, es primero aplicar el corrimiento cíclico usual a $\mathbf{X}$ obteniendo $(\mathbf{X}_{n-1}, \mathbf{X}_0, \ldots, \mathbf{X}_{n-2})$ y luego aplicar el mapeo $\sigma^{p^{m-1}}$ a $\mathbf{X}_{n-1}$ y el mapeo identidad a las otras entradas $\mathbf{X}_i$.

Definición 3.1. *Un código $\hat{\mathcal{C}} \subseteq \mathcal{W}_2(F)^n$ es llamado $\hat{\alpha}$-cíclico si $\nu_{\hat{\alpha}}(\hat{\mathcal{C}}) = \hat{\mathcal{C}}$.*

Proposición 3.1. *Para cualquier entero positivo n sea $\hat{\mathbf{A}} = (\hat{A}_0, \ldots, \hat{A}_{n-1}) \in \mathcal{W}_2(F)^n$ y supongámos que $\hat{A}_{n-1} = (a_0^{(n-1)}, a_1^{(n-1)})$ es tal que $a_0^{(n-1)} \in F_p$. Entonces*

$$\hat{\Phi} \circ \nu_\alpha = \tilde{\sigma} \circ \hat{\Phi}.$$

Demostración. A partir de la definición del producto en el anillo de Witt y de la hipótesis sobre $a_0^{(n-1)}$, se sigue que $\hat{\alpha}\hat{A}_{n-1} = (a_0^{(n-1)}, (p-1)a_0^{(n-1)} + a_1^{(n-1)})$.

Entonces

$$\tilde{\sigma}(\hat{\Phi}(\hat{\mathbf{A}})) = (\sigma^{p^{m-1}}(\hat{\phi}(\hat{A}_{n-1}), \hat{\phi}(\hat{A}_0), \ldots, \hat{\phi}(\hat{A}_{n-2}))).$$

Por otro lado,

$$\hat{\Phi}(\nu_\alpha(\hat{\mathbf{A}})) = (\hat{\phi}(\hat{\alpha}\hat{A}_{n-1}), \hat{\phi}(A_0), \ldots, \hat{\phi}(A_{n-2})).$$

Por consiguiente, la afirmación de la Proposición se sigue del Lema 3.1 □

Definición 3.2. *Un código $\tilde{\mathcal{D}} \subseteq F^{nq}$ es llamado cuasi-cíclico de primer-bloque de índice p^{m-1} si $\tilde{\sigma}(\tilde{\mathcal{D}}) = \tilde{\mathcal{D}}$.*

Como una consecuencia de la Proposición 3.1 se tiene el siguiente:

Teorema 3.1. *Sea $\hat{\mathcal{C}} \subseteq \mathcal{W}_2(F)^n$ un código tal que para cada $\hat{\mathbf{A}} = (\hat{A}_0, \ldots, \hat{A}_{n-1}) \in \hat{\mathcal{C}}$, $\hat{A}_{n-1} = (a_0^{(n-1)}, a_1^{(n-1)}) \in F_p \times F \subseteq \mathcal{W}_2(F)$. Entonces $\hat{\mathcal{C}}$ es $\hat{\alpha}$-cíclico si y sólo si su imagen de Gray $\hat{\Phi}(\hat{\mathcal{C}})$ es un código cuasi-cíclico de primer-bloque de índice p^{m-1}.*

Demostración. Si $\hat{\mathcal{C}} \subseteq \mathcal{W}_2(F)^n$ es un código tal que $\hat{\Phi}(\hat{\mathcal{C}})$ es cuasi-cíclico de primer-bloque de índice p^{m-1}, entonces de la Proposición 3.1,

$$\hat{\Phi}(\hat{\mathcal{C}}) = \tilde{\sigma}\left(\hat{\Phi}(\hat{\mathcal{C}})\right) = \hat{\Phi}\left(\nu_\alpha(\hat{\mathcal{C}})\right)$$

y la afirmación se sigue de la inyectividad del mapeo de Gray. El recíproco también es inmediato a partir de la Proposición 3.1. □

Obsérvese que como $\mathbb{Z}_{p^2} = GR(p^2, 1)$, el Teorema 3.1 proporciona el Teorema 2.4 para el caso $k = 1$, i.e. Corolario 2.5 de [LB02], salvo permutación.

3.2 IMÁGENES DE GRAY $\tilde{\tau}$-CUASI-CÍCLICAS DE UNA CLASE DE $\mathcal{R}$-CÓDIGOS

Sea $\mathcal{R} = GR(p^2, m)$ el anillo de Galois, $\mathcal{M}$ su ideal maximal, $F = F_q$, $(q = p^m)$ el campo residual y $\mathcal{T}$ el conjunto Teichmüller de $\mathcal{R}$. Sea $n \in \mathbb{N}$ tal que $(n, p) = 1$ y sea n' el único entero en $\{1, \ldots, p-1\}$ que satisface $nn' \equiv 1 \bmod p$. Sean $N' \in \mathcal{T}$ y $\mu(N') = n'$, sea $\gamma = 1 + N'p \in 1 + \mathcal{M}$ y $\hat{\gamma} = (1, n') \in \mathcal{W}_2(F)$ su imagen en el anillo de Witt. Obsérve que para cualquier entero positivo k, $\hat{\gamma}^k = (1, (kn')_p)$, donde $(*)_p$ significa reducción módulo p. En particular $\hat{\gamma}^n = (1, 1)$.

Ahora definimos los mapeos siguientes:

i) Con la notación dada arriba,

$$\begin{aligned} \chi_{\hat{\gamma}} : \mathcal{W}_2(F)^n &\longrightarrow \mathcal{W}_2(F)^n, \\ \hat{\mathbf{A}} &\longrightarrow (\hat{A}_0, \ldots, \hat{\gamma}^i \hat{A}_i, \ldots, \hat{\gamma}^{n-1} \hat{A}_{n-1}) \end{aligned}$$

donde $\hat{\mathbf{A}} = (\hat{A}_0, \ldots, \hat{A}_{n-1})$.

ii) Sea σ el corrimiento cíclico usual y sea $\tau = \sigma^{p^{m-1}}$.

$$\begin{aligned} \tilde{\tau} : F^{nq} &\longrightarrow F^{nq}, \\ \mathbf{X} &\longrightarrow (\tau^{(-0n')_p}(\mathbf{X}_0), \ldots, \tau^{(-in')_p}(\mathbf{X}_i), \ldots \\ &\qquad \ldots, \tau^{(-(n-1)n')_p}(\mathbf{X}_{n-1})) \end{aligned}$$

donde $\mathbf{X} = (\mathbf{X}_0, \ldots, \mathbf{X}_{n-1})$, $\mathbf{X}_i \in F^q$ y $(*)_p$ significa reducción módulo p.

Definición 3.3. *Un código $\hat{\mathcal{C}} \subseteq \mathcal{W}_2(F)^n$ se dice $\hat{\gamma}$-cíclico si $\chi_{\hat{\gamma}}(\hat{\mathcal{C}}) = \hat{\mathcal{C}}$.*

Definición 3.4. *Si F es el campo residual del anillo de Galois $\mathcal{R}$, un código $\mathcal{D} \subseteq F^{nq}$ se dice $\tilde{\tau}$-cuasi-cíclico si $\tilde{\tau}(\mathcal{D}) = \mathcal{D}$.*

Proposición 3.2. *Con la notación anterior, para cualquier $\hat{\mathbf{A}} = (\hat{A}_0, \ldots, \hat{A}_{n-1}) \in \mathcal{W}_2(F)^n$ con $\hat{A}_i = (a_0^{(i)}, a_1^{(i)})$, $a_0^{(i)} \in F_p$ para $i = 0, 1, \ldots, n-1$, se tiene que:*

$$\hat{\Phi}\left(\chi_{\hat{\gamma}}(\hat{\mathbf{A}})\right) = \tilde{\tau}\left(\hat{\Phi}(\hat{\mathbf{A}})\right)$$

donde $\hat{\Phi}$ es el mapeo de Gray en $\mathcal{W}_2(F)^n$.

Demostración. A partir de la definición del mapeo $\chi_{\hat{\gamma}}$ y del mapeo de Gray en $\mathcal{W}_2(F)^n$

$$\hat{\Phi}\left(\chi_{\hat{\gamma}}(\hat{\mathbf{A}})\right) = (\hat{\phi}(\hat{A}_0), \ldots, \hat{\phi}(\hat{\gamma}^i \hat{A}_i), \ldots, \hat{\phi}(\hat{\gamma}^{n-1}\hat{A}_{n-1})).$$

Por otro lado, de la definición del mapeo $\tilde{\tau}$, tenemos

$$\begin{aligned}\tilde{\tau}(\Phi(\hat{\mathbf{A}})) &= (\tau^{(-0n')_p}(\hat{\phi}(\hat{A}_0)), \ldots, \tau^{(-in')_p}(\hat{\phi}(\hat{A}_i)), \ldots \\ &\quad \ldots, \tau^{(-(n-1)n')_p}(\hat{\phi}(\hat{A}_{n-1})).\end{aligned}$$

De la definición del producto en el anillo de Witt y la hipótesis en $\hat{A}_i$,

$$\begin{aligned}\hat{\phi}(\hat{\gamma}^i \hat{A}_i) &= (a_0^{(i)}\mathbf{B}_{(\mathbf{in'})_p} + a_1^{(i)}\mathbf{1}, \ldots, a_0^{(i)}\mathbf{B}_{(\mathbf{j+in'})_p} + a_1^{(i)}\mathbf{1}, \ldots \\ &\quad \ldots, a_0^{(i)}\mathbf{B}_{(\mathbf{p-1+in'})_p} + a_1^{(i)}\mathbf{1})\end{aligned}$$

y

$$\begin{aligned}\tau^{(-in')_p}(\hat{\phi}(\hat{A}_i)) &= (\tau^{-1})^{(in')_p}(a_0^{(i)}\mathbf{B_0} + a_1^{(i)}\mathbf{1}, \ldots \\ &= \ldots, a_0^{(i)}\mathbf{B_j} + a_1^{(i)}\mathbf{1}, \ldots, a_0^{(i)}\mathbf{B_{p-1}} + a_1^{(i)}\mathbf{1}).\end{aligned}$$

Obsérvese que si $\Lambda = (\Lambda_0, \Lambda_1, \ldots, \Lambda_{p-1})$ donde $\Lambda_j = a_0^{(i)}\mathbf{B_j} + a_1^{(i)}\mathbf{1}$, es fácil ver que $\tau = \sigma^{p^{m-1}}$ actua sobre Λ como el corrimiento cíclico usual, i.e., $\tau(\Lambda) = (\Lambda_{p-1}, \Lambda_0, \ldots, \Lambda_{p-2})$ y para cualquier entero positivo k, $\tau^{-k}(\Lambda) = (\Lambda_k, \Lambda_{k+1}, \ldots\ldots, \Lambda_{j+k}, \ldots, \Lambda_{p-2+k})$, (donde $j+k$ es tomado módulo p).

A partir de ésta observación concluimos que $\hat{\phi}(\hat{\gamma}^i \hat{A}_i) = \tau^{(-in')_p}(\hat{\phi}(\hat{A}_i))$ para $i = 0, 1, \ldots, n-1$, con lo cual probamos la afirmación. □

Ahora tenemos el siguiente:

Teorema 3.2. *Sea $\hat{\mathcal{C}} \subseteq \mathcal{W}_2(F)^n$ un código de longitud n primo relativo con p tal que para cualquier $\hat{\mathbf{A}} = (\hat{A}_0, \ldots, \hat{A}_{n-1}) \in \hat{\mathcal{C}}$, $\hat{A}_i = (a_0^{(i)}, a_1^{(i)}) \in F_p \times F$, $0 \leqslant i \leqslant n-1$. Entonces el código $\hat{\mathcal{C}}$ es $\hat{\gamma}$-cíclico si y sólo si $\hat{\Phi}(\hat{\mathcal{C}})$ es un código $\tilde{\tau}$-cuasi-cíclico de longitud nq sobre F.*

Demostración. Si $\hat{\mathcal{C}} \subseteq \mathcal{W}_2(F)^n$ es un código tal que $\hat{\Phi}(\hat{\mathcal{C}})$ es un código $\tilde{\tau}$-cuasi-cíclico de la Proposición 3.2 se tiene que

$$\hat{\Phi}(\hat{\mathcal{C}}) = \tilde{\tau}\left(\hat{\Phi}(\hat{\mathcal{C}})\right) = \hat{\Phi}\left(\chi_{\hat{\gamma}}(\hat{\mathcal{C}})\right)$$

y la afirmación se sigue de la inyectividad del mapeo de Gray. El recíproco tambiés es inmediato a partir de la Proposición 3.2. □

4 IMÁGENES DE GRAY CUASI CÍCLICAS

En éste capítulo se dan condiciones necesarias y suficientes para que la imagen de Gray de un $(1-p)$-código cíclico definido sobre el anillo de Galois $GR(p^2, m)$ sea cuasi-cíclica también se dan condiciones necesarias y suficientes para la cuasi-ciclicidad no necesariamente lineal de la imagen de Gray de códigos cíclicos lineales sobre el anillo de Galois $GR(p^2, m)$. Los resultados de este capítulo están publicados en [LATR11].

Para establecer los resultados de este capítulo vamos a expresar y enumerar los elementos del campo residual $F = F_{p^m}$ del anillo de Galois $\mathcal{R} = GR(p^2, m)$ en una forma diferente a la empleada en la sección 3.1

Sea $\{1, \omega, \omega^2, \ldots, \omega^{m-1}\}$ una base para el campo residual $F = F_{p^m}$ sobre F_p. Como se tiene una biyección entre $\mathbb{Z}_{p^m}$ y F_{p^m} dada por

$$h = h_0 + h_1 p + \cdots + h_{m-1} p^{m-1} \to \omega_h = h_0 + h_1 \omega + \cdots + h_{m-1} \omega^{m-1}$$

donde $0 \leqslant h_i \leqslant p-1$ para $i = 0, 1, ..., m-1$, los elementos del campo residual F_{p^m} se tomarán en el orden siguiente:

$$F_{p^m} = \{w_h : h = 0, \ldots, p^m - 1\}.$$

Obsérvese que,

$$\begin{aligned} \omega_{ip} + k &= \omega_{ip+k} \text{ para } 0 \leqslant k \leqslant p-1 \text{ y } 0 \leqslant i \leqslant p^m - 1, \\ \omega_{ip+j} + k &= \omega_{ip+(j+k)_p} \text{ para } 0 \leqslant j \leqslant p-1,\ 0 \leqslant k \leqslant p-1,\ 0 \leqslant i \leqslant p^m - 1 \end{aligned} \tag{4.1}$$

donde $(*)_p$ denota reducción módulo p.

Sea

$$\Omega_i = (\omega_{ip}, \omega_{ip+1}, \ldots, \omega_{ip+j}, \ldots, \omega_{ip+p-1}),$$

para $i = 0, \ldots, p^{m-1} - 1$ y $j = 0, \ldots, p-1$.

Entonces los elementos del campo finito F_{p^m} se pueden expresar y enumerar en la forma:

$$[\omega_0, \ldots, \omega_{p^m-1}] = [\Omega_0, , \ldots, \Omega_i, \ldots, \Omega_{p^{m-1}-1}] \tag{4.2}$$

Sea $q = p^m$ y $\mathbf{c_0} = [\Omega_0, , \ldots, \Omega_i, \ldots, \Omega_{p^{m-1}-1}] = (\omega_0, \ldots, \omega_{p^m-1}) \in F_q^q$ el vector que enlista a todos los elementos del campo residual en el orden dado en (4.2), sea $\mathbf{c_1} = 1_q$ el vector cuyas entradas son todas iguales a 1 de longitud q y sea Φ el mapeo de Gray como previamente se definió (cf. (2.1)).

4.1 IMÁGENES DE GRAY DE CÓDIGOS $(1-p)$-CÍCLICOS

Sea $\mathcal{R} = GR(p^2, m)$ el anillo de Galois, $\mathcal{M}$ su ideal maximal, $F = F_q$, $(q = p^m)$ el campo residual de $\mathcal{R}$ y $\mathcal{T}$ el conjunto Teichmüller de $\mathcal{R}$. Sea $\lambda = 1 - p = 1 + Tp$ una unidad (principal) del anillo de Galois $\mathcal{R} = GR(p^2, m)$ donde $T \in \mathcal{T}$ es tal que $\mu(T) = -1$.

Definimos los mapeos siguientes:

i) Sea $\lambda = 1 - p$. Entonces,

$$\begin{aligned} \nu_\lambda : \mathcal{R}^n &\longrightarrow \mathcal{R}^n, \\ (a_0, a_1, \ldots, a_{n-1}) &\longrightarrow (\lambda a_{n-1}, a_0, \ldots, a_{n-2}). \end{aligned}$$

ii) Para cualesquiera enteros positivos s y t sea

$$\begin{aligned} \sigma^{\otimes t} : F^{st} &\longrightarrow F^{st}, \\ (\mathbf{a}^{(1)}|\mathbf{a}^{(2)}|\cdots|\mathbf{a}^{(t)}) &\longrightarrow (\sigma(\mathbf{a}^{(1)})|\sigma(\mathbf{a}^{(2)})|\cdots|\sigma(\mathbf{a}^{(t)})) \end{aligned}$$

donde $\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(t)} \in F^s$ y $\sigma : F^s \longrightarrow F^s$ es el corrimiento cíclico usual. En particular, $\sigma^{\otimes 1} = \sigma$.

Definición 4.1. *Un código $\mathcal{C} \subseteq \mathcal{R}^n$ es llamado λ-cíclico si $\nu_\lambda(\mathcal{C}) = \mathcal{C}$, mientras que un código $C \subseteq F^{st}$ que satisface $\sigma^{\otimes t}(C) = C$ es llamado cuasi-cíclico de índice t y longitud st.*

Proposición 4.1. *Sean Φ el mapeo de Gray y los mapeos ν_λ, $\sigma^{\otimes p^{m-1}}$ definidos anteriormente. Entonces,*

$$\Phi \circ \nu_\lambda = \sigma^{\otimes p^{m-1}} \circ \Phi. \tag{4.3}$$

Demostración. Sea $\mathbf{A} = (a_0, a_1, \ldots, a_{n-1})$ un elemento de $\mathcal{R}^n$ y sea $\mathbf{B} = (b_0, b_1, \ldots, b_{n-1}) = \nu_\lambda(\mathbf{A}) = (\lambda a_{n-1}, a_0, \ldots, a_{n-2})$, i.e., $b_0 = \lambda a_{n-1}$ y $b_i = a_{i-1}$ para $i = 1, \ldots, n-1$. A partir de Lema 1.4 se sigue que $b_0 = \lambda a_{n-1} = \rho_0(\lambda a_{n-1}) + p\rho_1(\lambda a_{n-1})$ donde $\rho_0(\lambda a_{n-1})$, $\rho_1(\lambda a_{n-1}) \in \mathcal{T}$ es tal que $r_0(\lambda a_{n-1}) = r_0(a_{n-1})$ y $r_1(\lambda a_{n-1}) = r_1(a_{n-1}) - r_0(a_{n-1})$ de manera que $r_0(b_0) = r_0(a_{n-1})$ y $r_1(b_0) = r_1(a_{n-1}) - r_0(a_{n-1})$. Entonces,

$$\begin{aligned} r_0(\mathbf{B}) &= (r_0(a_{n-1}), r_0(a_0), \ldots, r_0(a_{n-2})) \\ r_1(\mathbf{B}) &= (r_1(a_{n-1}) - r_0(a_{n-1}), r_1(a_0), \ldots, r_1(a_{n-2})) \\ &= (r_1(a_{n-1}) + (p-1)r_0(a_{n-1}), r_1(a_0), \ldots, r_1(a_{n-2})). \end{aligned}$$

Por consiguiente,

$$\begin{aligned} \Phi(\nu_\lambda(\mathbf{A})) = \Phi(\mathbf{B}) &= \mathbf{c_0} \otimes r_0(\mathbf{B}) + \mathbf{c_1} \otimes r_1(\mathbf{B}) \\ &= [\Omega_0, \ldots, \Omega_i, \ldots, \Omega_{p^{m-1}-1}] \otimes r_0(\mathbf{B}) + [\underline{1}_p, \ldots, \underline{1}_p, \ldots, \underline{1}_p] \otimes r_1(\mathbf{B}) \\ &= [, \ldots, \Omega_i \otimes r_0(\mathbf{B}) + \underline{1}_p \otimes r_1(\mathbf{B}), \ldots,]. \end{aligned}$$

Sea $\mathcal{B}_i = \Omega_i \otimes r_0(\mathbf{B}) + \underline{1}_p \otimes r_1(\mathbf{B})$ el i-iésimo bloque de longitud np del vector $\Phi(\mathbf{B})$, $i = 0, \ldots, p^{m-1} - 1$. Entonces,

$$\begin{aligned} \mathcal{B}_i &= [\omega_{ip}, \ldots, \omega_{ip+j}, \ldots, \omega_{ip+p-1}] \otimes r_0(\mathbf{B}) + [1, \ldots, 1, \ldots, 1] \otimes r_1(\mathbf{B}) \\ &= [\omega_{ip} r_0(\mathbf{B}) + r_1(\mathbf{B}), \ldots, \omega_{ip+j} r_0(\mathbf{B}) + r_1(\mathbf{B}), \ldots, \omega_{ip+p-1} r_0(\mathbf{B}) + r_1(\mathbf{B})] \end{aligned}$$

y sea $\omega_{ip+j}r_0(\mathbf{B}) + r_1(\mathbf{B})$ el j-iésimo bloque de longitud n de $\mathcal{B}_i$, $j = 0, \ldots, p-1$.

Por consiguiente,

$$\begin{aligned}
&\omega_{ip+j}r_0(\mathbf{B}) + r_1(\mathbf{B}) \\
&= [\omega_{ip+j}r_0(b_0) + r_1(b_0), \omega_{ip+j}r_0(b_1) + r_1(b_1), \ldots, \omega_{ip+j}r_0(b_{n-1}) + r_1(b_{n-1})] \\
&= [\omega_{ip+j}r_0(a_{n-1}) + r_1(a_{n-1}) + (p-1)r_0(a_{n-1}), \omega_{ip+j}r_0(a_0) \\
&+ r_1(a_0), \ldots, \omega_{ip+j}r_0(a_{n-2}) + r_1(a_{n-2})] \\
&= [(\omega_{ip+j} + p - 1)r_0(a_{n-1}) + r_1(a_{n-1}), \omega_{ip+j}r_0(a_0) \\
&+ r_1(a_0), \ldots, \omega_{ip+j}r_0(a_{n-2}) + r_1(a_{n-2})] \\
&= [\omega_{ip+j-1}r_0(a_{n-1}) + r_1(a_{n-1}), \omega_{ip+j}r_0(a_0) + r_1(a_0), \ldots \\
&\quad \ldots, \omega_{ip+j}r_0(a_{n-2}) + r_1(a_{n-2})]
\end{aligned}$$

donde $\omega_{ip+j} + (p-1) = \omega_{ip+(j+p-1)_p} = \omega_{ip+j-1}$, por la propiedad 4.1.

Por lo tanto, el j-ésimo bloque de longitud n de $\mathcal{B}_i$, para $j = 0, \ldots, p-1$, es igual a

$$[\omega_{ip+j-1}r_0(a_{n-1}) + r_1(a_{n-1}), \omega_{ip+j}r_0(a_0) + r_1(a_0), \ldots \\ \ldots, \omega_{ip+j}r_0(a_{n-2}) + r_1(a_{n-2})]. \tag{4.4}$$

Por otro lado, el i-ésimo bloque de longitud np del vector $\Phi(\mathbf{A})$, para cada $i = 0, \ldots, p^{m-1} - 1$ es:

$$\begin{aligned}
\mathcal{A}_i \;=\; & \Omega_i \otimes r_0(\mathbf{A}) + \underline{1}_p \otimes r_1(\mathbf{A}) = [\omega_{ip}r_0(\mathbf{A}) + r_1(\mathbf{A}), \ldots \\
& \ldots, \omega_{ip+j}r_0(\mathbf{A}) + r_1(\mathbf{A}), \ldots, \omega_{ip+p-1}r_0(\mathbf{A}) + r_1(\mathbf{A})]
\end{aligned}$$

y éste bloque $\mathcal{A}_i$ puede ser visto como la concatenación de las filas del siguiente arreglo de tamaño pn:s

$$\begin{pmatrix}
\omega_{ip}r_0(a_0) + r_1(a_0) & \omega_{ip}r_0(a_1) + r_1(a_1) & \ldots & \omega_{ip}r_0(a_{n-1}) + r_1(a_{n-1}) \\
\ldots & \ldots & \ldots & \ldots \\
\omega_{ip+j}r_0(a_0) + r_1(a_0) & \omega_{ip+j}r_0(a_1) + r_1(a_1) & \ldots & \omega_{ip+j}r_0(a_{n-1}) + r_1(a_{n-1}) \\
\ldots & \ldots & \ldots & \ldots \\
\omega_{ip+p-1}r_0(a_0) + r_1(a_0) & \omega_{ip+p-1}r_0(a_1) + r_1(a_1) & \ldots & \omega_{ip+p-1}r_0(a_{n-1}) + r_1(a_{n-1})
\end{pmatrix}.$$

Aplicando el corrimiento cíclico σ de longitud np al bloque $\mathcal{A}_i$ obtenemos:

$$\begin{pmatrix}
\omega_{ip+p-1}r_0(a_{n-1}) + r_1(a_{n-1}) & \omega_{ip}r_1(a_0) + r_1(a_0) & \ldots & \omega_{ip}r_0(a_{n-2}) + r_1(a_{n-2}) \\
\ldots & \ldots & \ldots & \ldots \\
\omega_{ip+j-1}r_0(a_{n-1}) + r_1(a_{n-1}) & \omega_{ip+j}r_0(a_0) + r_1(a_0) & \ldots & \omega_{ip+j}r_0(a_{n-2}) + r_1(a_{n-2}) \\
\ldots & \ldots & \ldots & \ldots \\
\omega_{ip+p-2}r_0(a_{n-1}) + r_1(a_{n-1}) & \omega_{ip+p-1}r_0(a_0) + r_1(a_0) & \ldots & \omega_{ip+p-1}r_0(a_{n-2}) + r_1(a_{n-2})
\end{pmatrix}$$

Entonces el j-ésimo bloque de longitud n de $\sigma(\mathcal{A}_i)$ es:

$$[\omega_{ip+j-1}r_0(a_{n-1}) + r_1(a_{n-1}), \omega_{ip+j}r_0(a_0) + r_1(a_0), \ldots \\ \ldots, \omega_{ip+j}r_0(a_{n-2}) + r_1(a_{n-2})] \tag{4.5}$$

A partir de las relaciones (4.4) y (4.5) concluimos que el j-ésimo bloque de longitud n de $\mathcal{B}_i$ es igual al j-ésimo bloque de longitud n de $\sigma(\mathcal{A}_i)$ y por consiguiente, $\mathcal{B}_i = \sigma(\mathcal{A}_i)$ para cada $i = 0, \ldots, p^{m-1} - 1$. Como tenemos que $\sigma^{\otimes p^{m-1}}(\Phi(\mathbf{A})) = (\sigma(\mathcal{A}_0)|\cdots|\sigma(\mathcal{A}_i)|\cdots\cdots|\sigma(\mathcal{A}_{p^{m-1}-1}))$, donde "|" significa concatenación y puesto que $\Phi(\nu_\lambda(\mathbf{A})) = \Phi(\mathbf{B}) = (\mathcal{B}_0|\cdots|\mathcal{B}_i|\cdots|\mathcal{B}_{p^{m-1}-1})$ la afirmación de la Proposición se sigue. □

Teorema 4.1. *Un $\mathcal{R}$-código $\mathcal{C}$ de longitud n es $\lambda = (1-p)$-cíclico si y sólo si su imagen de Gray $\Phi(\mathcal{C})$ es un código cuasi-cíclico sobre F_{p^m} de índice p^{m-1} y longitud np^m.*

Demostración. Sea $\mathcal{C} \subseteq \mathcal{R}^n$ un código tal que $\Phi(\mathcal{C})$ es cuasi-cíclico, de la Proposición 4.1 se implica que

$$\Phi(\mathcal{C}) = \sigma^{\otimes p^{m-1}}(\Phi(\mathcal{C})) = \Phi(\nu_\lambda(\mathcal{C}))$$

y la afirmación se sigue de la inyectividad del mapeo de Gray. El recíproco también es inmediato de la Proposición 4.1. □

Este resultado generaliza el que aparece en [Wol99] y [LB02].

4.2 IMÁGENES DE GRAY DE CÓDIGOS CÍCLICOS LINEALES

Sea $n \in \mathrm{N}$ tal que $(n,p) = 1$ y n' su inverso, i.e., $nn' \equiv 1 \bmod p$. Sea $N' \in \mathcal{T}$ tal que $\mu(N') = n'$, sea $\gamma = 1 + N'p \in 1 + \mathcal{M}$ y $\lambda = 1 - p$ su inverso (cuando así sucede).

Nótese que $\gamma^k = \rho_0(\gamma^k) + p\rho_1(\gamma^k)$ donde $\rho_0(\gamma^k), \rho_1(\gamma^k) \in \mathcal{T}$ son tales que $\rho_0(\gamma^k) = \rho_0(\gamma) = 1$ y $r_1(\gamma^k) = \mu(\rho_1(\gamma^k)) = kn'$, en particular, $\gamma^n = 1 + p\rho_1(\gamma^n)$ con $r_1(\gamma^n) = nn' = 1$.

Sea $a \in \mathcal{R}$. Entonces $\gamma^i a = \rho_0(\gamma^i a) + p\rho_1(\gamma^i a)$ donde $\rho_0(\gamma^i a)$, $\rho_1(\gamma^i a) \in \mathcal{T}$ y $\rho_0(\gamma^i a) = \rho_0(a)$ con

$$r_0(\gamma^i a) = r_0(a) \tag{4.6}$$

y

$$\begin{aligned} r_1(\gamma^i a) &= r_1(a) + r_1(\gamma^i)\, r_0(a) = r_1(a) + i\mu(N')r_0(a) \\ &= r_1(a) + (in')_p r_0(a). \end{aligned} \tag{4.7}$$

Sea $\mathcal{A}_n = \mathcal{R}[x]/\langle x^n - 1\rangle$, $\mathcal{B}_n = \mathcal{R}[x]/\langle x^n - \lambda\rangle$ y sean

$$\begin{aligned} P : \mathcal{R}^n &\longrightarrow \mathcal{A}_n, \\ (a_0, a_1, ..., a_{n-1}) &\longrightarrow a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle \end{aligned}$$

$$\begin{aligned} P' : \mathcal{R}^n &\longrightarrow \mathcal{B}_n, \\ (b_0, b_1, ..., b_{n-1}) &\longrightarrow b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} + \langle x^n - \lambda\rangle \end{aligned}$$

los mapeos representación polinomial de $\mathcal{R}^n$ en los anillos $\mathcal{A}_n$ y $\mathcal{B}_n$, respectivamente.

Con la notación anterior, definimos los mapeos siguientes:

i) $\mu_\gamma : \mathcal{A}_n \longrightarrow \mathcal{B}_n$, $\mu_\gamma(A(x)) = A(\gamma x)$

ii) $\chi_\gamma : \mathcal{R}^n \longrightarrow \mathcal{R}^n$, $\chi_\gamma(\mathbf{A}) = (a_0, ..., \gamma^k a_k, ..., \gamma^{n-1}a_{n-1})$ donde $\mathbf{A} = (a_0, ..., a_{n-1})$.

Las afirmaciones siguientes son fáciles de probar a partir de las definiciones:

i) μ_γ es un isomorfismo de anillos y en particular I es un ideal de $\mathcal{A}_n$ si y sólo si $\mu_\gamma(I)$ es un ideal de $\mathcal{B}_n$.

ii) Un código $\mathcal{C} \subset \mathcal{R}^n$ es un cíclico lineal si y sólo si $P(\mathcal{C})$ es un ideal de $\mathcal{A}_n$.

iii) Un código $\mathcal{C} \subset \mathcal{R}^n$ es lineal λ-cíclico si y sólo si $P'(\mathcal{C})$ es un ideal de $\mathcal{B}_n$.

iv) $\mu_\gamma \circ P = P' \circ \chi_\gamma$.

Definición 4.2. *Un código $\mathcal{C} \subseteq \mathcal{R}^n$ se dice γ-cíclico if $\chi_\gamma(\mathcal{C}) = \mathcal{C}$.*

Proposición 4.2. *Sea $\mathcal{C} \subseteq \mathcal{R}^n$ un código de longitud n primo relativo con p. Entonces $\mathcal{C}$ es un código cíclico lineal si y sólo si $\chi_\gamma(\mathcal{C})$ es un código lineal λ-cíclico.*

Demostración. $\mathcal{C}$ es un código cíclico lineal sobre $\mathcal{R} \Leftrightarrow P(\mathcal{C})$ es un ideal de $\mathcal{A}_n \Leftrightarrow \mu_\gamma(P(\mathcal{C}))$ es un ideal de $\mathcal{B}_n \Leftrightarrow P'(\chi_\gamma(\mathcal{C}))$ es un ideal de $\mathcal{B}_n \Leftrightarrow \chi_\gamma(\mathcal{C})$ es un código lineal λ-cíclico sobre $\mathcal{R}$. □

La definición siguiente es parecida a la que aparece en [LB02] para el primo $p \neq 2$ y es una generalización de la enunciada en [Wol01] para el primo $p = 2$, pero es un caso particular de la permutación global de Nechaev (A.1) que se introduce en el Apéndice.

Sea $n \in \mathbb{N}$ tal que $(n, p) = 1$ y sea n' su inverso, i.e., $nn' \equiv 1 \bmod p$.

Definición 4.3. *Sea π la permutación en $\{0, 1, \ldots, np-1\}$ dada por:*

$$\pi(v) = \left((vn' - u)_p n + v\right)_{np}.$$

donde $0 \leqslant u \leqslant p-1$ y $un \leqslant v \leqslant (u+1)n-1$

Una generalización de la permutación de Nechaev en $\mathbb{F}_q^{np}$ es la siguiente:

$$\Pi(c_0, c_1, \ldots, c_v, \ldots, c_{np-1}) = (c_{\pi(0)}, c_{\pi(1)}, \ldots, c_{\pi(v)}, \ldots, c_{\pi(np-1)}).$$

Ejemplo 4.1. *Sean $n = 4$, $p = 3$ y sea n' en $\{1, 2\}$ tal que $nn' \equiv 1 \bmod p$, i.e., $n' = 1$ y sea σ el corrimiento cíclico usual de longitup p.*

Considérese el arreglo

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \end{array}$$

Si en la segunda columa aplicamos $\sigma^{(1n')_p} = \sigma$ (ésto significa corrimiento cíclico ("hacia arriba") $(1n')_p$ lugares, donde $(*)_p$ denota reducción módulo p) y en la tercera columa aplicamos $\sigma^{(2n')_p} = \sigma^2$ (ésto significa corrimiento cíclico (hacia arriba) $(2n')_p$ lugares), i.e., aplicando el corrimiento cíclico indicado en cada columna como se ilustra a continuación,

$$\begin{array}{cccc} \sigma^{(0n')_p} & \sigma^{(1n')_p} & \sigma^{(2n')_p} & \sigma^{(3n')_p} \\ 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \end{array}$$

obtenemos,

$$\begin{matrix} 0 & 5 & 10 & 3 \\ 4 & 9 & 2 & 7 \\ 8 & 1 & 6 & 11 \end{matrix}$$

Si concatenamos las tres filas en el arreglo previo, obtenemos la permutación:

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 0 & 5 & 10 & 3 & 4 & 9 & 2 & 7 & 8 & 1 & 6 & 11 \end{pmatrix}$$

Por consiguiente, $\pi : \{0, 1, \ldots, 11\} \to \{0, 1, \ldots, 11\}$ *es la permutación dada por (4.3) con los parámetros indicados.*

Una extensión de Π puede ser dada en la forma siguiente:

Definición 4.4. *Para cualquier entero positivo* t *sea*

$$\Pi^{\otimes t} : F_q^{npt} \longrightarrow F_q^{npt}$$

la permutación definida como

$$\Pi^{\otimes t}(\mathbf{a}^{(1)}|\mathbf{a}^{(2)}|\cdots|\mathbf{a}^{(t)}) = (\Pi(\mathbf{a}^{(1)})|\Pi(\mathbf{a}^{(2)})|\cdots|\Pi(\mathbf{a}^{(t)}))$$

donde $\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(t)} \in F_q^{np}$ *y* $\Pi : F_q^{np} \longrightarrow F_q^{np}$ *es como se definió anteriormente. En particular,* $\Pi^{\otimes 1} = \Pi$.

Proposición 4.3. *Para cualquier* $\mathbf{A} = (a_0, \ldots\ldots, a_{n-1}) \in \mathcal{R}^n$ *la relación siguiente se satisface*

$$\Phi\left(\chi_\gamma(\mathbf{A})\right) = \Pi^{\otimes p^{m-1}}\left(\Phi(\mathbf{A})\right). \tag{4.8}$$

Demostración. Sea $\mathbf{A} = (a_0, ..., a_{n-1}) \in \mathcal{R}^n$ y sea $\mathbf{D} = \chi_\gamma(\mathbf{A})$ tal que

$$(D_0, D_1, \ldots, D_{n-1}) = (a_0, \ldots, \gamma^k a_k, \ldots, \gamma^{n-1} a_{n-1}).$$

Entonces,

$$\begin{aligned} \Phi(\chi_\gamma(\mathbf{A})) = \Phi(\mathbf{D}) &= \mathbf{c_0} \otimes r_0(\mathbf{D}) + \mathbf{c_1} \otimes r_1(\mathbf{D}) \\ &= [\Omega_0, \ldots, \Omega_i, \ldots, \Omega_{p^{m-1}-1}] \otimes r_0(\mathbf{D}) + [\underline{1}_p, \ldots, \underline{1}_p, \ldots, \underline{1}_p] \otimes r_1(\mathbf{D}) \\ &= [, \ldots, \Omega_i \otimes r_0(\mathbf{D}) + \underline{1}_p \otimes r_1(\mathbf{D}), \ldots,] \end{aligned}$$

Sea $\mathcal{D}_i = \Omega_i \otimes r_0(\mathbf{D}) + \underline{1}_p \otimes r_1(\mathbf{D})$ el i-ésimo bloque de longitud np del vector $\Phi(\mathbf{D})$ para $i = 0, \ldots, p^{m-1} - 1$.

Entonces,

$$\begin{aligned} \mathcal{D}_i &= [\omega_{ip}, \ldots, \omega_{ip+j}, \ldots, \omega_{ip+p-1}] \otimes r_0(\mathbf{D}) + [1, \ldots, 1, \ldots, 1] \otimes r_1(\mathbf{D}) \\ &= [\omega_{ip} r_0(\mathbf{D}) + r_1(\mathbf{D}), \ldots, \omega_{ip+j} r_0(\mathbf{D}) + r_1(\mathbf{D}), \ldots, \omega_{ip+p-1} r_0(\mathbf{D}) + r_1(\mathbf{D})] \end{aligned}$$

Sea $\omega_{ip+j} r_0(\mathbf{D}) + r_1(\mathbf{D})$ el j-ésimo bloque de longitud n de $\mathcal{D}_i$, $j = 0, \ldots, p-1$, i.e.,

$$\begin{aligned}
&\omega_{ip+j} r_0(\mathbf{D}) + r_1(\mathbf{D}) \\
&= [\omega_{ip+j} r_0(D_0) + r_1(D_0), \ldots, \omega_{ip+j} r_0(D_k) + r_1(D_k), \ldots, \\
&\quad \ldots, \omega_{ip+j} r_0(D_{n-1}) + r_1(D_{n-1})] \\
&= [\omega_{ip+j} r_0(a_0) + r_1(a_0), \ldots, \omega_{ip+j} r_0(\gamma^k a_k) + r_1(\gamma^k a_k), \ldots \\
&\quad \ldots, \omega_{ip+j} r_0(\gamma^{n-1} a_{n-1}) + r_1(\gamma^{n-1} a_{n-1})]
\end{aligned}$$

Aplicando las relaciones (4.6) y (4.7) a $\omega_{ip+j} r_0(\mathbf{D}) + r_1(\mathbf{D})$ obtenemos:

$$[\omega_{ip+j} r_0(a_0) + r_1(a_0), \ldots, \omega_{ip+j} r_0(a_k) + r_1(a_k) + (kn')_p r_0(a_k), \ldots \\ \ldots, \omega_{ip+j} r_0(a_{n-1}) + r_1(a_{n-1}) + ((n-1)n')_p r_0(a_{n-1})],$$

i.e.,

$$[\omega_{ip+j} r_0(a_0) + r_1(a_0), \ldots, (\omega_{ip+j} + (kn')_p) r_0(a_k) + r_1(a_k), \ldots \\ \ldots, (\omega_{ip+j} + ((n-1)n')_p) r_0(a_{n-1}) + r_1(a_{n-1})].$$

Entonces, el j-ésimo bloque de longitud n de $\mathcal{D}_i$, para $j = 0, \ldots, p-1$, es igual a:

$$[\omega_{ip+j} r_0(a_0) + r_1(a_0), \ldots, \omega_{ip+(j+kn')_p} r_0(a_k) + r_1(a_k), \ldots \\ \ldots, \omega_{ip+(j+(n-1)n')_p} r_0(a_{n-1}) + r_1(a_{n-1})]. \quad (4.9)$$

Por otro lado, el i-ésimo bloque de longitud np del vector $\Phi(\mathbf{A})$, para cada $i = 0, \ldots, p^{m-1} - 1$ es:

$$\begin{aligned}
\mathcal{A}_i &= \Omega_i \otimes r_0(\mathbf{A}) + \underline{1}_p \otimes r_1(\mathbf{A}) \\
&= [\omega_{ip} r_0(\mathbf{A}) + r_1(\mathbf{A}), \ldots, \omega_{ip+j} r_0(\mathbf{A}) + r_1(\mathbf{A}), \ldots \\
&\quad \ldots, \omega_{ip+p-1} r_0(\mathbf{A}) + r_1(\mathbf{A})]
\end{aligned}$$

Este bloque $\mathcal{A}_i$ puede ser visto como la concatenación de las filas del siguiente arreglo de tamaño pn:

$$\begin{pmatrix}
\omega_{ip} r_0(a_0) + r_1(a_0) & \ldots & \omega_{ip} r_0(a_k) + r_1(a_k) & \ldots & \omega_{ip} r_0(a_{n-1}) + r_1(a_{n-1}) \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
\omega_{ip+j} r_0(a_0) + r_1(a_0) & \ldots & \omega_{ip+j} e r_0(a_k) + r_1(a_k) & \ldots & \omega_{ip+j} r_0(a_{n-1}) + r_1(a_{n-1}) \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
\omega_{ip+p-1} r_0(a_0) + r_1(a_0) & \ldots & \omega_{ip+p-1} r_0(a_k) + r_1(a_k) & \ldots & \omega_{ip+p-1} r_0(a_{n-1}) + r_1(a_{n-1})
\end{pmatrix}$$

Aplicando la permutación Π al bloque $\mathcal{A}_i$, ésto significa aplicar $\sigma^{(kn')_p}$ a la k-ésima columna del arreglo previo, para cada $k = 0, \ldots, n-1$, i.e., aplicando el corrimiento cíclico moviendo ("hacia arriba") $(kn')_p$ lugares de manera que la k-ésima columna del arreglo $\Pi(\mathcal{A}_i)$ se convierte en:

$$\begin{pmatrix}
\omega_{ip+(kn')_p} r_0(a_k) + r_1(a_k) \\
\vdots \\
\omega_{ip+(j+kn')_p} r_0(a_k) + r_1(a_k) \\
\vdots \\
\omega_{ip+(p-1+kn')_p} r_0(a_k) + r_1(a_k)
\end{pmatrix}$$

para cada $k = 0, \ldots, n-1$.

Por consiguiente, la j-ésima fila de longitud n de $\Pi(\mathcal{A}_i)$, para $j = 0, \ldots, p-1$, es igual a

$$[\omega_{ip+j} r_0(a_0) + r_1(a_0) \ldots \omega_{ip+(j+kn')_p} r_0(a_k) + r_1(a_k) \ldots \\ \ldots \omega_{ip+(j+(n-1)n')_p} r_0(a_{n-1}) + r_1(a_{n-1})]. \tag{4.10}$$

La expresión dada en (4.10) es el j-ésimo bloque de longitud n de $\Pi(\mathcal{A}_i)$ y de (4.9) concluimos que es el j-ésimo bloque de longitud n de $\mathcal{D}_i$ para $j = 0, \ldots, p-1$. Por lo tanto, $\mathcal{D}_i = \Pi(\mathcal{A}_i)$ para $i = 0, \ldots, p^{m-1} - 1$ y como $\Pi^{\otimes p^{m-1}}(\Phi(\mathbf{A})) = (\Pi(\mathcal{A}_0)| \cdots |\Pi(\mathcal{A}_i)| \cdots \cdots |\Pi(\mathcal{A}_{p^{m-1}-1}))$ y $\Phi(\chi_\gamma(\mathbf{A})) = \Phi(\mathbf{D}) = (\mathcal{D}_0| \cdots |\mathcal{D}_i| \cdots |\mathcal{D}_{p^{m-1}-1})$, se sigue la afirmación. □

El resultado siguiente es una consecuencia inmediata de la Proposición 4.2, del Teorema 4.1 y la Proposición 4.3.

Teorema 4.2. *Sea $\mathcal{C} \subseteq \mathcal{R}^n$ un código de longitud n primo relativo con p. Entonces el código $\mathcal{C}$ es cíclico lineal si y sólo si $\Pi^{\otimes p^{m-1}}(\Phi(\mathcal{C}))$ es un código cuasi-cíclico de índice p^{m-1} y longitud np^m sobre F.*

Demostración. $\mathcal{C}$ es un código cíclico lineal sobre $\mathcal{R} \Leftrightarrow \chi_\gamma(\mathcal{C})$ es un código lineal $\lambda = (1-p)$-cíclico $\Leftrightarrow \Phi(\chi_\gamma(\mathcal{C}))$ es un código cuasi-cíclico sobre F_{p^m} de índice p^{m-1} y longitud $np^m \Leftrightarrow \Pi^{\otimes p^{m-1}}(\Phi(\mathcal{C}))$ es un código cuasi-cíclico sobre F_{p^m} de índice p^{m-1} y longitud np^m. □

Este resultado generaliza el que aparece en [LB02] para códigos sobre el anillo $\mathbb{Z}_{p^2}$.

5 IMÁGENES DE GRAY CÍCLICAS LINEALES

En éste capítulo $\mathcal{R}$ denota un anillo finito de cadena (AFC) de índice de nilpotencia 2, π es un generador fijo del ideal maximal $\mathcal{M}$ de $\mathcal{R}$, $\mathcal{T}$ es el conjunto de Teichmüller de $\mathcal{R}$, F es el campo residual de $\mathcal{R}$, el cual es isomorfo a F_q, donde $q = p^m$ para algún primo p y un entero $m \geqslant 1$, y además n es un entero positivo que no es divisible por p. Se considera el mapeo de Gray definido sobre $\mathcal{R}$ y se introduce la representación polinomial de $\Phi(A)$, donde $A \in \mathcal{R}^n$, también se obtiene un teorema que caracteriza al polinomio generador de un $\mathcal{R}$-código cíclico lineal de longitud n primo relativo con la característica del campo residual y finalmente se da un teorema que establece la ciclicidad lineal de la imagen de Gray de una clase de $\mathcal{R}$-códigos cíclicos lineales cuyo polinomio generador es de la forma $\pi A(\xi)$, donde $A(\xi)|\xi^n - 1$.

5.1 LA REPRESENTACIÓN POLINOMIAL DEL MAPEO DE GRAY

Sea $F = \{0, \omega^0, ..., \omega^{q-2}\}$ el campo residual del anillo $\mathcal{R}$, donde ω es un elemento primitivo, sea $u = (0, 1, ..., \omega^{q-2})$ el vector que enlista a todos los elementos de F en el orden dado y sea $v = 1_q$ el vector cuyas entradas son todas iguales a 1 de longitud q. Sea a un elemento cualesquiera de $\mathcal{R}$ cuya representación π-ádica es: $a = \rho_0(a) + \rho_1(a)\pi$ donde $\rho_0(a), \rho_1(a) \in \mathcal{T}$ y sea $r_i(a) = \mu(\rho_i(a))$, $i = 0, 1$.

Como el índice de nilpotencia de $\mathcal{R}$ es 2, la imagen de Gray de $A = (a_0, a_1, \ldots a_{n-1}) \in \mathcal{R}^n$ es:

$$\Phi(A) = C_0 \otimes r_0(A) + C_1 \otimes r_1(A) \tag{5.1}$$

donde $r_j(A) = (r_j(a_0), r_j(a_1), \ldots, r_j(a_{n-1}))$, $j = 0, 1$, $C_0 = u$ y $C_1 = v$.

Sea

$$b_j(a_k) = \begin{cases} r_1(a_k), & \text{para } j = k \text{ y } k = \overline{0, n-1}, \\ \omega^{s-1} r_0(a_k) + r_1(a_k), & \text{para } j = sn + k,\ s = \overline{1, q-1},\ k = \overline{0, n-1}. \end{cases}$$

Entonces,

$$\Phi(A) = (\ldots, b_j(a_k), \ldots) \in F^{qn}.$$

Sea $\mathcal{S}$ un anillo finito conmutativo, $\mathcal{A}(t) = \mathcal{S}[\xi]/\langle \xi^t - 1 \rangle$ y

$$\begin{aligned} \mathcal{P} : \mathcal{S}^t &\longrightarrow \mathcal{A}(t), \\ (a_0, a_1, ..., a_{t-1}) &\longrightarrow a_0 + a_1\xi + \cdots + a_{t-1}\xi^{t-1} + \langle \xi^t - 1 \rangle \end{aligned}$$

el mapeo representación polinomial de $\mathcal{S}^t$ en el anillo $\mathcal{A}(t)$, abusando de la notación, se suele denotar $\mathcal{P}(a_0, a_1, ..., a_{t-1}) = a_0 + a_1\xi + \cdots + a_{t-1}\xi^{t-1}$ en lugar de $\mathcal{P}(a_0, a_1, ..., a_{t-1}) = a_0 + a_1\xi + \cdots + a_{t-1}\xi^{t-1} + \langle \xi^t - 1 \rangle$.

Se denota $\mathcal{A}_{\mathcal{R}}(t)$ si $\mathcal{S} = \mathcal{R}$ y $\mathcal{A}_F(t)$ si $\mathcal{S} = F$. Además $\mathcal{P}_F^t$ y $\mathcal{P}_{\mathcal{R}}^t$ denotan respectivamente, las representaciones polinomiales de F^t y $\mathcal{R}^t$.

Definición 5.1. *El mapeo polinomial de Gray es el mapeo $\Phi_{\mathcal{P}}$ de $\mathcal{A}_{\mathcal{R}}(n)$ a $\mathcal{A}_F(qn)$ definido por*

$$\Phi_{\mathcal{P}} = \mathcal{P}_F^{qn}\Phi(\mathcal{P}_{\mathcal{R}}^n)^{-1}$$

Si $A(\xi)$ es la representación polinomial en $\mathcal{A}_{\mathcal{R}}(n)$ de A entonces $\Phi_{\mathcal{P}}(A(\xi))$ es la representación polinomial en $\mathcal{A}_F(qn)$ de $\Phi(A)$.

La representación polinomial de $\Phi(A)$ en $\mathcal{A}_F(qn)$ está dada por:

$$\Phi_{\mathcal{P}}(A(\xi)) = \sum_{s=0}^{q-1}\sum_{k=0}^{n-1} b_{sn+k}(a_k)\xi^{sn+k}. \tag{5.2}$$

Para $s \in \{0, 1, \ldots, q-1\}$ sea $f_s(\xi) = \sum_{k=0}^{n-1} b_{sn+k}(a_k)\xi^k$ entonces

$$\Phi_{\mathcal{P}}(A(\xi)) = \sum_{s=0}^{q-1} f_s(\xi)\xi^{sn}.$$

Las siguientes identidades son fáciles de probar y serán útiles más adelante

Lema 5.1. *Para $q = p^m$, en $F_q[\xi]$ se cumplen las siguientes relaciones:*

i) $1 + \xi^n + \xi^{2n} + \cdots + \xi^{(p^m-1)n} = (\xi^{p^m n} - 1)/(\xi^n - 1) = (\xi^n - 1)^{p^m-1}$,

ii) $\xi^n + \omega\xi^{2n} + \ldots + \omega^{p^m-2}\xi^{(p^m-1)n} = \omega^{p^m-2}\xi^n \prod_{i=0}^{p^m-2}(\xi^n - \omega^i)$.

Sea $A(\xi) = a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1}$ en $\mathcal{A}_{\mathcal{R}}(n)$ la representación polinomial de $A = (a_0, \ldots, a_{n-1})$, dado que, $a_i = \rho_0(a_i) + \pi\rho_1(a_i)$, donde $\rho_0(a_i)$, $\rho_1(a_i) \in \mathcal{T}$ para cada $i \in \{0, 1, \ldots, n-1\}$ entonces

$$\begin{aligned} A(\xi) &= (\rho_0(a_0) + \pi\rho_1(a_0)) + (\rho_0(a_1) + \pi\rho_1(a_1))\xi + \cdots \\ &\quad \cdots + (\rho_0(a_{n-1}) + \pi\rho_1(a_{n-1}))\xi^{n-1} \\ &= (\rho_0(a_0) + \rho_0(a_1)\xi + \cdots + \rho_0(a_{n-1})\xi^{n-1}) + \\ &\quad \pi(\rho_1(a_0) + \rho_1(a_1)\xi + \cdots + \rho_1(a_{n-1})\xi^{n-1}) \\ &= \rho_0(A)(\xi) + \pi\rho_1(A)(\xi) \end{aligned}$$

donde $\rho_0(A)(\xi)$ y $\rho_1(A)(\xi)$ son las representaciones polinomiales en $\mathcal{A}_{\mathcal{R}}(n)$ de

$$\begin{aligned} \rho_0(A) &= (\rho_0(a_0), \rho_0(a_1), \ldots, \rho_0(a_{n-1})) \text{ y} \\ \rho_1(A) &= (\rho_1(a_0), \rho_1(a_1), \ldots, \rho_1(a_{n-1})) \end{aligned}$$

respectivamente.

Proposición 5.1. *Si* $A(\xi) = \rho_0(A)(\xi) + \pi\rho_1(A)(\xi)$. *Entonces*

$$\Phi_{\mathcal{P}}(A(\xi)) = r_0(A)(\xi)\omega^{p^m-2}\xi^n \prod_{i=0}^{p^m-2}(\xi^n - \omega^i) + r_1(A)(\xi)(\xi^n - 1)^{p^m-1}$$

donde $r_0(A)(\xi)$, $r_1(A)(\xi)$ *están en* $\mathcal{A}_F(n)$ *y son las representaciones polinomiales de* $r_0(A) = (r_0(a_0), r_0(a_1), \ldots, r_0(a_{n-1}))$ *y* $r_1(A) = (r_1(a_0), r_1(a_1), \ldots\ldots, r_1(a_{n-1}))$ *respectivamente. Más aún,* $r_0(A)(\xi)$ *y* $r_1(A)(\xi)$ *son las* μ*-reducciones de* $\rho_0(A)(\xi)$ *y* $\rho_1(A)(\xi)$ *respectivamente.*

Demostración. Reagrupando los términos del polinomio (5.2) obtenemos

$$\begin{aligned}
&\Phi_{\mathcal{P}}(A(\xi)) \\
&= \left[r_0(a_0)\sum_{i=0}^{p^m-2}\omega^i\xi^{(i+1)n}\right] + \left[r_0(a_1)\sum_{i=0}^{p^m-2}\omega^i\xi^{(i+1)n}\right]\xi + \cdots \\
&\quad + \cdots\left[r_0(a_{n-1})\sum_{i=0}^{p^m-2}\omega^i\xi^{(i+1)n}\right]\xi^{n-1} \\
&\quad + \left[r_1(a_0)\sum_{i=0}^{p^m-1}\xi^{in}\right] + \left[r_1(a_1)\sum_{i=0}^{p^m-1}\xi^{in}\right]\xi + \cdots \\
&\quad + \cdots\left[r_1(a_{n-1})\sum_{i=0}^{p^m-1}\xi^{in}\right]\xi^{n-1} \\
&= \left[\sum_{i=0}^{n-1} r_0(a_i)\xi^i\right]\left[\sum_{i=0}^{p^m-2}\omega^i\xi^{(i+1)n}\right] + \left[\sum_{i=0}^{n-1} r_1(a_i)\xi^i\right]\left[\sum_{i=0}^{p^m-1}\xi^{in}\right] \\
&= \left[\sum_{i=0}^{n-1} r_0(a_i)\xi^i\right]\left[\omega^{p^m-2}\xi^n\prod_{i=0}^{p^m-2}(\xi^n - \omega^i)\right] \\
&\quad + \left[\sum_{i=0}^{n-1} r_1(a_i)\xi^i\right]\left[(\xi^n-1)^{p^m-1}\right], \\
&= r_0(A)(\xi)\omega^{p^m-2}\xi^n\prod_{i=0}^{p^m-2}(\xi^n - \omega^i) + r_1(A)(\xi)(\xi^n-1)^{p^m-1}
\end{aligned}$$

de lo cual se sigue la afirmación. □

Este resultado generaliza el inciso c) de la Proposición 12 de [Wol01].

Lema 5.2. *Sea* $H = (h_0, h_1, \ldots, h_{n-1})$ *un elemento cualquiera en* $\mathcal{R}^n$, $H(\xi)$ *en* $\mathcal{A}_{\mathcal{R}}(n)$ *la correspondiente representación polinomial de* H *y* $h(\xi)$ *en* $\mathcal{A}_F(n)$ *su* μ*-reducción. Si* $\Phi_{\mathcal{P}}(\pi H(\xi))$ *en* $\mathcal{A}_F(qn)$ *es la representación polinomial de* $\Phi(\pi H)$ *entonces*

$$\Phi_{\mathcal{P}}(\pi H(\xi)) = h(\xi)(\xi^n - 1)^{p^m-1}$$

Demostración. Sea $H = (h_0, h_1, \ldots, h_{n-1}) \in \mathcal{R}^n$ donde

$$h_i = \rho_0(h_i) + \pi\rho_1(h_i) \in \mathcal{R},\ \rho_0(h_i), \rho_1(h_i) \in \mathcal{T},$$

entonces

$$\begin{aligned} \pi H &= (\pi h_0, \ldots, \pi h_{n-1}) \\ &= (\pi(\rho_0(h_0) + \pi\rho_1(h_0)), \ldots, \pi(\rho_0(h_{n-1}) + \pi\rho_1(h_{n-1}))) \\ &= (0 + \pi\rho_0(h_0), \ldots, 0 + \pi\rho_0(h_{n-1})) \end{aligned}$$

Aplicando la Proposición 5.1 a πH tenemos:

$$\begin{aligned} \Phi_{\mathcal{P}}(\pi H)(\xi) &= \left[\sum_{i=0}^{n-1} r_1(\pi h_i)\xi^i\right]\left[(\xi^n - 1)^{p^m-1}\right] \\ &= \left[\sum_{i=0}^{n-1} r_0(h_i)\xi^i\right]\left[(\xi^n - 1)^{p^m-1}\right] \\ &= h(\xi)(\xi^n - 1)^{p^m-1} \end{aligned}$$

donde $h(\xi) := \mu(H(\xi)) = \sum_{i=0}^{n-1} r_0(h_i)\xi^i$, y la afirmación se sigue. □

5.2 $\mathcal{R}$-CÓDIGOS CÍCLICOS LINEALES

En ésta sección consideramos códigos cíclicos lineales de longitud n sobre un anillo finito de cadena $\mathcal{R}$ cuyo único ideal maximal es generado por π, i.e., $\mathcal{M} = \langle\pi\rangle$ y $t \geqslant 2$ es el índice de nilpotencia de π.

Sea el anillo $\mathcal{A}_n = \mathcal{R}[x]/\langle x^n - 1\rangle$ y sea

$$\begin{aligned} \mathcal{P} : \mathcal{R}^n &\longrightarrow \mathcal{A}_n, \\ (a_0, a_1, ..., a_{n-1}) &\longrightarrow a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle \end{aligned}$$

el mapeo representación polinomial de $\mathcal{R}^n$ en el anillo $\mathcal{A}_n$.

La siguiente proposición es la análoga de un resultado conocido para los códigos cíclicos lineales sobre campos finitos (cf. [MS77, Sec. 7.2]) la demostración es básicamente la misma que para el caso de campos por éso se omite.

Proposición 5.2. *Con la notación anterior, $\mathcal{C} \subseteq \mathcal{R}^n$ es un código cíclico lineal si y sólo si $\mathcal{P}(\mathcal{C})$ es un ideal de $\mathcal{A}_n$*

Abusando de la terminología cuando nos referimos a un $\mathcal{R}$-código cíclico lineal $\mathcal{C}$ podemos pensar indistintamente en un $\mathcal{R}$-submódulo de $\mathcal{R}^n$ ó en un ideal de $\mathcal{A}_n$.

A continuación se enuncian un par de resultados cuya demostración se puede consultar en [DLP04].

Teorema 5.1. *[DLP04, Teorema 3.4] Sea $\mathcal{C}$ un código cíclico lineal de longitud n sobre un anillo finito de cadena $\mathcal{R}$. Entonces existe una única familia de polinomios mónicos coprimos por parejas $F_0, F_1, \ldots, F_t$ en $\mathcal{R}[\xi]$ tales que $F_0F_1 \cdots F_t = \xi^n - 1$ y $\mathcal{C} = \langle \hat{F_1}, \pi\hat{F_2}, \ldots, \pi^{t-1}\hat{F_t} \rangle$, donde $\hat{F_i} = (\xi^n - 1)/F_i = \prod_{j \neq i} F_j$, para $1 \leqslant i \leqslant t$. Más aún*

$$|\mathcal{C}| = (|\mathcal{R}|)^{\sum_{i=0}^{t-1}(t-i)\deg(F_{i+1})}$$

Con la notación como en el Teorema 5.1 se tiene:

Teorema 5.2. *[DLP04, Teorema 3.6] Sea $\mathcal{C}$ un código cíclico lineal de longitud n y $F = \hat{F_1} + \pi\hat{F_2} + \ldots + \pi^{t-1}\hat{F_t}$. Entonces $\mathcal{C} = \langle F \rangle$.*

Usando éstos dos resultados para un anillo finito de cadena $\mathcal{R}$ de índice de nilpotencia $t = 2$ se prueba el siguiente resultado:

Teorema 5.3. *Supóngase que n es un entero positivo que no es divisible por p y sea $\mathcal{C}$ un $\mathcal{R}$-código cíclico lineal de longitud n. Entonces existe una única familia de polinomios mónicos coprimos por pareja $A(\xi), B(\xi), C(\xi)$ en $\mathcal{R}[\xi]$ tales que $A(\xi)B(\xi)C(\xi) = \xi^n - 1$ y $\mathcal{C} = \langle A(\xi)(B(\xi) + \pi) \rangle$ en $\mathcal{R}[\xi]/\langle \xi^n - 1 \rangle$.*

Demostración. Sea I un ideal no trivial de $\mathcal{A}(n) = \mathcal{R}[\xi]/\langle \xi^n - 1 \rangle$. Por el Teorema 5.1, existe una única familia de polinomios mónicos coprimos por parejas $A(\xi), B(\xi), C(\xi)$ en $\mathcal{R}[\xi]$ tales que $A(\xi)B(\xi)C(\xi) = \xi^n - 1$ en $\mathcal{R}[\xi]$ e $I = \langle \hat{C}(\xi), \pi\hat{B}(\xi) \rangle$ donde $\hat{B}(\xi) = A(\xi)C(\xi)$ y $\hat{C}(\xi) = A(\xi)B(\xi)$. Del Teorema 5.2 se tiene que $I = \langle \hat{C}(\xi) + \pi\hat{B}(\xi) \rangle$. Sea $J = \langle G(\xi) \rangle$ donde $G(\xi) = A(\xi)[B(\xi) + \pi]$. Se mostrará que $I = J$. Primero se verá que $I \supseteq J$, como $C(\xi)$ y $B(\xi)$ son polinomios coprimos por parejas existen $U(\xi), V(\xi) \in \mathcal{R}[\xi]$ tales que $U(\xi)C(\xi) + V(\xi)B(\xi) = 1$. Después de reducir módulo $(\xi^n - 1)$ se tiene una relación similar con $U(\xi)$ y $V(\xi)$ en $\mathcal{A}(n)$. Por consiguiente,

$$\pi U(\xi)A(\xi)C(\xi) + \pi V(\xi)A(\xi)B(\xi) = \pi A(\xi).$$

Entonces

$$\begin{aligned} & G(\xi) \\ &= A(\xi)[B(\xi) + \pi] = A(\xi)B(\xi) + \pi A(\xi) \\ &= A(\xi)B(\xi) + \pi U(\xi)A(\xi)C(\xi) + \pi V(\xi)A(\xi)B(\xi) \\ &= [\pi V(\xi) + 1][A(\xi)B(\xi)] + \pi U(\xi)A(\xi)C(\xi) \\ &= [\pi V(\xi) + 1]\hat{C}(\xi) + U(\xi)\pi\hat{B}(\xi), \end{aligned}$$

i.e.,

$$G(\xi) = [\pi V(\xi) + 1]\hat{C}(\xi) + U(\xi)\pi\hat{B}(\xi) \in I = \langle \hat{C}(\xi), \pi\hat{B}(\xi) \rangle,$$

de manera que $G(\xi) \in I$, por consiguiente, $J \subseteq I$.

Por otro lado, como $A(\xi)B(\xi)C(\xi) = \xi^n - 1$ en $\mathcal{R}[\xi]$ se tiene que $C(\xi)G(\xi) = A(\xi)B(\xi)C(\xi) + \pi A(\xi)C(\xi)$ en $\mathcal{R}[\xi]$, i.e.,

$$C(\xi)G(\xi) = \pi A(\xi)C(\xi) = \pi\hat{B}(\xi) \text{ in } \mathcal{A}(n) \tag{5.3}$$

También, se tiene en $\mathcal{A}(n)$ que:

$$\pi G(\xi) = \pi A(\xi)[B(\xi) + \pi] = \pi A(\xi)B(\xi) = \pi\hat{C}(\xi) \tag{5.4}$$

Así, por (5.3) y (5.4) se establece que $\pi\hat{B}(\xi)$ y $\pi\hat{C}(\xi)$ pertenece a J, por lo tanto,

$$\pi U(\xi)A(\xi)C(\xi) + \pi V(\xi)A(\xi)B(\xi) = \pi A(\xi),$$

i.e., $\pi U(\xi)\hat{B}(\xi) + \pi V(\xi)\hat{C}(\xi) = \pi A(\xi)$ lo cual implica que $\pi A(\xi) \in J$. Como $A(\xi)B(\xi) = G(\xi) - \pi A(\xi)$ se tiene que $A(\xi)B(\xi) = \hat{C}(\xi) \in J$. Por consiguiente $\hat{C}(\xi) + \pi\hat{B}(\xi) \in J$ mostrando que $I \subseteq J$ y por consiguiente $I = J$, por lo tanto, $G(\xi)$ es un generador de I. □

Si el polinomio generador $G(\xi)$ de un $\mathcal{R}$-código cíclico lineal $\mathcal{C}$ es como en el teorema anterior, se tienen los casos:

i) Si $C(\xi) = 1$ entonces $G(\xi) = \pi A(\xi)$.

ii) Si $A(\xi) = 1$ entonces $G(\xi) = B(\xi) + \pi$.

5.3 IMAGEN DE GRAY DE UNA CLASE DE CÓDIGOS CÍCLICOS LINEALES SOBRE $\mathcal{R}$

En esta sección se da un teorema que establece la ciclicidad lineal de la imagen de Gray de $\mathcal{R}$-códigos cíclicos lineales de la forma descrita en el inciso i) al final de la sección anterior.

Teorema 5.4. *Sea $\mathcal{C}$ un $\mathcal{R}$-código cíclico lineal de longitud n primo relativo con la característica del campo residual, generado por el polinomio $G(\xi) = \pi A(\xi)$ de grado r. Entonces $\Phi_{\mathcal{P}}(G(\xi)) = a(\xi)(\xi^n - 1)^{p^m - 1}$ donde $a(\xi) = \mu(A(\xi))$ y $\Phi_{\mathcal{P}}(G(\xi))$ divide a $\xi^{np^m} - 1$. Más aún, la imagen de Gray de $\mathcal{C}$, $\Phi(\mathcal{C})$, es un $[qn, n - r]$ código cíclico lineal sobre F_q.*

Demostración. Aplicando el Lema 5.2 al polinomio generador $G(\xi)$ del código $\mathcal{C}$, se sigue que,

$$\Phi_{\mathcal{P}}(G(\xi)) = a(\xi)(\xi^n - 1)^{p^m - 1}.$$

Además, como $A(\xi)$ divide a $\xi^n - 1$ en $\mathcal{R}[\xi]$ entonces $a(\xi)|(\xi^n - 1)$ en $F_q[\xi]$ y por lo tanto $\xi^n - 1 = a(\xi)q(\xi)$ para algún $q(\xi) \in F_q[\xi]$. Como, $\xi^{p^m n} - 1 = (\xi^n - 1)(\xi^n - 1)^{p^m - 1} = a(\xi))q(\xi)(\xi^n - 1)^{p^m - 1}$, i.e., $\xi^{p^m n} - 1 = \Phi_{\mathcal{P}}(G(\xi))q(\xi)$ se sigue que $\Phi_{\mathcal{P}}(G(\xi))$ divide a $\xi^{p^m n} - 1$ en $F_q[\xi]$. En consecuencia, el polinomio $\Phi_{\mathcal{P}}(G(\xi))$ genera un F_q-código cíclico lineal de longitud np^m.

Además,

$$\Phi_{\mathcal{P}}(UG)(\xi) \in \langle \Phi_{\mathcal{P}}(G(\xi)) \rangle$$

para cada $U(\xi) \in \mathcal{R}[\xi]/(\xi^n - 1)$.

Sea $U(\xi) \in \mathcal{R}[\xi]/(\xi^n - 1)$. Entonces $U(\xi)G(\xi) = \pi U(\xi)A(\xi) = \pi H(\xi)$ donde $H(\xi) = U(\xi)A(\xi)$. Otra vez, a partir del Lema 5.2 aplicado al polinomio $\hat{U}(\xi)\hat{G}(\xi)$ tenemos,

$$\begin{aligned}\Phi_{\mathcal{P}}(UG)(\xi) &= \Phi_{\mathcal{P}}(\pi H)(\xi) = h(\xi)(\xi^n - 1)^{p^m-1} \\ &= u(\xi)a(\xi)(\xi^n - 1)^{p^m-1} = u(\xi)\Phi_{\mathcal{P}}(G(\xi)),\end{aligned}$$

i.e., $\Phi_{\mathcal{P}}(UG)(\xi) = u(\xi)\Phi_{\mathcal{P}}(G(\xi))$. Por lo tanto,

$$\Phi_{\mathcal{P}}(UG)(\xi) \in \langle \Phi_P(G)(\xi)\rangle.$$

y en consecuencia,

$$\Phi_P(\langle G(\xi)\rangle) \subseteq \langle \Phi_P(G)(\xi)\rangle.$$

Sea $\deg(A(\xi)) = r$. Como $C(s) = 1$, $\deg(B(\xi)) = n - r$ y $|\mathcal{C}| = |F|^{2\deg(C(\xi))+1\deg(B(\xi))} = (p^m)^{n-r}$ (cf. [DLP04]). Por otro lado,

$$\begin{aligned}|\langle \Phi_{\mathcal{P}}(G(\xi))\rangle| &= (p^m)^{p^m n - \deg(\Phi_{\mathcal{P}}(G(\xi))} = (p^m)^{p^m n-(n(p^m-1)+r)} \\ &= (p^m)^{n-r},\end{aligned}$$

y concluimos que $\Phi(\mathcal{C})$ es un $[qn, n-r]$ código cíclico lineal sobre F_q. □

Este teorema generaliza parcialmente al Teorema 4.13 de [LB02].

A APÉNDICE

A.1 LA PERMUTACIÓN GLOBAL DE NECHAEV

Sea $n \in \mathbb{N}$ tal que $(n, p) = 1$ y sea n' su inverso, i.e., $nn' \equiv 1 \bmod p$. Además, sea $q = p^m$.

Definición A.1. *Sea π la permutación definida sobre $\{0, 1, \ldots\ldots, nq-1\}$:*

$$\forall u : \ 0 \leqslant u \leqslant p^m - 1 \ y \ \forall v : \ un \leqslant v \leqslant (u+1)n - 1$$

$$\pi(v) = \Big((vn' - u)_p p^{m-1} n + v \Big)_{np^m}.$$

Se define la permutación global de Nechaev Π en F^{np^m} como

$$\Pi(c_0, c_1, \ldots, c_v, \ldots, c_{nq-1}) = (c_{\pi(0)}, c_{\pi(1)}, \ldots, c_{\pi(v)}, \ldots, c_{\pi(nq-1)}).$$

Ejemplo A.1. *Sean $n = 4$, $p = 3$, $m = 2$ y sea n' en $\{1, \ldots, p-1\}$ tal que $nn' \equiv 1 \bmod p$, i.e., $n' = 1$ y sea $\tau = \sigma^{p^{m-1}}$ donde σ es el corrimiento cíclico usual de longitud p^m, de manera que, $\tau^0 = \mathrm{Id}$.*

Considérese el arreglo

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
32	33	34	35

obsérvese que el arreglo tiene $n = 4$ columnas y $p^m = 9$ filas.

Si en la segunda columna se aplica $\tau^{(1n')_p} = \tau^1 = \sigma^3$ (ésto significa corrimiento cíclico (hacia arriba) $(1n')_p$ bloques de longitud $p^{m-1} = 3$, donde $(*)_p$ denota reducción modulo p)) y en la tercer columna se aplica $\tau^{(2n')_p} = \tau^2 = \sigma^6$ (ésto significa corrimiento cíclico (hacia arriba) $(2n')_p$ bloques de longitud $p^{m-1} = 3$), i.e., aplicando el corrimiento cíclico indicado en cada columna como se ilustra abajo

$\tau^{(0n')_p}$	$\tau^{(1n')_p}$	$\tau^{(2n')_p}$	$\tau^{(3n')_p}$
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
32	33	34	35

se obtiene,

0	13	26	3
4	17	30	7
8	21	34	11
12	25	2	15
16	29	6	19
20	33	10	23
24	1	14	27
28	5	18	31
32	9	22	35

Si se concatenan las nueve filas del arreglo anterior, se obtiene la segunda fila de la permutación siguiente:

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 \\ 0 & 13 & 26 & 3 & 4 & 17 & 30 & 7 & 8 & 21 & 34 & 11 & 12 & 25 & 2 & 15 & 16 & 29 \end{pmatrix}$$

$$\begin{pmatrix} 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 \\ 6 & 19 & 20 & 33 & 10 & 23 & 24 & 1 & 14 & 27 & 28 & 5 & 18 & 31 & 32 & 9 & 22 & 35 \end{pmatrix}.$$

Por consiguiente, $\pi : \{0, 1, \ldots, 35\} \to \{0, 1, \ldots, 35\}$ *realmente es la permutación dada por (A.1) con los parámetros indicados.*

Observación A.1. *Nótese que si* $m = 1$ *en (A.1) se obtiene la generalización de la permutación de Nechaev dada en (4.3).*

BIBLIOGRAFÍA

[BF02] G. Bini and F. Flamini, *Finite commutative rings and their applications*, Kluwer Academic Publishers, 2002. (Citado en la página 4.)

[BSC95] A. Bonnecaze, P. Solé, and A. R. Calderbank, *Quaternary quadratic residue codes and unimodular lattices*, IEEE Trans. Inform. Theory **41** (1995), 366–377. (Citado en la página vii.)

[BU99] A. Bonnecaze and P. Udaya, *Cyclic codes and self-dual codes over* $\mathcal{F}_2 + u\mathcal{F}_2$, IEEE Trans. Inform. Theory **45** (1999), 1250–1255. (Citado en la página vii.)

[Car98] C. Carlet, $\mathbb{Z}_{2^k}$*-linear codes*, IEEE Trans. Inform. Theory **44** (1998), 1543–1547. (Citado en la página vii.)

[CH97] I. Constantinescu and W. Heise, *A metric for codes over residue class rings*, Problems of Information Transmission **33** (1997), no. 3, 208–213. (Citado en la página vii.)

[CL73] W. E. Clark and J. J. Liang, *Enumeration of finite commutative chain rings*, J. Algebra (1973), no. 27, 445–453. (Citado en la página 3.)

[Cla77] H. L. Claasen, *The group of units in* $GF(q)[x]/(a(x))$, Indag. Math. (1977), no. 39, 245–255. (Citado en la página 4.)

[CS95] A. R. Calderbank and N. J. A. Sloane, *Modular and* p*-adic cyclic codes*, Des., Codes and Cryptogr. **6** (1995), no. 1, 21–35. (Citado en las páginas vii y viii.)

[dH01] Xiang don Hou, *Finite commutative chain rings*, Finite Field and Their Applications **7** (2001), 382–396. (Citado en las páginas 3 y 4.)

[DLP04] H. Q. Dinh and S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory **50** (2004), no. 8, 1728–1744. (Citado en las páginas vii, 2, 9, 34, 35 y 37.)

[GS99] M. Greferath and S. E. Schmidt, *Gray isometries for finite chain rings and a nonlinear ternary* $(36, 3^{12}, 15)$ *code*, IEEE Trans. Inform. Theory **45** (1999), 2522–2524. (Citado en las páginas vii, viii, 11, 12 y 17.)

[JKC+94] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319. (Citado en las páginas vii, viii, ix, 4, 5 y 15.)

[HN99] T. Honold and A. A. Nechaev, *Weighted modules and representations of codes*, Problems Inform. Transmission **35** (1999), no. 3, 205–223. (Citado en la página 12.)

[Jac80] Nathan Jacobson, *Basic algebra ii*, firts ed., W H Freeman and Co, San Francisco, 1980. (Citado en la página 5.)

[Jan66] G. J. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc. **122** (1966), no. 2, 461–479. (Citado en la página 3.)

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

[AH98] P. V. Kumar A. G. Shanbhag and T. Helleseth, *An upper bound for the extended kloosterman sums over Galois rings*, Finite Fields and Their Applications (1998), no. 4, 218–238. (Citado en las páginas viii y 6.)

[KN01] A. Kuzmin and A. Nechaev, *Complete weight enumerators of generalized Kerdock code and related linear codes over Galois ring*, Discrete Applied Mathematics (2001), no. 111, 117–137. (Citado en la página vii.)

[LATR08] C. A. López-Andrade and H. Tapia-Recillas, *On the quasi-cyclicity of the gray map image of a class of codes over Galois rings*, ICMCTA '08: Proceedings of the 2nd international Castle meeting on Coding Theory and Applications (Berlin, Heidelberg), Springer-Verlag, 2008, pp. 107–116. (Citado en las páginas viii y 17.)

[LATR11] ———, *On the linearity and quasi-cyclicity of the gray image of codes over a Galois ring*, Groups, Algebras and Applications, vol. CONM/537, AMS, 2011, pp. 255–268. (Citado en las páginas viii, 11 y 23.)

[LB02] S. Ling and J. T. Blackford, *$\mathbb{Z}_{p^{k+1}}$-linear codes*, IEEE Trans. Inform. Theory **48** (2002), no. 9, 2592–2605. (Citado en las páginas vii, viii, ix, x, 13, 15, 17, 20, 26, 27, 30 y 37.)

[LN97] R. Lidl and H. Niederreiter, *Finite fields*, second ed., vol. Encyclopedia of Mathematics and its applications 20, Cambridge University Press, UK, 1997. (Citado en la página 1.)

[McD74] B. R. McDonald, *Finite rings with identity*, first ed., vol. 28: Pure and Applied Mathematics, Marcel Deckker, New York, 1974. (Citado en las páginas 3, 4 y 5.)

[MS77] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North Holland, 1977. (Citado en las páginas 1, 8 y 34.)

[Nec91] A. A. Nechaev, *Kerdock code in a cyclic form*, Discrete Math. Appl. **1** (1991), no. 4, 365–384. (Citado en la página vii.)

[NSM00] G. Norton and A. Salagean-Mandache, *On the structure of linear cyclic codes over finite chain rings*, AAECC **10** (2000), no. 6, 489–506. (Citado en las páginas vii y 3.)

[PQ96] V. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory **42** (1996), 1594–1600. (Citado en las páginas vii y viii.)

[Rag69] R. Raghavendran, *Finite associative rings*, Composition Math. **21** (1969), 195–229. (Citado en la página 3.)

[Ser62] J. P. Serre, *Corps locaux*, Publications de L'Institute de Mathématique de L'Université de Nancago VIII, Paris, 1962. (Citado en la página 5.)

[TR06] H. Tapia-Recillas, *Some results on codes over Galois rings*, IEEE Information Theory Workshop, Punta del Este, Uruguay, 2006, pp. 112–115. (Citado en la página 17.)

[TRV01] H. Tapia-Recillas and G. Vega, *A generalization of negacyclic codes*, Proc. Int. Workshop on Coding and Cryptography, 2001, pp. 519–524. (Citado en la página vii.)

[TRV03] ———, *On the $\mathbb{Z}_{2^k}$-linear and quaternary codes*, SIAM Journal on Discrete Mathematics **17** (2003), no. 1, 103–113. (Citado en la página vii.)

[US98] P. Udaya and M. U. Siddiqi, *Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings*, IEEE Trans. Inform. Theory **44** (1998), 1492–1503. (Citado en la página 3.)

[vv01] B. van Ash and H. C. A. van Tilborg, *Two "dual" families of nearly-linear codes over $\mathbb{Z}_p$, p odd*, AAECC **11** (2001), 313–329. (Citado en la página vii.)

[Wan03] Z. X. Wan, *Lectures on finite fields and Galois rings*, first ed., World Scientific Publish. Co., Singapore, 2003. (Citado en las páginas 1, 4 y 5.)

[Wol99] J. Wolfmann, *Negacyclic and cyclic codes over $\mathbb{Z}_4$*, IEEE, Trans. Inform. Theory **45** (1999), 2527–2532. (Citado en las páginas vii, viii, ix y 26.)

[Wol01] ———, *Binary images of cyclic codes over $\mathbb{Z}_4$*, IEEE, Trans. Inform. Theory **47** (2001), 1773–1779. (Citado en las páginas vii, viii, 27 y 33.)

BIBLIOGRAFÍA

[BF02] G. Bini and F. Flamini, *Finite commutative rings and their applications*, Kluwer Academic Publishers, 2002. (Citado en la página 4.)

[BSC95] A. Bonnecaze, P. Solé, and A. R. Calderbank, *Quaternary quadratic residue codes and unimodular lattices*, IEEE Trans. Inform. Theory **41** (1995), 366–377. (Citado en la página vii.)

[BU99] A. Bonnecaze and P. Udaya, *Cyclic codes and self-dual codes over* $\mathcal{F}_2 + u\mathcal{F}_2$, IEEE Trans. Inform. Theory **45** (1999), 1250–1255. (Citado en la página vii.)

[Car98] C. Carlet, $\mathbb{Z}_{2^k}$*-linear codes*, IEEE Trans. Inform. Theory **44** (1998), 1543–1547. (Citado en la página vii.)

[CH97] I. Constantinescu and W. Heise, *A metric for codes over residue class rings*, Problems of Information Transmission **33** (1997), no. 3, 208–213. (Citado en la página vii.)

[CL73] W. E. Clark and J. J. Liang, *Enumeration of finite commutative chain rings*, J. Algebra (1973), no. 27, 445–453. (Citado en la página 3.)

[Cla77] H. L. Claasen, *The group of units in* $GF(q)[x]/(a(x))$, Indag. Math. (1977), no. 39, 245–255. (Citado en la página 4.)

[CS95] A. R. Calderbank and N. J. A. Sloane, *Modular and* p*-adic cyclic codes*, Des., Codes and Cryptogr. **6** (1995), no. 1, 21–35. (Citado en las páginas vii y viii.)

[dH01] Xiang don Hou, *Finite commutative chain rings*, Finite Field and Their Applications **7** (2001), 382–396. (Citado en las páginas 3 y 4.)

[DLP04] H. Q. Dinh and S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory **50** (2004), no. 8, 1728–1744. (Citado en las páginas vii, 2, 9, 34, 35 y 37.)

[GS99] M. Greferath and S. E. Schmidt, *Gray isometries for finite chain rings and a nonlinear ternary* $(36, 3^{12}, 15)$ *code*, IEEE Trans. Inform. Theory **45** (1999), 2522–2524. (Citado en las páginas vii, viii, 11, 12 y 17.)

[JKC+94] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319. (Citado en las páginas vii, viii, ix, 4, 5 y 15.)

[HN99] T. Honold and A. A. Nechaev, *Weighted modules and representations of codes*, Problems Inform. Transmission **35** (1999), no. 3, 205–223. (Citado en la página 12.)

[Jac80] Nathan Jacobson, *Basic algebra ii*, firts ed., W H Freeman and Co, San Francisco, 1980. (Citado en la página 5.)

[Jan66] G. J. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc. **122** (1966), no. 2, 461–479. (Citado en la página 3.)

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

[AH98] P. V. Kumar A. G. Shanbhag and T. Helleseth, *An upper bound for the extended kloosterman sums over Galois rings*, Finite Fields and Their Applications (1998), no. 4, 218–238. (Citado en las páginas viii y 6.)

[KN01] A. Kuzmin and A. Nechaev, *Complete weight enumerators of generalized Kerdock code and related linear codes over Galois ring*, Discrete Applied Mathematics (2001), no. 111, 117–137. (Citado en la página vii.)

[LATR08] C. A. López-Andrade and H. Tapia-Recillas, *On the quasi-cyclicity of the gray map image of a class of codes over Galois rings*, ICMCTA '08: Proceedings of the 2nd international Castle meeting on Coding Theory and Applications (Berlin, Heidelberg), Springer-Verlag, 2008, pp. 107–116. (Citado en las páginas viii y 17.)

[LATR11] ———, *On the linearity and quasi-cyclicity of the gray image of codes over a Galois ring*, Groups, Algebras and Applications, vol. CONM/537, AMS, 2011, pp. 255–268. (Citado en las páginas viii, 11 y 23.)

[LB02] S. Ling and J. T. Blackford, *$\mathbb{Z}_{p^{k+1}}$-linear codes*, IEEE Trans. Inform. Theory **48** (2002), no. 9, 2592–2605. (Citado en las páginas vii, viii, ix, x, 13, 15, 17, 20, 26, 27, 30 y 37.)

[LN97] R. Lidl and H. Niederreiter, *Finite fields*, second ed., vol. Encyclopedia of Mathematics and its applications 20, Cambridge University Press, UK, 1997. (Citado en la página 1.)

[McD74] B. R. McDonald, *Finite rings with identity*, first ed., vol. 28: Pure and Applied Mathematics, Marcel Deckker, New York, 1974. (Citado en las páginas 3, 4 y 5.)

[MS77] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North Holland, 1977. (Citado en las páginas 1, 8 y 34.)

[Nec91] A. A. Nechaev, *Kerdock code in a cyclic form*, Discrete Math. Appl. **1** (1991), no. 4, 365–384. (Citado en la página vii.)

[NSM00] G. Norton and A. Salagean-Mandache, *On the structure of linear cyclic codes over finite chain rings*, AAECC **10** (2000), no. 6, 489–506. (Citado en las páginas vii y 3.)

[PQ96] V. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory **42** (1996), 1594–1600. (Citado en las páginas vii y viii.)

[Rag69] R. Raghavendran, *Finite associative rings*, Composition Math. **21** (1969), 195–229. (Citado en la página 3.)

[Ser62] J. P. Serre, *Corps locaux*, Publications de L'Institute de Mathématique de L'Université de Nancago VIII, Paris, 1962. (Citado en la página 5.)

[TR06] H. Tapia-Recillas, *Some results on codes over Galois rings*, IEEE Information Theory Workshop, Punta del Este, Uruguay, 2006, pp. 112–115. (Citado en la página 17.)

[TRV01] H. Tapia-Recillas and G. Vega, *A generalization of negacyclic codes*, Proc. Int. Workshop on Coding and Cryptography, 2001, pp. 519–524. (Citado en la página vii.)

[TRV03] ———, *On the $\mathbb{Z}_{2^k}$-linear and quaternary codes*, SIAM Journal on Discrete Mathematics **17** (2003), no. 1, 103–113. (Citado en la página vii.)

[US98] P. Udaya and M. U. Siddiqi, *Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings*, IEEE Trans. Inform. Theory **44** (1998), 1492–1503. (Citado en la página 3.)

[vv01] B. van Ash and H. C. A. van Tilborg, *Two "dual" families of nearly-linear codes over $\mathbb{Z}_p$, p odd*, AAECC **11** (2001), 313–329. (Citado en la página vii.)

[Wan03] Z. X. Wan, *Lectures on finite fields and Galois rings*, first ed., World Scientific Publish. Co., Singapore, 2003. (Citado en las páginas 1, 4 y 5.)

[Wol99] J. Wolfmann, *Negacyclic and cyclic codes over $\mathbb{Z}_4$*, IEEE, Trans. Inform. Theory **45** (1999), 2527–2532. (Citado en las páginas vii, viii, ix y 26.)

[Wol01] ———, *Binary images of cyclic codes over $\mathbb{Z}_4$*, IEEE, Trans. Inform. Theory **47** (2001), 1773–1779. (Citado en las páginas vii, viii, 27 y 33.)