UNIVERSIDAD AUTÓNOMA METROPOLITANA - IZTAPALAPA
DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA
Departamento de Matemáticas

Casa abierta al tiempo

IMÁGENES DE GRAY DE CÓDIGOS CONSTA-CÍCLICOS SOBRE $\mathbb{Z}_{2^{k+1}}$

Presenta

L.M. Henry Chimal Dzul

para obtener el grado académico de

Maestro en Ciencias (Matemáticas)

Asesor: Dr. Horacio Tapia Recillas

Jurado Calificador

Presidente:	Dr. Gabriel Villa Salvador	CINVESTAV-IPN
Secretario:	Dr. Horacio Tapia Recillas	UAM-I
Vocal:	Dr. Rogelio Fernández-Alonso González	UAM-I
Vocal:	Dr. José Noé Gutiérrez Herrera	UAM-I

México D. F. a 12 de julio de 2013

Agradecimientos

Estas líneas son para expresar mis más profundo y sincero agradecimiento a todas aquellas personas que con su ayuda han colaborado de forma directa o inderecta en la realización del presente trabajo.

Debo agradecer de manera especial y sincera al Dr. Horacio Tapia Recillas por aceptar ser mi asesor de tesis. Asimismo, le agradezco su confianza y paciencia durante estos anõs.

A mis sinodales: Dr. Rogelio Fernández-Alonso González, Dr. José Noé Gutiérrez Herrera, Dr. Horacio Tapia Recillas y Dr. Gabriel Villa Salvador; por su disponibiliad, paciencia y amabilidad para revisar con sumo detalle este trabajo.

Al Consejo Nacional de Ciencia y Tecnología (CONACyT) por haber financiado gran parte de mis estudios otorgándome una beca a partir del año 2007 hasta el año 2009.

A mis amigos y profesores, Rogelio Fernández-Alonso, Carlos Alberto López (BUAP, Puebla), Noé Gutiérrez, Adolfo Torres, Mario Pineda y Bernardo Llano, por sus interesantes conversaciones.

Por supuesto, el agradecimiento más profundo y sentido va para mi querdia familia, ya que sin su apoyo, paciencia e inspiración durante todo este tiempo habría sido imposible llevar a cabo esta tarea.

¡ ...por ellos y para ellos !

Contenido

Introducción

Los códigos detectores-correctores de error tuvieron sus orígenes con los trabajos de R. W. Hamming [22] y C. E. Shannon [47] en la década de los 40's del siglo XX. En ese entonces los primeros códigos correctores de error fueron diseñados en el ambiente de los espacios vectoriales sobre el campo binario, lo cual se debió a sus aplicaciones en el medio computacional. Sin embargo, al poco tiempo, los trabajos de Shannon y Hamming inspiraron a M. J. E. Golay [20] a preguntarse por códigos en el contexto general de espacios vectoriales sobre campos finitos, dando el siguiente paso para potenciar una nueva rama de las matemáticas: la *Teoría de Códigos Algebraicos.* Actualmente, se han realizado una gran cantidad de investigaciones en esta área, produciendo códigos que ahora se encuentran implementados en dispositivos de almacenamiento masivo de información (discos duros, CD's, DVD's, USB's, entre otros), en sistemas de navegación marítima y aérea, en dispositivos de comunicación inalámbrica, en la exploración del espacio exterior, etcétera.

Por su parte, la Teoría de Códigos Algebraicos sobre anillos finitos (conmutativos y con identidad) tuvo sus inicios en la década de los 70's del siglo XX, con los trabajos de I. F. Blake [5, 6] y E. Spiegel [48, 49], aunque en esos momentos la comunidad científica no mostró demasiado interés en estos temas. No obstante, a principios de la década de los 90's del siglo pasado, la Teoría de Códigos sobre anillos finitos fue notablemente impulsada por los resultados de Nechaev [40] y Hammons et al. [23], quienes mostraron que los códigos binarios no lineales de Kerdock, Preparata, etc. pueden ser obtenidos como imágenes de *códigos cíclicos lineales extendidos* sobre $\mathbb{Z}_4$ bajo la *isometría de Gray* definida como:

$$\begin{array}{rccc} \phi: & \mathbb{Z}_4 & \to & \mathbb{F}_2 \times \mathbb{F}_2 \\ & 0 & \mapsto & (0,0) \\ & 1 & \mapsto & (0,1) \\ & 2 & \mapsto & (1,1) \\ & 3 & \mapsto & (1,0) \end{array}$$

Desde entonces, se han generado un gran número de investigaciones, las cuales se han encaminado principalmente en dos direcciones. Dado un entero $n \geq 1$, un anillo finito R y una unidad $\gamma \in R$, la primera consiste en estudiar la estructura algebraica de los *códigos consta-cíclicos (o γ-cíclicos) lineales* de longitud n sobre R; mismos que son definidos como aquellos submódulos de R^n que permanecen fijos bajo el *corrimiento γ-cíclico* $\nu_\gamma : R^n \to R^n$ dado por la regla

$$\nu_\gamma : (a_0, a_1, \ldots, a_{n-1}) \mapsto (\gamma a_{n-1}, a_0, \ldots, a_{n-2}).$$

En especial, se han realizado diversas aportaciones para las familias de códigos cíclicos ($\gamma = 1$) y negacíclicos ($\gamma = -1$) [1, 8, 9, 13–16, 25, 30, 31, 46, 57, 59]. La segunda dirección consiste

en generalizar la definición de la isometría de Gray a múltiples familias de anillos finitos e investigar las propiedades −tales como linealidad y ciclicidad− de los códigos obtenidos como *imágenes bajo la isometría de Gray* (o brevemente *imágenes de Gray*) de los códigos consta-cíclicos sobre tales anillos [11, 21, 29, 33, 35, 36, 50–52, 57, 59]. Es en esta última dirección donde reside nuestro interés y en la que el presente trabajo se sitúa.

El estudio de las propiedades de linealidad y ciclicidad de las imágenes de Gray de códigos consta-cíclicos sobre anillos finitos fue iniciada por J. Wolfman [54, 55], quien demostró que la imagen de Gray de un código negacíclico de longitud n (impar) sobre $\mathbb{Z}_4$ es un código cíclico binario de longitud $2n$, y que la imagen de Gray de un código cíclico lineal de longitud n (impar) sobre $\mathbb{Z}_4$ es *permutación-equivalente* a un código cíclico binario (no necesariamente lineal) de longitud $2n$. A la fecha, varios autores han generalizado algunos de los resultados presentados en [54, 55] para los códigos consta-cíclicos sobre distintas clases de *anillos finitos de cadena* [9, 29, 33, 35, 36, 50–52]. Recuerde que un anillo finito R es llamado de cadena si y sólo si R es un anillo local de ideales principales [14, Proposición 2.1]. Si θ es un generador del ideal maximal de R, lo anterior implica que $\theta^{t+1} = 0$ y $\theta^t \neq 0$ para algún $t \geq 1$, llamado el *índice de nilpotencia*, y que los ideales de R forman una cadena

$$R = \langle \theta^0 \rangle \supsetneq \langle \theta \rangle \supsetneq \langle \theta^2 \rangle \supsetneq \cdots \supsetneq \langle \theta^{t-1} \rangle \supsetneq \langle \theta^t \rangle \supsetneq \langle \theta^{t+1} \rangle = \langle 0 \rangle.$$

Es de particular interés resaltar en este momento que en todos esos trabajos se han considerado únicamente códigos consta-cíclicos que permanecen fijos bajo el **corrimiento γ-cíclico**, donde la unidad γ de R es **precisamente** $\gamma = 1 - \theta^t$. Esto es, ninguno de esos trabajos ha estudiado códigos que permanezcan fijos con respecto a otra aplicación que generalize al corrimiento γ-cíclico, o códigos consta-cíclicos que permanezcan fijos con respecto al corrimiento γ-cíclico, donde γ no sea de la forma $1 - \theta^t$. Una aplicación que naturalmente generaliza al corrimiento γ-cíclico es el *corrimiento γ-casi-cíclico de índice $m \geq 1$*, $\nu_\gamma^{\otimes m} : R^{mn} \to R^{mn}$, definido como

$$\nu_\gamma^{\otimes m} : \left(A^{(0)} | A^{(1)} | \cdots | A^{(m-1)} \right) \mapsto \left(\nu_\gamma \left(A^{(0)} \right) | \nu_\gamma \left(A^{(1)} \right) | \cdots | \nu_\gamma \left(A^{(m-1)} \right) \right),$$

donde $A^{(i)} \in R^n$, $0 \leq i \leq m-1$, y "|" es la concatenación. Así, un primer paso sería considerar a la familia de *códigos γ-casi-cíclicos deíncide m*, los cuales permanecen fijos bajo el corrimiento γ-casi-cíclico de índice $m \geq 1$.

Con base en lo anterior, es natural formular los siguientes problemas:

Problema 1. Investigar las propiedades de las imágenes de Gray de la familia de códigos γ-casic-íclicos sobre un anillo finito de cadena, donde γ sea una de las unidades consideradas en la literatura.

Problema 2. Investigar las propiedades de las imágenes de Gray de la familia de códigos γ-cíclicos sobre un anillo finito de cadena R, donde γ sea una unidad diferente a $1 - \theta^t$.

El propósito de esta tesis es abordar ambos problemas para códigos sobre el anillo $\mathbb{Z}_{2^{k+1}}$ de enteros módulo 2^{k+1}, $k \geq 1$, el cual es un anillo finito de cadena con $\theta = 2$ y $t = k$. De manera más específica, en esta tesis investigaremos algunas propiedades de las imágenes de Gray de los códigos γ-casi-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, donde $k \geq 1$ y γ es una de las siguientes unidades:

$$1, \qquad \lambda = 1 + 2^k. \tag{1}$$

Asimismo, investigaremos algunas propiedades de la imagen de Gray de códigos consta-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, donde $k \geq 2$ y γ es una de las siguientes unidades:

$$\delta_1 = 1 + 2^{k-1}, \qquad \delta_2 = 1 + 2^{k-1} + 2^k. \tag{2}$$

En el desarrollo de este trabajo, análogamente a [51, 52], introduciremos una isometría φ de $\mathbb{Z}_{2^{k+1}}^n$ a $\mathbb{Z}_4^{2^{k-1}n}$ en la que nos apoyaremos para estudiar propiedades de ciclicidad y negaciclicidad de la imagen bajo φ de códigos sobre $\mathbb{Z}_{2^{k+1}}$. Usaremos los resultados obtenidos para definir isometrías de Gray sobre $\mathbb{Z}_{2^{k+1}}^n$ que resultan ser *permutación-equivalentes*, e inducir propiedades de casi-ciclicidad en la imagen de Gray de dichos códigos. Cuando la unidad γ sea 1 o λ, los resultados que obtendremos serán generalizaciones naturales de las principales aportaciones presentadas en [33, 36, 51, 52]. Pero cuando la unidad γ sea δ_1 o δ_2 y $k \geq 3$, obtendremos familias de códigos sobre $\mathbb{Z}_4$ que son invariantes con respecto a un *producto de Kronecker del corrimiento cíclico y negacíclico* (cf. Teorema 5.2.17 de la Sección 5.2), mismas que no han sido reportadas en la literatura. Por otra parte, si $k = 2$, entonces la imagen bajo φ de un código δ_1-cíclico o δ_2-cíclico será la traslación de un código negacíclico sobre $\mathbb{Z}_4$. Este último resultado nos permitirá obtener códigos cíclicos trasladados como imágenes de Gray de códigos δ_1-cíclicos y δ_2-cíclicos sobre $\mathbb{Z}_8$.

Las aportaciones más importantes de este trabajo residen en los Teoremas 4.2.1, 4.4.1, 4.7.10, 5.2.17, 5.3.3, 6.3.10 y 6.4.2, pues en conjunto dan respuesta a los Problemas 1 y 2 planteados anteriormente. Sin embargo, sobresalen los Teoremas 5.2.17, 5.3.3, 6.3.10 y 6.4.2 a raíz de que las familias de códigos caracterizadas en ellos, hasta el momento no han sido reportadas en la literatura. El Teorema 5.2.17 establece una caracterización de los códigos δ_1-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, $k \geq 3$, en términos de sus imágenes bajo φ. El Teorema 5.3.3 proporciona un resultado similar para códigos δ_2-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, $k \geq 3$. Por su parte, los Teoremas 6.3.10 y 6.4.2 dan una respuesta completa al Problema 2 cuando el anillo R es $\mathbb{Z}_8$. En especial caracterizan a los códigos 3-cíclicos y 7-cíclicos sobre $\mathbb{Z}_8$, y ofrecen una alternativa de construir códigos cíclicos binarios como la imágenes de Gray de dichos códigos (Teorema 6.5.1).

La organización de este manuscrito es la siguiente. El Capítulo 1 contiene la notación general y algunos resultados preliminares que serán necesarios a lo largo de este trabajo. En el Capítulo 2 analizaremos la definición de la isometría de Gray propuesta en [21] y definiremos una isometría $\varphi : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}_4^{2^{k-1}n}$ que resultará ser permutación-equivalente a la isometría φ^k introducida en [51, 52]. Esto nos permite generalizar la Proposición 3.1 de [51], las Proposiciones 4 y 7 de [52], y obtener nuevas relaciones para la isometría de Gray.

Posteriormente, en el Capítulo 3, investigamos algunas relaciones entre las isometrías φ, de Gray y el corrimiento γ-casi-cíclico, donde γ es una unidad del anillo $\mathbb{Z}_{2^{k+1}}$. En especial, enfocamos nuestra atención en las unidades mencionadas en (1) y (2); obteniendo generalizaciones de algunos resultados establecidos en [51, 52, 54, 55].

En el Capítulo 4 caracterizamos a los códigos casi-cíclicos y λ-casi-cíclicos en términos de sus imágenes con respecto a las isometrías φ y de Gray. Estas contribuciones responden al Problema 1 cuando $R = \mathbb{Z}_{2^{k+1}}$. Asimismo, generalizan las principales aportaciones de [51, 52, 54, 55].

Los Capítulos 5 y 6 dan respuesta al Problema 2 cuando el anillo R es $\mathbb{Z}_{2^{k+1}}$ y la unidad γ es δ_1 o δ_2. En el Capítulo 5 examinamos algunas propiedades de las imágenes de códigos δ_1-cíclicos y δ_2-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$ cuando $k \geq 3$. En este caso, nuestras principales contribuciones se encuentran en los Teoremas 5.2.17 y 5.3.3, los cuales caracterizan a los códigos δ_1-cíclicos y δ_2-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$ con respecto a sus imágenes bajo la isometría φ. En el Capítulo 6, analizamos algunas propiedades de las imágenes de los códigos 3-cíclicos y 7-cíclicos sobre $\mathbb{Z}_8$ (el caso $k = 2$ que no fue considerado en el Capítulo 5). Dado que $7 = -1$ en $\mathbb{Z}_8$, los códigos 7-cíclicos sobre $\mathbb{Z}_8$ son llamados *códigos negacíclicos*. En específico, demostramos que la imagen bajo φ de un código 3-cíclico es un código negacíclico sobre $\mathbb{Z}_4$, módulo una traslación. Similarmente, probamos que la imagen bajo φ de un código negacíclico sobre $\mathbb{Z}_8$ es un código negacíclico sobre $\mathbb{Z}_4$, módulo una traslación. Es a partir de estos resultados, y de los que fueron establecidos por J. Wolfman en [54], que es posible caracterizar a los códigos 3-cíclicos y negacíclicos con respecto a sus imágenes de Gray. Tales caracterizaciones son establecidas en los Teoremas 6.3.10 y 6.4.2. En particular, hacemos énfasis en el Teorema 6.5.1 que establece que un código sobre $\mathbb{Z}_8$ es 3-cíclico y negacíclico a la vez si y sólo si su imagen de Gray es un código cíclico binario. Dichas aportaciones permiten construir códigos cíclicos, módulo una traslación, a partir de códigos 3-cíclicos y negacíclicos sobre $\mathbb{Z}_8$.

Las conclusiones y perspectivas del presente trabajo son expuestas en el Capítulo 7. Finalmente, hemos incluido dos apéndices. El Apéndice A contiene tablas de códigos consta-cíclicos sobre $\mathbb{Z}_8$ y $\mathbb{Z}_{16}$ las cuales se incluyen con la finalidad de ilustrar los resultados alcanzados en esta tesis. Dichas tablas, así como la gran mayoría de los ejemplos mencionados en el interior de este tranajo, fueron construidas con la ayuda del programa computacional **MAGMA® V2.15-13 (Student Version)** en el **Laboratorio de Códigos y Criptografía: Claude Shannon,** del Departamento de Matemáticas de esta casa de estudios. Por otro lado, el Apéndice B, ofrece una prueba distinta a la que aparece en el Corolario 2.2.7, el cual establece que la función φ es una isometría.

Capítulo 1

Códigos consta-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$

El presente capítulo contiene la notación general y algunos de los resultados preliminares a este trabajo. En particular, incluye la descripción de una técnica para construir códigos cíclicos y consta-cíclicos lineales de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$ ($k \geq 1$), los cuales serán de utilidad para ilustrar los resultados alcanzados en los siguientes capítulos. Asimismo, demostramos que los códigos cíclicos lineales de longitud impar y los códigos consta-cíclicos lineales de la misma longitud sobre $\mathbb{Z}_{2^{k+1}}$, tienen los mismos pesos homogéneos.

1.1. Notación general

A menos que explícitamente se indique lo contrario, en todo este manuscrito la palabra *anillo* significa *anillo finito conmutativo y con elemento identidad*. La única excepción será cuando hablemos del anillo (infinito) de polinomios. Entre la clase de anillos finitos se encuentran los anillos $\mathbb{Z}_{p^k}$ de enteros módulo p^k (p primo), los anillos $GR(p^s,m)$ de Galois, los anillos de cadena finita y los anillos finitos de Frobenius, por mencionar algunos de ellos. Para una referencia acerca de estos tópicos, el lector puede consultar [14, 39].

Dado un anillo R y un entero $n \geq 1$, recordemos que el conjunto R^n, cuyos elementos son las n-adas con entradas en R, adquiere una estructura de R-módulo con las operaciones de suma y multiplicación definidas coordenada a coordenada:

$$A+B=(a_0+b_0,\ldots,a_{n-1}+b_{n-1}), \qquad \alpha A=(\alpha a_0,\ldots,\alpha a_{n-1}),$$

donde $A=(a_0,\ldots,a_{n-1}), B=(b_0,\ldots,b_{n-1}) \in R^n$ y $\alpha \in R$. Análogamente a la teoría de espacios vectoriales, llamaremos *vectores* a los elementos de R^n y *escalares* a los elementos del anillo R.

Por brevedad y claridad en la notación, el vector $(a,\ldots,a) \in R^n$ será escrito como $(a)_n$. Como es usual en teoría de anillos, el ideal de R generado por $\{a_1,\ldots,a_l\} \subseteq R$ será escrito como $\langle a_1,\ldots,a_l\rangle$, y el gurpo de unidades de R será denotado por $U(R)$.

Recordemos que la *concatenación* de dos elementos $A=(a_0,\ldots,a_{n-1})$ y $B=(b_0,\ldots,b_{n-1})$ de R^n, denotada por $(A|B)$, es definida como

$$(A|B)=(a_0,\ldots,a_{n-1},b_0,\ldots,b_{n-1}) \in R^{2n}.$$

Esta definición es extendida naturalmente a cualquier número finito de vectores en R^n. Así, la conctenación define una biyección entre $(R^n)^m$ y R^{nm}. En efecto, si $A^{(0)},A^{(1)},\ldots,A^{(m-1)} \in R^n$,

la biyección está dada de la siguiente manera:

$$\left(A^{(0)},A^{(1)},\ldots,A^{(m-1)}\right) \mapsto \left(A^{(0)}|A^{(1)}|\cdots|A^{(m-1)}\right).$$

Por lo tanto, para cualquier entero d que divida a n, digamos $n = de$, mediante la función inversa de la concatenación podemos identificar a R^n con $(R^d)^e$, o bien con $(R^e)^d$, según sea conveniente.

Para cualquier entero positivo m y cualquier función $f : R^n \to R^n$ definimos la aplicación

$$f^{\otimes m} : R^{nm} \to R^{nm}$$

dada por

$$\left(A^{(0)}\,|\,A^{(1)}\,|\cdots|\,A^{(m-1)}\right) \mapsto \left(f(A^{(0)})\,|\,f(A^{(1)})\,|\cdots|\,f(A^{(m-1)})\right),$$

donde $A^{(0)},A^{(1)},\ldots,A^{(m-1)} \in R^n$. Claramente, si f es un R-homorfismo (de R-módulos), entonces $f^{\otimes m}$ también lo es. Más aún, es claro que la función $f^{\otimes m}$ preserva las propiedades de inyectividad, suprayectividad o biyectividad de la función f. En particular, si f es una permutación, entonces $f^{\otimes m}$ también lo es. Además, note que si $g : R^{nm} \to R^{nm}$, entonces $(f \circ g)^{\otimes m} = f^{\otimes m} \circ g^{\otimes m}$.

Dado un anillo R, sea $R[x]$ el anillo (infinito) de polinomios con coeficientes en R y sean f,g polinomios en $R[x]$. Recordemos que (cf. [14, 30, 39]):

1. f es llamado *regular* si no es un divisor de cero en $R[x]$, es decir, si $fh = 0$ para algún $h \in R[x]$, entonces necesariamente $h = 0$.
2. f es llamado *primario* si $\langle f\rangle$ es un ideal primario de $R[x]$, esto es, la condición $gh \in \langle f\rangle$ implica que $g \in \langle f\rangle$ o para algún entero $k \geq 1$, $h^k \in \langle f\rangle$.
3. f y g son llamados *coprimos* (*primos relativos*) si $\langle f\rangle + \langle g\rangle = \langle 1\rangle = R[x]$.

Debido a que todos los anillos (finitos conmutativos y con identidad) son isomorfos a una suma directa de anillos locales (cf. [39]), es suficiente (desde el punto de vista matemático y para las necesidades de este trabajo) enfocarnos en los anillos locales. Recuerde que un anillo es llamado *local* si tiene un único ideal maximal. Por ejemplo, $\mathbb{Z}_{p^k}$ es un anillo local con ideal maximal $\langle p\rangle$; asimismo $GR(p^s,m)$ es un anillo local con ideal maximal $\langle p\rangle$.

Dado un anillo local R con ideal maximal M y $\mathbb{F} = R/M$ su *campo residual*, note que la proyección natural $- : R \to \mathbb{F}$ induce el homomorfismo de anillos $- : R[x] \to \mathbb{F}[x]$ definido como

$$f = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \quad \mapsto \quad \overline{f} = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_{n-1}}x^{n-1}.$$

Consecuentemente, para cualesquiera $f,g \in R[x]$ se tiene que (cf. [14, 30, 39]):

1. f es una unidad si y sólo si $\overline{f}$ es una unidad.

2. f es regular si y sólo si $\overline{f} \neq 0$. En particular, para cualquier $\gamma \in U(R)$, el polinomio $x^n - \gamma$ es regular.
3. Si f y g son regulares, entonces f y g son coprimos si y sólo si $\overline{f}$ y $\overline{g}$ son coprimos.
4. Si $\overline{f}$ es irreducible, entonces f es irreducible.
5. Si f es irreducible, entonces $\overline{f} = uf_1^n$, donde u es una unidad, f_1 es un polinomio irreducible en $\mathbb{F}[x]$ y $n \geq 1$ es un entero.

Como una aplicación de las observaciones 4) y 5), la siguiente definición tiene sentido. Un polinomio $f \in R[x]$ es llamado *básico irreducible* si $\overline{f}$ es irreducible.

Es bien conocido que el anillo $F[x]$ de polinomios con coeficientes en un campo F es un dominio de factorización única. Esto es, dado $f \in F[x]$, existe una familia $a_1(x), a_2(x), \ldots, a_k(x)$ de polinomios irreducibles tales que $f = a_1(x)a_2(x)\cdots a_k(x)$. Esta factorización es única en el sentido de que si $f = b_1(x)b_2(x)\cdots b_l(x)$, donde $b_1(x), b_2(x), \ldots, b_l(x)$ son irreducibles, entonces $k = l$ y, salvo una permutación en los subíndices, $\langle a_i(x)\rangle = \langle b_i(x)\rangle$, $1 \leq i \leq k$. Para polinomios regulares en un anillo de polinomios $R[x]$ sobre un anillo local R se tiene el siguiente resultado.

Teorema 1.1.1 ([39, Teorema XIII.11]). *Sea $f \in R[x]$ un polinomio regular. Entonces*

1. *$f = ua_1(x)a_2(x)\cdots a_k(x)$, donde u es una unidad y $a_1(x), a_2(x), \ldots, a_k(x)$ son polinomios regulares, primarios y coprimos; y*
2. *si $f = vb_1(x)b_2(x)\cdots b_l(x)$, donde v es una unidad y $b_1(x), b_2(x), \ldots, b_l(x)$ son polinomios regulares, primarios y coprimos, entonces $k = l$ y, salvo una permutación en los subíndices, $\langle a_i(x)\rangle = \langle b_i(x)\rangle$, $i \leq i \leq k$.*

Observe que la factorización de polinomios regulares en $R[x]$ ocurre en términos de polinomios primarios, en lugar de polinomios irreducibles como es el caso de $F[x]$. Sin embargo, si $R = \mathbb{Z}_{p^k}$ ($k \geq 1$ y p un primo) y $\mathrm{mcd}(n, p) = 1$, entonces para el polinomio $x^n - 1 \in R[x]$ se tiene lo siguiente.

Corolario 1.1.2 ([14, Proposición 2.7]). *Sea n un entero tal que* $\mathrm{mcd}(n, p) = 1$. *Entonces existe una familia $a_1(x), a_2(x), \ldots, a_k(x)$ de polinomios mónicos, básicos irreducibles y coprimos en $\mathbb{Z}_{p^k}[x]$, única en el sentido del Teorema 1.1.1, tales que $x^n - 1 = a_1(x)a_2(x)\cdots a_k(x)$.*

Observe que, en particular, si $\mathrm{mcd}(n, p) = 1$ y $x^n - 1 = g_1g_2\cdots g_k = h_1h_2\cdots h_k$, donde los polinomios g_i, h_i son mónicos, entonces (salvo una permutación) $g_i = h_i$, $1 \leq i \leq k$.

Aunque gran parte de las definiciones que daremos en la siguiente subsección serán válidas para cualquier anillo finito, el problema principal de este trabajo se restringe al anillo $\mathbb{Z}_{2^{k+1}}$ ($k \geq 1$) de enteros módulo 2^{k+1}. Por tal razón es conveniente mencionar algunas de propiedades algebraicas.

Para todo entero $k \geq 1$, en este manuscrito, se considerará al anillo $\mathbb{Z}_{2^{k+1}}$ como el conjunto de enteros $\{0,1,\ldots,2^{k+1}-1\}$ con las operaciones de suma y producto módulo 2^{k+1}. Es bien conocido que $\mathbb{Z}_{2^{k+1}}$ es un anillo local de ideales principales, los cuales están linealmente ordenados con respecto a la inclusión:

$$\mathbb{Z}_{2^{k+1}} = \langle 1 \rangle \supset \langle 2 \rangle \supset \langle 2^2 \rangle \supset \cdots \supset \langle 2^{k-1} \rangle \supset \langle 2^k \rangle \supset \langle 0 \rangle.$$

En particular, esto quiere decir que $\mathbb{Z}_{2^{k+1}}$ es un anillo finito de cadena. Asimismo, es conocido que el campo residual de $\mathbb{Z}_{2^{k+1}}$ es isomorfo al campo binario $\mathbb{F}_2$, el cual será considerado como el conjunto $\{0,1\}$ dotado de las operaciones de suma y producto módulo 2. En consecuencia, pensaremos a $\mathbb{F}_2$ como subconjunto de $\mathbb{Z}_{2^{k+1}}$. Debido a lo anterior, la suma en el campo binario será denotada por "$\oplus$" mientras que la suma en $\mathbb{Z}_{2^{k+1}}$ será denotada de manera usual con el símbolo "$+$". Emplearemos las mismas notaciones para la suma de vectores con entradas en $\mathbb{F}_2^n$ o $\mathbb{Z}_{2^{k+1}}^n$. El producto de dos elementos a,b en cualesquiera de los anillos $\mathbb{Z}$, $\mathbb{Z}_{2^{k+1}}$ o $\mathbb{F}_2$, será escrito simplemente como ab, pues esta operación coincide en las tres estructuras.

Por último, recordemos que dado un entero $k \geq 1$ fijo, cualquier $z \in \mathbb{Z}_{2^{k+1}}$ puede ser escrito de manera única como

$$z = r_0(z) + r_1(z)2 + \cdots + r_{k-1}(z)2^{k-1} + r_k(z)2^k,$$

donde $r_i(z) \in \{0,1\}$, $1 \leq i \leq k$. Esta expresión es conocida como la *representación 2-ádica de z* (o *expansión binaria de z*). Es bastante claro que z es una unidad en $\mathbb{Z}_{2^{k+1}}$ si y sólo si $r_0(z) = 1$. En consecuencia, un elemento de $\mathbb{Z}_{2^{k+1}}$ es una unidad o pertenece al ideal maximal $\langle 2 \rangle$.

Si $Z = (z_0, z_1, \ldots, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$, entonces cada coordenada z_i de Z puede ser escrito en su representación 2-ádica, digamos

$$z_i = r_0(z_i) + r_1(z_i)2 + \cdots + r_{k-1}(z_i)2^{k-1} + r_k(z_i)2^k.$$

Esto implica que, haciendo uso de la estructura de $\mathbb{Z}_{2^{k+1}}$-módulo de $\mathbb{Z}_{2^{k+1}}^n$, el elemento Z puede ser escrito de manera única como

$$Z = r_0(Z) + r_1(Z)2 + \cdots + r_{k-1}(Z)2^{k-1} + r_k(Z)2^k,$$

donde $r_j(Z) = (r_j(z_0), r_j(z_1), \ldots, r_j(z_{n-1})) \in \{0,1\}^n$. A lo largo de este trabajo, nos referiremos a esta expresión como la *representación 2-ádica de Z*.

1.2. Códigos sobre anillos finitos

En esta sección recordaremos las principales definiciones relacionadas con la Teoría de Códigos sobre anillos [14, 25, 30, 34], las cuales son modificaciones naturales de sus homólogas en la Teoría de Códigos sobre campos finitos [7, 27, 38, 44, 45].

Sea $n \geq 1$ un entero y R un anillo. Un *código $\mathscr{C}$ de longitud n sobre R* es cualquier subconjunto no vacío de R^n. Si además $\mathscr{C}$ es un submódulo de R^n, entonces $\mathscr{C}$ es llamado un *código lineal*; de lo contrario, $\mathscr{C}$ es llamado un *código no lineal*.

Cuando $R = \mathbb{F}$ es un campo finito, un código lineal $\mathscr{C}$ de longitud n sobre $\mathbb{F}$ es precisamente un subespacio vectorial de $\mathbb{F}^n$. Si $k \leq n$ es la dimensión de $\mathscr{C}$ como subespacio de $\mathbb{F}^n$, entonces es común decir que $\mathscr{C}$ es un $[n,k]$ código sobre $\mathbb{F}$. Para códigos no lineales de longitud n sobre $\mathbb{F}$ y cardinalidad M, la notación (n,M) es la usual.

La existencia de una base para cualquier subespacio vectorial de $\mathbb{F}^n$ nos permiten definir la *matriz generadora* de un $[n,k]$ código $\mathscr{C} \neq \{(0)_n\}$ sobre $\mathbb{F}$ como cualquier matriz de tamaño $k \times n$ con entradas en el campo $\mathbb{F}$ cuyos renglones forman una base para $\mathscr{C}$. Observe que cualquier matriz generadora G de $\mathscr{C}$ permite describir al código de manera sencilla y, de hecho, proporciona una técnica eficiente para la codificación de mensajes. Esto se debe a que $\mathscr{C} = \{vG : v \in \mathbb{F}^k\}$.

Por otra parte, a pesar de que R^n no es un espacio vectorial cuando R es un anillo que no es campo, observe que los vectores $e_i = (0,\ldots,1,0,\ldots,0)$, donde el 1 aparece en la posición i, $1 \leq i \leq n$, forman una *base de R^n*. Esto significa que cualquier elemento de R^n puede ser escrito de manera única como combinación lineal de los e_i, y que si consideramos la combinación lineal

$$\alpha_1 e_1 + \cdots + \alpha_n e_n = (0)_n,$$

entonces $\alpha_1 = \cdots = \alpha_n = 0$. Recuérdese que en teoría de módulos se dice que un R-módulo M es *libre* si existe un conjunto $B \subseteq M$ tal que cada elemento de M puede ser expresado de manera única como R-combinaciones lineales de elementos de B. Como consecuencia de esta definición concluimos que R^n es un R-módulo libre. Sin embargo, no todo submódulo de un R-módulo libre es libre. En particular, este resultado implica que no todo código lineal sobre un anillo finito tiene una base. (En [27, Ejemplo 12.1.1.] se presenta un código lineal sobre $\mathbb{Z}_4$ que no es libre.) Afortunadamente, dado que cualquier código lineal $\mathscr{C}$ de longitud n sobre R es un conjunto finito, entonces existen $A_0, A_1, \ldots, A_s \in \mathscr{C}$ que *generan a $\mathscr{C}$ como submódulo de R^n*, es decir, todo elemento de $\mathscr{C}$ se escribe como combinación lineal (aunque no necesariamente única) de $A_0, A_1, \ldots, A_s$, o sea, $\mathscr{C} = \{r_0A_0 + \cdots + r_sA_s : r_0, \ldots, r_s \in R\}$. En otros términos una forma sencilla de definir un código lineal $\mathscr{C}$ de longitud n sobre R es dando un conjunto finito de vectores que generan a $\mathscr{C}$. Cada elemento del conjunto que genera a $\mathscr{C}$ será llamado un *generador* del código.

Para los propósitos de este trabajo, será suficiente tener un conjunto de generadores del código. Sin embargo, vale la pena mencionar que para cualquier código lineal sobre un anillo de cadena finita, es posible enontrar un conjunto mínimo de generadores y entonces definir de manera adecuada una matriz generadora del código (cf. [34]).

Dado un número natural $n \geq 1$, consideremos el conjunto $I_n = \{0, 1, \ldots, n-1\}$ y una permutación $\tau : I_n \to I_n$. Definimos la *permutación $\widetilde{\tau} : R^n \to R^n$ inducida* por τ de la siguiente

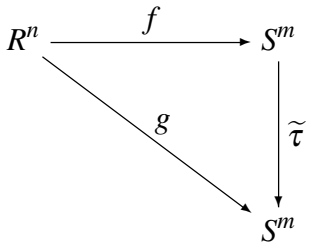
manera:

$$\widetilde{\tau} : (a_0, a_1, \ldots, a_{n-1}) \mapsto \left(a_{\tau(0)}, a_{\tau(1)}, \ldots, a_{\tau(n-1)}\right).$$

Si $\mathscr{C}$ y $\mathscr{D}$ son dos códigos de longitud n sobre R, diremos que $\mathscr{C}$ es *permutación-equivalente* a $\mathscr{D}$ si existe una permutación $\tau : I_n \to I_n$ tal que $\widetilde{\tau}(\mathscr{C}) = \mathscr{D}$. Es importante señalar que de manera más general, se dice que dos códigos $\mathscr{C}$ y $\mathscr{D}$ de longitud n sobre R son *monomial-equivalentes* si para algunas unidades $u_0, \ldots, u_{n-1}$ de R y una permutación $\tau : I_n \to I_n$ se tiene que

$$\mathscr{D} = \{(u_0 a_{\tau(0)}, u_1 a_{\tau(1)}, \ldots, u_{n-1} a_{\tau(n-1)}) : (a_0, a_1, \ldots, a_{n-1}) \in \mathscr{C}\}.$$

Sean R, S anillos y $m, n \geq 1$ enteros. Motivados en la definición de códigos permutación-equivalentes, diremos que dos *funciones* $f, g : R^n \to S^m$ *son permutación-equivalentes* si existe una permutación τ sobre I_m tal que para todo $A \in R^n$ tenemos que $g(A) = \widetilde{\tau}(f(A))$, es decir, el siguiente diagrama es conmutativo



Consecuentemente, si $\mathscr{C}$ es un código de longitud n sobre R y $f, g : R^n \to S^m$ son permutación-equivalentes, entonces los códigos $f(\mathscr{C})$ y $g(\mathscr{C})$ de longitud m sobre S son permutación-equivalentes puesto que $g(\mathscr{C}) = \widetilde{\tau}(f(\mathscr{C}))$.

En la Teoría de Códigos es necesario conocer qué tan diferentes son dos vectores de R^n. Con tal fin, se han definido varias funciones, llamadas *pesos*, que inducen métricas sobre R^n. Nuestro interés se centra escencialmente en aquellas métricas que están inducidas por el peso de Hamming, el peso de Lee y el peso homogéneo. Como veremos en los siguientes párrafos, las dos últimas dependen de la estructura del anillo. Por tal motivo, restringiremos la definición del peso de Lee al anillo $\mathbb{Z}_4$, y la del peso homogéneo, al anillo $\mathbb{Z}_{2^{k+1}}$, las cuales van de acuerdo a nuestras necesidades. El lector interesado en conocer las definiciones generales de estas funciones, puede consultar las referencias [21, 44].

El *peso de Hamming* $\omega_H : R^n \to \mathbb{Z}$ de un vector A se define como el número de coordenadas distintas de cero de A. La métrica $\delta_H : R^n \times R^n \to \mathbb{Z}$ inducida por ω_H es definida como $\delta_H(A, B) = \omega_H(A - B)$ y llamada la *distancia de Hamming*.

El *peso de Lee* $\omega_L : \mathbb{Z}_4 \to \mathbb{Z}$ está definido como $\omega_L(0) = 0, \omega_L(1) = \omega_L(3) = 1$ y $\omega_L(2) = 2$. De manera natural, el *peso de Lee* es extendido a una función, también denotada por ω_L, de $\mathbb{Z}_4^n$ a $\mathbb{Z}$. Esto es, dado $A = (a_0, \ldots, a_{n-1}) \in \mathbb{Z}_4^n$, se define su *peso de Lee* como $\omega_L(A) = \omega_L(a_0) + \cdots + \omega_L(a_{n-1})$, donde la suma es realizada sobre $\mathbb{Z}$. La métrica $\delta_L : \mathbb{Z}_4^n \times \mathbb{Z}_4^n \to \mathbb{Z}$ inducida por ω_L es definida como $\delta_L(A, B) = \omega_L(A - B)$ y llamada la *distancia de Lee*.

Para todo $k \geq 1$ definimos el *peso homogéneo* $\omega_h : \mathbb{Z}_{2^{k+1}} \to \mathbb{Z}$ como

$$\omega_h(a) = \begin{cases} 0, & \text{si } a = 0 \\ 2^k, & \text{si } a = 2^k \\ 2^{k-1}, & \text{en otro caso} \end{cases}$$

De igual modo que se ha hecho para el peso de Lee, el peso homogéneo se extiende a una función $\omega_h : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}$. En efecto, el *peso homogéneo* de un vector en $\mathbb{Z}_{2^{k+1}}^n$ se define como la suma sobre $\mathbb{Z}$ del peso homogéneo de cada una de sus coordenadas. Análogamente a los casos anteriores, la métrica $\delta_h : \mathbb{Z}_{2^{k+1}}^n \times \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}$ inducida por ω_h es llamada la *distancia homogénea* y definida como $\delta_h(A,B) = \omega_h(A-B)$.

Claramente, para el caso particular $k = 1$, el peso de Lee y homogéneo coinciden. En consecuencia, también coinciden las respectivas métricas inducidas por ellos.

Sea ω cualquiera de estos pesos y δ cualquiera de estas métricas. El *peso (mínimo)* y la *distancia (mínima)* (de Hamming, de Lee u homogéneo, según corresponda) de un código $\mathscr{C}$ están definidos, respectivamente, como

$$\omega(\mathscr{C}) = \min\{\omega(A) : A \in \mathscr{C},\ A \neq (0)_n\}$$

y

$$\delta(\mathscr{C}) = \min\{\delta(A,B) : A,B \in \mathscr{C},\ A \neq B\}.$$

Si el código $\mathscr{C}$ es lineal, entonces es fácil demostrar que $\omega(\mathscr{C}) = \delta(\mathscr{C})$. Por lo tanto, el cálculo de pesos y distancias mínimas de códigos lineales puede simplificarse a partir de este resultado.

Para el caso de campos finitos, $\delta_H(\mathscr{C})$ está relacionada con la cantidad de errores que el código puede detectar y corregir: si d es la distancia mínima de Hamming de $\mathscr{C}$, entonces $\mathscr{C}$ puede detectar $d-1$ errores y corregir $\lfloor (d-1)/2 \rfloor$, donde $\lfloor x \rfloor$ denota al mayor entero menor o igual que x. Para más detalles ver, por ejemplo [45, Sección 4.2] o bien [27, 38].

Cuando se trata de códigos lineales sobre campos finitos, la notación $[n,k,d]$ es usada para indicar los parámetros del código: longitud n, dimensión k y distancia mínima de Hamming d. Si el código no es lineal, la notación (n,M,d) es la más común.

Claramente, *dos códigos permutación-equivalentes tienen la misma cardinalidad, el mismo peso y distancia de Hamming, de Lee u homogénea*, según sea el caso. Por lo tanto, para fines de detección y corrección de errores, códigos permutación-equivalentes sobre campos finitos tienen las mismas capacidades. En algunos casos, esto nos permitirá dotar a ciertos códigos de algunas propiedades deseadas sin temor a que los parámetros del nuevo código sean distintos a los del primero.

Dados dos vectores $A = (a_0, \ldots, a_{n-1})$ y $B = (b_0, \ldots, b_{n-1})$ en R^n, se define su *producto escalar* (o *producto punto*) como

$$A \cdot B = a_0 b_0 + \cdots + a_{n-1} b_{n-1} \in R.$$

Análogamente a la teoría de espacios vectoriales, dos vectores $A, B \in R^n$ son llamados *ortogonales* si $A \cdot B = 0$. Asimismo, si $\mathscr{C}$ es un código de longitud n sobre R, entonces se define su *código ortogonal* como el conjunto

$$\mathscr{C}^{\perp} = \{A \in R^n \ : \ A \cdot B = 0, \ \forall B \in \mathscr{C}\}.$$

Un código $\mathscr{C}$ es llamado *auto-ortogonal* si $\mathscr{C}^{\perp} \subseteq \mathscr{C}$ y *auto-dual* si $\mathscr{C}^{\perp} = \mathscr{C}$. Nótese que si $\mathscr{C}$ es lineal, entonces $\mathscr{C}^{\perp}$ también lo es. En particular, esto aplica para códigos sobre campos finitos. En tal caso, cualquier matriz generadora de $\mathscr{C}^{\perp}$ es llamada una *matriz verificadora de paridad* para $\mathscr{C}$.

Para cualquier $\gamma \in U(R)$, definimos el *corrimiento $\gamma-$cíclico* como el R-automorfismo sobre R^n dado por

$$\nu_\gamma : (a_0, a_1, \ldots, a_{n-1}) \mapsto (\gamma a_{n-1}, a_0, \ldots, a_{n-2}).$$

Un ***código*** $\mathscr{C} \subseteq R^n$ es llamado ***consta-cíclico***, o de manera más específica *γ-cíclico*, si $\mathscr{C}$ permanece invariante con respecto a ν_γ, es decir, $\nu_\gamma(\mathscr{C}) = \mathscr{C}$. Un código 1-cíclico es llamado simplemente un *código cíclico* y un código (-1)-cíclico es llamado un *código negacíclico*. Para preservar la notación existente en la literatura [14, 54, 55], el corrimiento 1-cíclico será escrito como σ y llamado el *corrimiento cíclico*; el corrimiento (-1)-cíclico será denotado como ν y llamado *corrimiento negacíclico*.

Para cualesquiera enteros $n, m \geq 1$ y cualquier $\gamma \in U(R)$, el *corrimiento γ-casi-cíclico de índice m* es definido como la función $\nu_\gamma^{\otimes m} : R^{nm} \to R^{nm}$ dada por

$$\left(\mathbf{a}^{(0)} \,|\, \mathbf{a}^{(1)} \,|\, \cdots \,|\, \mathbf{a}^{(m-1)}\right) \mapsto \left(\nu_\gamma(\mathbf{a}^{(0)}) \,|\, \nu_\gamma(\mathbf{a}^{(1)}) \,|\, \cdots \,|\, \nu_\gamma(\mathbf{a}^{(m-1)})\right).$$

Observese que $\nu_\gamma^{\otimes 1} = \nu_\gamma$. En este sentido, el corrimiento γ-casi-cíclico es una generalización del corrimiento γ-cíclico.

Siguiendo con la terminología y la notación introducida anteriormente, el corrimiento 1-casi-cíclico será simplemente llamado el *corrimiento casi-cíclico de índice m* y denotado por $\sigma^{\otimes m}$. Análogamente, el corrimiento (-1)-casi-cíclico será escrito como $\nu^{\otimes m}$ y llamado el *corrimiento casi-negacíclico de índice m.*

Un *código* $\mathscr{C} \subseteq R^{nm}$ es llamado *γ-casi-cíclico de índice m* si $\nu_\gamma^{\otimes m}(\mathscr{C}) = \mathscr{C}$. En particular, si $\gamma = 1$, entonces $\mathscr{C}$ es llamado *casi-cíclico de índice m* y, si $\gamma = -1$, entonces $\mathscr{C}$ es llamado *casi-negacíclico de índice m.*

Observación. Formalmente, el término *consta-cíclico* hace referencia al concepto de código γ-cíclico más no al concepto de código γ-casi-cíclico. Así, el título del presente material sugiere que se abordan resultados únicamente para códigos γ-cíciclos sobre $\mathbb{Z}_{2^{k+1}}$. Sin embargo, también se obtienen resultados para códigos casi-cíclicos y $(1+2^k)$-casi-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, $k \geq 1$ (Capítulo 4). Pero dado que las aportaciones más importantes son para códigos $(1+2^{k-1})$-cíclicos y $(1+2^{k-1}+2^k)$-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, $k \geq 2$ (Capítulos 5 y 6), se decidió hacer énfasis en ello en el título de este material.

Veamos dos ejemplos de códigos sobre el anillo $\mathbb{Z}_4$. El primero de ellos es un código cíclico y que a su vez es un código casi-cíclico. El segundo, es un código casi-cíclico que no es cíclico. Aunque formalmente hemos usado la notación vectorial $(a_0, a_1, \ldots, a_{n-1})$ para escribir a los elementos de R^n, en los ejemplos escribiremos $a_0 a_1 \cdots a_{n-1}$ en lugar de $(a_0, a_1, \ldots, a_{n-1})$.

Ejemplo 1.2.1. Sea $\mathscr{C}_H$ el código lineal de longitud 4 sobre $\mathbb{Z}_4$ generado por $g_1 = 1111$, $g_2 = 0202$ y $g_3 = 0022$, es decir, $\mathscr{C}_H = \{\alpha g_1 + \beta g_2 + \gamma g_3 \ : \ \alpha, \beta, \gamma \in \mathbb{Z}_4\}$. Haciendo variar α, β y γ en $\mathbb{Z}_4$, obtenemos que los elementos de $\mathscr{C}$ son los siguientes 16 vectores:

$$\begin{array}{cccccccc} 0000 & 1111 & 2222 & 3333 & 0202 & 1313 & 2020 & 3131 \\ 0022 & 1133 & 2200 & 3311 & 0220 & 1331 & 2002 & 3113 \end{array}$$

Del arreglo anterior es fácil verificar por inspección directa que el código $\mathscr{C}_H$ es un código cíclico. Asimismo, observe que también este código es casi-cíclico de índice $m = 2$, es decir, para todo $a_0 a_1 a_2 a_3 \in \mathscr{C}$ se tiene que $\sigma^{\otimes 2}(a_0 a_1\ a_2 a_3) = a_1 a_0\ a_3 a_2$ es un vector que nuevamente está en $\mathscr{C}$. Por otra parte, ya que $\mathscr{C}_H$ es lineal, su distancia mínima de Lee coincide con su peso mínimo de Lee, el cual es $\omega_L(\mathscr{C}_H) = 4$. De hecho, note que $\omega_L(z) = 4$, para todo $z \in \mathscr{C}_H \setminus \{0000, 2222\}$.

Ejemplo 1.2.2. Sea $ZRM(2,4)$ el código lineal de longitud 8 sobre $\mathbb{Z}_4$ generado por los vectores $g_0 = 1111\ 1111$, $g_1 = 0101\ 0101$, $g_2 = 0011\ 0011$, $g_3 = 0002\ 0002$, $g_4 = 0000\ 1111$, $g_5 = 0000\ 0202$ y $g_6 = 0000\ 0022$. Esto quiere decir que $ZRM(2,4)$ consiste de todas las combinaciones lineales $a_0 g_0 + a_1 g_1 + \cdots + a_6 g_6$, las cuales pueden ser expresadas de forma más precisa como un producto de matrices:

$$Z = \begin{pmatrix} a_0\ a_1\ a_2\ a_3\ a_4\ a_5\ a_6 \end{pmatrix} \begin{pmatrix} 1111\ 1111 \\ 0101\ 0101 \\ 0011\ 0011 \\ 0002\ 0002 \\ 0000\ 1111 \\ 0000\ 0202 \\ 0000\ 0022 \end{pmatrix} = \begin{pmatrix} a_0 \\ a_0 + a_1 \\ a_0 + a_2 \\ a_0 + a_1 + a_2 + 2a_3 \\ a_0 + a_4 \\ a_0 + a_1 + a_4 + 2a_5 \\ a_0 + a_2 + a_4 + 2a_6 \\ a_0 + a_1 + a_2 + 2a_3 + a_4 + 2a_5 + 2a_6 \end{pmatrix},$$

donde $a_0, \ldots, a_6 \in \mathbb{Z}_4$. De aquí es claro que $Z = 0000\ 0000$ si y sólo si $a_0 = a_1 = a_2 = 2a_3 = a_4 = 2a_5 = 2a_6 = 0$. En otros términos, esto significa que un mismo vector lo podemos escirbir de 2^3

formas distintas pues $2a_3 = 2a_5 = 2a_6 = 0$ si y sólo si a_3, a_5, a_6 están en el ideal maximal de $\mathbb{Z}_4$, o sea, $a_3, a_5, a_6 \in \{0,2\}$. Por lo tanto, tenemos que el número total de combinaciones lineales distintas que se pueden formar con los vectores g_i es $4^7/2^3 = 2^{11}$. Así, el código $ZRM(2,4)$ tiene $2^{11} = 2048$ elementos y, por lo tanto, es impráctico listar todos estos vectores para verificar que este código es casi-cíclico de índice 2. Sin embargo, como $ZRM(2,4)$ está generado por los g_i, se sigue que $ZRM(2,4)$ es casi-cíclico de índice 2 si y sólo si $\sigma^{\otimes 2}(g_i) \in ZRM(2,4)$ para todo i. Probaremos que $\sigma^{\otimes 2}(g_i) \in ZRM(2,4)$ escribiendo a cada uno de estos vectores como combinación lineal de los g_i:

$$\begin{array}{ccc} & \sigma^{\otimes 2} & \\ g_0 = 1111\ 1111 & \longrightarrow & 1111\ 1111 = g_0 \\ g_1 = 0101\ 0101 & \longrightarrow & 0101\ 0101 = g_1 \\ g_2 = 0011\ 0011 & \longrightarrow & 1001\ 1001 = g_0 + 3g_2 + 3g_3 + g_6 \\ g_3 = 0002\ 0002 & \longrightarrow & 1010\ 1010 = g_0 + 3g_3 \\ g_4 = 0000\ 1111 & \longrightarrow & 0000\ 2002 = 2g_1 + g_4 + g_5 \\ g_5 = 0000\ 0202 & \longrightarrow & 0000\ 2020 = 2g_1 + g_5 \\ g_6 = 0000\ 0022 & \longrightarrow & 2000\ 2000 = 2g_0 + 2g_2 + 2g_3 + g_6 \end{array}$$

Por lo tanto, el código $ZRM(2,4)$ es casi-cíclico de índice 2. No obstante, este código no es cíclico pues, por ejemplo, $g_1 \in ZRM(2,4)$ pero $\sigma(g_1) = 10000111 \notin ZRM(2,4)$. Finalmente, ya que $ZRM(2,4)$ es lineal, $d_L(ZRM(2,4)) = \omega_L(ZRM(2,4))$. Observe que $\omega_L(g_1) = 4$, de donde concluimos que $\omega_L(ZRM(2,4)) \leq 4$. Más aún, con la ayuda del programa computacional MAGMA® V2.15-13 (Student Version) obtuvimos que $\omega_L(ZRM(2,4)) = 4$.

Es conocido que el código ortogonal de un código cíclico es también un código cíclico. Asimismo, se sabe que el código dual de un código negacíclico es nuevamente un código negacíclico. En general, tenemos el siguiente resultado acerca del código dual de un código γ-casi-cíclico. Este resultado generaliza a [13, Proposición 2.4].

Proposición 1.2.3. *Sea R un anillo, $\gamma \in U(R)$, $n, m \geq 1$ enteros y $\mathscr{C}$ un código γ-casi-cíclico de índice m y longitud nm. Entonces $\mathscr{C}^{\perp}$ es un código γ^{-1}-casi cíclico de índice m y longitud nm.*

Demostración. Sea $A = \left(A^{(0)}|\cdots|A^{(m-1)}\right) \in \mathscr{C}$ y sea $B = \left(B^{(0)}|\cdots|B^{(m-1)}\right) \in \mathscr{C}^{\perp}$. Entonces

$$\begin{aligned} \nu_{\gamma}^{\otimes m}(A) \cdot \nu_{\gamma^{-1}}^{\otimes m}(B) &= \nu_{\gamma}\left(A^{(0)}\right) \cdot \nu_{\gamma^{-1}}\left(B^{(0)}\right) + \cdots + \nu_{\gamma}\left(A^{(m-1)}\right) \cdot \nu_{\gamma^{-1}}\left(B^{(m-1)}\right) \\ &= \sigma\left(A^{(0)}\right) \cdot \sigma\left(B^{(0)}\right) + \cdots + \sigma\left(A^{(m-1)}\right) \cdot \sigma\left(B^{(m-1)}\right) \\ &= A^{(0)} \cdot B^{(0)} + \cdots + A^{(m-1)} \cdot B^{(m-1)} = 0. \end{aligned}$$

Haciendo variar el vector A en todo $\mathscr{C}$, las relaciones anteriores muestran que $\nu_{\gamma^{-1}}^{\otimes m}(B)$ es ortogonal a cada elemento del código $\nu_{\gamma}^{\otimes m}(\mathscr{C}) = \mathscr{C}$. Esto significa que $\nu_{\gamma^{-1}}^{\otimes m}(B) \in \mathscr{C}^{\perp}$ y, por lo tanto, $\mathscr{C}^{\perp}$ es invariante con respecto a la acción de $\nu_{\gamma^{-1}}^{\otimes m}$. □

Ejemplo 1.2.4. Dado que el código $\mathscr{C}_H$ introducido en el Ejemplo 1.2.1 es cíclio lineal de longitud 4 sobre $\mathbb{Z}_4$, entonces $\mathscr{C}_H^\perp$ es también un código cíclico lineal de índice 2 y longitud 4 sobre $\mathbb{Z}_4$. Los elementos de $\mathscr{C}_H^\perp$ son:

$$\begin{array}{cccccccc} 0000 & 1012 & 2020 & 3032 & 0121 & 1133 & 2101 & 3311 \\ 3113 & 0202 & 1210 & 2222 & 3230 & 0323 & 1331 & 2303 \end{array}$$

Observe que $\mathscr{C}_H^\perp$ está generado por los vectores 1012 y 0121. Asimismo, ya que $\mathscr{C}$ es un código casi-cíclico lineal de índice 2, entonces $\mathscr{C}^\perp$ es un código casi-cíclico lineal de índice 2. Finalmente, note que $\mathscr{C}_H$ no es un código auto-dual, pues $\mathscr{C} \neq \mathscr{C}^\perp$, y que su peso mínimo de Lee es $\omega_L(\mathscr{C}_H^\perp) = 4$. Nótese además que $\mathscr{C} \cap \mathscr{C}^\perp = \{0000, 2020, 1331, 3113, 2222\}$, a diferencia de los espacios vectoriales sobre los reales o los complejos, en donde $\mathscr{C} \cap \mathscr{C}^\perp$ es precisamente el vector cero.

Ejemplo 1.2.5. Por la Proposicón 1.2.3, el código dual del código $ZRM(2,4)$ desarrollado en el Ejemplo 1.2.2 es un código casi-cíclico de índice 2 y longitud 8 sobre $\mathbb{Z}_8$. Más aún, ya que $ZRM(2,4)$ es lineal, entonces $ZRM(2,4)^\perp$ también lo es y, por lo tanto, podemos describir a $ZRM(2,4)^\perp$ en términos de sus generadores. Con la ayuda del programa computacional MAGMA® V2.15-13 (Student Version) obtuvimos que $ZRM(2,4)^\perp$ está generado por los vectores $g_0^\perp = 11111111$, $g_1^\perp = 02020202$, $g_2^\perp = 00220022$, $g_3^\perp = 00002222$. Usando argumentos similares a los del Ejemplo 1.2.2, es fácil verificar que $ZRM(2,4)^\perp$ tiene 32 vectores. El peso mínimo de Lee del código $ZRM(2,4)^\perp$ es 8.

Existe una manera natural de identificar a los elementos de R^n con los elementos del anillo $R[x]/\langle x^n - \gamma\rangle$, donde $\gamma \in U(R)$. Esta identificación es conocida como la *representación polinomial de* R^n y está determinada por el R-isomorfismo (de R-módulos)

$$P : R^n \to R[x]/\langle x^n - \gamma\rangle$$

definido como

$$A = (a_0, a_1, \ldots, a_{n-1}) \mapsto P(A) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle x^n - \gamma\rangle.$$

Con esta definición en mente, es claro que en el anillo $R[x]/\langle x^n - \gamma\rangle$, la multiplicación $(x + \langle x^n - \gamma\rangle)P(A)$ corresponde al corrimiento γ-cíclico de $A \in R^n$. Habitualmente, un código $\mathscr{C} \subseteq R^n$ también suele ser identificado con el conjunto $P(\mathscr{C}) = \{P(A) : A \in \mathscr{C}\}$, por lo que hablaremos indistintamente de un código γ-cíclico (o sus elementos) y de su representación polinomial.

La demostración del siguiente resultado es similar a su homólogo sobre campos finitos [7, 27, 38, 44, 45].

Proposición 1.2.6. *Un código $\mathscr{C}$ de longitud $n \geq 1$ sobre el anillo R es γ-cíclico lineal si y sólo si $P(\mathscr{C})$ es un ideal del anillo $R[x]/\langle x^n - \gamma\rangle$.*

Una construcción explícita de los ideales del anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n-\gamma\rangle$, cuando n es impar, será realizada en la siguiente sección y estará basada en las construcciones observadas en [30,54,55]. Esta información será utilizada para contruir ejemplos de códigos γ-cíclicos que ilustren los resultados obtenidos en este manuscrito.

1.3. Códigos consta-cíclicos lineales sobre $\mathbb{Z}_{2^{k+1}}$

En esta sección estudiaremos una forma de construir códigos consta-cíclicos lineales de longitud n impar sobre $\mathbb{Z}_{2^{k+1}}$. El método que emplearemos será construir códigos cíclicos lineales de longitud n sobre $\mathbb{Z}_{2^{k+1}}$ y después demostraremos que los códigos γ-cíclicos de la misma longitud sobre $\mathbb{Z}_{2^{k+1}}$ pueden ser obtenidos como imágenes del siguiente isomorfismo de anillos

$$\mu_\beta : \mathbb{Z}_{2^{k+1}}[x]/\langle x^n-1\rangle \to \mathbb{Z}_{2^{k+1}}[x]/\langle x^n-\gamma\rangle$$

dado por

$$A(x)+\langle x^n-1\rangle \mapsto A(\beta x)+\langle x^n-\gamma\rangle,$$

donde $\beta^n=\gamma^{-1}$ en $\mathbb{Z}_{2^{k+1}}$ y $A(\beta x)$ significa reemplazar x por βx en el polinomio $A(x)$. Esta técnica es una generalización de la que se empleó en [54, 55] para la construcción de códigos negacíclicos de longitud impar sobre $\mathbb{Z}_4$. Vale la pena mencionar que la restricción sobre la longitud del código se debe principalmente a dos razones: (1) La factorización de x^n-1 sobre $\mathbb{Z}_{2^{k+1}}[x]$ como producto de polinomios mónicos básicos irreducibles y primos relativos por parejas, es única ([30, Corolario 2.6]), mientras que para el caso $\mathrm{mcd}(n,2)\neq 1$ tal factorización no se da; (2) para n impar, el elemento β siempre existe y es único, mientras que para el caso $\mathrm{mcd}(n,2)\neq 1$ no siempre existe, y cuando existe no es único [28]. Por ejemplo, el polinomio x^4-1 se factoriza como un producto de polinomios irreducibles sobre $\mathbb{Z}_4$ de las siguientes formas:

$$\begin{aligned} x^4-1 &= (x-1)(x+1)(x^2+1) = (x-1)(x-1)(x^2+2x-1)\\ &= (x+1)(x+1)(x^2+2x-1)\end{aligned}$$

Note que, a diferencia del caso n impar, los polinomios (x^2+1), (x^2+2x-1) no son básicos irreducibles. De este modo, la factorización de x^4-1 no necesariamente se da como un producto de polinomios básicos irreducibles. Por otra parte, si $\gamma=-1$, entonces $\gamma^{-1}=-1=3$ en $\mathbb{Z}_4$. Pero en $\mathbb{Z}_4$, no existe una unidad β tal que $\beta^4=3$ (todas las unidades en $\mathbb{Z}_4$ son de orden 2). Por lo tanto, códigos cíclicos no pueden relacionarse con códigos negacíclicos mediante la aplicación μ_β. Sin emabrgo, en la descripción de los códigos cíclicos de longitud par (tambien llamados en la literatura como *códigos de raíces repetidas*) como ideales en el anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n-1\rangle$ se ha hecho uso de otras ideas (cf. [1,8,9,12,13,15,31,37,46]).

1.3.1. Códigos cíclicos lineales sobre $\mathbb{Z}_{2^{k+1}}$

En este apartado restringiremos los resultados presentados en [30] al caso $p = 2$. En [30] se investiga una forma de construir a los ideales del anillo $\mathbb{Z}_{p^k}[x]/\langle x^n - 1\rangle$, donde p es un primo y n un entero tal que $\mathrm{mcd}(p,n) = 1$. (Note que en consecuencia esto nos proporciona una técnica para construir códigos cíclicos de longitud n sobre $\mathbb{Z}_{p^{k+1}}$). Estos resultados fueron generalizados en [14], el cual puede ser una referencia alternativa a [30]. Para construcciones de códigos cíclicos sobre campos finitos (por ejemplo $\mathbb{F}_2$) el lector puede consultar [7, 27, 38, 44, 45].

Recordemos que a cada elemento de $\mathbb{Z}_{2^{k+1}}^n$ se le asocia de manera biúnivoca un polinomio en $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$ vía la *representación polinomial* definida como

$$P : (a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle,$$

y que un código $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ es cíclico lineal si y sólo si $P(\mathscr{C})$ es un ideal en $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$. Por lo tanto, para construir todos los códigos cíclicos lineales de longitud n sobre $\mathbb{Z}_{2^{k+1}}$, basta construir todos los ideales del anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$.

En [30] se presenta un método sistemático para construir los ideales del anillo cociente $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$. En términos generales, la idea consiste en obtener una factorización de $x^n - 1$ como un producto de polinomios mónicos, básicos ireeducibles y coprimos (Corolario 1.1.2), digamos $x^n - 1 = a_1(x)\cdots a_r(x)$, y entonces distribuir sin repetición estos r factores en $k+2$ casillas denominadas $f_0, \ldots, f_{k+1}$, con la condición de que si alguna casilla queda vacía, entonces se le asigna un uno. De este modo, se tiene que $x^n - 1 = f_0 \cdots f_{k+1}$. Consecuentemente los polinomios f_i dividen a $x^n - 1$ y, por lo tanto, tiene sentido construir los polinomios $\widehat{f}_i = x^n - 1/f_i$ y $\widehat{F}_i = \widehat{f}_i + \langle x^n - 1\rangle$. Así, es claro que $I = \langle \widehat{F}_1, 2\widehat{F}_2, \ldots, 2^k\widehat{F_{k+1}}\rangle$ es un ideal de $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$.

Lo que no es inmediato es que todo ideal de dicho anillo pueda ser construido de esa forma. De este modo, la aportación de [30] fue demostrar que eso es posible.

Teorema 1.3.1 ([30, Teorema 3.4]). *Sea $n \geq 1$ un entero impar e $I \subseteq \mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$ un ideal. Entonces existe una única colección $f_0, f_1, \ldots, f_{k+1}$ de polinomios (posiblemente algunos de ellos iguales al polinomio constante uno) mónicos y coprimos tales que $f_0 f_1 \cdots f_{k+1} = x^n - 1$ e $I = \langle \widehat{F}_1, 2\widehat{F}_2, \ldots, 2^k\widehat{F_{k+1}}\rangle$. Además, $|I| = 2^S$, donde $S = \sum_{i=0}^{k}(k+1-i)gr(f_{i+1})$.*

Más aún, en [30, Corolario 3.6] se demuestra que el ideal $I = \langle \widehat{F}_1, 2\widehat{F}_2, \ldots, 2^k\widehat{F_{k+1}}\rangle$ es generado por el polinomio

$$F = \widehat{F}_1 + 2\widehat{F}_2 + \ldots + 2^k\widehat{F_{k+1}}$$

y, por lo tanto, el anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$ es de ideales principales.

Ya que la colección de polinomios f_i es única, también lo son los $\widehat{F}_i$. Esto nos permite llamar a los polinomios $\widehat{F}_1, 2\widehat{F}_2, \ldots, 2^k\widehat{F_{k+1}}$ los *generadores del código cíclico* lineal $\mathscr{C} = P^{-1}(I)$, y al

polinomio $F = \widehat{F_1} + 2\widehat{F_2} + \ldots + 2^k\widehat{F_{k+1}}$ *el polinomio generador* de $\mathscr{C}$. A partir de este punto, usaremos la siguiente notación para expresar, respectivamente, estos términos:

$$\mathscr{C} = \langle \widehat{F_1}, 2\widehat{F_2}, \ldots, 2^k\widehat{F_{k+1}} \rangle, \qquad \mathscr{C} = \langle F \rangle.$$

Ilustremos el Teorema 1.3.1 con los enteros $k = 3$ y $n = 7$. Con la ayuda del programa computacional MAGMA® V2.15-13 (Student Version), calculamos la factorización de $x^7 - 1$ sobre $\mathbb{Z}_{16}[x]$ como un producto de polinomios mónicos, básicos irreducibles y coprimos:

$$x^7 - 1 = a_1(x)a_2(x)a_3(x),$$

donde $a_1(x) = x + 15$, $a_2(x) = x^3 + 6x^2 + 5x + 15$ y $a_3(x) = x^3 + 11x^2 + 10x + 15$. Con el fin de simplificar la notación, en lo sucesivo usaremos a los polinomios de grado a lo más $n-1$ para representar a sus correspondientes clases laterales en $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1 \rangle$.

Ejemplo 1.3.2. Sean

$$f_0 = a_1(x)a_2(x), \quad f_1 = a_3(x), \quad f_2 = 1, \quad f_3 = 1, \quad f_4 = 1. \tag{1.1}$$

Entonces

$$\widehat{f_0} = a_3(x), \quad \widehat{f_1} = a_1(x)a_2(x), \quad \widehat{f_2} = \widehat{f_3} = \widehat{f_4} = a_1(x)a_2(x)a_3(x) = x^7 - 1,$$

lo cual implica que en $\mathbb{Z}_{2^4}[x]/\langle x^7 - 1 \rangle$ se tiene

$$\widehat{F_0} = a_3(x), \quad \widehat{F_1} = a_1(x)a_2(x), \quad \widehat{F_2} = \widehat{F_3} = \widehat{F_4} = 0.$$

En consecuencia, tenemos que

$$\mathscr{C} = \left\langle \widehat{F_1}, 2\widehat{F_2}, 2^2\widehat{F_3}, 2^3\widehat{F_4} \right\rangle = \left\langle \widehat{F_1} \right\rangle = \langle a_1(x)a_2(x) \rangle = \langle x^4 + 5x^3 + 15x^2 + 10x + 1 \rangle$$

es un código cíclico lineal de longitud 7 sobre $\mathbb{Z}_{16}$ cuya cardinalidad es 2^S, donde S está dado por la fórmula $S = \sum_{i=0}^{i=3}(4+i)gr(f_{i+1})$. Sustituyendo se obtiene que $S = 12$. Por lo tanto, $\mathscr{C}$ es un código cíclico de cardinalidad es 2^{12} generado por los polinomios $\widehat{F_1}, 0, 0, 0$. El polinomio generador de $\mathscr{C}$ es en este caso $\widehat{F_1}$.

Ejemplo 1.3.3. Continuando con la misma notación de la factorización de $x^7 - 1$, sean ahora

$$f_0 = a_1(x), \quad f_1 = a_2(x), \quad f_2 = 1, \quad f_3 = a_3(x), \quad f_4 = 1.$$

Entonces

$$\widehat{f_0} = a_2(x)a_3(x), \quad \widehat{f_1} = a_1(x)a_3(x), \quad \widehat{f_2} = x^7 - 1, \quad \widehat{f_3} = a_1(x)a_2(x), \quad \widehat{f_4} = x^7 - 1.$$

Por lo tanto, en $\mathbb{Z}_{2^4}[x]/\langle x^7-1\rangle$ se tiene que

$$\widehat{F_0} = a_2(x)a_3(x), \quad \widehat{F_1} = a_1(x)a_3(x), \quad \widehat{F_2} = 0, \quad \widehat{F_3} = a_1(x)a_2(x), \quad \widehat{F_4} = 0.$$

Así,

$$\mathscr{C} = \left\langle \widehat{F_1}, 2\widehat{F_2}, 2^2\widehat{F_3}, 2^3\widehat{F_4} \right\rangle = \left\langle \widehat{F_1}, 2^2\widehat{F_3} \right\rangle = \langle a_1(x)a_3(x), 4a_1(x)a_2(x) \rangle$$

es un código cíclico lineal de longitud 7 sobre $\mathbb{Z}_{16}$ y cardinalidad 2^{24}. Explícitamente, los generadores del código $\mathscr{C}$ son $a_1(x)a_3(x) = x^4 + 10x^3 + 15x^2 + 5x + 1$ y $4a_1(x)a_2(x) = 4x^4 + 4x^3 + 12x^2 + 8x + 4$. En consecuencia, el polinomio generador de $\mathscr{C}$ es

$$F = a_1(x)a_3(x) + 4a_1(x)a_2(x) = 5x^5 + 14x^3 + 11x^2 + 13x + 5.$$

1.3.2. Códigos γ-cíclicos lineales sobre $\mathbb{Z}_{2^{k+1}}$

Recordemos que por la Proposición 1.2.2, los códigos γ-cíclicos lineales de longitud n sobre $\mathbb{Z}_{2^{k+1}}$, donde γ es una unidad en $\mathbb{Z}_{2^{k+1}}$, están en correspondencia biyectiva, por medio de la representación polinomial, con los ideales del anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \gamma\rangle$. Para el caso de códigos negacíclicos ($\gamma = -1$) ya existen resultados que describen una técnica para calcular a todos los ideales del anillo $R[x]/\langle x^n + 1\rangle$, donde n es impar y R es un anillo finito de cadena [14]. (Si n es par, también se tienen descripciones para esta clase de códigos [1, 8, 13, 14, 37]). Siendo $\mathbb{Z}_{2^{k+1}}$ un anillo de cadena, la misma técnica puede ser aplicada para calcular todos los ideales de $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n + 1\rangle$ y, consecuentemente, todos los códigos negacíclicos. Sin embargo, no conocemos algún trabajo que proporcione una técnica para calcular los ideales del anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \gamma\rangle$, donde $\gamma \neq 1, -1$. En esta sección demostraremos que cuando n es impar es posible describir a los ideales de $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \gamma\rangle$ a partir de los resultados de la sección anterior. El método que presentaremos es una generalización de la que aparece en [14, 54, 55].

Antes de proceder con el principal objetivo de este apartado, necesitamos algunos conceptos y resultados que son comunes en la Teoría de Números. Éstos pueden ser consultados, por ejemplo, en [28]. Recordemos que dado $\gamma \in U(\mathbb{Z}_{2^{k+1}})$ y $n \geq 1$ un entero, se le llama *raíz n-ésima* de γ a todo elemento $\eta \in U(\mathbb{Z}_{2^{k+1}})$ tal que $\eta^n = \gamma$. Para el caso n impar, la existencia de las raíces n-ésimas está garantizada por el siguiente resultado.

Lema 1.3.4 ([28, Proposición 4.4.2])**.** *Sean $k \geq 2$ un entero y $\gamma \in U(\mathbb{Z}_{2^{k+1}})$. Entonces para todo entero impar $n \geq 1$ existe una única raíz n-ésima de γ.*

Note que si γ es una unidad en $\mathbb{Z}_{2^{k+1}}$, entonces γ^{-1} también es una unidad y por lo tanto, el Lema 1.3.4 implica lo siguiente:

Corolario 1.3.5. *Para todo $k \geq 1$, $\gamma \in U(\mathbb{Z}_{2^{k+1}})$ y entero impar $n \geq 1$, existe un único β en $U(\mathbb{Z}_{2^{k+1}})$ tal que $\beta^n = \gamma^{-1}$ en $\mathbb{Z}_{2^{k+1}}$.*

La siguiente aportación establece que los códigos γ-cíclicos de longitud impar están estrechamente ligados a los códigos cíclicos de la misma longitud.

Lema 1.3.6. *Sean $k,n \geq 1$ enteros con n impar. Considere $\gamma \in U(\mathbb{Z}_{2^{k+1}})$ y sea β la raíz n-ésima de γ^{-1}. Definamos*

$$\mu_\beta : \mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle \to \mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \gamma\rangle$$

como

$$A(x) + \langle x^n - 1\rangle \mapsto A(\beta x) + \langle x^n - \gamma\rangle.$$

Entonces μ_β es un isomorfismo de anillos y, por lo tanto, un subconjunto I de $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$ es un ideal si y sólo si $\mu_\beta(I)$ es un ideal en $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \gamma\rangle$. En particular, $|I| = |\mu_\beta(I)|$.

Demostración. Ya que en esencia la acción de μ_β consiste en evaluar $A(x)$ en βx, se sigue que μ_β es un homomorfismo. Así, únicamente demostraremos que μ_β está bien definido. Argumentos similares muestran la inyectividad de esta aplicación y, por lo tanto, la biyectividad. Supongamos que $A(x) + \langle x^n - 1\rangle = B(x) + \langle x^n - 1\rangle$. Entonces existe un polinomio $H(x) \in \mathbb{Z}_{2^{k+1}}[x]$ tal que en $\mathbb{Z}_{2^{k+1}}[x]$

$$A(x) - B(x) = (x^n - 1)H(x)$$

Sustituyendo x por βx en la expresión anterior obtenemos

$$A(\beta x) - B(\beta x) = (\beta^n x^n - 1)H(\beta x) = \gamma^{-1}(x^n - \gamma)H(\beta x).$$

Por lo tanto, $A(\beta x) - B(\beta x) \in \langle x^n - \gamma\rangle$ y así, μ_β está bien definido. Como consecuencia de la inyectividad de μ_β, los ideales I y $\mu_\beta(I)$ tienen la misma cardinalidad. □

En [30, Corolario 3.3] se demostró que el número de ideales de $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$ es $(k+2)^r$, donde r es el número de factores en la factorización de $x^n - 1$ como un producto de polinomios mónicos, básicos irreducibles y coprimos. (Siendo n impar, el número de factores en dicha factorización es único y, por lo tanto, no existe ambigüedad en la cantidad $(k+2)^r$). Consecuentemente, por el Lema 1.3.6, tenemos el siguiente:

Corolario 1.3.7. *Siguiendo con la notación del Lema 1.3.6, el número de ideales en el anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \gamma\rangle$ es $(k+2)^r$, donde r es el número de factores en la factorización de $x^n - 1$ como un producto de polinomios mónicos, básicos irreducibles y coprimos.*

Como segundo punto importante mostraremos cómo recuperar la factorización de $x^n - \gamma$ en $\mathbb{Z}_{2^{k+1}}[x]$ a partir de una factorización de $x^n - 1$. Recuerde que dado un polinomio $a(x)$ con coeficientes en $\mathbb{Z}_{2^{k+1}}$, escribimos $a(\beta x)$ para entender que hemos sustituido x por βx en la expresión de $a(x)$.

Lema 1.3.8. *Sean $n \geq 1$ un entero impar, $\gamma \in U(\mathbb{Z}_{2^{k+1}})$ y β la raíz n-ésima de γ^{-1}. Sea $x^n - 1 = a_1(x)\cdots a_r(x)$ una factorización de $x^n - 1$ como un producto de polinomios mónicos y coprimos. Defina*

$$b_i(x) = \beta^{-gr(a_i)} a_i(\beta x), \qquad 1 \leq i \leq r.$$

Entonces $x^n - \gamma = b_1(x)\cdots b_r(x)$ es una factorización de $x^n - \gamma$ como un producto de polinomios mónicos y coprimos. Además, si los polinomios $a_i(x)$ son básicos irreducibles, entonces también lo son los polinomios $b_i(x)$, $1 \leq i \leq r$.

Demostración. Sustituyendo x por βx en la factorización de $x^n - 1$ obtenemos

$$a_1(\beta x)\cdots a_r(\beta x) = (\beta x)^n - 1 = \beta^n x^n - 1 = \gamma^{-1}x^n - 1.$$

Multiplicando ambos lados de la ecuación anterior por $\gamma = \beta^{-n}$ obtenemos

$$\beta^{-n} a_1(\beta x)\cdots a_r(\beta x) = x^n - \gamma.$$

Dado que los polinomios $a_i(x)$ son mónicos, básicos irrreducibles y coprimos, entonces es fácil verificar que los polinomios $b_i(x)$ también tienen esas propiedades. Además, ya que $\sum_{i=1}^{r} gr(a_i(x)) = n$ se sigue que $b_1(x)\cdots b_r(x) = x^n - \gamma$. □

Recuerde que si $\gamma \in U(\mathbb{Z}_{2^{k+1}})$ y $f(x) \in \mathbb{Z}_{2^{k+1}}[x]$ divide al polinomio $x^n - \gamma$, entonces escribiremos $\widehat{f(x)} = (x^n - \gamma)/f(x)$ y $\widehat{F(x)} = \widehat{f(x)} + \langle x^n - \gamma \rangle$. La demostración del siguiente resultado depende del Teorema 1.3.1.

Teorema 1.3.9. *Sean $n \geq 1$ un entero impar y $\gamma, \beta \in U(\mathbb{Z}_{2^{k+1}})$ tales que $\beta^n = \gamma^{-1}$. Supongamos que J es un ideal de $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \gamma \rangle$. Entonces existe una única colección $g_0, g_1, \ldots, g_{k+1}$ de polinomios (posiblemente algunos de ellos iguales al polinomio constante 1) mónicos y coprimos tales que $g_0 g_1 \cdots g_{k+1} = x^n - \gamma$ y $J = \langle \widehat{G_1}, 2\widehat{G_2}, \ldots, 2^k \widehat{G_{k+1}} \rangle$. Además, $|J| = 2^S$, donde $S = \sum_{i=0}^{k} (k+1-i) gr(g_{i+1})$.*

Demostración. Sea $I = \mu_\beta^{-1}(J)$. Entonces, se sigue del Lema 1.3.6 que I es un ideal del anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1 \rangle$. Por lo tanto, existe una única colección $f_0, f_1, \ldots, f_{k+1}$ de polinomios (posiblemente algunos de ellos iguales al polinomio constante 1) los cuales son mónicos, coprimos y son tales que $f_0 f_1 \cdots f_{k+1} = x^n - 1$ e $I = \langle \widehat{F_1}, 2\widehat{F_2}, \ldots, 2^k \widehat{F_{k+1}} \rangle$. Sea $g_i(x) = \beta^{-gr(f_i)} f_i(\beta x)$, $0 \leq i \leq k+1$. Entonces por el Lema 1.3.8, los polinomios g_i son mónicos, coprimos y su producto es igual a $x^n - \gamma$. Por otro lado, aplicando μ_β a $I = \langle \widehat{F_1}, 2\widehat{F_2}, \ldots, 2^k \widehat{F_{k+1}} \rangle$ obtenemos

$$J = \mu_\beta(I) = \langle \mu_\beta(\widehat{F_1}), 2\mu_\beta(\widehat{F_2}), \ldots, 2^k \mu_\beta(\widehat{F_{k+1}}) \rangle.$$

Como consecuencia de que β es una unidad se tiene que

$$J = \langle \beta^{-gr(\widehat{f_1})} \mu_\beta(\widehat{F_1}), 2\beta^{-gr(\widehat{f_2})} \mu_\beta(\widehat{F_2}), \ldots, 2^k \beta^{-gr(\widehat{f_{k+1}})} \mu_\beta(\widehat{F_{k+1}}) \rangle.$$

Ahora, afirmamos que $\widehat{G_i} = \beta^{-gr(\widehat{f_i})}\mu_\beta(\widehat{F_i})$. Para este fin, nótese que para todo $0 \leq i \leq k+1$, tenemos que

$$\widehat{G_i} = \widehat{g_i(x)} + \langle x^n - \gamma \rangle = \prod_{j=0, j\neq i}^{k+1} g_j(x) + \langle x^n - \gamma \rangle$$

Sustituyendo $g_j(x) = \beta^{-gr(f_j)} f_j(\beta x)$ en el producto del lado derecho de la ecuación anterior y simplificándolo obtenemos

$$\begin{aligned}\widehat{G_i} &= \left(\prod_{j=0, j\neq i}^{k+1} \beta^{-gr(f_j)} \right) \left(\prod_{j=0, j\neq i}^{k+1} f_j(\beta x) + \langle x^n - \gamma \rangle \right) \\ &= \beta^{-gr(\widehat{f_i})} \left(\prod_{j=0, j\neq i}^{k+1} f_j(\beta x) + \langle x^n - \gamma \rangle \right).\end{aligned}$$

Dado que

$$f_j(\beta x) + \langle x^n - \gamma \rangle = \mu_\beta \left(f_j(x) + \langle x^n - 1 \rangle \right)$$

podemos sustituir en la expresión de $\widehat{G_i}$ y usar que μ_β es un isomorfismo de anillos (Lema 1.3.6) para conseguir

$$\widehat{G_i} = \beta^{-gr(\widehat{f_i})} \left(\prod_{j=0, j\neq i}^{k+1} \mu_\beta \left(f_j(x) + \langle x^n - 1 \rangle \right) \right) = \beta^{-gr(\widehat{f_i})} \mu_\beta \left(\prod_{j=0, j\neq i}^{k+1} f_j(x) + \langle x^n - 1 \rangle \right),$$

de donde la afirmación se sigue al recordar que

$$\prod_{j=0, j\neq i}^{k+1} f_j(x) + \langle x^n - 1 \rangle = \widehat{f_i(x)} + \langle x^n - 1 \rangle = \widehat{F_i(x)}.$$

Finalmente, por el Lema 1.3.6, la cardinalidad de $J = \mu_\beta(I)$ coincide con la cardinalidad de I. Así, $|J| = 2^S$, donde $S = \sum_{i=0}^{k}(k+1-i)gr(f_{i+1})$. Dado que $gr(f_i) = gr(g_i)$, la prueba está ahora completa. □

Recuerde que si I es un ideal del anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1 \rangle$, entonces I es generado por

$$F = \widehat{F_1} + 2\widehat{F_2} + \cdots + 2^k \widehat{F_{k+1}},$$

donde $\widehat{F_1}, 2\widehat{F_2}, \cdots, 2^k\widehat{F_{k+1}}$ son los generadores del código cíclico $\mathscr{C} = P^{-1}(I)$ y P es la representación polinomial de $\mathbb{Z}_{2^{k+1}}^n$. Consecuentemente, el isomorfismo

$$\mu_\beta : \mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1 \rangle \to \mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \gamma \rangle$$

definido en el Lema 1.3.6 implica que $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n-\gamma\rangle$ es un anillo de ideales principales. Si $J=\mu_\beta(I)$, entonces es fácil verificar que

$$J=\langle\mu_\beta(F)\rangle=\langle\mu_\beta(\widehat{F_1})+2\mu_\beta(\widehat{F_2})+\cdots+2^k\mu_\beta(\widehat{F_{k+1}})\rangle,$$

y también,

$$\begin{aligned}J&=\langle\mu_\beta(\widehat{F_1}),2\mu_\beta(\widehat{F_2}),\ldots,2^k\mu_\beta(\widehat{F_{k+1}})\rangle\\&=\langle\beta^{-gr(\widehat{f_1})}\mu_\beta(\widehat{F_1}),2\beta^{-gr(\widehat{f_2})}\mu_\beta(\widehat{F_2}),\ldots,2^k\beta^{-gr(\widehat{f_{k+1}})}\mu_\beta(\widehat{F_{k+1}})\rangle\\&=\langle\widehat{G_1},2\widehat{G_2},\ldots,2^k\widehat{G_{k+1}}\rangle,\end{aligned}$$

donde $\widehat{G_i}=\beta^{-gr(\widehat{f_i})}\mu_\beta(\widehat{F_i})$. Siguiendo la demostración del Corolario 3.6 de [30], es fácil ver que

$$J=\langle\widehat{G_1}+2\widehat{G_2}+\cdots+2^k\widehat{G_{k+1}}\rangle.$$

En lo sucesivo, llamaremos a $G=\widehat{G_1}+2\widehat{G_2}+\cdots+2^k\widehat{G_{k+1}}$ el *polinomio generador del código γ-cíclico* $P^{-1}(J)$, y a los polinomios $\widehat{G_1},2\widehat{G_2},\ldots,2^k\widehat{G_{k+1}}$, los *generadores del código γ-cíclico* $\mathscr{C}=P^{-1}(J)$. Asimismo, a partir de este punto, usaremos la siguiente notación para expresar (respectivamente) a estos términos:

$$\mathscr{C}=\langle\widehat{G_1},2\widehat{G_2},\ldots,2^k\widehat{G_{k+1}}\rangle,\qquad\mathscr{C}=\langle G\rangle.$$

Observe que los polinomios $\widehat{G_i}$ del Teorema 1.3.9 dependen de los factores g_i y, que por otra parte, fueron obtenidos directamente de los polinomios $\widehat{F_i}$, los cuales también están en función de la factorización de x^n-1 sobre $\mathbb{Z}_{2^{k+1}}[x]$. Ya que los polinomios g_i están definidos a partir de los factores f_i de x^n-1, podemos simplificar los cálculos de los generadores y del polinomio generador de un código γ-cíclico en el siguiente sentido:

Corolario 1.3.10. *Con la notación de los Teoremas 1.3.1 y 1.3.9, para calcular a los generadores $\widehat{G_1},2\widehat{G_2},\ldots,2^k\widehat{G_{k+1}}$ basta reemplazar el factor $f_i+\langle x^n-1\rangle$ por $g_i+\langle x^n-\gamma\rangle$ en la expresión de $\widehat{F_i}$.*

Demostración. En la demostración del Teorema 1.3.9 probamos que $\widehat{G_i}=\beta^{-gr(\widehat{f_i})}\mu_\beta(\widehat{F_i})$. Así, el Corolario 1.3.10 es consecuencia inmediata de este hecho. □

A continuación presentamos algunos ejemplos que ilustran el Lema 1.3.8, el Teorema 1.3.9 y el Corolario 1.3.10. Recuerde que con el fin de simplificar la notación, usaremos a los polinomios de grado a lo más $n-1$ en $\mathbb{Z}_{2^{k+1}}[x]$ para representar a sus correspondientes clases laterales en el anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n-\gamma\rangle$. De nuevo, todos los cálculos han sido realizados con la ayuda del programa computacional MAGMA® V2.15-13 (Student Version).

Ejemplo 1.3.11. Sean $k=3$, $n=7$. Recordemos que la factorización de x^7-1 sobre $\mathbb{Z}_{16}[x]$ como un producto de polinomios mónicos, básicos irreducibles y coprimos es:

$$x^7-1 = a_1(x)a_2(x)a_3(x),$$

donde $a_1(x)=x+15$, $a_2(x)=x^3+6x^2+5x+15$, $a_3(x)=x^3+11x^2+10x+15$. Sea $\gamma=9\in\mathbb{Z}_{16}$. Entonces es fácil verificar que $\gamma^{-1}=9$ en $\mathbb{Z}_{16}$ y que $\beta=9$ es el único elemento de $\mathbb{Z}_{16}$ tal que $\beta^7=\gamma^{-1}$. Por lo tanto,

$$\begin{aligned}
b_1(x) &= 9^{-1}\mu_9(a_1(x)) = 9^{-1}(9x+15) = x+7,\\
b_2(x) &= 9^{-3}\mu_9(a_2(x)) = 9^{-3}(9^3x^3+6(9^2x^2)+5(9x)+15) = x^3+6x^2+5x+7,\\
b_3(x) &= 9^{-3}\mu_9(a_3(x)) = 9^{-3}(9^3x^3+11(9^2x^2)+10(9x)+15) = x^3+3x^2+10x+7.
\end{aligned}$$

De este modo, por el Lema 1.3.8, la factorización de x^7-9 sobre $\mathbb{Z}_{16}[x]$ como un producto de polinomios mónicos, básicos irreducibles y coprimos es:

$$x^7-9 = b_1(x)b_2(x)b_3(x) = (x+7)(x^3+6x^2+5x+7)(x^3+3x^2+10x+7).$$

Ahora ejemplificaremos cómo obtener códigos 9-cíclicos de longitud 7 sobre $\mathbb{Z}_{16}$ a partir de códigos cíclicos.

Ejemplo 1.3.12. De los Ejemplos 1.3.2 y 1.3.3 sabemos que los conjuntos $\mathscr{C}_1=\langle a_1(x)a_2(x)\rangle$ y $\mathscr{C}_2=\langle a_1(x)a_3(x), 4a_1(x)a_2(x)\rangle$, son códigos cíclicos lineales de longitud 7 sobre $\mathbb{Z}_{16}$, donde

$$a_1(x)=x+15,\quad a_2(x)=x^3+6x^2+5x+15,\quad a_3(x)=x^3+11x^2+10x+15.$$

Las cardinalidades de $\mathscr{C}_1$ y $\mathscr{C}_2$ son, respectivamente, 2^{12} y 2^{24}. Por el Lema 1.3.6 (tomando $\gamma=9$ y $\beta=9$) tenemos que $\mathscr{D}_1=\mu_9(P(\mathscr{C}_1))$ y $\mathscr{D}_2=\mu_9(P(\mathscr{C}_2))$ son ideales en $\mathbb{Z}_{16}[x]/\langle x^7-9\rangle$, y que por la Proposición 1.2.6, estos ideales corresponden a códigos 9-cíclicos lineales de longitud 7 sobre $\mathbb{Z}_{16}$. Ahora, por el Corolario 1.3.10, para encontrar los generadores de $\mathscr{D}_1$ y $\mathscr{D}_2$ basta sustituir f_i por g_i en los generadores de $\mathscr{C}_1$ y $\mathscr{C}_2$, o de forma equivalente, reemplazar a_i por b_i. Por lo tanto,

$$\mathscr{D}_1=\langle b_1(x)b_2(x)\rangle \qquad \text{y} \qquad \mathscr{D}_2=\langle b_1(x)b_3(x), 4b_1(x)b_2(x)\rangle,$$

donde $b_1(x)$ y $b_2(x)$ son como en el Ejemplo 1.3.11. Explícitamente, $b_1(x)b_2(x)=x^4+13x^3+15x^2+10x+1$, $b_1(x)b_3(x)=x^4+10x^3+15x^2+13x+1$ y $4b_1(x)b_2(x)=4x^4+4x^3+12x^2+8x+4$. Claramente, el polinomio generador de $\mathscr{D}_1$ es $b_1(x)b_2(x)$ y el polinomio generador de $\mathscr{D}_2$ es $G=b_1(x)b_3(x)+4b_1(x)b_2(x)=5x^4+14x^3+11x^2+5x+5$.

Como podemos notar, la técnica que hemos presentado en esta sección facilita el cálculo de los códigos γ-cíclicos a partir de los códigos cíclicos. Sin embargo, si observamos con detalle, esta técnica depende de calcular eficientemente la raíz n-ésima de la unidad γ^{-1} (a la cual denotamos como β). Cuando los enteros k y n son pequeños, es posible que no sea difícil calcular tal raíz n-ésima. Por el contrario, el problema se puede complicar si al menos uno de los enteros k o n es relativamente "grande". El tema de la siguiente subsección consiste en minimizar los esfuerzos para calcular la raíz n-ésima γ^{-1}.

1.3.3. Raíces n-ésimas en $1+\langle 2^{k-1}\rangle$

En la presente subsección, daremos una técnica práctica y sencilla para calcular la raíz n-ésima de γ^{-1}, donde γ es un elemento en $1+\langle 2^{k-1}\rangle = \{1, 1+2^{k-1}, 1+2^k, 1+2^{k-1}+2^k\}$ y n es un entero impar. Para lograr este propósito, primero necesitamos conocer la estructura algebraica del conjunto $1+\langle 2^{k-1}\rangle$. Recuerde que $\langle 2^{k-1}\rangle$ denota al ideal en $\mathbb{Z}_{2^{k+1}}$ generado por 2^{k-1}.

Proposición 1.3.13. *Para todo $k \geq 2$, el conjunto $1+\langle 2^{k-1}\rangle$ es un subgrupo de $U(\mathbb{Z}_{2^{k+1}})$. Si $k \geq 3$ entonces $1+\langle 2^{k-1}\rangle$ es un grupo cíclico generado por $\delta_1 = 1+2^{k-1}$. En tal caso, $\delta_1^2 = 1+2^k$ y $\delta_1^{-1} = 1+3\cdot 2^{k-1}$*

Demostración. Por definición, $1 \in 1+\langle 2^{k-1}\rangle$. Sean $a = 1+x, b = 1+y$ con $x, y \in \langle 2^{k-1}\rangle$. Entonces $ab = 1+x+y+xy$, y dado que $\langle 2^{k-1}\rangle$ es un ideal, $x+y+xy \in \langle 2^{k-1}\rangle$. Así, $ab \in 1+\langle 2^{k-1}\rangle$ y, por lo tanto, $1+\langle 2^{k-1}\rangle$ es multiplicativamente cerrado. Para demostrar la existencia del inverso, sea $\alpha \in 1+\langle 2^{k-1}\rangle$ fijo. Defina $\pi_\alpha : 1+\langle 2^{k-1}\rangle \to 1+\langle 2^{k-1}\rangle$ como $u \mapsto \alpha u$. Debido a que α es una unidad, π_α es una biyección y, por lo tanto, existe $x \in 1+\langle 2^{k-1}\rangle$ tal que $\alpha x = 1$ en $\mathbb{Z}_{2^{k+1}}$.
Si $k = 2$, entonces $U(\mathbb{Z}_8) = 1+\langle 2\rangle = \{1,3,5,7\}$ es un grupo en el que todos sus elementos son de orden 2. En consecuencia, $U(\mathbb{Z}_8)$ no es un grupo cíclico. Por otra parte, si $k \geq 3$, entonces es fácil verificar que $(1+2^{k-1})^2 = 1+2^k$ en $\mathbb{Z}_{2^{k+1}}$. Ya que para todo $k \geq 1$, $1+2^{k+1}$ es una unidad de orden 2, podemos concluir que $1+2^{k-1}$ es de orden 4. Consecuentemente, $1+\langle 2^{k-1}\rangle$ es cíclico. No es difícil verificar que, si $\delta_1 = 1+2^{k-1}$, entonces $\delta_1^2 = 1+2^k$ y $\delta_1^3 = \delta_1^{-1} = 1+3\cdot 2^{k-1}$. □

La técnica eficiente para calcular la raíz n-ésima de γ^{-1} resulta del siguiente análisis. Sean n, k enteros tales que $n \geq 1$ es impar y $k \geq 2$. Usando el algoritmo de la división en $\mathbb{Z}$, podemos expresar $n = 4q+n_0$, donde $0 \leq n_0 \leq 3$. Note que como n es impar, n_0 también lo es y por lo tanto, $n_0 \in U(\mathbb{Z}_4)$. De este modo, existe $n_1 \in U(\mathbb{Z}_4)$ tal que $n_0 n_1 = 1$ (en $\mathbb{Z}_4$).

Sea $\gamma \in 1+\langle 2^{k-1}\rangle$. Afirmamos que $\eta = \gamma^{n_1} \in U(\mathbb{Z}_{2^{k+1}})$ es la única raíz n-ésima de γ. En efecto, $\eta^n = (\gamma^{n_1})^n = \gamma^{nn_1} = \gamma^{4qn_1+n_0n_1} = \gamma^{4n_1q}\gamma^{n_0n_1} = \gamma$, donde la última igualdad se debe a que γ pertenece a un grupo de orden 4 y $n_0n_1 = 1$ en $\mathbb{Z}_4$.

Ahora, por el Corolario 1.3.5, $\beta = \eta^{-1}$ es la única raíz n-ésima de γ^{-1}. Ya que $-n_1 = 3n_1$ en $\mathbb{Z}_4$, tenemos una expresión alternativa para β, esta es, $\beta = \gamma^{3n_1}$. Analicemos los datos con más detalle, recordemos que $n_0 \in \{1,3\} = U(\mathbb{Z}_4)$. Si $n_0 = 1$, entonces $n_1 = 1$ y por lo tanto $\beta = \gamma^{3n_1} = \alpha^3$. Si $n_0 = 3$, entonces $n_1 = 3$ y $\beta = \gamma^{3n_1} = \gamma$. Por lo tanto, basta fijarnos en el residuo n_0 para determinar por completo a β.

En resumen, hemos demostrado la siguiente Proposición, en la que $n \equiv n_0 \pmod 4$ indica que n_0 es el residuo que resulta al dividir n entre 4.

Proposición 1.3.14. *Sea $n \geq 1$ un entero impar y $\gamma \in 1+\langle 2^{k-1}\rangle$, donde $k \geq 2$. Entonces la única raíz n-ésima de γ^{-1} está dada por las relaciones*

$$\beta = \begin{cases} \gamma^3, & si\ n \equiv 1 \pmod 4 \\ \gamma, & si\ n \equiv 3 \pmod 4 \end{cases}$$

En particular, observe que $\beta \in 1+\langle 2^{k-1}\rangle$.

Por ejemplo, sean $k=3$, $n=7$ y $\gamma=9$. Entonces $n \equiv 3 \pmod 4$ y por lo tanto, $\beta=\gamma=9$ es la raíz séptima de $\gamma^{-1}=9$ en $\mathbb{Z}_{16}$. Observe que estos cálculos coinciden con los que se usaron en los Ejemplos 1.3.11 y 1.3.12.

1.4. Acerca de los pesos homogéneos

Notemos que, en particular, el Corolario 1.3.5 establece que el número de códigos γ-cíclicos lineales de longitud n impar sobre $\mathbb{Z}_{2^{k+1}}$ es el mismo que el de códigos cíclicos. Además, el Lema 1.3.6 garantiza que los códigos γ-cíclicos de longitud n sobre $\mathbb{Z}_{2^{k+1}}$ no tienen más elementos que los códigos cíclicos. Aunado a esta serie de hechos, en esta sección demostraremos que los códigos γ-cíclicos "lineales" tienen los mismos pesos homogéneos que los códigos cíclicos. Para este fin, introduciremos el siguiente $\mathbb{Z}_{2^{k+1}}$-automorfismo sobre $\mathbb{Z}_{2^{k+1}}^n$.

Dado $n \geq 1$ un entero impar, una unidad $\gamma \in U(\mathbb{Z}_{2^{k+1}})$ y β la (única) raíz n-ésima de γ^{-1}, definimos la aplicación $\widetilde{\mu}_\beta : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}_{2^{k+1}}^n$ como

$$(a_0, a_1, a_2, \ldots, a_{n-1}) \mapsto (a_0, \beta a_1, \beta^2 a_2, \ldots, \beta^i a_i, \ldots, \beta^{n-1} a_{n-1}).$$

Para el caso particular $\gamma=-1 \in \mathbb{Z}_4$, tenemos que, para todo entero n impar, $\beta=-1 \in \mathbb{Z}_4$ y, por lo tanto, la función

$$\widetilde{\mu}_{-1} : \mathbb{Z}_4^n \to \mathbb{Z}_4^n$$

está dada por la relación

$$(a_0, a_1, a_2, \ldots, a_{n-1}) \mapsto (a_0, -a_1, a_2, \ldots, (-1)^i a_i, \ldots, (-1)^{n-1} a_{n-1}),$$

la cual coincide con la aplicación $\widetilde{\mu}$ que se introdujo en [54, Proposición 3.7]. De igual modo que en [54], se sigue de las definiciones de la representación polinomial P y de los isomorfismos μ_β y $\widetilde{\mu}_\beta$ que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} \mathbb{Z}_{2^{k+1}}[x]/\langle x^n-1\rangle & \xrightarrow{P^{-1}} & \mathbb{Z}_{2^{k+1}}^n \\ \Big\downarrow \mu_\beta & & \Big\downarrow \widetilde{\mu}_\beta \\ \mathbb{Z}_{2^{k+1}}[x]/\langle x^n-\gamma\rangle & \xrightarrow{P^{-1}} & \mathbb{Z}_{2^{k+1}}^n \end{array}$$

Como consecuencia inmediata de este hecho se tiene el siguiente resultado.

Lema 1.4.1. *Sean n, γ, β como antes. Entonces un código lineal $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ es cíclico si y sólo si $\widetilde{\mu}_\beta(\mathscr{C})$ es un código γ-cíclico.*

Recordemos que hemos definido el peso homogéneo $\omega_h : \mathbb{Z}_{2^{k+1}} \to \mathbb{Z}$ como la aplicación dada por la siguiente regla de asignación:

$$\omega_h(a) = \begin{cases} 0, & \text{si } a = 0 \\ 2^k, & \text{si } a = 2^k \\ 2^{k-1}, & \text{si } a \in \mathbb{Z}_{2^{k+1}} \setminus 2^k\mathbb{Z}_{2^{k+1}} \end{cases}$$

El siguiente Lema afirma que el peso homogéneo de un elemento $x \in \mathbb{Z}_{2^{k+1}}$ no cambia si a x lo multiplicamos por una unidad del anillo $\mathbb{Z}_{2^{k+1}}$.

Lema 1.4.2. *Sean $n \geq 1$ un entero y $u \in U(\mathbb{Z}_{2^{k+1}})$. Entonces para todo $x \in \mathbb{Z}_{2^{k+1}}$ se tiene que $\omega_h(x) = \omega_h(ux)$.*

Demostración. Claramente si $x = 0$, la afirmación del Lema 1.4.2 es válida. Si $x = 2^k$ y $u = 1 + 2d$, donde $d \in \mathbb{Z}_{2^{k+1}}$, entonces $ux = x$. Así que $\omega_h(2^{k+1}) = \omega_h(2^{k+1}u)$. Finalmente, si $x \in \mathbb{Z}_{2^{k+1}} \setminus 2^k\mathbb{Z}_{2^{k+1}}$, entonces tenemos que demostrar que también $ux \in \mathbb{Z}_{2^{k+1}} \setminus 2^k\mathbb{Z}_{2^{k+1}}$. Procediendo por contradicción, supongamos que $ux \in \langle 2^k \rangle = \{0, 2^k\}$ y $ux \neq 0$. (Si $ux = 0$, siendo u una unidad, necesariamente se tendría que $x = 0$, lo cual nos conduce al caso trivial.) Entonces $ux = 2^k$ y, pensando a los elementos u, x y 2^k como enteros, se tiene que 2^k divide a x pues u es impar. Así x es un múltiplo de 2^k, lo cual implica que $x \in 2^k\mathbb{Z}_{2^{k+1}}$, contradiciendo la elección de x. De este modo $x \in \mathbb{Z}_{2^{k+1}} \setminus 2^k\mathbb{Z}_{2^{k+1}}$ implica que $ux \in \mathbb{Z}_{2^{k+1}} \setminus 2^k\mathbb{Z}_{2^{k+1}}$, es decir, $\omega_h(x) = \omega_h(ux)$. Esto finaliza la prueba. □

Con esta herramienta a la mano, es posible demostrar que sobre el anillo $\mathbb{Z}_{2^{k+1}}$ los códigos cíclicos lineales y los códigos γ-cíclicos lineales tienen los mismos pesos homogéneos.

Teorema 1.4.3. *Sean n, γ y β como antes. Si $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ es un código cíclico lineal y $c \in \mathscr{C}$, entonces $\omega_h(c) = \omega_h(\widetilde{\mu}_\beta(c))$. En particular, $\omega_h(\mathscr{C}) = \omega_h(\widetilde{\mu}_\beta(\mathscr{C}))$.*

Demostración. Sea $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathscr{C}$. Entonces $\widetilde{\mu}_\beta(c) = (c_0, \beta c_1, \ldots, \beta^{n-1}c_{n-1})$. Siendo β una unidad en $\mathbb{Z}_{2^{k+1}}$, se sigue del Lema 1.4.2 que $\omega_h(\beta^i c_i) = \omega_h(c_i)$ para todo $0 \leq i \leq n-1$. Consecuentemente

$$\omega_h(c) = \sum_{i=0}^{n-1} \omega_h(c_i) = \sum_{i=0}^{n-1} \omega_h(\beta^i c_i) = \omega_h(\widetilde{\mu}_\beta(c)),$$

como queríamos demostrar. □

Hasta este momento hemos demostrado que sobre $\mathbb{Z}_{2^{k+1}}$, los códigos γ-cíclicos de longitud impar tienen los mismos parámetros (cardinalidad y peso homogéneo) que los códigos cíclicos de la misma longitud. En consecuencia, basta encontrar los parámetros de los códigos cíclicos para conocer los parámetros de los correspondientes códigos γ-cíclicos.

Por otra parte, se viene a la mente una pregunta muy natural: ¿qué ventaja tienen los códigos γ-cíclicos sobre los códigos cíclicos? Seguramente el lector puede encontrar varias ventajas en las aplicaciones prácticas o incluso en su riqueza matemática. Pero entre todas estas razones, la siguiente es de nuestro particular interés. Como se verá en el Capítulo 4 de este manuscrito, si $\mathscr{C}$ es un código cíclico de longitud n sobre $\mathbb{Z}_4$ y $\phi : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$ es la isometría de Gray, entonces $\phi(\mathscr{C})$ es un código casi-cíclico de índice 2 y longitud $2n$ sobre $\mathbb{F}_2$. Por otro lado, en [54, 55] se demostró que cuando $\mathscr{C}$ es un código negacíclico de longitud n sobre $\mathbb{Z}_4$, entonces $\phi(\mathscr{C})$ es un código cíclico de longitud $2n$ sobre $\mathbb{F}_2$. Para relacionar estos dos resultados, recuerde que en la Sección 1.3 demostramos que los códigos cíclicos lineales y los códigos negacíclicos lineales de longitud impar están relacionados biunívocamente mediante el isomorfismo μ_{-1}. Esto permite demostrar ([54,55]) que si $\mathscr{C}$ es código cíclico de longitud n (impar) sobre $\mathbb{Z}_4$, entonces $\phi(\mathscr{C})$ es un código cíclico binario de longitud $2n$, lo cual (para muchos) es una propiedad más elegante que la de casi-ciclicidad debido, entre otras cosas, a sus aplicaciones prácticas. Por lo tanto, códigos consta-cíclicos pueden ser usados para construir códigos cíclicos como imágenes bajo la isometría de Gray. Esta aplicación teórica de los códigos consta-cíclicos, en particular de los códigos negacíclicos, ha tenido entre sus consecuencias inmediatas la construcción de códigos cíclicos binarios no lineales que mejoran los parámetros de algunos códigos cíclicos lineales de longitud $2n$ sobre $\mathbb{F}_2$. Cabe mencionar que esta serie de implicaciones han sido parte de la motivación de la presente investigación.

Capítulo 2

Isometrías sobre $\mathbb{Z}_{2^{k+1}}^n$

El propósito de este capítulo se compone de dos partes. Primero, analizaremos la definición de la isometría de Gray $\Phi : (\mathbb{Z}_{2^{k+1}}^n, \delta_h) \to (\mathbb{F}_2^{2^k n}, \delta_H)$ propuesta en [21]. Segundo, definiremos la isometría $\varphi : (\mathbb{Z}_{2^{k+1}}^n, \delta_h) \to (\mathbb{Z}_4^{2^{k-1} n}, \delta_L)$ que resultará ser permutación-equivalente a la función φ^k expuesta en [51,52]. Las ventajas de la definición de φ son las siguientes: permite investigar una nueva propiedad que generaliza a las que se examinaron para φ^k en la Proposiciones 3.1 de [51] y 4, 7 de [52]. Asimismo, permite establecer de manera natural su relación con la isometría Φ de Gray; lo que derivará en la obtención de nuevas identidades para esa isometría.

2.1. La isometría de Gray sobre $\mathbb{Z}_{2^{k+1}}^n$

Uno de los propósitos básicos de un código es detectar y corregir los errores que ocurren cuando la información es transmitida a través de un canal de comunicación. Para esta finalidad, los códigos lineales tienen mucha ventaja sobre los códigos no lineales pues, debido a la riqueza de su estructura matemática, se tienen descripciones bastante prácticas de ellos. Sin embargo, si fijamos una longitud y queremos construir un código que tenga la mayor cantidad posible de elementos que estén a una distancia fija, en muchos casos terminamos construyendo un código no lineal. Por ejemplo, los códigos de Nodstrom-Robinson, Kerdock, Preparata, Goethals y Delsarte-Goethals, son familias de códigos binarios no lineales que tienen mayor cardinalidad que cualquier código lineal comparable con éstos [27, 38].

Entre las familias de códigos no lineales antes mencionadas, destacan los códigos de Kerdock y Preparata ya que tienen la propiedad de ser *formalmente duales*, es decir, aunque estos códigos no son lineales, la distribución de pesos[1] de uno está únicamente determinada por la distribución de pesos del otro a través de las *identidades de MacWilliams* [27, 38]. Una de las principales preguntas relacionadas con estos códigos y que se mantuvo vigente durante varios años fue: ¿los códigos de Kerdock y Preparata son duales en un sentido más algebraico? Esta pregunta originó una serie de investigaciones que intentaban explicar tal fenómeno, aunque sin mucho éxito. En 1994, Hammons et al. [23] descubrieron que los códigos de Kerdock y Preparata están relacionados con códigos lineales sobre $\mathbb{Z}_4$. Esta conexión fue establecida vía la isometría de Gray $\phi : (\mathbb{Z}_4^n, \delta_L) \to (\mathbb{F}_n^{2n}, \delta_H)$, donde δ_L y δ_H son las distancias de Lee y Hamming,

[1] La distribución de pesos de un código de longitud n especifica el número de vectores de peso $0, 1, \ldots, n$ que tiene el código.

respectivamente. Mediante la isometría de Gray, los códigos de Kerdock y Preparata fueron descritos como imágenes de esta función de códigos cíclicos lineales extendidos sobre $\mathbb{Z}_4$, con la propiedad de que uno es el dual del otro −en el sentido usual pues estos códigos son lineales en $\mathbb{Z}_4$−. De este modo, se dio una explicación satisfactoria para el fenómeno de las distribuciones de pesos de los códigos de Kerdock y Preparata.

En el proceso de este descubrimiento, se encontró que los códigos de Nodstrom-Robinson, Goethals, Delsarte-Goethals, algunos códigos de Reed-Muller y de Hamming extendidos, también están relacionados con códigos lineales sobre $\mathbb{Z}_4$.

Desde entonces la isometría de Gray ha sido generalizada y ampliamente estudiada en diferentes contextos y para distintos propósitos [11, 21, 23, 33, 51, 52, 54, 55]. Principalmente, esto se ha dado en conexión con los códigos cíclicos y, de manera más general, con algunos códigos consta-cíclicos sobre anillos finitos. Entre las aportaciones más relevantes que se han originado con estos trabajos, destaca la construcción de códigos óptimos (lineales o no) sobre campos finitos como imágenes de esta isometría de códigos lineales sobre anillos finitos, principalmente anillos finitos cuyo campo residual sea el de los números binarios, por ejemplo, el anillo $\mathbb{Z}_{2^{k+1}}$.

En este apartado, seguiremos los métodos empleados en [21] para definir la isometría de Gray sobre el anillo $\mathbb{Z}_{2^{k+1}}$ y luego extender esta definición al caso $\Phi : (\mathbb{Z}_{2^{k+1}}^n, \delta_h) \to (\mathbb{F}_2^{2^k n}, \delta_H)$. Asimismo, demostraremos que Φ es permutación-equivalente a las isometrías de Gray propuestas en [11, 51, 52]. La conexión de Φ con códigos sobre el anillo $\mathbb{Z}_{2^{k+1}}$ será realizada en los Capítulos 4, 5 y 6, donde expondremos los resultados más importantes de este trabajo.

2.1.1. Una base del código binario de Reed-Muller de primer orden

Sean $Y = (y_{ij})$ y $Z = (z_{kl})$ matrices de tamaño $m \times n$ y $p \times q$, respectivamente, con entradas en un anillo asociativo R. Recordemos que el *producto de Kronecker* de Y y Z, el cual denotaremos por $Y \otimes Z$, es definido como la matriz de tamaño $mp \times nq$ dada por

$$Y \otimes Z = \begin{pmatrix} y_{11}Z & \cdots & y_{1n}Z \\ \vdots & \ddots & \vdots \\ y_{m1}Z & \cdots & y_{mn}Z \end{pmatrix}.$$

Con base a esta definición es fácil ver que este producto, en general, *no es conmutativo* y que satisface las siguientes propiedades básicas:

$$\begin{aligned} &X \otimes (Y+Z) = X \otimes Y + X \otimes Z, \\ &(X+Y) \otimes Z = X \otimes Z + Y \otimes Z, \\ &\quad (\alpha Y) \otimes Z = Y \otimes (\alpha Z) = \alpha(Y \otimes Z), \quad \forall \alpha \in R \\ &(X \otimes Y) \otimes Z = X \otimes (Y \otimes Z), \end{aligned}$$

donde la suma está definida para matrices del mismo tamaño. Para más detalles, el lector puede consultar [26].

Sean $u=(0,1)$, $v=(1,1)$ y $k\geq 1$ un entero. Por medio del producto de Kronecker definimos una familia de vectores $c_i^k \in \mathbb{F}_2^{2^k}$, $0\leq i\leq k$, de la siguiente manera:

$$\begin{aligned}
c_0^k &= u\otimes c_{k-1}^{k-1} = u\otimes \underbrace{v\otimes v\otimes\cdots\otimes v}_{k-1},\\
c_1^k &= v\otimes c_0^{k-1} = v\otimes u\otimes \underbrace{v\otimes\cdots\otimes v}_{k-2},\\
&\vdots\\
c_{k-1}^k &= v\otimes c_{k-2}^{k-1} = \underbrace{v\otimes v\otimes\cdots\otimes v}_{k-1}\otimes u,\\
c_k^k &= v\otimes c_{k-1}^{k-1} = \underbrace{v\otimes v\otimes\cdots\otimes v\otimes v}_{k},
\end{aligned}$$

donde acordamos que $c_0^0 = 1\in\mathbb{F}_2$. Como podemos notar, estas expresiones son las mismas que aparecen en la definición de los vectores c_i introducidos en [21], en donde estos vectores fueron definidos sobre cualquier campo finito. Aquí, hemos restringido sus definiciones al caso $\mathbb{F}_2$ y las hemos presentado de manera recursiva. Por tal razón, dado que la longitud de los vectores cambia de acuerdo al número de iteración, hemos incluido un superíndice k que indica el espacio ambiente $\mathbb{F}_2^{2^k}$ en el que se encuentran estos vectores.

Ya que $u=(0,1)$ y $v=(1,1)$, se sigue de la definición del producto de Kronecker que los vectores c_i^k, $0\leq i\leq k-1$, están formados por la concatenación de 2^{i+1} vectores de la forma $(1)_{k-(i+1)}$ y $(0)_{k-(i+1)}$ ubicados de manera alternada e iniciando siempre a la izquierda con vector[2] $(0)_{k-(i+1)}$. Por otro lado, como u no se encuentra involucrado en la expresión de c_k^k, este vector tiene todas sus coordenadas iguales a 1, es decir, $c_k^k = (1)_{2^k}$.

Los siguientes ejemplos nos ayudarán a entender la definición de los vectores c_i^k.

Ejemplo 2.1.1. Con $k=1$ tenemos lo siguiente:

$$\begin{aligned}
c_0^1 &= u\otimes c_0^0 = u\otimes 1 = u = (0,1),\\
c_1^1 &= v\otimes c_0^0 = v\otimes 1 = v = (1,1).
\end{aligned}$$

Si $k=2$, entonces

$$\begin{aligned}
c_0^2 &= u\otimes c_1^1 = u\otimes v = (0,0,1,1),\\
c_1^2 &= v\otimes c_0^1 = v\otimes u = (0,1,0,1),\\
c_2^2 &= v\otimes c_1^1 = v\otimes v = (1,1,1,1).
\end{aligned}$$

[2] Si u fuese tomado como el vector $(1,0)$, entonces se iniciaría siempre a la izquierda con vector $(1)_{k-(i+1)}$.

Por otra parte, con $k=3$ obtenemos

$$\begin{aligned} c_0^3 &= u\otimes c_2^2 = u\otimes v\otimes v = (0,0,0,0,1,1,1,1),\\ c_1^3 &= v\otimes c_0^2 = v\otimes u\otimes v = (0,0,1,1,0,0,1,1),\\ c_2^3 &= v\otimes c_1^2 = v\otimes v\otimes u = (0,1,0,1,0,1,0,1),\\ c_3^3 &= v\otimes c_2^2 = v\otimes v\otimes v = (1,1,1,1,1,1,1,1). \end{aligned}$$

Observe que en los tres casos presentados en el Ejemplo 2.1.1, los vectores c_i^k son linealmente independientes. Esto es afirmado en [21] y, a continuación, incluimos una demostración de este hecho para el caso binario.

Proposición 2.1.2. *Sea $k\geq 1$ un entero. Entonces los vectores c_i^k, $0\leq i\leq k$, son linealmente independientes sobre $\mathbb{F}_2$.*

Demostración. Claramente u y v son linealmente independientes sobre $\mathbb{F}_2$. Procediendo ahora por inducción, supongamos que para algún $k\geq 1$, los vectores c_i^k son linealmente independientes sobre $\mathbb{F}_2$. Sean $\alpha_0,\ldots,\alpha_{k+1}$ elementos de $\mathbb{F}_2$ tales que

$$\alpha_0 c_0^{k+1}\oplus\alpha_1 c_1^{k+1}\oplus\alpha_2 c_2^{k+1}\oplus\cdots\oplus\alpha_{k+1}c_{k+1}^{k+1} = (0)_{2^{k+1}}, \tag{2.1}$$

donde "$\oplus$" denota la suma de vectores con coordenadas en $\mathbb{F}_2$. Observemos que a partir de la definición recursiva de los vectores c_i^{k+1}, se tiene que el lado izquierdo de la ecuación (2.1) es equivalente a lo siguiente:

$$\left(\alpha_0(u\otimes c_k^k)\right)\oplus\left(\alpha_1(v\otimes c_0^k)\right)\oplus\left(\alpha_2(v\otimes c_1^k)\right)\oplus\cdots\oplus\left(\alpha_{k+1}(v\otimes c_k^k)\right),$$

y que ésta a su vez, por las propiedades del producto de Kronecker, corresponde a la expresión:

$$\left(u\otimes(\alpha_0 c_k^k)\right)\oplus\left(v\otimes(\alpha_1 c_0^k)\right)\oplus\left(v\otimes(\alpha_2 c_1^k)\right)\oplus\cdots\oplus\left(v\otimes(\alpha_{k+1}c_k^k)\right). \tag{2.2}$$

Además, notemos que $u\otimes\alpha_0 c_k^k = ((0)_{2^k}|\alpha_0 c_k^k)$ y que

$$v\otimes\alpha_i c_{i-1}^k = (\alpha_i c_{i-1}^k|\alpha_i c_{i-1}^k),\quad 1\leq i\leq k,$$

donde " | " denota a la concatenación de vectores definida en la Sección 1.1. Por lo tanto, la ecuación (2.1) es verdadera si y sólo si la expresión (2.2) es igual al vector $(0)_{2^{k+1}}$. Pero si esto sucede, entonces

$$\alpha_1 c_0^k\oplus\cdots\oplus\alpha_{k+1}c_k^k = (0)_{2^k}$$

y, por lo tanto, por hipótesis de inducción, $\alpha_1=\cdots=\alpha_{k+1}=0$. Así, $(0)_{2^{k+1}} = ((0)_{2^k}|\alpha_0 c_k^k)$, lo cual sucede si y sólo si $\alpha_0=0$. □

Como consecuencia de la Proposición 2.1.2, para todo $k \geq 1$ los vectores $c_0^k, \ldots, c_k^k \in \mathbb{F}_2^{2^k}$ forman una base de un subespacio vectorial de $\mathbb{F}_2^{2^k}$ de dimensión $k+1$, es decir, forman una base de un $[2^k, k+1]$ código lineal sobre $\mathbb{F}_2$. En lo siguiente demostraremos que este código es el *código de Reed-Muller de primer orden* $\mathrm{RM}(1,k)$. Para este fin, se probará que la matriz $H(k)$, cuyo j-ésimo renglón es el vector c_{j-1}^k, es una matriz verificadora de paridad para el código binario de Hamming extendido. Entonces, ya que el código $\mathrm{RM}(1,k)$ es el dual del código de Hamming extendido, se habrá demostrado que H es una matriz generadora de $\mathrm{RM}(1,k)$.

Dado $k \geq 1$, construya una matriz H' de tamaño $k \times 2^k - 1$ cuyas columnas son los vectores distintos del vector $(0)_k$ de $\mathbb{F}_2^k$. Cualquier código con una matriz verificadora de paridad definida de esta forma es llamado un *código binario de Hamming de redundancia k*, denotado $\mathscr{H}(k)$. De este modo, diferentes matrices verificadoras de paridad pueden ser elegidas para diversos propósitos.

Sea $\mathscr{H}_e(k)$, $k \geq 1$, el código de longitud 2^k obtenido de $\mathscr{H}(k)$ añadiendo un dígito verificador de paridad, es decir, $\mathscr{H}_e(k)$ es el *código de Hamming extendido*. Una matriz verificadora de paridad para $\mathscr{H}_e(k)$ es de la forma ([27, Sección 1.5.2] o bien [38, Capítulo 1, Sección 9])

$$\begin{pmatrix} (0)_k^t & H' \\ 1 & (1)_{2^k-1} \end{pmatrix}$$

donde H' es una matriz verificadora de paridad de $\mathscr{H}(k)$.

Por otro lado, ya que para todo $0 \leq i \leq k-1$, los vectores c_i^k inician a la izquierda con un cero, la matriz $H(k)$ (cuyo j-ésimo renglón es el vector c_{j-1}^k, $1 \leq j \leq k+1$) puede ser escrita de la siguiente manera:

$$H(k) = \begin{pmatrix} (0)_k^t & G \\ 1 & (1)_{2^k-1} \end{pmatrix},$$

donde G es una matriz de tamaño $k \times 2^k - 1$. Afirmamos que G es una matriz verificadora de paridad para $\mathscr{H}(k)$, es decir, afirmamos que todas las columnas de G son distintas. Para demostrar esto, notemos que es suficiente probar que todas la columnas de $H(k)$ son distintas. En efecto, del Ejemplo 2.1.1 podemos notar que las columnas de $H(1), H(2)$ y $H(3)$ son distintas. Asimismo, podemos notar que para todo $k \geq 2$ se tiene la siguiente construcción recursiva:

$$H(k) = \begin{pmatrix} (0)_{2^{k-1}} & (1)_{2^{k-1}} \\ \\ H(k-1) & H(k-1) \end{pmatrix}.$$

Esencialmente, esto se debe a que por definición $c_0^k = u \otimes c_{k-1}^{k-1} = ((0)_{2^{k-1}} | (1)_{2^{k-1}})$ y, para todo

entero i tal que $1 \leq i \leq k$, se tiene que $c_i^k = v \otimes c_{i-1}^{k-1} = (c_{i-1}^{k-1} | c_{i-1}^{k-1})$. Así,

$$H(k) = \begin{pmatrix} c_0^k \\ c_1^k \\ \vdots \\ c_k^k \end{pmatrix} = \begin{pmatrix} (0)_{2^{k-1}} & (1)_{2^{k-1}} \\ c_0^{k-1} & c_0^{k-1} \\ \vdots & \vdots \\ c_{k-1}^{k-1} & c_{k-1}^{k-1} \end{pmatrix} = \begin{pmatrix} (0)_{2^{k-1}} & (1)_{2^{k-1}} \\ H(k-1) & H(k-1) \end{pmatrix}. \tag{2.3}$$

Por lo tanto, un argumento inductivo sobre k demuestra que las columnas de $H(k)$ son distintas. En particular, esto implica que G es una matriz verificadora de paridad para $\mathscr{H}(k)$, de donde concluimos que $H(k)$ es una matriz verificadora de paridad para $\mathscr{H}_e(k)$. Consecuentemente, los vectores c_i^k forman una base para el código de Reed-Muller de primer orden $\mathrm{RM}(1,k)$.

Otras alternativas para definir al código $\mathrm{RM}(1,k)$ son por medio de las funciones booleanas y de la construcción $(u|u+v)$ ([38, Capítulo 13]). De hecho, estas son las formas más comunes de introducirlos. Sin embargo, en este momento hemos decido presentarlo como el código ortogonal del código de Hamming extendido, ya que este punto de vista simplifica (y simplificará hasta cierto punto) las demostraciones de algunos resultados que serán presentados más adelante. No obstante, en la Sección 4.3 de este trabajo, usaremos la contrucción $(u|u+v)$ para dar una definición aternativa de los códigos de Reed-Muller.

En el Capítulo 13 de [38] se estudian varias propiedades de $\mathrm{RM}(1,k)$, entre ellas su distribución de pesos (de Hamming). En esta referencia se demuestra que todos los elementos de $\mathrm{RM}(1,k)$, excepto $(0)_{2^k}$ y $(1)_{2^k}$ tienen peso Hamming igual a 2^{k-1}.

Para cerrar la primera parte de esta sección, enunciamos el siguiente lema que resume las observaciones que hemos hecho hasta este momento. Más adelante haremos referencia a este resultado.

Lema 2.1.3. *Para $k \geq 1$, los vectores $c_0^k, \ldots, c_k^k \in \mathbb{F}_2^{2^k}$ forman una base del código de Reed-Muller $RM(1,k)$. Además, todos los elementos en $\mathrm{RM}(1,k)$, excepto $(1)_{2^k}$ y $(0)_{2^k}$, tienen peso de Hamming igual a 2^{k-1}.*

2.1.2. Definición de la isometría de Gray sobre $\mathbb{Z}_{2^{k+1}}$

Sean $k \geq 1$ y $z \in \mathbb{Z}_{2^{k+1}}$. Recuerde que z puede ser expresado de manera única como $z = r_0(z) + r_1(z)2 + \cdots + r_k(z)2^k$, donde $r_i(z) \in \{0,1\}$, $0 \leq i \leq k$, y que a esta expresión le hemos llamado la representación 2-ádica de z.

De igual forma que en [21], definimos la *función de Gray* $\Phi : \mathbb{Z}_{2^{k+1}} \to \mathbb{F}_2^{2^k}$ como

$$\Phi(z) = r_0(z)c_0^k \oplus r_1(z)c_1^k \oplus \cdots \oplus r_k(z)c_k^k.$$

z	$r_0(z)$	$r_1(z)$	$r_2(z)$	$\Phi(z) \in \mathbb{F}_2^4$
0	0	0	0	(0,0,0,0)
1	1	0	0	(0,0,1,1)
2	0	1	0	(0,1,0,1)
3	1	1	0	(0,1,1,0)
4	0	0	1	(1,1,1,1)
5	1	0	1	(1,1,0,0)
6	0	1	1	(1,0,1,0)
7	1	1	1	(1,0,0,1)

Cuadro 2.1: Imagen de $\Phi : \mathbb{Z}_8 \to \mathbb{F}_2^4$.

Debido a que los vectores c_i^k son linealmente independientes, Φ es una función inyectiva y, por lo tanto, $\Phi(\mathbb{Z}_{2^k+1}) = \mathrm{RM}(1,k)$.

Veamos algunos ejemplos de la función de Gray.

Ejemplo 2.1.4. Consideremos la situación $k = 1$. La función $\Phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ está dada por

$$\begin{aligned}\Phi(z) &= r_0(z)c_0^1 \oplus r_1(z)c_1^1 \\ &= r_0(z)(0,1) \oplus r_1(z)(1,1) \\ &= (r_1(z), r_1(z) \oplus r_0(z)).\end{aligned}$$

Por lo cual, en este caso Φ coincide con la definición de la función de Gray $\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ dada en [11, 23, 54, 55].

Ejemplo 2.1.5. Sea $k = 2$, entonces $\Phi : \mathbb{Z}_8 \to \mathbb{F}_2^4$ es tal que

$$\begin{aligned}\Phi(z) &= r_0(z)c_0^2 \oplus r_1(z)c_1^2 \oplus r_2(z)c_2^2 \\ &= r_0(z)(0,0,1,1) \oplus r_1(z)(0,1,0,1) \oplus r_2(z)(1,1,1,1) \\ &= (r_2(z), r_2(z) \oplus r_1(z), r_2(z) \oplus r_0(z), r_2(z) \oplus r_1(z) \oplus r_0(z)).\end{aligned}$$

El Cuadro 2.1 describe explícitamente la imagen de Φ para este caso.

Otras alternativas para definir la función de Gray sobre $\mathbb{Z}_{2^{k+1}}$ han sido propuestas en [11, 51, 52]. En particular, en [11, Proposición 4] se presentan condiciones necesarias y suficientes para que un código binario sea la imagen de la función de Gray (de manera abreviada, la *imagen de Gray*) de un código lineal sobre $\mathbb{Z}_8$. En los siguientes párrafos realizaremos una breve revisión

a la definición de la función de Gray dada en [11] y demostraremos que Φ es permutación-equivalente a función la propuesta en [11]. La definición presentada en [51, 52] será analizada en las siguientes secciones.

Sean $k \geq 1$, $z \in \mathbb{Z}_{2^{k+1}}$ y $z = r_0(z) + r_1(z)2 + \cdots + r_k(z)2^k$ su representación 2-ádica. En [11] se define la imagen de z bajo la función de Gray como la siguiente función booleana sobre $\mathbb{F}_2^k$:

$$G(z) : (y_0, \ldots, y_{k-1}) \mapsto y_0 r_0(z) \oplus \cdots \oplus y_{k-1} r_{k-1}(z) \oplus r_k(z). \tag{2.4}$$

De manera implícita, en esta definición se entiende que cada función booleana puede ser identificada de manera única con un vector en $\mathbb{F}_2^{2^k}$: supongamos que $\mathbb{F}_2^k = \{Y_0, Y_1, Y_2, \ldots, Y_{2^k-1}\}$, entonces identificamos la función $G(z)$ con el siguiente vector, al que llamamos la *imagen* ψ *de Gray de* z,

$$\psi(z) = (G(z)(Y_0), G(z)(Y_1), \ldots, G(z)(Y_{2^k-1})) \in \mathbb{F}_2^{2^k}.$$

Es importante aclarar que se debe usar un mismo orden entre los elementos de $\mathbb{F}_2^k$ para identificar a cada función booleana con el vector binario $\psi(z)$. En consecuencia, esta definición depende del orden que se le asigne a los elementos de $\mathbb{F}_2^k$ y, al mismo tiempo, permite tomar cualquier orden entre ellos. Sin embargo, es obvio de la definición de $\psi(z)$ que si consideramos otro orden entre los elementos de $\mathbb{F}_2^k$, entonces las correspondientes imágenes ψ de Gray de z difieren por una permutación. Para ser más precisos, la permutación es aquella que lleva un orden al otro. De este modo, la definición de [11] da lugar a diferentes funciones de Gray que son permutación-equivalentes. (Recordemos que dos funciones $f, g : R^n \to S^m$, R, S anillos, son permutación-equivalentes si existe una permutación τ sobre $I_m = \{1, \ldots, m\}$ tal que para todo $A \in R^n$ tenemos que $g(A) = \widetilde{\tau}(f(A))$, donde $\widetilde{\tau}$ es la permutación inducida por τ sobre S^m.)

A modo de ejemplo, se han escrito en el Cuadro 2.2 los vectores $\psi(z)$, $\psi'(z)$, con $z \in \mathbb{Z}_8$, considerando los siguientes órdenes:

$$\begin{array}{llll} Y_0 = (0,0), & Y_1 = (1,0), & Y_2 = (0,1), & Y_3 = (1,1), \\ Y_0' = (0,0), & Y_1' = (0,1), & Y_2' = (1,0), & Y_3 = (1,1). \end{array}$$

Claramente la permutación $\tau = (1 \quad 2)$ sobre el conjunto $I_4 = \{0,1,2,3\}$ de índices de los vectores de $\mathbb{F}_2^2$ lleva un orden al otro. Por lo tanto, la permutación $\widetilde{\tau}$ sobre $\mathbb{F}_2^4$ inducida por τ es tal que $\psi(z) = \widetilde{\tau}(\psi'(z))$. Más aún, si comparamos el Cuadro 2.2 con el Cuadro 2.1, observamos que para todo $z \in \mathbb{Z}_8$, $\Phi(z) = \widetilde{\tau}(\psi(z))$. Esto es, sobre $\mathbb{Z}_8$ las funciones ψ y Φ son permutación-equivalentes.

La libertad en el orden de los elementos de la definición de ψ nos permitirá demostrar que, tomando el orden adecuado, las funciones $\psi, \Phi : \mathbb{Z}_{2^{k+1}} \to \mathbb{F}_2^{2^k}$ son iguales, lo que en términos generales quiere decir que ψ y Φ son funciones permutación-equivalentes. Para este fin, expresaremos las definiciones de ψ y Φ como un producto de matrices.

Recordemos que la función boolena $G(z)$ dada en (2.4) está definida como:

$$(y_0, \ldots, y_{k-1}) \mapsto y_0 r_0(z) \oplus \cdots \oplus y_{k-1} r_{k-1}(z) \oplus r_k(z), \qquad z \in \mathbb{Z}_{2^{k+1}}.$$

z	$r_0(z)$	$r_1(z)$	$r_2(z)$	$\psi(z) \in \mathbb{F}_2^4$	$\psi'(z) \in \mathbb{F}_2^4$
0	0	0	0	(0,0,0,0)	(0,0,0,0)
1	1	0	0	(0,1,0,1)	(0,0,1,1)
2	0	1	0	(0,0,1,1)	(0,1,0,1)
3	1	1	0	(0,1,1,0)	(0,1,1,0)
4	0	0	1	(1,1,1,1)	(1,1,1,1)
5	1	0	1	(1,0,1,0)	(1,1,0,0)
6	0	1	1	(1,1,0,0)	(1,0,1,0)
7	1	1	1	(1,0,0,1)	(1,0,0,1)

Cuadro 2.2: Imagen de ψ y ψ'

En términos más algebraicos, $G(z)$ puede ser escrita como un producto de matrices, con entradas en $\mathbb{F}_2$, de tamaños $1 \times (k+1)$ y $(k+1) \times 1$. De manera más precisa,

$$G(z)(Y) = \begin{pmatrix} r_0(z) & \cdots & r_{k+1}(z) & r_k(z) \end{pmatrix} \begin{pmatrix} y_0 \\ \vdots \\ y_{k-1} \\ 1 \end{pmatrix}.$$

Haciendo variar $Y = (y_0, \ldots, y_{k-1})$ en todos los elementos de $\mathbb{F}_2^k$ obtenemos

$$\psi(z) = \begin{pmatrix} r_0(z) & \cdots & r_{k+1}(z) & r_k(z) \end{pmatrix} \begin{pmatrix} Y_0^t & Y_1^t & \cdots & Y_{2^k-1}^t \\ 1 & 1 & \cdots & 1 \end{pmatrix},$$

donde Y_i^t significa el vector transpuesto de Y_i. Sea

$$F = \begin{pmatrix} Y_0^t & Y_1^t & \cdots & Y_{2^k-1}^t \\ 1 & 1 & \cdots & 1 \end{pmatrix}.$$

La libertad en el orden de la definición de $\psi(z)$ nos permite tomar $Y_0 = (0)_k \in \mathbb{F}_2^k$. Por lo tanto,

$$F = \begin{pmatrix} (0)_k^t & Y_1^t & \cdots & Y_{2^k-1}^t \\ 1 & 1 & \cdots & 1 \end{pmatrix}, \tag{2.5}$$

donde $Y_1, \ldots Y_{2^k-1} \in \mathbb{F}_2^k \setminus \{(0)_k\}$. En consecuencia, F es ahora una matriz verificadora de paridad para el código de Hamming extendido $\mathscr{H}_e(k)$. Todavía más, podemos tomar $Y_1, \ldots, Y_{2^k-1}$ tales que F sea precisamente la matriz $H(k)$ definida en la relación (2.3).

Para conectar lo anterior con la isometría de Gray $\Phi : \mathbb{Z}_{2^{k+1}} \to \mathbb{F}_2^{2^k}$, basta observar que $\Phi(z)$ también puede ser expresada como un producto de matrices:

$$\begin{aligned}\Phi(z) &= r_0(z)c_0^k \oplus r_1(z)c_1^k \oplus \cdots \oplus r_k(z)c_k^k \\ &= \begin{pmatrix} r_0(z) & \cdots & r_k(z) \end{pmatrix} \begin{pmatrix} c_0^k \\ \vdots \\ c_k^k \end{pmatrix} \\ &= \begin{pmatrix} r_0(z) & \cdots & r_k(z) \end{pmatrix} H(k).\end{aligned}$$

En conclusión, la definición de ψ coincide con la definición de Φ si los elementos de $\mathbb{F}_2^k$ son ordenados de tal modo que la matriz F coincida con la matriz $H(k)$. En términos generales, este análisis conduce a la siguiente:

Proposición 2.1.6. *La función de Gray ψ definida en* [11] *y la isometría de Gray Φ definida en esta sección son permutación-equivalentes.*

Demostración. Se ha demostrado que para todo $z \in \mathbb{Z}_{2^{k+1}}$ se tiene que $\Phi(z) = \psi(z)$ siempre que la matriz F de la ecuación (2.5) sea igual a la matriz $H(k)$ dada en (2.3). Ahora, consideremos otro orden en $\mathbb{F}_2^k$, digamos $\mathbb{F}_2^k = \{X_0, X_1, \ldots, X_{2^k-1}\}$, y sea

$$\psi'(z) = (G(z)(X_0), G(z)(X_1), \ldots, G(z)(X_{2^k-1})).$$

Sea ρ la permutación sobre $I_{2^k} = \{0, 1, \ldots, 2^k - 1\}$ tal que $X_{\sigma(i)} = Y_i$, $0 \le i \le 2^k - 1$ y sea $\widetilde{\rho}$ la permutación sobre $\mathbb{F}_2^{2^k}$ inducida por ρ. Entonces

$$\begin{aligned}\Phi(z) = \psi(z) &= (G(z)(Y_0), G(z)(Y_1), \ldots, G(z)(Y_{2^k-1})) \\ &= (G(z)(X_{\sigma(0)}), G(z)(X_{\sigma(1)}), \ldots, G(z)(Y_{\sigma(2^k-1)})) \\ &= \widetilde{\rho}(G(z)(X_0), G(z)(X_1), \ldots, G(z)(X_{2^k-1})), \\ &= \widetilde{\rho}(\psi'(Z)),\end{aligned}$$

lo cual demuestra que Φ y ψ son permutación-equivalentes. □

2.1.3. Definición de la isometría de Gray sobre $\mathbb{Z}_{2^{k+1}}^n$

Con el propósito de construir códigos sobre $\mathbb{F}_2$ de longitud $2^k n$ a partir de códigos sobre $\mathbb{Z}_{2^{k+1}}$ de longitud n, la definición de la función de Gray es extendida al $\mathbb{Z}_{2^{k+1}}$-módulo $\mathbb{Z}_{2^{k+1}}^n$. Usualmente esto es hecho coordenada a coordenada [11, 51, 52], es decir, para todo $Z = (z_0, \ldots, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}$, la imagen de Z bajo la función de Gray es

$$\Phi'(z) = (\Phi(z_0)|\ldots|\Phi(z_{n-1})) \in \mathbb{F}_2^{2^k n}.$$

Sin embargo, la definición de la función de Gray que a continuación presentaremos difiere de este procedimiento usual. Más adelante demostraremos que ambas definiciones producen funciones de Gray que son permutación-equivalentes.

Recordemos que todo $Z = (z_0, \ldots, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$ puede ser escrito de manera única en su representación 2-ádica:

$$Z = r_0(Z) + r_1(Z)2 + \cdots + r_k(Z)2^k, \qquad r_i(Z) = (r_i(z_0), \ldots, r_i(z_{n-1})) \in \mathbb{F}_2^n.$$

De igual modo que en [21], definimos la *función de Gray* $\Phi : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{F}_2^{2^k n}$ de la siguiente manera:

$$\Phi(Z) = \Big(c_0^k \otimes r_0(Z)\Big) \oplus \Big(c_1^k \otimes r_1(Z)\Big) \oplus \cdots \oplus \Big(c_k^k \otimes r_k(Z)\Big) \qquad \forall Z \in \mathbb{Z}_{2^{k+1}}^n \tag{2.6}$$

donde "$\otimes$" es el producto de Kronecker. Note que si $n = 1$, entonces $c_i^k \otimes r_0(Z) = r_0(Z)c_i^k$ y, por lo tanto, la definición de Φ sobre $\mathbb{Z}_{2^{k+1}}$ es un caso particular de la definición dada en (2.6).

A continuación presentamos dos ejemplos que ilustran la definición de Φ sobre $\mathbb{Z}_{2^{k+1}}^n$.

Ejemplo 2.1.7. Sea $k = 1$ y $n \geq 1$. Para todo $Z = (z_0, \ldots, z_{n-1}) \in \mathbb{Z}_4^n$ tenemos que

$$\begin{aligned}
\Phi(Z) &= \Big(c_0^1 \otimes r_0(Z)\Big) \oplus \Big(c_1^1 \otimes r_1(Z)\Big) \\
&= \Big((0,1) \otimes r_0(Z)\Big) \oplus \Big((1,1) \otimes r_1(Z)\Big) \\
&= ((0)_n | r_0(Z)) \oplus (r_1(Z) | r_1(Z)) \\
&= (r_1(z_0), \ldots, r_1(z_{n-1}), r_0(z_0) \oplus r_1(z_0), \ldots, r_0(z_{n-1}) \oplus r_1(z_{n-1}))\,.
\end{aligned}$$

Por lo tanto, para este caso, la definición de Φ coincide con la definición de la función de Gray $\phi : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$ presentada en [23, 54, 55]. Por tal razón, sin temor a que exista alguna confusión, *emplearemos el símbolo* ϕ, en lugar de Φ, *para denotar a la función de Gray de* $\mathbb{Z}_4^n$ *a* $\mathbb{F}_2^{2n}$. Por otra parte, observemos que, si $\phi(Y) = \phi(Z)$, entonces $r_1(Y) = r_1(Z)$ y $r_1(Y) \oplus r_0(Y) = r_1(Z) \oplus r_0(Z)$. Estas ecuaciones implican que $Y = Z$. Por lo tanto, la función ϕ es inyectiva.

Ejemplo 2.1.8. Sean $k = 2$ y $n \geq 1$. La función $\Phi : \mathbb{Z}_8^n \to \mathbb{F}_2^{4n}$ está dada por

$$\Phi(Z) = \Big((0,0,1,1) \otimes r_0(Z)\Big) \oplus \Big((0,1,0,1) \otimes r_1(Z)\Big) \oplus \Big((1,1,1,1) \otimes r_2(Z)\Big),$$

igualdad que al ser desarrollada da como resultado

$$\Phi(Z) = (r_2(Z)\,|\,r_1(Z) \oplus r_2(Z)\,|\,r_0(Z) \oplus r_2(Z)\,|\,r_0(Z) \oplus r_1(Z) \oplus r_2(Z)).$$

Usando argumentos similares a los del Ejemplo 2.1.7, note que de la expresión anterior, se sigue que $\Phi : \mathbb{Z}_8^n \to \mathbb{F}_2^{4n}$ es también inyectiva.

La siguiente proposición establece formalmente la inyectividad de Φ observada en los Ejemplos 2.1.7 y 2.1.8.

Proposición 2.1.9. *Para todos los enteros $n,k \geq 1$, la función de Gray $\Phi : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{F}_2^{2^k n}$ es inyectiva.*

Demostración. La prueba es llevada a cabo por inducción sobre k. El caso $k = 1$, $n \geq 1$, fue probado en el Ejemplo 2.1.7. Ahora, supongamos que para algún $k \geq 1$ la afirmación es cierta para todo $n \geq 1$. Observemos que la acción de Φ sobre cualquier $X \in \mathbb{Z}_{2^{k+2}}^n$ puede ser escrita como

$$\Phi(X) = \Big((u \otimes c_k^k) \otimes r_0(X)\Big) \oplus \Big((v \otimes c_0^k) \otimes r_1(X)\Big) \oplus \cdots \oplus \Big((v \otimes c_k^k) \otimes r_{k+1}(X)\Big).$$

Asimismo, observe que por las propiedades de asociatividad y distributividad del producto de Kronecker, la expresión anterior es igual a la siguiente:

$$\Phi(X) = \Big(u \otimes (c_k^k \otimes r_0(X))\Big) \oplus \Big(v \otimes \Big((c_0^k \otimes r_1(X)) \oplus \cdots \oplus (c_k^k \otimes r_{k+1}(X))\Big)\Big).$$

Por lo tanto, si $Y, Z \in \mathbb{Z}_{2^{k+2}}^n$ son tales que $\Phi(Y) = \Phi(Z)$, entonces

$$\Big(c_0^k \otimes r_1(Y)\Big) \oplus \cdots \oplus \Big(c_k^k \otimes r_{k+1}(Y)\Big) = \Big(c_0^k \otimes r_1(Z)\Big) \oplus \cdots \oplus \Big(c_k^k \otimes r_{k+1}(Z)\Big).$$

Así, por hipótesis de inducción, obtenemos $r_i(Y) = r_i(Z)$ con $1 \leq i \leq k+1$. Consecuentemente, $c_k^k \otimes r_0(Y) = c_k^k \otimes r_0(Z)$, lo cual implica que $r_0(Y) = r_0(Z)$. Por lo tanto, $Y = Z$. □

Otras propiedades de la función de Gray serán investigadas en la Sección 2.3 de este manuscrito. El siguiente punto a tratar en este apartado es la relación que existe entre la función de Gray Φ definida en (2.6) y la función de Gray Φ' definida sobre el conjunto $\mathbb{Z}_{2^{k+1}}^n$ coordenada a coordenada.

Primero observemos que en general estas funciones son distintas. El caso más sencillo para ilustrar esto es sobre $\mathbb{Z}_4^n$. Del Ejemplo 2.1.7, sabemos que la función de Gray $\phi : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$ está dada para todo $Z = (z_0, \ldots, z_{n-1})$ como

$$\phi(Z) = (r_1(z_0), \ldots, r_1(z_{n-1}), r_0(z_0) \oplus r_1(z_0), \ldots, r_0(z_{n-1}) \oplus r_1(z_{n-1})). \tag{2.7}$$

Por otra parte, la función $\phi' : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$ extendida coordenada a coordenada está dada por

$$\phi'(Z) = (r_1(z_0), r_0(z_0) \oplus r_1(z_0), \ldots, r_1(z_{n-1}), r_0(z_{n-1}) \oplus r_1(z_{n-1})). \tag{2.8}$$

De aquí vemos que las funciones ϕ y ϕ' tienen reglas de asignación distintas. (Por ejemplo, si $Z = (3,2,0) \in \mathbb{Z}_4^3$, entonces $\phi(Z) = (1,1,0,0,1,0)$ mientras que $\phi'(Z) = (1,0,1,1,0,0)$). Asimismo, de (2.7) y (2.8), notamos que cada coordenada del vector $\phi(Z)$ es una coordenada del

vector $\phi'(Z)$ ubicada en una posición distinta. Por lo tanto, podemos inferir que estos vectores difieren por una permutación, lo cual implica que ϕ y ϕ' son permutación-equivalentes. De manera más precisa, sea τ la permutación sobre el conjunto $I_{2n} = \{0, \ldots, 2n-1\}$ definida como

$$\tau = \begin{pmatrix} 0 & 1 & 2 & \cdots & i & \cdots & n-1 & n & n+1 & n+2 & \cdots & n+i & \cdots & 2n-1 \\ 0 & 2 & 4 & \cdots & 2i & \cdots & 2n-2 & 1 & 3 & 5 & \cdots & 2i+1 & \cdots & 2n-1 \end{pmatrix} \quad (2.9)$$

Entonces no es difícil verificar que $\phi' = \widetilde{\tau} \circ \phi$, donde $\widetilde{\tau}$ es la permutación sobre $\mathbb{F}_2^{2n}$ inducida por τ. Por ejemplo, si $n = 3$, entonces

$$\tau = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 2 & 4 & 1 & 3 & 5 \end{pmatrix},$$

y, si consideramos $Z = (3,2,0) \in \mathbb{Z}_4^3$, entonces $\widetilde{\tau}(\phi(Z))) = (1,0,1,1,0,0)$, lo cual coincide con $\phi'(Z)$. Esto no es una propiedad exclusiva de la isometría de Gray sobre $\mathbb{Z}_4^n$ sino que también es válida para la función de Gray sobre $\mathbb{Z}_{2^{k+1}}^n$. Para este propósito, generalizamos la permutación τ dada en (2.9).

Sean $n \geq 1$ y $k \geq 0$ enteros. Sobre el conjunto $I_{2^k n}$ definimos la permutación τ de la siguiente manera. Sea $e \in I_{2^k n}$ y por medio del algoritmo de la división sobre los enteros, exprese a e como $e = in + j$, donde $0 \leq j \leq n-1$. Entonces definimos $\tau(e) = 2^k j + i$.

Veamos algunos ejemplos de la permutación τ.

Ejemplo 2.1.10. Sea $k = 0$ y $n \geq 1$. Entonces el dominio de la permutación τ es el conjunto I_n. Dado que al dividir cualquier elemento $e \in I_n$ entre n, la parte entera es $i = 0$ y el residuo es $j = e$, se tiene que $\tau(e) = e$. Esto implica que la permutación τ es la función identidad sobre I_n.

Ejemplo 2.1.11. Sea $k \geq 1$ y sea $n = 1$. Entonces la permutación τ actúa sobre el conjunto I_{2^k}. Ya que $n = 1$, todo elemento e de I_{2^k} queda trivialmente expresado como $e = e1 + 0$, es decir, $i = e$ y $j = 0$. Por lo tanto, de acuerdo a la definición de τ, $\tau(e) = 2^k(0) + e = e$. Esto es, τ es la permutación identidad sobre I_{2^k}.

Ejemplo 2.1.12. Sea $k = 1$ y sea $n \geq 1$ un entero. Entonces, para todo $e \in I_{2n}$ escrito como $e = in + j$, $0 \leq j \leq n-1$, se tiene que $\tau(e) = 2j + i$. Siendo más específicos, supongamos que $0 \leq e \leq n-1$, entonces $e = 0n + e$, lo cual implica que $\tau(e) = 2e$. Supongamos ahora que $n \leq e \leq 2n-1$. Entonces $e = 1n + i$, $0 \leq i \leq n-1$, lo cual dice que $\tau(e) = 2i + 1$. Con estas observaciones, es claro que esta permutación coincide con la permutación de la relación (2.9).

Sea $\widetilde{\tau}$ la permutación sobre $\mathbb{F}_2^{2^k n}$ inducida por τ. Una forma sencilla de interpretar a la permutación $\widetilde{\tau}$ es mediante la transposición de matrices. Para este fin, primero observemos que las coordenadas del vector

$$a = (a_0, a_1, \ldots, a_{n-1}, a_n, \ldots, a_{2n-1}, \ldots, a_{(2^k-1)n}, \ldots, a_{2^k n-1}) \in \mathbb{F}_2^{2^k n} \quad (2.10)$$

pueden ser etiquetadas en 2^k bloques de tamaño n obteniendo:

$$a = (a_{0,0}, \ldots, a_{0,n-1}, a_{1,0}, \ldots, a_{1,n-1}, \ldots, a_{2^k-1,0}, \ldots, a_{2^k-1,n-1}) \in \mathbb{F}_2^{2^k n} \tag{2.11}$$

y que a este último vector le podemos asociar la siguiente matriz binaria de tamaño $2^k \times n$:

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,j} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,j} & \cdots & a_{1,n-1} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i,0} & a_{i,1} & \cdots & a_{i,j} & \cdots & a_{i,n-1} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{2^k-1,0} & a_{2^k-1,1} & \cdots & a_{2^k-1,j} & \cdots & a_{2^k-1,n-1} \end{pmatrix}.$$

Sea a_e una coordenada del vector a con las coordenadas etiquetadas como en (2.10), es decir, $0 \leq e \leq 2^k n - 1$. Queremos determinar en qué renglón y en qué columna de la matriz A se encuentra a_e. Dado que la matriz A tiene n columnas, el residuo de la división de e entre n nos indicará en qué columna se encuentra a_e, mientras que la parte entera de esta división, nos indicará en qué renglón de A se encuentra a_e. Esto es, si $e = in + j$, donde $0 \leq j \leq n-1$, entonces la coordenada a_e del vector a dado en (2.10) ha sido etiqueda como $a_{i,j}$ en el vector a de la relación (2.11), es decir, a_e se encuentra en el renglón i y la columna j de la matriz A. Consecuentemente, a_e está en la columna i y el renglón j de la matriz transpuesta de A.

Invirtiendo el proceso, a la matriz transpuesta de A, que escribimos a continuación,

$$A^t = \begin{pmatrix} a_{0,0} & a_{1,0} & \cdots & a_{i,0} & \cdots & a_{2^k-1,0} \\ a_{0,1} & a_{1,1} & \cdots & a_{i,1} & \cdots & a_{2^k-1,1} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{0,j} & a_{1,j} & \cdots & a_{i,j} & \cdots & a_{2^k-1,j} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{0,n-1} & a_{1,n-1} & \cdots & a_{i,n-1} & \cdots & a_{2^k-1,n-1} \end{pmatrix},$$

le asociamos el vector $a^t \in \mathbb{F}_2^{2^k n}$ que se obtiene al concatenar (en orden) los renglones de A^t, es decir,

$$a^t = (a_{0,0}, \ldots, a_{2^k-1,0}, a_{0,1}, \ldots, a_{2^k-1,1}, \ldots, a_{0,n-1}, \ldots, a_{2^k-1,n-1}).$$

o bien, etiquetando de manera natural las coordenadas de a^t, obtenemos que

$$a^t = (b_0, b_1, \ldots, b_{n-1}, b_n, \ldots, a_{2n-1}, \ldots, b_{(2^k-1)n}, \ldots, b_{2^k n-1}) \in \mathbb{F}_2^{2^k n}$$

Claramente, a y a^t difieren por una permutación. Afirmamos que esta permutación es $\widetilde{\tau}$. En efecto, hemos señalado que la coordenada a_e de a, $0 \leq e \leq 2^k n - 1$, es la entrada $a_{i,j}$ de la

matriz A, donde $e = in + j$, $0 \leq j \leq n-1$. Por la definición de matriz transpuesta $a_{j,i}$ es igual a la coordenada $a_{i,j}$ de A^t. Ya que la matriz A^t tiene 2^k columnas, $a_{j,i}$ es igual a la coordenda b_f del vector a^t, donde $f = j2^k + i$. Por lo tanto, $f = \tau(e)$. Ya que esto es válido para cualquier coordenada de a, hemos demostrado que $a^t = \widetilde{\tau}(a)$.

Ahora relacionemos a la permutación $\widetilde{\tau}$ con la isometrías de Gray $\Phi, \Phi' : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{F}_2^{2^k n}$. Primero, recordemos que para todo $Z = (z_0, \ldots, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$ se ha definido la función de Gray Φ como

$$\Phi(Z) = c_0^k \otimes r_0(Z) \oplus \cdots \oplus c_k^k \otimes r_k(Z),$$

donde $r_i(Z) = (r_i(z_0), \ldots, r_i(z_{n-1})) \in \mathbb{F}_2^n$ son tales que $Z = r_0(Z) + 2r_1(Z) + \cdots + 2^k r_k(Z)$ es la representación 2-ádica de Z y $c_0^k, \ldots, c_k^k \in \mathbb{F}_2^{2^k}$ son los vectores definidos en la Sección 2.1.1. Para todo entero i, $0 \leq i \leq k$, denotemos

$$c_i^k = \left(\varepsilon_{i,0}, \varepsilon_{i,1}, \ldots, \varepsilon_{i,2^k-1}\right), \quad \varepsilon_{i,j} \in \mathbb{F}_2,\ 0 \leq j \leq 2^k - 1.$$

Note que con la introducción de esta notación, la función de Gray Φ queda expresada como

$$\Phi(Z) = \left(\bigoplus_{i=0}^{k} \varepsilon_{i,0} r_i(Z) \middle| \bigoplus_{i=0}^{k} \varepsilon_{i,1} r_i(Z) \middle| \cdots \middle| \bigoplus_{i=0}^{k} \varepsilon_{i,2^k-1} r_i(Z) \right).$$

Asimismo, note que en la expresión anterior cada componente $\bigoplus_{i=0}^{k} \varepsilon_{i,j} r_i(Z)$ es un vector en $\mathbb{F}_2^n$. De hecho,

$$\bigoplus_{i=0}^{k} \varepsilon_{i,j} r_i(Z) = \left(\bigoplus_{i=0}^{k} \varepsilon_{i,j} r_i(z_0), \bigoplus_{i=0}^{k} \varepsilon_{i,0} r_i(z_1), \ldots, \bigoplus_{i=0}^{k} \varepsilon_{i,0} r_i(z_{n-1}) \right).$$

Como antes, al vector $\Phi(Z) \in \mathbb{F}_2^{2^k n}$ le asociamos la siguiente matriz binaria de tamaño $2^k \times n$:

$$M_{\Phi(Z)} = \begin{pmatrix} \oplus\varepsilon_{i,0} r_i(z_0) & \oplus\varepsilon_{i,0} r_i(z_1) & \cdots & \oplus\varepsilon_{i,0} r_i(z_{n-1}) \\ \oplus\varepsilon_{i,1} r_i(z_0) & \oplus\varepsilon_{i,1} r_i(z_1) & \cdots & \oplus\varepsilon_{i,1} r_i(z_{n-1}) \\ \vdots & \vdots & & \vdots \\ \oplus\varepsilon_{i,2^k-1} r_i(z_0) & \oplus\varepsilon_{i,2^k-1} r_i(z_1) & \cdots & \oplus\varepsilon_{i,2^k-1} r_i(z_{n-1}) \end{pmatrix},$$

donde $\oplus\varepsilon_{i,j} r_i(z_j)$ significa $\oplus_{i=0}^{k} \varepsilon_{i,j} r_i(z_j)$, $0 \leq j \leq 2^k - 1$.

Por otro lado, recordemos que se ha definido

$$\Phi'(Z) = (\Phi(z_0)|\Phi(z_1)|\ldots|\Phi(z_{n-1})).$$

Usando la misma notación de los vectores c_i^k, observemos que para cada j, $0 \leq j \leq n-1$, la imagen de Φ en cada coordenada del vector $Z = (z_0, z_1, \ldots, z_{n-1})$ puede ser escrita como

$$\Phi(z_j) = \left(\bigoplus_{i=0}^{k} \varepsilon_{i,0} r_i(z_j), \bigoplus_{i=0}^{k} \varepsilon_{i,1} r_i(z_j), \ldots, \bigoplus_{i=0}^{k} \varepsilon_{i,2^k-1} r_i(z_j) \right) \in \mathbb{F}_2^{2^k}.$$

De manera análoga, al vector $\Phi'(Z) \in \mathbb{F}_2^{2^k n}$ le asociamos la siguiente matriz binaria de tamaño $n \times 2^k$:

$$M_{\Phi'(Z)} = \begin{pmatrix} \oplus\varepsilon_{i,0} r_i(z_0) & \oplus\varepsilon_{i,1} r_i(z_0) & \cdots & \oplus\varepsilon_{i,2^k-1} r_i(z_0) \\ \oplus\varepsilon_{i,0} r_i(z_1) & \oplus\varepsilon_{i,1} r_i(z_1) & \cdots & \oplus\varepsilon_{i,2^k-1} r_i(z_1) \\ \vdots & \vdots & & \vdots \\ \oplus\varepsilon_{i,0} r_i(z_{n-1}) & \oplus\varepsilon_{i,0} r_i(z_{n-1}) & \cdots & \oplus\varepsilon_{i,2^k-1} r_i(z_{n-1}) \end{pmatrix}.$$

Claramente, $M_{\Phi'(Z)} = M^t_{\Phi(Z)}$, lo cual da una demostración del siguiente resultado:

Teorema 2.1.13. *Sean $n,k \geq 1$ enteros y $\Phi, \Phi' : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{F}_2^{2^k n}$ las funciones de Gray definidas anteriormente. Entonces*

$$\Phi' = \widetilde{\tau} \circ \Phi,$$

donde $\widetilde{\tau}$ es la permutación sobre $\mathbb{F}_2^{2^k n}$ inducida por la permutación τ previamente definida. En particular, esto establece que las funciones de Gray Φ' y Φ son permutación-equivalentes.

La función de Gray $\psi : \mathbb{Z}_{2^{k+1}} \to \mathbb{F}_2^{2^k}$ definida en la Sección 2.1.2 (e introducida en [11]), es extendida a una función $\psi : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{F}_2^{2^k n}$ coordenada a coordenada. Consecuentemente, tenemos el siguiente:

Corolario 2.1.14. *Las funciones de Gray $\psi, \Phi : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{F}_2^{2^k n}$ son permutación-equivalentes. Más aún, si sobre $\mathbb{Z}_{2^{k+1}}$ las funciones ψ y Φ son iguales, entonces sobre $\mathbb{Z}_{2^{k+1}}^n$ tenemos que $\psi = \widetilde{\tau} \circ \Phi$.*

Demostración. Anteriormente demostramos que sobre $\mathbb{Z}_{2^{k+1}}$, $\psi = \Phi$ si consideramos que los elementos de $\mathbb{F}_2^k$ están ordenados de manera adecuada. Esto implica, por el Teorema 2.1.13, que sobre $\mathbb{Z}_{2^{k+1}}^n$, $\psi = \widetilde{\tau} \circ \Phi$. Ahora, si ψ no coincide con Φ sobre $\mathbb{Z}_{2^{k+1}}$, entonces por la Proposición 2.1.6 existe una permutación $\widetilde{\rho}$ tal que $\Phi = \widetilde{\rho} \circ \psi$. Por lo tanto, para todo $Z = (z_0, \ldots, z_{n-1})$ en $\mathbb{Z}_{2^{k+1}}^n$ tenemos que

$$(\widetilde{\tau} \circ \Phi)(Z) = ((\widetilde{\rho} \circ \psi)(z_0) | \cdots | (\widetilde{\rho} \circ \psi)(z_{n-1})) = \widetilde{\rho}^{\otimes n}(\psi(Z)),$$

donde $\widetilde{\rho}^{\otimes n} : \mathbb{F}^{2^k n} \to \mathbb{F}^{2^k n}$ es la permutación definida como

$$\left(A^{(0)} | \cdots | A^{(n-1)}\right) \mapsto \left(\widetilde{\rho}\left(A^{(0)}\right) | \cdots | \widetilde{\rho}\left(A^{(n-1)}\right)\right), \quad A^{(j)} \in \mathbb{F}_2^{2^k}, 0 \leq j \leq n-1.$$

Entonces $\Phi(Z) = \left((\widetilde{\tau})^{-1} \circ \widetilde{\rho}^{\otimes n}\right) \psi(Z))$, lo que finaliza la prueba. □

2.2. La isometría φ sobre $\mathbb{Z}_{2^{k+1}}^n$

En esta sección definiremos una función $\varphi : \mathbb{Z}_{2^{k+1}} \to \mathbb{Z}_4^{2^{k-1}}$ y demostraremos que esta aplicación es permutación equivalente a la isometría φ^k introducida en [51, 52] y, por lo tanto, también φ será una isometría. Asimismo, de igual forma que hemos hecho con la función de Gray, extenderemos el dominio de φ al $\mathbb{Z}_{2^{k+1}}$-módulo $\mathbb{Z}_{2^{k+1}}^n$, y estableceremos de manera natural su relación con la función de Gray Φ definida en la Sección 2.1.3. Esta relación, enunciada en el Lema 2.2.8, juega un papel central en nuestro trabajo ya que nos permitirá relacionar códigos de longitud n definidos sobre $\mathbb{Z}_{2^{k+1}}$ con códigos de longitud $2^{k-1}n$ sobre $\mathbb{Z}_4$, y a éstos, a través de la isometría de Gray sobre $\mathbb{Z}_4$, con códigos binarios de longitud $2^k n$. Además, esta relación nos dará la facultad de derivar propiedades de la función de Gray a partir de propiedades de la función φ.

2.2.1. Definición de la isometría φ sobre $\mathbb{Z}_{2^{k+1}}$

Inspirados en los trabajos [51] y [52], introducimos la siguiente definición. Sean $k \geq 1$ un entero, $z \in \mathbb{Z}_{2^{k+1}}$ y $z = r_0(z) + r_1(z)2 + \cdots + r_k(z)2^k$ la representación 2-ádica de z. Definimos la función $\varphi : \mathbb{Z}_{2^{k+1}} \to \mathbb{Z}_4^{2^{k-1}}$ mediante la regla de asignación

$$z \mapsto r_0(z)c_{k-1}^{k-1} + 2\left[r_1(z)c_0^{k-1} \oplus \cdots \oplus r_k(z)c_{k-1}^{k-1}\right],$$

donde los vectores c_i^{k-1}, $0 \leq i \leq k-1$, son aquellos que fueron definidos en la Sección 1.1.1.

Dado que $r_1(z)c_0^{k-1} \oplus \cdots \oplus r_k(z)c_k^{k-1}$ y $r_0(z)c_0^{k-1}$ pertenecen al espacio $\mathbb{F}_2^{2^{k-1}}$, el vector $\varphi(z) \in \mathbb{Z}_4^{2^{k-1}}$ está expresado en su representación 2-ádica, es decir,

$$r_0(\varphi(z)) = c_{k-1}^{k-1} r_0(z), \qquad r_1(\varphi(z)) = c_0^{k-1} r_1(z) \oplus \cdots \oplus c_{k-1}^{k-1} r_k(z),$$

lo cual ofrece una ventaja al momento de componer a φ con la función de Gray ϕ sobre $\mathbb{Z}_4$.

Ejemplo 2.2.1. Recordemos que en la Sección 2.1.1 hemos definido $c_0^0 = 1$ y, por lo tanto, la función $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_4$ es igual a la función identidad. Por otro lado, la función $\varphi : \mathbb{Z}_{2^3} \to \mathbb{Z}_4^2$ está dada por

$$\begin{aligned}\varphi(z) &= r_0(z)c_1^1 + 2\left[r_1(z)c_0^1 \oplus r_2(z)c_1^1\right] \\ &= r_0(z)(1,1) + 2\left[r_1(z)(0,1) \oplus r_2(z)(1,1)\right] \\ &= (r_0(z) + 2r_2(z), r_0(z) + 2\left[r_1(z) \oplus r_2(z)\right]).\end{aligned}$$

En el Cuadro 2.3 describimos la imagen de φ para este caso. Por otra parte, notemos que al

z	$r_0(z)$	$r_1(z)$	$r_2(z)$	$\varphi(z) \in \mathbb{Z}_4^2$
0	0	0	0	(0,0)
1	1	0	0	(1,1)
2	0	1	0	(0,2)
3	1	1	0	(1,3)
4	0	0	1	(2,2)
5	1	0	1	(3,3)
6	0	1	1	(2,0)
7	1	1	1	(3,1)

Cuadro 2.3: Imagen de $\varphi : \mathbb{Z}_8 \to \mathbb{Z}_4^2$

aplicar la función de Gray ϕ a $\varphi(z)$ obtenemos

$$\begin{aligned}\phi(\varphi(z)) &= (0,1) \otimes r_0(\varphi(z)) \oplus (1,1) \otimes r_1(\varphi(z)) \\ &= (r_1(\varphi(z)) \,|\, r_1(\varphi(z)) \oplus r_0(\varphi(z))) \\ &= (r_2(z), r_1(z) \oplus r_2(z), r_2(z) \oplus r_0(z), r_1(z) \oplus r_2(z) \oplus r_0(z)).\end{aligned}$$

Comparando esta última expresión con la fórmula obtenida en el Ejemplo 2.1.5, vemos que para todo $z \in \mathbb{Z}_8$, $\Phi(z) = (\phi \circ \varphi)(z)$.

Ejemplo 2.2.2. La función $\varphi : \mathbb{Z}_{16} \to \mathbb{Z}_4^4$ está dada por

$$\begin{aligned}\varphi(z) =& r_2(z)c_0^2 + 2\left[r_1(z)c_0^2 \oplus r_2(z)c_1^2 \oplus r_3(z)c_2^2\right] \\ =& r_0(z)(1,1,1,1) + 2\left[r_1(z)(0,0,1,1) \oplus r_2(z)(0,1,0,1) \oplus r_3(z)(1,1,1,1)\right].\end{aligned}$$

Dasarrollando la expresión de $\varphi(z)$ obtenemos la relación

$$\begin{aligned}\varphi(z) =& (r_0(z) + 2r_3(z), r_0(z) + 2[r_2(z) \oplus r_3(z)], \\ & r_0(z) + 2[r_1(z) \oplus r_3(z)], r_0(z) + 2[r_1(z) \oplus r_2(z) \oplus r_3(z)]),\end{aligned}$$

la cual nos será útil más adelante. Por otra parte, sin desarrollar la expresión de $\varphi(z)$, podemos verificar fácilmente que la aplicación $\phi \circ \varphi : \mathbb{Z}_{2^4} \to \mathbb{F}_2^8$ resulta ser

$$(\phi \circ \varphi)(z) = \left(v \otimes \left[r_1(z)c_0^2 \oplus r_2(z)c_1^2 \oplus r_3(z)c_2^2\right]\right) \oplus \left(u \otimes r_0(z)c_2^2\right) \qquad \forall z \in \mathbb{Z}_{2^4}$$

Por las propiedades de distributividad del producto de Kronecker, esta última expresión es precisamente

$$r_0(z)c_0^3 \oplus r_1(z)c_1^3 \oplus r_2(z)c_2^3 \oplus r_3(z)c_3^3 = \Phi(z),$$

y, por lo tanto, nuevamente hemos obtenido que $\Phi(z) = (\phi \circ \varphi)(z)$ para todo $z \in \mathbb{Z}_{16}$.

En los Ejemplos 2.2.1 y 2.2.2 notamos que $\Phi = \phi \circ \varphi$. Esta igualdad será demostrada para el caso general más adelante (Lema 2.2.8, Sección 2.2.2). El siguiente punto a tratar en esta sección es demostrar que la función φ es permutación-equivalente a la isometría φ^k definida en [51, 52]. En ambos trabajos este concepto fue definido de la siguiente manera.

Sea $k \geq 2$ un entero y sea $\rho_k : \mathbb{Z}_{2^{k+1}} \to \mathbb{F}_2^{k-1}$ la función definida como

$$\rho_k(z) = (r_{k-1}(z), \ldots, r_2(z), r_1(z)), \tag{2.12}$$

donde $z = r_0(z) + 2r_1(z) + \cdots + 2^k r_k(z)$ es la representación 2-ádica de z. Para cada entero i tal que $0 \leq i \leq 2^{k-1} - 1$ (es decir, $i \in \mathbb{Z}_{2^{k-1}}$) sea

$$\alpha_i^k = (r_{k-2}(i), \ldots, r_1(i), r_0(i)) \in \mathbb{F}_2^{k-1}, \tag{2.13}$$

donde $i = r_0(i) + 2r_1(i) + \cdots + 2^{k-2} r_{k-2}(i)$ está escrito en su representación 2-ádica. Por medio de la función ρ_k y los vectores α_i^k, se definen las funciones $\varphi_i^k : \mathbb{Z}_{2^{k+1}} \to \mathbb{Z}_4$ como:

$$\varphi_i^k(z) = r_0(z) + 2\left[r_k(z) \oplus (\rho_k(z) \cdot \alpha_i^k)\right],$$

donde " $\cdot$ " es el producto escalar usual sobre $\mathbb{F}_2^{k-1}$. Finalmente, la función $\varphi^k : \mathbb{Z}_{2^{k+1}} \to \mathbb{Z}_4^{2^{k-1}}$ es definida como

$$\varphi^k(z) = (\varphi_0^k(z), \ldots, \varphi_{2^{k-1}-1}^k(z)).$$

Por completez, en [51, 52] la aplicación $\varphi^1 : \mathbb{Z}_4 \to \mathbb{Z}_4$ es definida como la función identidad.

Veamos algunos ejemplos.

Ejemplo 2.2.3. Sea $k = 2$, entonces $\rho_2(z) = r_1(z)$, $\alpha_0^2 = 0$, $\alpha_1^2 = 1$ y

$$\begin{aligned}
\varphi_0^2(z) =& r_0(z) + 2\left[r_2(z) \oplus 0 \cdot r_1(z)\right] = r_0(z) + 2r_2(z), \\
\varphi_1^2(z) =& r_0(z) + 2\left[r_2(z) \oplus 1 \cdot r_1(z)\right] = r_0(z) + 2\left[r_2(z) \oplus r_1(z)\right].
\end{aligned}$$

Por lo tanto, $\varphi^2(z) = (r_0(z) + 2r_2(z), r_0(z) + 2\left[r_2(z) \oplus r_1(z)\right])$, lo cual coincide con la función $\varphi : \mathbb{Z}_{2^3} \to \mathbb{Z}_4^2$ del Ejemplo 2.2.1. Así, a primera impresión, estas definiciones son exactamente las mismas. Sin embargo, el siguiente ejemplo descarta esta sospecha.

Ejemplo 2.2.4. Sea $k = 3$. Dado que $\rho_3(z) = (r_2(z), r_1(z))$, $\alpha_0^3 = (0,0)$, $\alpha_1^3 = (0,1)$, $\alpha_2^3 = (1,0)$, $\alpha_3^3 = (1,1)$, tenemos que

$$\begin{aligned}
\varphi_0^3(z) =& r_0(z) + 2r_3(z), \\
\varphi_1^3(z) =& r_0(z) + 2\left[r_1(z) \oplus r_3(z)\right], \\
\varphi_2^3(z) =& r_0(z) + 2\left[r_2(z) \oplus r_3(z)\right], \\
\varphi_3^3(z) =& r_0(z) + 2\left[r_1(z) \oplus r_2(z) \oplus r_3(z)\right].
\end{aligned}$$

Por consiguiente,

$$\begin{aligned}\varphi^3(z) =&(r_0(z)+2r_3(z), r_0(z)+2\left[r_1(z)\oplus r_3(z)\right], r_0(z)+2\left[r_2(z)\oplus r_3(z)\right],\\ & r_0(z)+2\left[r_1(z)\oplus r_2(z)\oplus r_3(z)\right]).\end{aligned}$$

Comparando $\varphi^3(z)$ con la función $\varphi(z)$ del Ejemplo 2.2.2 podemos constatar que las funciones difieren en la segunda y en la tercera coordenada. Por lo tanto, si consideramos la permutación $\omega = (1 \quad 2)$, entonces $\varphi^3(z) = \widetilde{\omega}(\varphi(z))$, donde $\widetilde{\omega}$ es la permutación sobre $\mathbb{Z}_4^4$ inducida por ω. Esto implica que φ es permutación-equivalente a φ^3. Por otra parte, analizando la definición de la función φ^3 notamos que al sustituir en la definición de φ^3, $\rho_3(z)$ por $\widetilde{\rho}_3(z) = (r_1(z), r_2(z))$, obtenemos directamente que $\varphi^3 = \varphi$. Note que la diferencia entre ρ_3 y $\widetilde{\rho}_3$ es precisamente la permutación ω. Esto presenta los indicios de lo que será una prueba del caso general.

Con el propósito de probar que las funciones φ y φ^k son permutación-equivalentes, a continuación daremos una definición alternativa de la matriz $H(k)$ dada en la relación (2.3). Primero recordemos que los renglones de $H(k)$ son los vectores c_i^k, $0 \leq i \leq k$, y que para todo $k \geq 2$, esta matriz puede ser obtenida de manera recursiva mediante la fórmula

$$H(k) = \begin{pmatrix} c_0^k \\ c_1^k \\ \vdots \\ c_k^k \end{pmatrix} = \begin{pmatrix} (0)_{2^{k-1}} & (1)_{2^{k-1}} \\ H(k-1) & H(k-1) \end{pmatrix}.$$

Para todo entero $k \geq 2$, sea β_i^k el transpuesto del vector α_i^k, $0 \leq i \leq 2^k - 1$ y considere la matriz $H'(k)$ de tamaño $(k+1) \times 2^k$ definida como

$$H'(k) = \begin{pmatrix} \beta_0^k & \beta_1^k & \cdots & \beta_{2^k-1}^k \\ 1 & 1 & \cdots & 1 \end{pmatrix} = \begin{pmatrix} r_{k-1}(0) & r_{k-1}(1) & \cdots & r_{k-1}(2^k-1) \\ r_{k-2}(0) & r_{k-2}(1) & \cdots & r_{k-2}(2^k-1) \\ \vdots & \vdots & & \vdots \\ r_1(0) & r_1(1) & \cdots & r_1(2^k-1) \\ r_0(0) & r_0(1) & \cdots & r_0(2^k-1) \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Claramente, la primera columna de $H'(k)$ tiene todas sus entradas iguales a 0, excepto en la última posición, en donde aparece un 1. Además, es claro que la submatriz de $H'(k)$ cuyas columnas son los β_i^k, $1 \leq i \leq 2^k - 1$, es una matriz verificadora de paridad del código de Hamming $\mathscr{H}(k)$. Así, al igual que $H(k)$, $H'(k)$ es una matriz verificadora de paridad del código de Hamming extendido $\mathscr{H}_e(k)$. Más aún, se tiene el siguiente resultado.

Lema 2.2.5. *Para todo $k \geq 2$, $H(k) = H'(k)$.*

Demostración. Por inducción sobre k. Mediante cálculos directos vemos que

$$H'(2) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \qquad H'(3) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

y del Ejemplo 2.1.1 se sigue que $H'(2) = H(2)$ y $H'(3) = H(3)$. Supongamos ahora que las matrices $H(k)$ y $H'(k)$ son idénticas, y demostremos que las matrices $H'(k+1)$ y $H(k+1)$ también lo son. Por definición

$$H'(k+1) = \begin{pmatrix} r_k(0) & \cdots & r_k(2^k-1) & r_k(2^k) & \cdots & r_k(2^{k+1}-1) \\ r_{k-1}(1) & \cdots & r_{k-1}(2^k-1) & r_{k-1}(2^k) & \cdots & r_{k-1}(2^{k+1}-1) \\ \vdots & & \vdots & \vdots & & \vdots \\ r_1(0) & \cdots & r_1(2^k-1) & r_1(2^k) & \cdots & r_1(2^{k+1}-1) \\ r_0(0) & \cdots & r_0(2^k-1) & r_0(2^k) & \cdots & r_0(2^{k+1}-1) \\ 1 & \cdots & 1 & 1 & \cdots & 1 \end{pmatrix}$$

$$= \begin{pmatrix} r_k(0) & \cdots & r_0(2^k-1) & r_(2^k) & \cdots & r_0(2^{k+1}-1) \\ & H'(k) & & & H'(k) & \end{pmatrix}.$$

Observemos que si $i \in \mathbb{Z}_{2^{k+1}}$ es tal que $0 \leq i \leq 2^k - 1$, entonces i puede ser considerado como un elemento de $\mathbb{Z}_{2^k}$ y, por lo tanto, en su representación 2-ádica se tiene que $r_k(i) = 0$. Por el contrario, si $2^k \leq i \leq 2^{k+1} - 1$, entonces en su representación 2-ádica, necesariamente, $r_k(i) = 1$. Consecuentemente,

$$H'(k+1) = \begin{pmatrix} (0)_{2^{k-1}} & (1)_{2^{k-1}} \\ H'(k) & H'(k) \end{pmatrix}$$

Por hipótesis de inducción, $H'(k) = H(k)$, lo cual implica que $H'(k+1) = H(k+1)$. □

Para relacionar el Lema 2.2.5 con las funciones φ y φ^k, analicemos con más detalle sus definiciones. Si $k = 1$, ambas funciones son la función identidad sobre $\mathbb{Z}_4$. Así, supondremos que $k \geq 2$. Recordemos que para todo $k \geq 2$ y todo $z = r_0(z) + 2r_1(z) + \cdots + 2^k r_k(z) \in \mathbb{Z}_{2^{k+1}}$ expresado en su representación 2-ádica, se ha definido

$$\varphi(z) = r_0 c_{k-1}^{k-1} + 2\left[r_1(z)c_0^{k-1} \oplus \cdots \oplus r_k(z)c_{k-1}^{k-1}\right].$$

Prestando más atención a la componente $r_1(\varphi(z))$ notamos que ésta puede ser interpretada como

un producto de matrices con entradas en el campo binario. De manera más precisa,

$$\begin{aligned} r_1(\varphi(z)) &= r_1(z)c_0^{k-1} \oplus \cdots \oplus r_{k-1}(z)c_{k-2}^{k-1} \oplus r_k(z)c_{k-1}^{k-1} \\ &= \begin{pmatrix} r_1(z) & \cdots & r_{k-1}(z) & r_k(z) \end{pmatrix} \begin{pmatrix} c_{k-1}^{k-1} \\ \vdots \\ c_{k-2}^{k-1} \\ c_{k-1}^{k-1} \end{pmatrix} \\ &= \begin{pmatrix} r_1(z) & \cdots & r_{k-1}(z) & r_k(z) \end{pmatrix} H(k-1). \end{aligned}$$

Por lo tanto,

$$\varphi(z) = r_0(z) + 2\left[\begin{pmatrix} r_1(z) & \cdots & r_{k-1}(z) & r_k(z) \end{pmatrix} H(k-1)\right].$$

Por otra parte, recordemos que para todo $z = r_0(z) + 2r_1(z) + \cdots + 2^k r_k(z) \in \mathbb{Z}_{2^{k+1}}$ expresado en su representación 2-ádica, se ha definido

$$\varphi^k(z) = (\varphi_0^k(z), \ldots, \varphi_{2^{k-1}-1}^k(z)),$$

donde $\rho_k(z)$ y α_i^k han sido definidas en las relaciones (2.12) y (2.13). De nuevo, para cada entero i, $0 \leq i \leq 2^{k-1}-1$, la componente $r_1(\varphi^k(z))$ puede ser expresada como un producto escalar de dos vectores en $\mathbb{F}_2^k$:

$$r_1(\varphi^k(z)) = \left(\rho_k(z) \cdot \alpha_i^k\right) \oplus r_k(z) = \left(\rho_k(z) | r_k(z)\right) \cdot \left(\alpha_i^k | 1\right),$$

o de forma equivalente, como el producto de dos matrices binarias de tamaño $1 \times k$ y $k \times 1$, respectivamente:

$$r_1(\varphi_i^k(z)) = \begin{pmatrix} r_{k-1}(z) & \cdots & r_1(z) & r_k(z) \end{pmatrix} \begin{pmatrix} \beta_i^k \\ 1 \end{pmatrix}.$$

(Observemos que β_i^k es la columna $(i+1)$ de $H(k-1)$.) Haciendo variar i en el conjunto $\{0, \ldots, 2^{k-1}-1\}$, obtenemos que

$$\varphi^k(z) = (r_0(z))_{2^{k-1}} + \left[\begin{pmatrix} r_{k-1}(z) & \cdots & r_1(z) & r_k(z) \end{pmatrix} H(k-1)\right].$$

Resumiendo, hasta este punto se han interpretado las definiciones de φ y φ^k de tal modo que ahora escribimos

$$\varphi(z) = r_0(z)c_{k-1}^{k-1} + 2\left[\begin{pmatrix} r_1(z) & \cdots & r_{k-2}(z) & r_k(z) \end{pmatrix} H(k-1)\right]$$

y, dado que $c_{k-1}^{k-1} = (1)_{2^{k-1}}$,

$$\varphi^k(z) = r_0(z)c_{k-1}^{k-1} + \left[\begin{pmatrix} r_{k-1}(z) & \cdots & r_1(z) & r_k(z) \end{pmatrix} H(k-1)\right],$$

de donde podemos notar que la única diferencia en estas definiciones es el orden en el que aparecen las entradas $r_i(z)$ en las componentes $r_1(\varphi(z))$ y $r_1(\varphi^k(z))$. La equivalencia entre las funciones φ y φ^k será consecuencia de esta diferencia en el orden, la cual está modelada por la siguiente permutación.

Para todo entero $k \geq 3$ e $i = r_0(i) + 2r_1(i) + \cdots + 2^{k-1}r_{k-1}(i) \in \mathbb{Z}_{2^{k-1}}$ escrito en su representación 2-ádica, definimos la permutación ω sobre el conjunto $\mathbb{Z}_{2^{k-1}}$ como

$$\omega(i) = r_{k-2}(i) + 2r_{k-3}(i) + \cdots + 2^{k-2}r_0(i). \tag{2.14}$$

Por completez, para $k = 1,2$ definimos a ω como la permutación identidad. Por ejemplo, si $k = 3$, entonces $\omega(0) = 0$, $\omega(1) = 2$, $\omega(2) = 1$ y $\omega(3) = 3$. Por lo tanto, $\omega = (1 \quad 2)$ y note que esta es la misma permutación que aparece en el Ejemplo 2.2.4.

En el siguiente resultado, $\widetilde{\omega}$ denota a la permutación sobre $\mathbb{Z}_4^{2^{k-1}}$ inducida por ω, es decir,

$$\widetilde{\omega} : (a_0, \ldots, a_{2^{k-1}-1}) \mapsto \left(a_{\omega(0)}, \ldots, a_{\omega(2^{k-1}-1)}\right).$$

Teorema 2.2.6. *Para todo entero $k \geq 1$, las funciones $\varphi, \varphi^k : \mathbb{Z}_{2^{k+1}} \to \mathbb{Z}_4^{2^{k-1}}$ son tales que*

$$\varphi = \widetilde{\omega} \circ \varphi^k.$$

En particular, esto afirma que φ y φ^k son permutación-equivalentes.

Demostración. Si $k = 1$, entonces φ, φ^1 y ω son la función identidad sobre $\mathbb{Z}_4$. Si $k = 2$, entonces del Ejemplo 2.2.4 sabemos que φ y φ^2 son las mismas funciones. Dado que para $k = 2$ se ha definido ω como la permutación identidad, la proposición se tiene. Supongamos que $k \geq 3$ y sea h_i la i-ésima columna de $H(k-1)$, $1 \leq i \leq 2^{k-1}$. Entonces $h_i^t = (r_{k-2}(i), \ldots, r_1(i), r_0(i), 1)$, donde $i = r_0(i) + 2r_1(i) + \cdots + 2^{k-2}r_{k-2}(i)$ está escrito en su representación 2-ádica. De aquí

$$h_{\omega(i)}^t = (r_1(i), \ldots, r_{k-2}(i), r_0(i), 1).$$

Sea $\varphi(z) = (a_0, \ldots, a_{2^{k-1}-1})$ y $\varphi(z) = (b_0, \ldots, b_{2^{k-1}-1})$. Esto implica que

$$a_{i-1} = r_0(z) + \left[(r_1(i), \ldots, r_{k-2}(i), r_0(i), 1) \cdot h_i^t\right]$$

y

$$b_{i-1} = r_0(z) + \left[(r_{k-2}(i), \ldots, r_1(i), r_0(i), 1) \cdot h_i^t\right].$$

Observemos que si invertimos el orden de las primeras $k-1$ coordenadas del vector binario $(r_1(i), \ldots, r_{k-2}(i), r_0(i), 1)$, entonces tenemos que invertir el orden de las primeras $k-1$ coordenadas de h_i^t para que el producto escalar de estos vectores no se vea afectado. Pero invertir el

orden en las primeras $k-1$ coordenadas de h_i^t da lugar a $h_{\omega(i)}^t$. Por lo tanto,

$$\begin{aligned} a_{i-1} &= r_0(z) + 2\left[(r_1(i),\ldots,r_{k-2}(i),r_0(i),1)\cdot h_i^t\right] \\ &= r_0(z) + 2\left[(r_{k-2}(i),\ldots,r_1(i),r_0(i),1)\cdot h_{\omega(i)}^t\right] \\ &= b_{\omega(i-1)}. \end{aligned}$$

Esto demuestra que $\varphi(z) = \widetilde{\omega}(\varphi^k(z))$, para todo $z \in \mathbb{Z}_{2^{k+1}}$. □

Una de las principales implicaciones que tiene el Teorema 2.2.6 y, quizás, una de las propiedades más interesantes de la función φ es la siguiente.

Corolario 2.2.7. *Para todo entero $k \geq 1$, la función $\varphi : (\mathbb{Z}_{2^{k+1}}, \delta_h) \to (\mathbb{Z}_4^{2^{k-1}}, \delta_L)$ es una isometría, donde δ_h y δ_H son la distancia homogénea y la distancia de Lee, respectivamente.*

Demostración. En la Proposición 2.4 de [51] (y también la sección 2.4 de [52]) se demuestra que la función $\varphi^k : (\mathbb{Z}_{2^{k+1}}, \delta_h) \to (\mathbb{Z}_4^{2^{k-1}}, \delta_L)$ es una isometría. Ya que por el Teorema 2.2.6, la función φ es permutación equivalente a la función φ^k, el resultado se sigue. □

Observación. El concepto de isometría es condierado como aquella función entre dos *espacios métricos* que preserva las distancias. Formalmente, si X, Y son dos conjuntos no vacíos y $d_1 : X \times X \to \mathbb{N} \cup \{0\}$, $d_2 : Y \times Y \to \mathbb{N} \cup \{0\}$ son métricas[3], entonces una isometría entre X y Y es una función $I : X \to Y$ tal que para todo par $(x_1, x_2) \in X \times X$, se tiene que $d_1(x_1, x_2) = d_2(I(x_1), I(x_2))$.

Finalmente, debemos mencionar que la permutación ω definida en la relación (2.14) es análoga a la permutación que relaciona a un polinomio con su polinomio recíproco. La importancia de esta permutación radica en el estudio de los códigos cíclicos lineales sobre campos finitos ([27, 38, 45]). Para ser más precisos, sea $\mathbb{F}$ un campo finito de característica $p \geq 2$ y $n \geq 1$ un entero primo relativo a p. Mediante la identificación polinomial de los vectores de $\mathbb{F}^n$ con polinomios en el anillo $R_n = \mathbb{F}[x]/\langle x^n - 1\rangle$, los códigos cíclicos lineales de longitud n sobre $\mathbb{F}$ corresponden a ideales en el anillo R_n. Ya que $\mathbb{F}[x]$ es un dominio de ideales principales, el anillo R_n también lo es. Por lo tanto, un código cíclico $\mathscr{C}$, visto como un ideal en el anillo R_n, tiene un polinomio generador $g(x) + \langle x^n - 1\rangle$. Como $\mathscr{C}^\perp$, el código dual de $\mathscr{C}$, es también un código cíclico lineal, existe un polinomio $f(x) + \langle x^n - 1\rangle$ que lo genera (como ideal de R_n). Si $g(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$, entonces ([27, Teorema 4.2.7]) los coeficientes de $f(x)$ son los mismos que los de $g(x)$ pero escritos en orden inverso. Esto es, $f(x) = a_{n-1} + a_{n-2}x + \cdots + a_0 x^{n-1}$. Al polinomio $f(x)$ se le llama *el polinomio recíproco de* $g(x)$. La analogía de la permutación ω con la aplicación que calcula el polinomio recíproco de $g(x)$ es ahora clara.

[3]Esto hace que (X, d_1) y (Y, d_2) sean espacios métricos.

2.2.2. Definición de la isometría φ sobre $\mathbb{Z}_{2^{k+1}}^n$

Con el fin de relacionar códigos de longitud n sobre $\mathbb{Z}_{2^{k+1}}$ con códigos de longitud $2^{k-1}n$ sobre $\mathbb{Z}_4$, el dominio de la isometría φ es extendido al conjunto $\mathbb{Z}_{2^{k+1}}^n$. Una forma sencilla y natural de hacer esto es coordenada a coordenada, es decir, para cualesquiera enteros $n,k \geq 1$ y cualquier $Z = (z_0, \ldots, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$, se define $\varphi'(Z)$ como

$$\varphi'(Z) = (\varphi(z_0)|\cdots|\varphi(z_{n-1})) \in \mathbb{Z}_4^{2^{k-1}n}. \tag{2.15}$$

Como veremos más adelante, en la Proposición 2.2.10, una ventaja de esta definición es que permite demostrar de manera fácil que la función φ' es una isometría. Sin embargo, si queremos relacionar de manera natural a la función de Gray Φ con la definición que se pretende dar de φ sobre $\mathbb{Z}_{2^{k+1}}^n$, la función φ' no es la más adecuada (esto será ilustrado en el ejemplo 2.2.8). Por tal motivo, introducimos la siguiente alternativa para extender la definición de φ al conjunto $\mathbb{Z}_{2^{k+1}}^n$.

Sean $k,n \geq 1$ enteros arbitrarios. Para todo $Z \in \mathbb{Z}_{2^{k+1}}^n$ definimos la función $\varphi : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}_4^{2^{k-1}n}$ como

$$\varphi(Z) = c_{k-1}^{k-1} \otimes r_0(Z) + 2\left[\left(c_0^{k-1} \otimes r_1(Z)\right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes r_k(Z)\right)\right]. \tag{2.16}$$

Note que si $n = 1$, entonces la relación (2.16) se reduce a la definición de φ sobre $\mathbb{Z}_{2^{k+1}}$, y si $k = 1$, entonces φ es la función identidad sobre $\mathbb{Z}_4^n$. Asimismo, note que esta forma de extender a φ nos da la ventaja de conocer inmediatamente cuál es la representación 2-ádica del vector $\varphi(Z)$ pues, dado que los vectores $c_{k-1}^{k-1} \otimes r_0(Z)$ y $\left(c_0^{k-1} \otimes r_1(Z)\right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes r_k(Z)\right)$ son elementos de $\mathbb{F}_2^{2^{k-1}n}$, el vector $\varphi(Z)$ está escrito de tal forma que

$$r_0(\varphi(Z)) = c_{k-1}^{k-1} \otimes r_0(Z), \quad r_1(\varphi(Z)) = \left(c_0^{k-1} \otimes r_1(Z)\right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes r_k(Z)\right),$$

es decir, la definición de $\varphi(Z)$ está dada en términos de su representación 2-ádica. De igual modo, note que dos claras desventajas de la definición de φ son que no es evidente si esta función es una isometría, y tampoco es obvio si φ' y φ son permutación-equivalentes. Por lo tanto, en lo que sigue tendremos en mente ambas definiciones y aprovecharemos las bondades de cada una de ellas.

Antes de dar a conocer los principales resultados de este apartado, veamos un ejemplo que ilustre las definiciones de estas funciones.

Ejemplo 2.2.8. Sean $k = n = 2$ y sea $Z = (z_0, z_1) \in \mathbb{Z}_{2^3}^2$. Ya que $c_0^1 = u$ y $c_1^1 = v$, tenemos que

$$\varphi(Z) = v \otimes r_0(Z) + 2\left[(u \otimes r_1(Z)) \oplus (v \otimes r_2(Z))\right].$$

De forma desarrollada, la expresión anterior es igual a la siguiente

$$\varphi(Z) = (r_0(z_0) + 2r_2(z_0), r_0(z_1) + 2r_2(z_1), \\ r_0(z_0) + 2(r_1(z_0) \oplus r_2(z_0)), r_0(z_1) + 2(r_1(z_1) \oplus r_2(z_1))).$$

Ahora, del Ejemplo 2.2.1 vemos que

$$\varphi'(Z) = (r_0(z_0)+2r_2(z_0), r_0(z_0)+2(r_1(z_0)\oplus r_2(z_0)), \\ r_0(z_1)+2r_2(z_1), r_0(z_1)+2(r_1(z_1)\oplus r_2(z_1))).$$

Por lo tanto, note que $\varphi(Z)$ difiere de $\varphi'(Z)$. Sin embargo, si consideramos la permutación $\tau = (1 \quad 2)$, entonces $\varphi'(Z) = \widetilde{\tau}(\varphi(Z))$, donde $\widetilde{\tau}$ es la permutación sobre $\mathbb{Z}_4^4$ inducida por τ. En particular, esto quiere decir que φ y φ' son permutación-equivalentes. Por otro lado, sea ϕ la isometría de Gray definida sobre $\mathbb{Z}_4^4$. Entonces al aplicar ϕ a $\varphi(Z)$ obtenemos que

$$\begin{aligned}(\phi\circ\varphi)(Z) &= [u\otimes(v\otimes r_0(Z))]\oplus[v\otimes((u\otimes r_1(Z))\oplus(v\otimes r_2(Z)))] \\ &= ((0,0,1,1)\otimes r_0(Z))\oplus((0,0,1,1)\otimes r_1(Z))\oplus((1,1,1,1)\otimes r_2(Z)),\end{aligned}$$

de donde notamos que $\Phi(Z) = (\phi\circ\varphi)(Z) \neq (\phi\circ\varphi')(Z)$ lo cual, de acuerdo al Ejemplo 2.1.8, coincide con $\Phi(Z)$. En contraste, al aplicar ϕ a $\varphi'(z)$ obtenemos

$$(\phi\circ\varphi')(Z) = (r_2(z_0), r_1(z_0)\oplus r_2(z_0), r_2(z_1), r_1(z_1)\oplus r_2(z_1)), \\ r_0(z_0)\oplus r_2(z_0), r_0(z_0)\oplus r_1(z_0)\oplus r_2(z_0), r_0(z_1)\oplus r_2(z_1), r_0(z_1)\oplus r_1(z_1)\oplus r_2(z_1)))$$

lo cual no deriva en una relación directa con $\Phi(Z)$. Por lo tanto, la función φ tiene la ventaja que $(\phi\circ\varphi)(Z) = \Phi(Z)$. Esta es la relación natural que mencionamos anteriormente.

En el Ejemplo 2.2.8 quedaron en claro dos situaciones particulares. Primero, las funciones φ y φ' son equivalentes y segundo, existe una conección natural entre las isometrías de Gray Φ, ϕ y la función φ. Estos dos temas son los que a continuación desarrollaremos para el caso general.

Sean $k \geq 0$, $n \geq 1$ enteros y recuerde que sobre el conjunto $I_{2^k n}$ se ha definido la permutación τ de la siguiente manera: para todo $e \in I_{2^k n}$ escrito (con el algoritmo de la división en los enteros) de la forma $e = in + j$, $0 \leq j \leq n-1$, se define $\tau(e) = j2^k + i$.

La demostración del siguiente resultado es similar a la del Teorema 2.1.13 y, por lo tanto, la omitimos.

Proposición 2.2.9. *Sean $n, k \geq 1$ enteros. Entonces las funciones $\varphi', \varphi : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}_4^{2^{k-1}n}$ son permutación-equivalentes. De manera más específica,*

$$\varphi'(Z) = (\widetilde{\tau}\circ\varphi)(Z), \qquad \forall Z \in \mathbb{Z}_{2^{k+1}}^n$$

donde τ es la permutación sobre $I_{2^{k-1}n}$ definida como $\tau(e) = j2^{k-1} + i$, $e = in + j$, $0 \leq j \leq n-1$.

En vista de la Proposición 2.2.9, basta probar que una de las funciones φ o φ' es una isometría para que la otra lo sea. Para este punto usaremos la definición de φ'. Una demostración directa de que φ es una isometría se presenta en el Apéndice B.

Proposición 2.2.10. *La función* $\varphi' : \left(\mathbb{Z}_{2^{k+1}}^n, \delta_h\right) \to \left(\mathbb{Z}_4^{2^{k-1}n}, \delta_L\right)$ *dada en* (2.15) *es una isometría.*

Demostración. Sean $Y = (y_0, \ldots, y_{n-1})$ y $Z = (z_0, \ldots, z_{n-1})$ dos elementos de $\mathbb{Z}_{2^{k+1}}^n$. Supongamos que $\varphi'(Y) = (a_0, \ldots, a_{2^{k-1}n-1})$ y $\varphi'(Z) = (b_0, \ldots, b_{2^{k-1}n-1})$. Entonces, por definición,

$$\delta_L(\varphi'(Y), \varphi'(Z)) = \sum_{i=0}^{m} \delta_L(a_i, b_i), \qquad m = 2^{k-1}n - 1. \tag{2.17}$$

Note ahora que las primeras 2^{k-1} coordenadas de $\varphi'(Y)$ y $\varphi'(Z)$ son precisamente las coordenadas de $\varphi(a_0)$ y $\varphi(b_0)$ respectivamente; las segundas 2^{k-1} coordenadas de $\varphi'(Y)$ y $\varphi'(Z)$ son las coordenadas de $\varphi(a_1)$ y $\varphi(b_1)$ respectivamente. Continuando de esta manera, vemos que el lado derecho de (2.17) puede ser expresado como

$$\sum_{i=0}^{m} \delta_L(a_i, b_i) = \sum_{i=0}^{n-1} \delta_L(\varphi(y_i), \varphi(z_i)).$$

Dado que φ es una isometría, se tiene que $\delta_L(\varphi(y_i), \varphi(z_i)) = \delta_h(y_i, z_i)$, de donde el resultado se sigue. □

Corolario 2.2.11. *La función* $\varphi : \left(\mathbb{Z}_{2^{k+1}}^n, \delta_h\right) \to \left(\mathbb{Z}_4^{2^{k-1}n}, \delta_L\right)$ *es una isometría.*

El siguiente punto a tratar en esta sección corresponde a la relación entre la isometría φ y la función de Gray Φ que se observó en los Ejemplos 2.2.1, 2.2.2 y 2.2.8. En éstos se dieron indicios de que la igualdad $\Phi = \phi \circ \varphi$ es cierta. De manera general, se tiene el siguiente resultado.

Proposición 2.2.12. *Con la notación anterior, se tiene que* $\Phi = \phi \circ \varphi$.

Demostración. Para todo $n, k \geq 1$ y $Z \in \mathbb{Z}_{2^{k+1}}^n$, se tiene que[4]

$$(\phi \circ \varphi)(Z) = v \otimes \left[\left(c_0^{k-1} \otimes r_1(Z)\right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes r_k(Z)\right)\right] \oplus \left(u \otimes \left(c_{k-1}^{k-1} \otimes r_0(Z)\right)\right).$$

Pero $v \otimes c_i^{k-1} = c_{i+1}^k$ para todo $0 \leq i \leq k-1$, y $u \otimes c_{k-1}^{k-1} = c_0^k$. Así, por las propiedades de linealidad, asociatividad y distributividad del producto de Kronecker, obtenemos

$$(\phi \circ \varphi)(Z) = \left(c_1^k \otimes r_1(Z)\right) \oplus \cdots \oplus \left(c_k^k \otimes r_k(Z)\right) \oplus \left(c_0^k \otimes r_0(Z)\right) = \Phi(Z),$$

lo que demuestra el resultado. □

[4]Observe que en este momento se está haciendo uso del conocimiento de la representación 2-ádica de $\varphi(Z)$.

En [23] se demostró que la función de Gray $\phi : (\mathbb{Z}_4^n, \delta_L) \to (\mathbb{F}_2^{2n}, \delta_H)$ es una isometría. Como consecuencia de este hecho y de la Proposición 2.2.12 se deriva una de las propiedades más importantes de la función de Gray Φ.

Teorema 2.2.13. *La función de Gray* $\Phi : \left(\mathbb{Z}_{2^{k+1}}^n, \delta_h\right) \to \left(\mathbb{F}_2^{2^k n}, \delta_H\right)$ *es una isometría.*

Demostración. Sean $Y, Z \in \mathbb{Z}_{2^{k+1}}^n$. Ya que $\Phi = \phi \circ \varphi$ y la función de Gray ϕ es una isometría, se tiene que $\delta_H(\Phi(Y), \Phi(Z)) = \delta_L(\varphi(Y), \varphi(Z))$. Asimismo, por el Corolario 2.2.11 φ es una isometría y, por lo tanto, $\delta_L(\varphi(Y), \varphi(Z)) = \delta_h(Y, Z)$. En consecuencia, $\delta_H(\Phi(Y), \Phi(Z)) = \delta_h(Y, Z)$. □

Dado que la función de Gray Φ sobre $\mathbb{Z}_{2^{k+1}}^n$ es inyectiva y $\phi \circ \varphi = \Phi$, la isometría de φ es también inyectiva. Enunciamos esto formalmente en el siguiente

Corolario 2.2.14. *La isometría* $\varphi : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}_4^{2^{k-1}n}$ *es inyectiva.*

Hasta este punto se han presentado los resultados más importantes de esta sección. Sin embargo, con el fin de englobar a todas las definiciones de las isometrías que se han presentado a lo largo de este capítulo, en lo siguiente analizaremos la definición de la función φ^k (introducida en [51, 52]) sobre el módulo $\mathbb{Z}_{2^{k+1}}^n$ y demostraremos que ésta es permutación-equivalente a la isometría φ sobre el $\mathbb{Z}_{2^{k+1}}$-módulo $\mathbb{Z}_{2^{k+1}}^n$.

Recuerde que en el Teorema 2.2.6 de la sección 2.2.1 se demostró que las funciones φ y φ^k están relaciondas por la identidad $\varphi = \widetilde{\omega} \circ \varphi^k$, donde $\widetilde{\omega}$ es la permutación sobre $\mathbb{Z}_4^{2^{k-1}}$ inducida por la permutación ω dada en (2.14).

En [51, 52] la función φ^k es definida sobre $\mathbb{Z}_{2^{k+1}}^n$ extendiendo cada una de las funciones φ_i^k a $\mathbb{Z}_{2^{k+1}}^n$ coordenada a coordenada. Esto es, para todo $Z = (z_0, \ldots, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$

$$\varphi_i^k : Z \mapsto (\varphi_i^k(z_0), \ldots, \varphi_i^k(z_{n-1})).$$

Por ejemplo, si $Z = (z_0, z_1) \in \mathbb{Z}_{16}^2$, entonces $\varphi_i^3(Z) = (b_{2i}, b_{2i+1})$, donde $0 \leq i \leq 3$ y

$$\begin{aligned}
b_0 &= r_0(z_0) + 2r_3(z_0),\\
b_1 &= r_0(z_1) + 2r_3(z_1),\\
b_2 &= r_0(z_0) + 2(r_1(z_0) \oplus r_3(z_0)),\\
b_3 &= r_0(z_1) + 2(r_1(z_1) \oplus r_3(z_1)),\\
b_4 &= r_0(z_0) + 2(r_2(z_0) \oplus r_3(z_0)),\\
b_5 &= r_0(z_1) + 2(r_2(z_1) \oplus r_3(z_1)),\\
b_6 &= r_0(z_0) + 2(r_1(z_0) \oplus r_2(z_0) \oplus r_3(z_0)),\\
b_7 &= r_0(z_1) + 2(r_1(z_0) \oplus r_2(z_1) \oplus r_3(z_0)).
\end{aligned}$$

De este modo, $\varphi^3(Z) = (b_0, b_1, \ldots, b_7)$. Por otra parte, si $\varphi(Z) = (a_0, a_1, \ldots, a_7)$, entonces la definición de φ implica que

$$\begin{aligned}
a_0 &= r_0(z_0) + 2r_3(z_0),\\
a_1 &= r_0(z_1) + 2r_3(z_1),\\
a_2 &= r_0(z_0) + 2(r_2(z_0) \oplus r_3(z_0)),\\
a_3 &= r_0(z_1) + 2(r_2(z_1) \oplus r_3(z_1)),\\
a_4 &= r_0(z_0) + 2(r_1(z_0) \oplus r_3(z_0)),\\
a_5 &= r_0(z_1) + 2(r_1(z_1) \oplus r_3(z_1)),\\
a_6 &= r_0(z_0) + 2(r_1(z_0) \oplus r_2(z_0) \oplus r_3(z_1)),\\
a_7 &= r_0(z_1) + 2(r_1(z_1) \oplus r_2(z_1) \oplus r_3(z_1)).
\end{aligned}$$

Comparando las coordenadas de $\varphi^3(Z)$ con las coordenadas de $\varphi(Z)$, vemos que la única diferencia es una permutación que actúa sobre sus subíndices. Con el propósito de dar a conocer cuál es esta permutación, introducimos la siguiente definición.

Sea $Z = \left(Z_0|Z_1|\cdots|Z_{2^{k-1}-1}\right) \in \mathbb{Z}_4^{2^{k-1}n}$, donde $Z_i \in \mathbb{Z}_4^n$, $0 \le i \le 2^{k-1}-1$. Entonces la permutación $\widetilde{\omega}$ sobre $\mathbb{Z}_4^{2^{k-1}}$ inducida por la permutación ω definida en (2.14) es extendida coordenada a coordenada a una permutación, denotada también por $\widetilde{\omega}$, sobre $\mathbb{Z}_4^{2^{k-1}n}$ de la siguiente manera:

$$\widetilde{\omega} : Z \mapsto \left(Z_{\omega(0)}|Z_{\omega(1)}|\cdots|Z_{\omega(2^{k-1}-1)}\right). \tag{2.18}$$

Por ejemplo, si $k = 3$, $n = 2$ y $Z = (B_0|B_1|B_2|B_3) \in \mathbb{Z}_4^8$, donde $B_i = ((b_{2i}, b_{2i+1})$, $0 \le i \le 3$, entonces

$$\begin{aligned}
\widetilde{\omega}(Z) &= \left(B_{\omega(0)}|B_{\omega(1)}|B_{\omega(2)}|B_{\omega(3)}\right)\\
&= (B_0|B_2|B_1|B_3)\\
&= (b_0, b_1, b_4, b_5, b_2, b_3, b_6, b_7).
\end{aligned}$$

De esta última expresión, notamos que para las funciones φ y φ' definidas sobre $\mathbb{Z}_{16}^2$, se tiene $\varphi(Z) = \widetilde{\omega}(\varphi^3(Z))$.

Lo anterior es un caso particular de la siguiente:

Proposición 2.2.15. *Sean $n, k \ge 1$ enteros. Entonces las funciones φ y φ^k definidas sobre $\mathbb{Z}_{2^{k+1}}^n$ son permutación-equivalentes. De hecho, $\varphi = \widetilde{\omega} \circ \varphi^k$, donde $\widetilde{\omega}$ es la permutación definida en* (2.18)*.*

Demostración. Sea $k \ge 1$ y supongamos que los vectores $c_0^{k-1}, \ldots, c_{k-1}^{k-1} \in \mathbb{F}_2^{2^{k-1}}$ tienen coordenadas $c_i^{k-1} = (\varepsilon_{i,0}, \ldots, \varepsilon_{i,2^{k-1}-1})$, $0 \le i \le k-1$. Note que con esta notación, la función φ queda

expresada como

$$\varphi(z) = r_0(z)c_{k-1}^{k-1} + 2\left(\bigoplus_{i=0}^{k-1}\varepsilon_{i,0}r_{i+1}(z), \ldots, \bigoplus_{i=0}^{k-1}\varepsilon_{i,2^{k-1}-1}r_{i+1}(z)\right), \quad \forall z \in \mathbb{Z}_{2^{k+1}}$$

Esto es, si $\varphi(z) = (a_0, \ldots, a_{2^{k-1}-1})$, entonces

$$a_j = r_0(z) + 2\bigoplus_{i=0}^{k-1}\varepsilon_{i,j}r_{i+1}(z).$$

Por otro lado, recordemos que por definición

$$\varphi^k(z) = \left(\varphi_0^k(z), \ldots, \varphi_{2^{k-1}-1}^k(z)\right), \quad \varphi_j^k(z) \in \mathbb{Z}_4,\ 0 \leq j \leq 2^{k-1}-1.$$

Ya que por el Teorema 2.2.6 se tiene que $\varphi = \widetilde{\omega} \circ \varphi^k$, inferimos que para todo $0 \leq j \leq 2^{k-1}-1$, lo siguiente es cierto:

$$a_j = \varphi_{\omega(j)}^k(z).$$

Supongamos ahora que $Z \in \mathbb{Z}_{2^{k+1}}^n$. Entonces, por la definición de φ sobre $\mathbb{Z}_{2^{k+1}}^n$, se obtiene que

$$\varphi(Z) = r_0(Z)c_{k-1}^{k-1} + 2\left(\bigoplus_{i=0}^{k-1}\varepsilon_{i,0}r_{i+1}(Z), \ldots, \bigoplus_{i=0}^{k-1}\varepsilon_{i,2^{k-1}-1}r_{i+1}(Z)\right),$$

es decir, si $\varphi(Z) = (A_0|\cdots|A_{2^{k-1}-1})$, $A_j \in \mathbb{Z}_4^n$, entonces

$$A_j = r_0(Z) + 2\left(\bigoplus_{i=0}^{k-1}\varepsilon_{i,j}r_{i+1}(Z)\right), \quad \forall\ 0 \leq j \leq 2^{k-1}-1.$$

Como las funciones φ_i^k han sido extendidas coordenada a coordenada, se sigue que

$$A_j = \varphi_{\omega(j)}^k(Z), \quad 0 \leq j \leq 2^{k-1}-1,$$

lo cual demuestra que $\varphi(Z) = (\widetilde{\omega} \circ \varphi^k)(Z)$. □

En [51, 52], la isometría φ^k es usada, entre otras cosas, para dar dos definiciones de la isometría de Gray. En específico, en [51] se define una isometría de Gray como

$$G_1 = \phi \circ \varphi^k,$$

y en [52], la isometría de Gray sobre $\mathbb{Z}_4^n$ es compuesta con las funciones φ_i^k, es decir,

$$G_2 = \left(\phi \circ \varphi_0^k, \ldots, \phi \circ \varphi_{2^{k-1}-1}^k\right).$$

Es claro que ambas funciones de Gray son permutación-equivalentes y por lo tanto, basta demostrar que alguna de ellas es permutación-equivalente a Φ para que ambas lo sean.

Proposición 2.2.16. *Para cualesquiera enteros $n,k \geq 1$, las isometrías Φ y G_1 sobre $\mathbb{Z}_{2^{k+1}}^n$ satisfacen la relación*

$$\Phi = \widetilde{\omega}^{\otimes 2} \circ G_1.$$

Demostración. Sea $Z \in \mathbb{Z}_{2^{k+1}}^n$, entonces por la Proposición 2.2.15, $\varphi(Z) = (\widetilde{\omega} \circ \varphi^k)(Z)$, lo cual implica que $\Phi(Z) = \phi(\widetilde{\omega}(\varphi^k(Z)))$ pues $\Phi = \phi \circ \varphi$ (Proposición 2.2.12). Como

$$r_i\left((\widetilde{\omega} \circ \varphi^k)(Z)\right) = \widetilde{\omega}\left(r_i(\varphi^k(Z))\right), \quad 0 \leq i \leq 1,$$

se sigue de la definición de la isometría ϕ que

$$\begin{aligned}\phi\left(\widetilde{\omega}(\varphi^k(Z))\right) &= \left(\widetilde{\omega}\left(r_1(\varphi^k(Z))\right) \mid \widetilde{\omega}\left(r_0(\varphi^k(Z))\right) \oplus \widetilde{\omega}\left(r_1(\varphi^k(Z))\right)\right) \\ &= \left(\widetilde{\omega}\left(r_1(\varphi^k(Z))\right) \mid \widetilde{\omega}\left(r_0(\varphi^k(Z)) \oplus r_1(\varphi^k(Z))\right)\right).\end{aligned}$$

Sea $\widetilde{\omega}^{\otimes 2}$ la permutación sobre $\mathbb{F}_2^{2^k n}$ definida como $(A,B) \mapsto (\widetilde{\omega}(A)|\widetilde{\omega}(B))$, donde $A,B \in \mathbb{F}_2^{2^{k-1}n}$. Entonces de las relaciones anteriores se sigue que $\phi\left(\widetilde{\omega}(\varphi^k(Z))\right) = \widetilde{\omega}^{\otimes 2}((\phi \circ \varphi^k)(Z))$, lo cual se quería demostrar. □

2.3. Algunas propiedades de las isometrías φ y de Gray

Nuestro propósito en esta sección es establecer algunas propiedades de la isometría φ y, en consecuencia, de la isometría Φ de Gray. Algunas de ellas han sido reportadas en la literatura [51, 52] pero otras no. Tales son los casos del Teorema 2.3.5, el Corolario 2.3.6, el Teorema 2.3.7 y el Corolario 2.3.8.

Iniciamos recordando que para todos los enteros $n,k \geq 1$ y todo $Z \in \mathbb{Z}_{2^{k+1}}^n$, la definición de la isometría $\varphi(Z)$, dada en (2.16), está expresada en su representación 2-ádica. De este modo, aplicando la función ϕ de Gray a $\varphi(Z)$, en virtud de la Proposición 2.2.12, podemos calcular fácilmente $\Phi(Z) = (\phi \circ \varphi)(Z)$. Sin embargo, si no conocemos la representación 2-ádica de $\varphi(Z)$, no podemos calcular directamente al vector $\Phi(Z)$ y, por la misma razón, nos vemos en la necesidad de conocer previamente algunas propiedades de la función ϕ. Con este objetivo en mente, primero estudiaremos una alternativa para expresar la suma de vectores en $\mathbb{Z}_{2^{k+1}}^n$ y recordaremos algunas de las propiedades elementales de ϕ.

2.3.1. Alternativa para la suma en $\mathbb{Z}_{2^{k+1}}^n$

Siguiendo las ideas de [51, 52], nos permitimos introducir las siguientes dos operaciones sobre $\mathbb{Z}_{2^{k+1}}$. Sea $k \geq 1$ un entero y sean $y,z \in \mathbb{Z}_{2^{k+1}}$. Usando las representaciones 2-ádicas de y

y z definimos las operaciones "$\oplus$" y "$\odot$" sobre $\mathbb{Z}_{2^{k+1}}$ como

$$y \oplus z = \sum_{i=0}^{k} (r_i(y) \oplus r_i(z)) 2^i, \qquad y \odot z = \sum_{i=0}^{k} (r_i(y) r_i(z)) 2^i, \tag{2.19}$$

donde acordamos que la operación "$\oplus$" del lado derecho de la definición de $y \oplus z$ será considerada como la suma sobre $\mathbb{F}_2$. En efecto, observemos que si permitimos $k = 0$ en la definición anterior, entonces la operación "$\oplus$" coincide con la suma sobre $\mathbb{F}_2$ y, por lo tanto, esta suma puede ser considerada como una generalización de la suma sobre el campo binario. Esto justifica el abuso de notación.

Note que ambas operaciones dan como resultado un elemento que está escrito en su representación 2-ádica, es decir, para todo $y, z \in \mathbb{Z}_{2^{k+1}}$ y entero i tal que $0 \leq i \leq k$,

$$\begin{aligned} r_i(y \oplus z) &= r_i(y) \oplus r_i(z) \in \mathbb{F}_2, \\ r_i(y \odot z) &= r_i(y) r_i(z) \in \mathbb{F}_2, \end{aligned}$$

y, por lo tanto, el conjunto $\mathbb{Z}_{2^{k+1}}$ es cerrado con respecto a $\oplus$ y $\odot$. Además, note que como la suma y el producto definidos en $\mathbb{F}_2$ son conmutativos y asociativos, las operaciones definidas en (2.19) son también conmutativas y asociativas. Asimismo, note que para todo $z \in \mathbb{Z}_{2^{k+1}}$ se tienen las siguientes relaciones

$$0 \oplus z = z, \quad (2^{k+1} - 1) \odot z = z, \quad z \oplus z = 0.$$

Y también notemos que no para todo $z \in \mathbb{Z}_{2^{k+1}}$ existe $y \in \mathbb{Z}_{2^{k+1}}$ tal que $z \odot y = 2^{k+1} - 1$. Por lo tanto, $(\mathbb{Z}_{2^{k+1}}, \oplus)$ es un grupo abeliano y $(\mathbb{Z}_{2^{k+1}}, \odot)$ es un monoide.

Análogamente a la Proposición 2.1 de [51], una alternativa para encontrar el valor de $y + z$ es vía la siguiente:

Proposición 2.3.1. *Sea $k \geq 1$ un entero y sean $y, z \in \mathbb{Z}_{2^{k+1}}$. Entonces*

$$y + z = (y \oplus z) + 2(y \odot z).$$

Demostración. La prueba se sigue por inducción sobre k. Sean $y, z \in \mathbb{Z}_4$, entonces

$$y + z = [r_0(y) + 2r_1(y)] + [r_0(z) + 2r_1(z)] = [r_0(y) + r_0(z)] + 2[r_1(y) + r_1(z)]. \tag{2.20}$$

Teniendo en cuenta que para todo $x \in \mathbb{Z}_4$, la componente $r_i(x) \in \{0, 1\} \subset \mathbb{Z}_4$, se tienen las siguientes relaciones:

$$r_0(y) + r_0(z) = [r_0(y) \oplus r_0(z)] + 2r_0(y) r_0(z), \qquad 2[r_1(y) + r_1(z)] = 2[r_1(y) \oplus r_1(z)].$$

Sustituyendo estas expresiones en la identidad (2.20), se tiene que $y+z = y \oplus z + 2(y \odot z)$ y, por lo tanto, la Proposición 2.3.1 es cierta para $k = 1$. Ahora, supongamos que dicha Proposición es válida para algún $k \geq 1$, y sean $y, z \in \mathbb{Z}_{2^{k+2}}$. Por hipótesis de inducción tenemos que

$$y - r_0(y) + z - r_0(z) = 2 \sum_{i=1}^{k+1} \left[(r_i(y) \oplus r_i(z)) + 2(r_i(y) r_i(z)) \right] 2^{i-1},$$

la cual puede ser escrita como

$$y + z = r_0(y) + r_0(z) + \sum_{i=1}^{k+1} \left[(r_i(y) \oplus r_i(z)) + 2(r_i(y) r_i(z)) \right] 2^i.$$

Ya que

$$r_0(y) + r_0(z) = (r_0(y) \oplus r_0(z)) + 2(r_0(y) r_0(z)),$$

la prueba se sigue. □

Continuando con las ideas de los trabajos [54, 55], para cualquier entero $n \geq 1$, definamos la operación binaria "$*$" sobre $\mathbb{F}_2^n$ de la siguiente manera: si $X = (x_0, \ldots, x_{n-1})$, $Y = (y_0, \ldots, y_{n-1})$ son dos elementos de $\mathbb{F}_2^n$, entonces

$$X * Y = (x_0 y_0, \ldots, x_{n-1} y_{n-1}).$$

Con la introducción de la operación[5] "$*$" extendemos de manera natural la definición de las operaciones "$\oplus$" y "$\odot$" al conjunto $\mathbb{Z}_{2^{k+1}}^n$:

$$Y \oplus Z = \sum_{i=0}^{k} (r_i(Y) \oplus r_i(Z)) 2^i, \qquad Y \odot Z = \sum_{i=0}^{k} (r_i(Y) * r_i(Z)) 2^i, \tag{2.21}$$

donde, de igual manera que para $n = 1$, estamos considerando que la operación "$\oplus$" del lado derecho de la definición de $Y \oplus Z$ es la suma sobre $\mathbb{F}_2^n$.

Vale la pena aclarar que en ambas definiciones estamos haciendo un juego entre elementos del conjunto $\{0,1\}^n \subseteq \mathbb{Z}_{2^{k+1}}^n$ y elementos del espacio $\mathbb{F}_2^n$. Es decir, para que la suma "$\oplus$" y el producto "$*$" del lado derecho de cada relación de (2.21) estén bien definidos, consideramos que $r_i(Y), r_i(Z) \in \mathbb{F}_2^n$ y, por lo tanto, $r_i(Y) \oplus r_i(Z)$ y $r_i(Y) * r_i(Z)$ están en $\mathbb{F}_2^n$. Pero al mismo tiempo, para que tenga sentido la multiplicación de $r_i(Y) \oplus r_i(Z)$ y $r_i(Y) * r_i(Z)$ por 2^i, es necesario ver a los vectores $r_i(Y) \oplus r_i(Z)$ y $r_i(Y) * r_i(Z)$ como elementos del conjunto $\{0,1\}^n \subseteq \mathbb{Z}_{2^{k+1}}^n$.

La úlima interpretación nos permite llevar la Proposición 2.3.1 al caso $n \geq 1$.

[5] Claramente esta operación es asociativa, conmutativa y el conjunto $\mathbb{F}_2^n$ es cerrado con respecto a "$*$". Más aún, el elemento $(1)_n \in \mathbb{F}_2^n$ tiene la propiedad de que $(1)_n * X = X$ para todo $X \in \mathbb{F}_2^n$. Por lo tanto, $(\mathbb{F}_2^n, *)$ es un monoide.

Proposición 2.3.2. *Sean $k,n \geq 1$ enteros y sean $Y,Z \in \mathbb{Z}_{2^{k+1}}^n$. Entonces*

$$Y+Z = (Y \oplus Z) + 2(Y \odot Z).$$

Demostración. Sean $Y = (y_0,\ldots,y_{n-1}), Z = (z_0,\ldots,z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$. Tomando en cuenta que las funciones r_i han sido extendidas coordenada a coordenada, y apoyándonos en la estructura de $\mathbb{Z}_{2^{k+1}}^n$ como $\mathbb{Z}_{2^{k+1}}$-módulo, vemos que

$$Y \oplus Z = (y_0 \oplus z_0,\ldots,y_{n-1} \oplus z_{n-1}),$$

y

$$Y \odot Z = (y_0 \odot z_0,\ldots,y_{n-1} \odot z_{n-1}).$$

Por lo tanto, por la Proposición 2.3.1, $(Y \oplus Z) + 2(Y \odot Z) = Y + Z$. □

Con base en la Proposición anterior, establecemos el siguiente vínculo entre la suma módulo 4 y la suma módulo 2.

Corolario 2.3.3. *Para cualesquiera $A,B \in \{0,1\}^n \subseteq \mathbb{Z}_4^n$ y cualesquiera $y,z \in \mathbb{Z}_4$*

$$2(Ay+Bz) = 2(Ar_0(y) \oplus Br_0(z)),$$

donde la suma "$\oplus$" del lado derecho de la expresión anterior es la suma sobre $\mathbb{F}_2^n$.

Demostración. Por la Proposición 2.3.2

$$Ay+Bz = (Ay \oplus Bz) + 2(Ay \odot Bz).$$

Así, $2(Ay+Bz) = 2(Ay \oplus Bz)$. Por otro lado, por definición,

$$Ay \oplus Bz = [r_0(Ay) \oplus r_0(Bz)] + 2[r_1(Ay) \oplus r_2(Bz)].$$

De este modo, $2(Ay+2Bz) = 2(Ay \oplus Bz) = 2[r_0(Ay) \oplus r_0(Bz)]$. Para concluir la prueba basta notar que como $A,B \in \{0,1\}^n \subseteq \mathbb{Z}_4^n$, entonces $r_0(Ay) = Ar_0(y)$ y $r_0(Bz) = Br_0(z)$. □

2.3.2. Propiedades de la isometría de Gray sobre $\mathbb{Z}_4$

Las tres propiedades de la función ϕ que presentamos en esta breve sección pueden ser encontradas en [54, Proposición 3.2] y [23, Ecuación 30].

Recordemos que la función de Gray ϕ sobre $\mathbb{Z}_4^n$ está definida como

$$\phi(Z) = (u \otimes r_0(Z)) \oplus (v \otimes r_1(Z)) = (r_1(Z)|r_0(Z) \oplus r_1(z)) \in \mathbb{F}_2^{2n}.$$

Lema 2.3.4. *Sea $n \geq 1$ un entero y sean $Y, Z \in \mathbb{Z}_4^n$. Entonces*

1. $\phi(2Z) = v \otimes r_0(Z)$,
2. $\phi(Y + 2Z) = \phi(Y) \oplus \phi(2Z)$,
3. $\phi(Y + Z) = \phi(Y) \oplus \phi(Z) \oplus \phi(2r_0(Y) * r_0(Z)) = \phi(Y) \oplus \phi(Z) \oplus \phi(2(Y \odot Z))$.

Demostración. Es claro que para todo $Y, Z \in \mathbb{Z}_4^n$, se tiene

$$2Z = 2r_0(Z), \qquad Y + 2Z = r_0(Y) + 2(r_1(Y) \oplus r_0(Z)).$$

y, por la Proposición 2.3.2,

$$Y + Z = r_0(Y) \oplus r_0(Z) + 2(r_1(Y) \oplus r_1(Z) \oplus r_0(Y) * r_0(Z)).$$

Por lo que el lema se sigue al aplicar la definición de ϕ a las expresiones anteriores. □

2.3.3. Propiedades de la isometría φ

Sea $\gamma \in 1 + \langle 2^{k-1} \rangle = \{1, 1+2^{k-1}, 1+2^k, 1+2^{k-1}+2^k\}$. Con el propósito de analizar algunas propiedades de las imágenes bajo φ de códigos γ-cíclicos definidos sobre $\mathbb{Z}_{2^{k+1}}$, es conveniente encontrar expresiones para $\varphi(2^{k-1}X + 2^k Y + Z)$, donde $X, Y, Z \in \mathbb{Z}_{2^{k+1}}^n$ y $n \geq 1$ es un entero. El método que emplearemos para lograr esto es simple: aplicar la definición de φ a la representación 2-ádica de $2^{k-1}X + 2^k Y + Z$, la cual obtendremos como consecuencia de la Proposición 2.3.2 y de las representaciones 2-ádicas de $2^{k-1}X, 2^k Y$ y Z.

Sea $k \geq 1$ y sea s un entero tal que $0 \leq s \leq k$. En general, si $Z \in \mathbb{Z}_{2^{k+1}}$, la representación 2-ádica de $2^s Z$ es

$$2^s Z = 2^s r_0(Z) + 2^{s+1} r_1(Z) + \cdots + 2^k r_{k-s}(Z). \tag{2.22}$$

En particular, para todo $k \geq 1$ y todo $X, Y \in \mathbb{Z}_{2^{k+1}}^n$, de la relación (2.22) se derivan las siguientes relaciones:

$$2^{k-1}X = 2^{k-1} r_0(X) + 2^k r_1(X) \tag{2.23}$$

$$2^k Y = 2^k r_0(Y). \tag{2.24}$$

Por lo tanto, aplicando la definición de φ a (2.23) y (2.24), obtenemos

$$\varphi(2^{k-1}X) = 2\left[\left(c_{k-2}^{k-1} \otimes r_0(X)\right) \oplus \left(c_{k-1}^{k-1} \otimes r_1(X)\right)\right] \qquad \forall k \geq 2, \tag{2.25}$$

$$\varphi(2^k Y) = 2\, c_{k-1}^{k-1} \otimes r_0(Y) = 2\varphi(Y) \qquad \forall k \geq 1, \tag{2.26}$$

siendo la identidad (2.26) similar a la Proposición 3.1 de [51]. Esto no debe sorprendernos pues las isometrías φ y φ^k son equivalentes (Proposición 2.2.15).

Observe que, aunque (2.23) es válida para todo entero $k \geq 1$, en la ecuación (2.25) es necesaria la condición $k \geq 2$ pues $\varphi : \mathbb{Z}_4^n \to \mathbb{Z}_4^n$ es la función identidad para todo $n \geq 1$ y, de este modo, (2.25) sería falsa con $k = 1$.

Por otro lado, por la Proposición 2.3.2, para todo $k \geq 1$ y todo $Y, Z \in \mathbb{Z}_{2^{k+1}}^n$ se tiene

$$2^k Y + Z = \left(\sum_{i=0}^{k} (r_i(2^k Y) \oplus r_i(Z)) 2^i \right) + 2 \left(\sum_{i=0}^{k} (r_i(2^k Y) * r_i(Z)) 2^i \right).$$

Pero, por la relación (2.24), $r_k(2^k Y) = r_0(Y)$ y $r_i(2^k Y) = 0$ siempre que $0 \leq i \leq k-1$. Así, la expresión 2-ádica de $2^k Y + Z$ es

$$2^k Y + Z = r_0(Z) + \cdots + 2^{k-1} r_{k-1}(Z) + 2^k (r_0(Y) \oplus r_k(Z)) \quad \forall k \geq 1 \tag{2.27}$$

Repitiendo el mismo proceso, añadimos el término $2^{k-1}X$ a $2^k Y + Z$. De este modo, para todo $k \geq 1$ se tiene

$$\begin{aligned} 2^{k-1}X + 2^k Y + Z = r_0(Z) + \cdots + 2^{k-2} r_{k-2}(Z) + 2^{k-1}(r_{k-1}(Z) \oplus r_0(X)) \\ + 2^k (r_0(Y) \oplus r_1(X) \oplus r_k(Z) \oplus r_{k-1}(Z) * r_0(X)). \end{aligned} \tag{2.28}$$

Es conveniente notar que para $k = 1$, el término $r_0(Z) + \cdots + 2^{k-2} r_{k-2}(Z)$ de (2.28) no tiene sentido. Así que éste debe ser omitido y únicamente debemos escribir los últimos dos sumandos de la ecuación (2.28), esto es, si $k = 1$, entonces

$$\begin{aligned} 2^{k-1}X + 2^k Y + Z &= X + 2Y + Z \\ &= [r_0(X) \oplus r_0(Z)] + 2[r_0(Y) \oplus r_1(X) \oplus r_1(Z) \oplus r_0(X) * r_0(Z)] \end{aligned}$$

Este es el único caso en el que $r_0(2^{k-1}X + 2^k Y + Z) = r_0(X) \oplus r_0(Z)$. En los otros casos, es decir, para todo $k \geq 2$, se tiene que $r_0(2^{k-1}X + 2^k Y + Z) = r_0(Z)$.

El siguiente teorema es una de las aportaciones de este trabajo.

Teorema 2.3.5. *Con la notación anterior,*

$$\varphi(2^{k-1}X + 2^k Y + Z) = \varphi(2^{k-1}X) + 2\varphi(Y) + \varphi(Z) + \varphi(2^k X \odot 2Z).$$

Demostración. La prueba consiste en aplicar la definición de φ a la representación 2-ádica de $2^{k-1}X + 2^k Y + Z$ dada en (2.28). Ya que $k \geq 2$, podemos escribir $\varphi(2^{k-1}X + 2^k Y + Z) = A + B$, donde $A = c_{k-1}^{k-1} \otimes r_0(Z)$ y

$$\begin{aligned} B = 2 \Big[\Big(c_0^{k-1} \otimes r_1(Z) \Big) \oplus \cdots \oplus \Big(c_{k-3}^{k-1} \otimes r_{k-2}(Z) \Big) \oplus \Big(c_{k-2}^{k-1} \otimes (r_{k-1}(Z) \oplus r_0(X)) \Big) \\ \oplus c_{k-1}^{k-1} \otimes (r_0(Y) \oplus r_1(X) \oplus r_k(Z) \oplus r_{k-1}(Z) * r_0(X)) \Big]. \end{aligned}$$

Por el Corolario 2.3.3 y las propiedades del producto de Kronecker, $A+B$ puede ser expresado como

$$A+2\left[\left(c_0^{k-1}\otimes r_1(Z)\right)\oplus\cdots\oplus\left(c_{k-3}^{k-1}\otimes r_{k-2}(Z)\right)\oplus\left(c_{k-2}^{k-1}\otimes r_{k-1}(Z)\right)\oplus\left(c_{k-1}^{k-1}\otimes r_k(Z)\right)\right]$$
$$+2\left[\left(c_{k-2}^{k-1}\otimes r_0(X)\right)\oplus\left(c_{k-1}^{k-1}\otimes(r_0(Y)\oplus r_1(X)\oplus r_{k-1}(Z)*r_0(X))\right)\right],$$

o de forma similar,

$$\varphi(Z)+2\left[\left(c_{k-2}^{k-1}\otimes r_0(X)\right)\oplus\left(c_{k-1}^{k-1}\otimes r_1(X)\right)\right]+2c_{k-1}^{k-1}\otimes r_0(Y)+2c_{k-1}^{k-1}\otimes r_{k-1}(Z)*r_0(X).$$

Note ahora que por las ecuaciones (2.25) y (2.26), el segundo y el tercer sumando de la expresión anterior son precisamente $2\varphi(Z)$ y $\varphi(2^{k-1}X)$. Por lo tanto, sutituyendo obtenemos

$$\varphi(2^{k-1}X+2^kY+Z)=\varphi(Z)+2\varphi(Y)+\varphi(2^{k-1}X)+2c_{k-1}^{k-1}\otimes r_{k-1}(Z)*r_0(X).$$

Finalmente, por las identidades (2.22) y (2.24), se tiene que la representación 2-ádica de 2^kX y $2Z$ es:

$$2^kX=2^kr_0(X),\qquad 2Z=2r_0(Z)+2^2r_1(Z)+\cdots+2^kr_{k-1}(Z).$$

Por lo tanto, de la definición de la operación $\odot$ dada en (2.21) se sigue que

$$2^kX\odot 2Z=2^k\left[r_0(X)*r_{k-1}(Z)\right].$$

Consecuentemente,

$$\varphi(2^kX\odot 2Z)=2c_{k-1}^{k-1}\otimes r_0(X)*r_{k-1}(Z),\tag{2.29}$$

lo que completa la demostración del resultado. □

Una aplicación inmediata del Teorema 2.3.5 proporciona el siguiente resultado.

Corolario 2.3.6. *Con la notación anterior,*

(1) $\varphi(2^kY+Z)=\varphi(2^kY)+\varphi(Z)=2\varphi(Y)+\varphi(Z)$,

(2) $\varphi(2^kZ+Z)=-\varphi(Z)$,

(3) $\varphi(2^{k-1}Z+Z)=\varphi(2^{k-1}Z)+\varphi(Z)+\varphi(2^kZ\odot 2Z)$,

(4) $\varphi(2^{k-1}Z+2^kZ+Z)=\varphi(2^{k-1}Z)-\varphi(Z)+\varphi(2^kZ\odot 2Z)$.

Dado que $\varphi:\mathbb{Z}_4^n\to\mathbb{Z}_4^n$ es la función identidad, las relaciones (1) y (2) del Corolario 2.3.6 son también válidas para todo $k\geq 1$. Éstas fueron demostradas para la isometría φ^k en la Proposición 3.1 de [51]. Ya que φ y φ^k son permutación equivalentes, el Teorema 2.3.5 puede ser considerado como una generalización de la Proposición 3.1 de [51].

2.3.4. Propiedades de la isometría de Gray sobre $\mathbb{Z}_{2^{k+1}}$

Como consecuencia inmediata del Teorema 2.3.5 y de la relación natural entre las isometrías Φ, ϕ y φ descrita en la Proposición 2.2.12, en este apartado derivamos algunas propiedades para la isometría Φ de Gray sobre $\mathbb{Z}_{2^{k+1}}^n$, que son similares a las que se presentaron en el Corolario 2.3.6 para la isometría φ.

Teorema 2.3.7. *Sean $n \geq 1, k \geq 2$ enteros y sean $X, Y, Z \in \mathbf{Z}_{2^{k+1}}^n$. Entonces*

$$\Phi(2^{k-1}X + 2^kY + Z) = \Phi(2^{k-1}X) \oplus \Phi(2^kY) \oplus \Phi(Z) \oplus \Phi(2^kX \odot 2Z).$$

Demostración. La prueba se sigue de aplicar sucesivamente el Lema 2.3.4 al Teorema 2.3.5. Primero recuerde que, por la Proposicón 2.2.12, $\Phi = \phi \circ \varphi$, donde ϕ es la isometría de Gray sobre $\mathbb{Z}_4^n$. De este modo, para todo $X, Y, Z \in \mathbb{Z}_{2^{k+1}}^n$ obtenemos que

$$\begin{aligned}\Phi(2^{k-1}X + 2^kY + Z) &= \phi\left(\varphi(2^{k-1}X + 2^kY + Z)\right) \\ &= \phi\left(\varphi(2^{k-1}X) + 2\varphi(Y) + \varphi(Z) + \varphi(2^kX \odot 2Z)\right).\end{aligned}$$

Ahora, por la relación 2 del Lema 2.3.4, se tiene:

$$\Phi(2^{k-1}X + 2^kY + Z) = \phi\left(\varphi(2^{k-1}X) + \varphi(Z) + \varphi(2^kX \odot 2Z)\right) \oplus \phi\left(2\varphi(Y)\right).$$

Así, sólo necesitamos simplificar las expresiones de los sumandos del lado derecho de la ecuación anterior. Como primer punto, note que de la ecuación (2.26) se sigue que

$$\phi(2\varphi(Y)) = \phi(\varphi(2^k(Y))) = \Phi(2^kY).$$

En consecuencia, solo resta simplicar el sumando $\phi\left(\varphi(2^{k-1}X) + \varphi(Z) + \varphi(2^kX \odot 2Z)\right)$. Para tal fin, note que, por la relación (2.29), $\varphi(2^kX \odot 2Z)$ puede ser escrito como $\varphi(2^kX \odot 2Z) = 2A$, donde $A = c_{k-1}^{k-1} \otimes r_0(X) * r_{k-1}(Z) \in \mathbb{Z}_4^{2^{k-1}n}$. Así, en virtud de la identidad 2 del Lema 2.3.4,

$$\begin{aligned}\phi\left(\varphi(2^{k-1}X) + \varphi(Z) + \varphi(2^kX \odot 2Z)\right) &= \phi\left([\varphi(2^{k-1}X) + \varphi(Z)] + 2A\right) \\ &= \phi\left(\varphi(2^{k-1}X) + \varphi(Z)\right) \oplus \phi\left(2A\right) \\ &= \phi\left(\varphi(2^{k-1}X) + \varphi(Z)\right) \oplus \phi\left(\varphi(2^kX \odot 2Z)\right).\end{aligned}$$

De este modo, $\phi\left(\varphi(2^{k-1}X) + \varphi(Z) + \varphi(2^kX \odot 2Z)\right) = \phi\left(\varphi(2^{k-1}X) + \varphi(Z)\right) \oplus \Phi\left(2^kX \odot 2Z\right)$. Ahora, como $k \geq 2$, se sigue de (2.25) que las coordenadas del vector $\varphi(2^{k-1}X)$ están en el ideal maximal de $\mathbb{Z}_4$. En consecuencia, por la identidad 2 del Lema 2.3.4,

$$\phi\left(\varphi(Z) + \varphi(2^{k-1}X)\right) = \phi\left(\varphi(Z)\right) \oplus \phi\left(\varphi(2^{k-1}X)\right) = \Phi(Z) \oplus \Phi(2^{k-1}X),$$

lo que finaliza la prueba. □

De igual modo que antes, como consecuencia inmediata del Teorema 2.3.7, se tiene el siguiente resultado.

Corolario 2.3.8. *Sean $n \geq 1, k \geq 2$ enteros y $Y, Z \in \mathbf{Z}_{2^{k+1}}^n$. Entonces*

1. $\Phi(2^k Y + Z) = \Phi(2^k Y) \oplus \Phi(Z)$,
2. $\Phi(2^k Z + Z) = \Phi(2^k Z) \oplus \Phi(Z)$,
3. $\Phi(2^{k-1} Z + 2^k Z + Z) = \Phi(2^{k-1} Z) \oplus \Phi(2^k Z) \oplus \Phi(Z) \oplus \Phi(2^k Z \odot 2Z)$,
4. $\Phi(2^{k-1} Z + Z) = \Phi(2^{k-1} Z) \oplus \Phi(Z) \oplus \Phi(2^k Z \odot 2Z)$.

Note que a partir del Lema 2.3.4 se sigue que las primeras dos identidades del Corolario 2.3.8 son también válidas para $k = 1$. Asimismo, vale la pena aclarar que el Teorema 2.3.7, puede ser demostrado directamente aplicando la definición de Φ a la representación 2-ádica del elemento $2^{k-1}X + 2^k Y + Z$ dada en la relación (2.28). Los argumentos que guían esta demostración son similares a los que se emplearon en la demostración el Teorema 2.3.5. Más aún, nótese que debido a la inyectividad de la isometría de Gray, el Teorema 2.3.7 es equivalente al Teorema 2.3.5 en el sentido que si conocemos una de las dos relaciones, entonces podemos derivar la otra a partir de la primera. En gran medida, esto se debe a que cada uno de los argumentos dados en las demostraciones de estos resultados puede ser establecido en el sentido contrario.

En resumen, en este capítulo hemos estudiado diferentes isometrías y hemos mostrado cuáles de ellas son permutación equivalentes. Asimismo, hemos analizado algunas relaciones básicas de las isometrías φ y Φ de Gray (Teoremas 2.3.5, 2.3.7 y sus respectivos Corolarios). Como mencionamos, estas relaciones forman parte de las contribuciones de este trabajo. En el siguiente capítulo continuaremos con el análisis de algunas otras relaciones en las que las unidades de nuestro interés, 1, $\lambda = 1 + 2^k$, $\delta_1 = 1 + 2^{k-1}$ y $\delta_2 = 1 + 2^{k-1} + 2^k$, se ven inmediatamente involucradas. Todos estos resultados, y el del presente capítulo, van encaminados a la determinación de las propiedades de las imágenes de los códigos consta-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$.

Capítulo 3

Las isometrías φ, de Gray y el corrimiento γ-casi-cíclico

El propósito de este capítulo es presentar algunas relaciones entre las isometrías φ y Φ de Gray introducidas en las Secciones 2.1 y 2.2, y el corrimiento γ-casi-cíclico, donde γ es una unidad del anillo $\mathbb{Z}_{2^{k+1}}$. En especial, analizaremos con más detalle estas relaciones cuando γ sea un elemento del grupo $1+\langle 2^{k-1}\rangle = \{1, 1+2^{k-1}, 1+2^k, 1+2^{k-1}+2^k\} \subseteq U(\mathbb{Z}_{2^{k+1}})$. Para los casos $\gamma \neq 1+2^k$ las relaciones constituyen una aportación más de este trabajo; mientras que para el caso $\gamma = 1+2^k$, se probará que éstas generalizan a aquellas que se establecieron en [51, 52, 54, 55].

3.1. Introducción

Después de la publicación de los trabajos [54, 55], en los que se explicó la conexión entre códigos negacíclicos sobre $\mathbb{Z}_4$ y códigos cíclicos binarios (no necesariamente lineales) vía la isometría de Gray $\phi : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$, varios autores han investigado propiedades de casi-ciclicidad y linealidad de las imágenes de Gray de códigos γ-cíclicos definidos sobre ciertas familias de anillos finitos R, donde γ es una unidad en R ([8, 9, 13, 21, 29, 33, 35, 50–52, 56, 57, 59]). La pieza clave en la mayor parte de estos trabajos fue demostrar que existen relaciones entre las isometrías de Gray que se definieron en esos trabajos y el corrimiento γ-cíclico.

Por ejemplo, la idea clave en los trabajos [54, 55] fue demostrar las relaciones $\phi \circ \nu = \sigma \circ \phi$ y $\Psi \circ \sigma = \sigma \circ \Psi$, donde σ es el corrimiento cíclico, ν es el corrimiento negacíclicoy Ψ la *isometría de Nechaev-Gray*, que resulta de la composición de la *permutación de Nechaev* y la isometría ϕ de Gray. Asimismo, con el propósito de estudiar propiedades de ciclicidad de la imagen de Gray de un código $(1+2^k)$-cíclico sobre $\mathbb{Z}_{2^{k+1}}$, en [51, 52], se define la isometría[1] $\varphi^k : (\mathbb{Z}_{2^{k+1}}^n, \delta_h) \to (\mathbb{Z}_4^{2^{k-1}n}, \delta_L)$ y se demuestra la relación $\varphi^k \circ \nu_\lambda = \nu^{\otimes 2^{k-1}} \circ \nu$, donde $\lambda = 1+2^k$, ν_λ es el corrimiento λ-cíclico y $\nu^{\otimes 2^{k-1}}$ es el corrimiento casi-negacíclico de índice 2^{k-1} sobre $\mathbb{Z}_4^{2^{k-1}n}$. A partir de esta relación, una isometría de Gray G_1 fue introducida[2] de tal modo que la relación $G_1 \circ \nu_\lambda = \sigma^{\otimes 2^{k-1}} \circ G_1$ fuese válida; generalizando algunas de las principales aportaciones de [54, 55].

De manera similar, con el fin de estudiar las propiedades de casi-ciclicidad de la imagen de Gray de un código λ-cíclico sobre un anillo finito de cadena, la idea fue encontrar una relación

[1] La definición de esta isometría la hemos estudiado en la Sección 2.2 de este material.

[2] Hemos estudiado esta isometría al final de la Sección 2.2.

análoga a las que se encontraron en [51, 52, 54, 55]. En concreto, en [29] se demuestra que $\Phi \circ \nu_\lambda = \sigma^{\otimes p^{mk-1}} \circ \Phi$, donde $\lambda = 1+\theta^k$, θ es el generador del ideal maximal del anillo de cadena R, k es el *índice de nilpotencia de* θ, p^m es la cardinalidad del campo residual de R y Φ es la isometría de Gray definida sobre R^n. Cabe aclarar que si $R = \mathbb{Z}_4$, entonces $\theta = 2$ y $k = 1$, de donde se obtiene que $\lambda = 1+2 = 3 = -1$ en $\mathbb{Z}_4$. Asimismo, si $R = \mathbb{Z}_{2^{k+1}}$, entonces $\theta = 2$ y el índice de nilpotencia es k, lo cual, implica que $\lambda = 1+2^k$. Consecuentemente, la unidad que se estudió en [29] generaliza a las unidades que se estudiaron en [51,52,54,55].

El propósito de este capítulo es investigar algunas relaciones generales entre las isometrías φ y Φ de Gray introducidas en el Capítulo 2, y el corrimiento γ-casi-cíclico, donde γ es cualquier unidad del anillo $\mathbb{Z}_{2^{k+1}}$ (Sección 3.2). En particular, analizaremos con más detalles las situaciones cuando γ es un elemento del subgrupo $1+\langle 2^{k-1}\rangle = \{1, 1+2^{k-1}, 1+2^k, 1+2^{k-1}+2^k\}$ (Proposición 1.3.13). En la Sección 3.3 estudiaremos las relaciones entre la isometría φ y el corrimiento γ-casi-cíclico, donde $\gamma \in 1+\langle 2^{k-1}\rangle$. Para los casos $\gamma \in \{1, 1+2^{k-1}, 1+2^{k-1}+2^k\}$, los resultados que probaremos constituyen una aportación más de este trabajo. Para el caso $\gamma = 1+2^k$ encontraremos relaciones que generalizan a aquellas que se establecieron en [54,55] y, posteriormente, en [51,52]. En la Sección 3.4, tomaremos como punto de partida los resultados de la sección 3.3 para obtener relaciones entre la isometría Φ de Gray y el corrimiento γ-casi-cíclico, donde $\gamma \in 1+\langle 2^{k-1}\rangle$, similares a las que probamos en la Sección 3.3 para la isometría φ.

Tal como sucedió en [29, 51, 52, 54, 55], estas relaciones serán la clave para estudiar las propiedades de casi-ciclicidad y casi-negaciclicidad de la imagen, con respecto a las isometrías φ y Φ, de un código γ-casi-cíclico sobre $\mathbb{Z}_{2^{k+1}}$, donde $\gamma \in 1+\langle 2^{k-1}\rangle$ y $k \geq 2$.

3.2. Relaciones fundamentales

Primero recordemos algunos conceptos introducidos en el Capítulo 1 de este manuscrito. Sea R un anillo (finito conmutativo y con elemento identidad), $n \geq 1$ un entero y $f : R^n \to R^n$ una función. Recordemos que para cualquier entero $m \geq 1$, definimos la aplicación $f^{\otimes m} : R^{nm} \to R^{nm}$ como

$$\left(A^{(0)} \,|\, A^{(1)} \,|\, \cdots \,|\, A^{(m-1)}\right) \mapsto \left(f(A^{(0)}) \,|\, f(A^{(1)}) \,|\, \cdots \,|\, f(A^{(m-1)})\right),$$

donde $A^{(0)}, A^{(1)}, \ldots, A^{(m-1)} \in R^n$ y "|" denota la concatenación de vectores. Es claro a partir de esta definición que $(f \circ g)^{\otimes m} = f^{\otimes m} \circ g^{\otimes m}$, donde f, g son funciones para las cuales la composición esté bien definida.

Asimismo, recordemos que si γ es una unidad de R, se ha definido el corrimiento γ-cíclico como el R-automorfismo sobre R^n dado por $\nu_\gamma : (a_0, a_1 \ldots, a_{n-1}) \mapsto (\gamma a_{n-1}, a_0, \ldots, a_{n-2})$. El corrimiento γ-casi-cíclico de índice m se ha definido como la función $\nu_\gamma^{\otimes m}$. Dos casos particulares de esta aplicación son el corrimiento casi-cíclico ($\gamma = 1$) y el corrimiento casi-negacíclico

($\gamma = -1$), denotados respectivamente como $\sigma^{\otimes m}$ y $\nu^{\otimes m}$.

En esta sección estamos interesados en describir relaciones generales que involucren a los automorfismos $\nu_\gamma^{\otimes m}$, $\sigma^{\otimes m}$, $\nu^{\otimes m}$ y a las isometrías $\varphi : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}_4^{2^{k-1}n}$ y $\Phi : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{F}_2^{2^k n}$ que se han definido en las secciones 2.1 y 2.2 como

$$\varphi(Z) = c_{k-1}^{k-1} \otimes r_0(Z) + \left[\left(c_0^{k-1} \otimes r_1(Z) \right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes r_k(Z) \right) \right],$$

y

$$\Phi(Z) = \left(c_0^k \otimes r_0(Z) \right) \oplus \cdots \oplus \left(c_k^k \otimes r_k(Z) \right), \qquad \forall Z \in \mathbb{Z}_{2^{k+1}}^s$$

donde $Z = r_0(Z) + 2r_1(Z) + \cdots + 2^k r_k(Z) \in \mathbb{Z}_{2^{k+1}}^n$ está expresado en su representación 2-ádica. La unidad γ que estaremos considerando en esta sección será cualquier elemento del grupo de unidades de $\mathbb{Z}_{2^{k+1}}$. En la siguiente sección nos enfocaremos a encontrar relaciones más específicas entre las isometrías φ y Φ de Gray, y el corrimiento γ-casi-cíclico, donde γ es un elemento del subgrupo de $U(\mathbb{Z}_{2^{k+1}})$:

$$1 + \langle 2^{k-1} \rangle = \{1, 1+2^{k-1}, 1+2^k, 1+2^{k-1}+2^k\}, \qquad k \geq 2.$$

Para los propósitos de este trabajo, a continuación introducimos un $\mathbb{Z}_{2^{k+1}}$-automorfismo sobre $\mathbb{Z}_{2^{k+1}}^n$. Sean $k, n \geq 1$ enteros y sea $\gamma \in U(\mathbb{Z}_{2^{k+1}})$. Sobre $\mathbb{Z}_{2^{k+1}}^n$ definimos el $\mathbb{Z}_{2^{k+1}}$-automorfismo η_γ dado por

$$\eta_\gamma : (z_0, z_1, \ldots, z_{n-1}) \mapsto (z_0, z_1, \ldots, \gamma z_{n-1}).$$

Es bastante claro que para todo entero $n \geq 1$ y $a, \gamma \in U(\mathbb{Z}_{2^{k+1}})$, se tiene que $\eta_\gamma \circ \eta_a = \eta_{a\gamma}$, $\nu_\gamma = \sigma \circ \eta_\gamma$ y $\nu_\gamma \circ \eta_a = \nu_{a\gamma}$, donde $\sigma = \sigma^{\otimes 1}$ es el corrimiento cíclico. En consecuencia, estas propiedades son también válidas para $\eta_\gamma^{\otimes m}$ y los corrimientos γ-casi-cíclico y casi-cíclico. Formalmente, tenemos el siguiente resultado.

Proposición 3.2.1. *Sean $k, m, n \geq 1$ enteros y $a, \gamma \in U(\mathbb{Z}_{2^{k+1}})$. Entonces, para todo $Z \in \mathbb{Z}_{2^{k+1}}^{nm}$,*

(1) $\left(\eta_\gamma^{\otimes m} \circ \eta_a^{\otimes m} \right)(Z) = \eta_{a\gamma}^{\otimes m}(Z)$,

(2) $\nu_\gamma^{\otimes m}(Z) = \left(\sigma^{\otimes m} \circ \eta_\gamma^{\otimes m} \right)(Z)$,

(3) $\left(\nu_\gamma^{\otimes m} \circ \eta_a^{\otimes m} \right)(Z) = \nu_{a\gamma}^{\otimes m}(Z)$.

Las relaciones establecidas en la proposición anterior aparecerán constantemete en el desarrollo de los principales resultados de este trabajo. Por ejemplo, observe que para encontrar una identidad para la aplicación $\varphi \circ \nu_\gamma^{\otimes m}$, similar a la relación $\varphi^k \circ \nu_\lambda = \nu^{\otimes 2^{k-1}} \circ \nu$ (implícitamente) establecida en [52], es necesario aplicar la definición de φ al elemento $\nu_\gamma^{\otimes m}(Z)$, donde

$Z \in \mathbb{Z}_{2^{k+1}}^{nm}$. Esto implica el cálculo explícito de los vectores $r_i(\nu_\gamma^{\otimes m}(Z))$, los cuales dependen de la unidad γ que estemos considerando. Por el contrario, usando la relación (2) de la Proposición 3.2.1, tenemos que

$$r_i(\nu_\gamma^{\otimes m}(Z)) = r_i((\sigma^{\otimes m} \circ \eta_\gamma^{\otimes m})(Z)) = (r_i \circ \sigma^{\otimes m})(\eta_\gamma^{\otimes m}(Z)).$$

Consecuentemente, el cálculo de $r_i(\nu_\gamma^{\otimes m}(Z))$ se puede dividir en dos problemas más sencillos: primero, encontrar expresiones para $r_i \circ \sigma^{\otimes m}$ y, después, considerar al factor $\eta_\gamma^{\otimes m}(Z)$; ésta es la idea que se desarrollará a continuación.

Lema 3.2.2. *Sean $m,n,k \geq 1$ enteros y $0 \leq i \leq k$. Entonces*

$$\left(r_i \circ \sigma^{\otimes m}\right)(Z) = \left(\sigma^{\otimes m} \circ r_i\right)(Z), \qquad \forall Z \in \mathbb{Z}_{2^{k+1}}^{nm}. \tag{3.1}$$

Demostración. Sea $Z = \left(\mathbf{z}^{(1)}|\mathbf{z}^{(2)}|\cdots|\mathbf{z}^{(m)}\right) \in \mathbb{Z}_{2^{k+1}}^{nm}$, donde $\mathbf{z}^{(j)} \in \mathbb{Z}_{2^{k+1}}^{n}$, $1 \leq j \leq m$. Entonces, por definición de la función r_i, se tiene que

$$\left(r_i \circ \sigma^{\otimes m}\right)(Z) = \left(r_i(\sigma(\mathbf{z}^{(1)}))|r_i(\sigma(\mathbf{z}^{(2)}))|\cdots|r_i(\sigma(\mathbf{z}^{(m)}))\right),$$

y el resultado se sigue del hecho que $r_i(\sigma(w)) = \sigma(r_i(w))$ para cada $w \in \mathbb{Z}_{2^{k+1}}^{n}$. □

Note que en el lado izquierdo de la relación (3.1), el corrimiento casi-cíclico $\sigma^{\otimes m}$ es considerado como un $\mathbb{Z}_{2^{k+1}}$-automorfismo sobre $\mathbb{Z}_{2^{k+1}}^{nm}$, mientras que en el lado derecho de (3.1), $\sigma^{\otimes m}$ es considerado como un $\mathbb{F}_2$-automorfismo sobre $\mathbb{F}_2^{nm}$. Por lo tanto, para eludir cualquier tipo de confusión, debemos usar distintas notaciones para $\sigma^{\otimes m}$ en cada una de estas situaciones. Sin embargo, ya que es claro el contexto en el que se están empleando estos automorfismos, no introduciremos diferentes notaciones para cada caso que se presente.

Como la definición de las isometrías φ y Φ involucran al producto de Kronecker, también es indispensable concocer técnicas para calcular el producto de Kronecker de un vector con el corrimiento γ-casi-cíclico. El siguiente resultado proporciona esta información, la que es suficiente para los propósitos de este capítulo.

Lema 3.2.3. *Sean $k,m,n,s \geq 1$ enteros y C,Z elementos de $\mathbb{Z}_{2^{k+1}}^{s}$ y $\mathbb{Z}_{2^{k+1}}^{mn}$, respectivamente. Entonces para toda unidad γ de $\mathbb{Z}_{2^{k+1}}$ se tiene que*

$$C \otimes \nu_\gamma^{\otimes m}(Z) = \nu_\gamma^{\otimes sm}(C \otimes Z).$$

En particular, si $k \geq 2$ y $s = 2^{k-1}$,

$$C \otimes \nu_\gamma^{\otimes m}(Z) = \left(\nu_\gamma \otimes \nu_\gamma\right)^{\otimes 2^{k-2}m}(C \otimes Z).$$

Demostración. Sea $C = (c_0, c_1, \ldots, c_{s-1}) \in \mathbb{Z}_{2^{k+1}}^s$. Por la definición del producto de Kronecker se sigue que

$$\begin{aligned} C \otimes \nu_\gamma^{\otimes m}(Z) &= (c_0 \nu_\gamma^{\otimes m}(Z) | c_1 \nu_\gamma^{\otimes m}(Z) | \cdots | c_{s-1} \nu_\gamma^{\otimes m}(Z)) \\ &= (\nu_\gamma^{\otimes m}(c_0 Z) | \nu_\gamma^{\otimes m}(c_1 Z) | \cdots | \nu_\gamma^{\otimes m}(c_{s-1} Z)), \end{aligned}$$

donde la última relación se debe a que $\nu_\gamma^{\otimes m}$ es un $\mathbb{Z}_{2^{k+1}}$-automorfismo sobre $\mathbb{Z}_{2^{k+1}}^{nm}$. Además, como en la expresión de cada $\nu_\gamma^{\otimes m}(c_j Z)$ el corrimiento γ-cíclico está actuando m veces y j varía entre 0 y $s-1$, se concluye que en el vector $(\nu_\gamma^{\otimes m}(c_0 Z) | \nu_\gamma^{\otimes m}(c_1 Z) | \ldots | \nu_\gamma^{\otimes m}(c_{s-1} Z))$, el corrimiento γ-cíclico está aplicado sm veces. Por lo tanto,

$$C \otimes \nu_\gamma^{\otimes m}(Z) = \nu_\gamma^{\otimes sm}(c_0 Z | c_1 Z | \ldots | c_{m-1} Z) = \nu_\gamma^{\otimes sm}(C \otimes Z).$$

En pariticular, si $k \geq 2$ y $s = 2^{k-1}$, en el vector $\nu_\gamma^{\otimes sm}(C \otimes Z)$ el corrimiento γ-cíclico está actuando $2^{k-1}m$ veces, el cual es un número par puesto que $k \geq 2$. De este modo, al asociar por parejas a ν_γ se obtiene que $\nu_\gamma^{\otimes 2^{k-1}m}(C \otimes Z) = \left(\nu_\gamma \otimes \nu_\gamma\right)^{\otimes 2^{k-2}m}(C \otimes Z)$. □

Observe que en la demostración del Lema 3.2.3 no se ha hecho uso particular de la definición del corrimiento γ-casi-cíclico; sólo se ha hecho uso de la propiedad $\nu_\gamma^{\otimes m}(cZ) = c\nu_\gamma^{\otimes m}(Z)$, donde $c \in \mathbb{Z}_{2^{k+1}}$. Por lo tanto, el Lema 3.2.3 es válido para cualquier automorfismo sobre $\mathbb{Z}_{2^{k+1}}^{nm}$.

Una consecuencia inmediata de los Lemas 3.2.2 y 3.2.3 es el siguiente resultado, el cual, rigurosamente hablando, establece que la función ϕ de Gray sobre $\mathbb{Z}_4^{ns}$ evaluada en el corrimiento casi-cíclico de índice s sobre $\mathbb{Z}_4^{ns}$ es igual al corrimiento casi-cíclico de índice $2s$ sobre $\mathbb{F}_2^{2ns}$ evaluado en la función ϕ de Gray sobre $\mathbb{Z}_4^{ns}$. Para enunciar de manera más precisa este resultado, recuerde que la función de Gray ϕ sobre $\mathbb{Z}_4^n$ está definida como $\phi(Z) = (0,1) \otimes r_0(Z) \oplus (1,1) \otimes r_1(Z)$, donde $Z = r_0(z) + 2r_1(Z)$ está escrito en su representación 2-ádica.

Proposición 3.2.4. *Sean $s, n \geq 1$ enteros. Entonces*

$$\left(\phi \circ \sigma^{\otimes s}\right)(Z) = \left(\sigma^{\otimes 2s} \circ \phi\right)(Z), \qquad \forall\, Z \in \mathbb{Z}_4^{ns}. \tag{3.2}$$

Demostración. De la definición de ϕ y del Lema 3.2.2 se sigue que

$$(\phi \circ \sigma^{\otimes s})(Z) = (0,1) \otimes \sigma^{\otimes s}(r_0(Z)) \oplus (1,1) \otimes \sigma^{\otimes s}(r_1(Z)).$$

Ahora, por el Lema 3.2.3, cada sumando de la expresión anterior se puede escribir como

$$\begin{aligned} (0,1) \otimes \sigma^{\otimes s}(r_0(Z)) &= \sigma^{\otimes 2s}\left((0,1) \otimes r_0(Z)\right), \\ (1,1) \otimes \sigma^{\otimes s}(r_1(Z)) &= \sigma^{\otimes 2s}\left((1,1) \otimes r_0(Z)\right). \end{aligned}$$

Por lo tanto, siendo $\sigma^{\otimes 2s}$ un $\mathbb{F}_2$-automorfismo,

$$(\phi \circ \sigma^{\otimes s})(Z) = \sigma^{\otimes 2s}((0,1) \otimes r_0(Z) \oplus (1,1) \otimes r_1(Z)),$$

de donde el resultado se sigue. □

El siguiente y último punto de esta sección, es introducir relaciones en las que el $\mathbb{Z}_{2^{k+1}}$-automorfismo $\eta_\gamma^{\otimes m}$ se vea involucrado con la isometría Φ de Gray sobre $\mathbb{Z}_{2^{k+1}}^s$ ($s \geq 1$) y γ sea cualquier unidad del anillo $\mathbb{Z}_{2^{k+1}}$. Estas relaciones son los pilares de los principales resultados de este Capítulo.

Teorema 3.2.5. *Sean $k, m, n \geq 1$ enteros y $\gamma \in U(\mathbb{Z}_{2^{k+1}})$. Entonces*

(1) $\varphi \circ \nu_\gamma^{\otimes m} = \sigma^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_\gamma^{\otimes m}$.

(2) $\Phi \circ \nu_\gamma^{\otimes m} = \sigma^{\otimes 2^k m} \circ \Phi \circ \eta_\gamma^{\otimes m}$.

Demostración. Note que $\varphi \circ \nu_\gamma^{\otimes m} = \varphi \circ \sigma^{\otimes m} \circ \eta_\gamma^{\otimes m}$ y que $\Phi \circ \nu_\gamma^{\otimes m} = \Phi \circ \sigma^{\otimes m} \circ \eta_\gamma^{\otimes m}$. Por lo tanto, dado que $\eta_\gamma^{\otimes m}$ es un $\mathbb{Z}_{2^{k+1}}$-automorfismo sobre $\mathbb{Z}_{2^{k+1}}^{nm}$, basta verificar que las siguientes relaciones son ciertas:

$$\varphi \circ \sigma^{\otimes m} = \sigma^{\otimes 2^{k-1}m} \circ \varphi$$

y

$$\Phi \circ \sigma^{\otimes m} = \sigma^{\otimes 2^k m} \circ \Phi.$$

Sean $Z \in \mathbb{Z}_{2^{k+1}}^{nm}$ y $A = \varphi(\sigma^{\otimes m}(Z))$. Como consecuencia de los Lemas 3.2.2, 3.2.3 y de la definición de φ, se obtiene:

$$\begin{aligned}
A &= c_{k-1}^{k-1} \otimes r_0\left(\sigma^{\otimes m}(Z)\right) + 2\left[c_0^{k-1} \otimes r_1\left(\sigma^{\otimes m}(Z)\right) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes r_k\left(\sigma^{\otimes m}(Z)\right)\right] \\
&= c_{k-1}^{k-1} \otimes \sigma^{\otimes m}(r_0(Z)) + 2\left[c_0^{k-1} \otimes \sigma^{\otimes m}(r_1(Z)) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes \sigma^{\otimes m}(r_k(Z))\right] \\
&= \sigma^{\otimes 2^{k-1}m}\left(c_{k-1}^{k-1} \otimes r_0(Z)\right) + 2\left[\sigma^{\otimes 2^{k-1}m}\left(c_0^{k-1} \otimes r_1(Z) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes r_k(Z)\right)\right] \\
&= \sigma^{\otimes 2^{k-1}m}\left(c_{k-1}^{k-1} \otimes r_0(Z) + 2\left[c_0^{k-1} \otimes r_1(Z) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes r_k(Z)\right]\right) \\
&= \sigma^{\otimes 2^{k-1}m}(\varphi(Z)).
\end{aligned}$$

Por lo tanto, $\varphi(\sigma^{\otimes m}(Z)) = \sigma^{\otimes 2^{k-1}m}(\varphi(Z))$. De igual modo, se demuestra la igualdad para Φ. Para probar la equivalencia entre las relaciones (1) y (2) del Teorema 3.2.5, note que sustituyendo $\Phi = \phi \circ \varphi$ (Proposicón 2.2.12) en la relación (2) del Teorema 3.2.5 se obtiene

$$\phi \circ \varphi \circ \nu_\gamma^{\otimes m} = \sigma^{\otimes 2^k m} \circ \phi \circ \varphi \circ \eta_\gamma^{\otimes m}.$$

Por lo tanto, aplicando la relación $\sigma^{\otimes 2^k m} \circ \phi = \phi \circ \sigma^{\otimes 2^{k-1} m}$ (Proposición 3.2.4), la identidad anterior puede ser expresada como

$$\phi \circ \varphi \circ \nu_\gamma^{\otimes m} = \phi \circ \sigma^{\otimes 2^{k-1} m} \circ \varphi \circ \eta_\gamma^{\otimes m}.$$

Finalmente, como ϕ es una función inyectiva, se concluye que $\varphi \circ \nu_\gamma^{\otimes m} = \sigma^{\otimes 2^{k-1} m} \circ \varphi$. Esto demuestra que (2) implica (1). Invirtiendo el sentido de las implicaciones, se demuestra que (1) implica (2). □

Como se ha mencionado previamente, el objetivo de este capítulo es encontrar identidades que permitan calcular $(\varphi \circ \nu_\gamma^{\otimes m})(Z)$ y $(\Phi \circ \nu_\gamma^{\otimes m})(Z)$ conociendo únicamente a los vectores $\varphi(Z)$ y $\Phi(Z)$, $Z \in \mathbb{Z}_{2^{k+1}}^{nm}$. En esta dirección el Teorema 3.2.5 propone una alternativa. Sin embargo, en lugar de conocer únicamente a los vectores $\varphi(Z)$ y $\Phi(Z)$, es necesario conocer a los vectores $(\varphi \circ \eta_\gamma^{\otimes m})(Z)$ y $(\Phi \circ \eta_\gamma^{\otimes m})(Z)$, los cuales están relacionados con $(\varphi \circ \nu_\gamma^{\otimes m})(Z)$ y $(\Phi \circ \nu_\gamma^{\otimes m})(Z)$ por medio del corrimiento casi-cíclico de índice $2^{k-1}m$ sobre $\mathbb{Z}_4$ y de índice $2^k m$ sobre $\mathbb{F}_2$, respectivamente.

Por otra parte, no debe causar asombro el hecho que el corrimiento casi-cíclico sea un automorfismo involucrado en las expresiones del Teorema 3.2.5, puesto que el corrimiento γ-casi-cíclico de índice m ha sido expresado en términos del corrimiento casi-cíclico de índice m y la aplicación $\eta_\gamma^{\otimes m}$. Sin embargo, sobre $\mathbb{Z}_4$, se tiene otro automorfismo que se asemeja al corrimiento casi-cíclico: el corrimiento casi-negacíclico. En las siguientes secciones, se explorará la posibilidad de reemplazar a $\sigma^{\otimes 2^{k-1} m}$ por $\nu^{\otimes 2^{k-1} m}$ en la primera relación del Teorema 3.2.5; esto será hecho con el propósito de especializar las relaciones del Teorema 3.2.5 para las unidades γ del grupo $1 + \langle 2^{k-1} \rangle$, donde $k \geq 2$.

3.3. Relaciones particulares para la isometría φ

En este apartado especializaremos la relación (1) del Teorema 3.2.5 para las unidades γ del grupo $1 + \langle 2^{k-1} \rangle = \{1, 1 + 2^{k-1}, 1 + 2^k, 1 + 2^{k-1} + 2^k\}$, donde $k \geq 2$. Recuerde que si $k = 2$, todos los elementos de este grupo son de orden 2, mientras que si $k \geq 3$, este grupo es cíclico generado por $\delta_1 = 1 + 2^{k-1}$ o bien $\delta_2 = 1 + 2^{k-1} + 2^k$ (Proposición 1.3.13). Más aún, si $k \geq 3$ y $\lambda = 1 + 2^k$, entonces $\delta_2 = (\delta_1)^{-1}$ y $\delta_1^2 = \delta_2^2 = \lambda$. A partir de este punto, nos referiremos a los elementos del grupo $1 + \langle 2^{k-1} \rangle$ distintos de 1 con la notación δ_1, δ_2 y λ que hemos introducido en este párrafo.

A diferencia de los elementos δ_1 y δ_2, note que los elementos 1 y λ son unidades en $\mathbb{Z}_{2^{k+1}}$ para todo entero $k \geq 1$. Por esta razón, en la medida de lo posible, algunas de las relaciones que aportaremos serán establecidas para todo $k \geq 1$, en lugar de $k \geq 2$.

Las pruebas de los principales resultados de este apartado, requieren de las siguientes observaciones y lemas preliminares.

Sean n,m enteros positivos y $Z=\left(\mathbf{z}^{(1)}|\mathbf{z}^{(2)}|\cdots|\mathbf{z}^{(m)}\right)\in\mathbb{Z}_{2^{k+1}}^{nm}$, donde

$$\mathbf{z}^{(j)}=\left(z_0^{(j)},z_1^{(j)},\ldots,z_{n-2}^{(j)},z_{n-1}^{(j)}\right)\in\mathbb{Z}_{2^{k+1}}^{n},\qquad 1\leq j\leq m.$$

Para cada entero j, $0\leq j\leq m$, defina

$$\mathbf{a}^{(j)}=\left(z_0^{(j)},z_1^{(j)},\ldots,z_{n-2}^{(j)},0\right)\quad\text{y}\quad\mathbf{b}^{(j)}=\left(0,0,\ldots,0,z_{n-1}^{(j)}\right).$$

En este punto acordamos que si $n=1$, entonces $\mathbf{a}^{(j)}=0$ y $\mathbf{b}^{(j)}=z_0^{(j)}$ para todo $0\leq j\leq m$.

Con base a lo anterior, es claro que cada $\mathbf{z}^{(j)}$ puede ser expresado como $\mathbf{z}^{(j)}=\mathbf{a}^{(j)}+\mathbf{b}^{(j)}$ y, en consecuencia, Z puede ser escrito como $Z=A+B$, donde

$$A=\left(\mathbf{a}^{(1)}|\mathbf{a}^{(2)}|\cdots|\mathbf{a}^{(m)}\right)\quad\text{y}\quad B=\left(\mathbf{b}^{(1)}|\mathbf{b}^{(2)}|\cdots|\mathbf{b}^{(m)}\right).\tag{3.3}$$

Esta forma de escribir a Z también se ve reflejada en los términos $r_i(Z)$ que aparecen en su representación 2-ádica, es decir,

$$r_i(Z)=r_i(A+B)=r_i(A)\oplus r_i(B),\qquad\forall i,\ 0\leq i\leq k.\tag{3.4}$$

En particular, esto implica que

$$c_j^{k-1}\otimes r_i(Z)=\left(c_j^{k-1}\otimes r_j(A)\right)\oplus\left(c_j^{k-1}\otimes r_i(B)\right),\quad 0\leq j\leq k-1.\tag{3.5}$$

Por otra parte, con el propósito de simplificar y darle claridad a las demostraciones que presentaremos más adelante, para cualesquiera dos enteros $m,n\geq 1$ definimos los conjuntos

$$I(m,n)=\{n-1,2n-1,3n-1,\ldots,mn-1\},\tag{3.6}$$
$$J(m,n)=\mathbb{Z}_{mn}\setminus I(m,n).\tag{3.7}$$

Con la introducción de esta notación, y basados en la definición del producto de Kronecker, es fácil verificar que los vectores $c_j^{k-1}\otimes r_i(A)$, $0\leq i\leq k$ y $0\leq j\leq k-1$, tienen sus coordenadas con índice en el conjunto $I(2^{k-1}m,n)$ iguales a cero. De igual modo, es fácil convencerse de que los vectores $c_j^{k-1}\otimes r_i(B)$ tienen sus coordenadas con índice en el conjunto $J(2^{k-1}m,n)$ iguales a cero. Por lo tanto, ya que los conjuntos $I(2^{k-1}m,n)$ y $J(2^{k-1}m,n)$ son ajenos, la suma binaria del lado derecho de las expresiones (3.4) y (3.5), puede ser reemplazada por la suma módulo 2^s del anillo $\mathbb{Z}_{2^s}$, $s\geq 2$. En especial, esto implica que la representación 2-ádica de Z sea la suma de las representaciones 2-ádicas de A y B. Vale la pena aclarar que, en general, si $x,y,z\in\mathbb{Z}_{2^{k+1}}$ y $x=y+z$, entonces la representación 2-ádica de x no siempre coincide con la suma componente a componente (sobre $\mathbb{Z}_{2^{k+1}}$) de las representaciones 2-ádicas de y y z.

Lema 3.3.1. *Sean k,m,n enteros positivos y sea $Z = A+B \in \mathbb{Z}_{2^{k+1}}^{mn}$, donde A y B son como en la relación* (3.3)*. Entonces*

(1) $\varphi(Z) = \varphi(A) + \varphi(B)$,

(2) $\Phi(Z) = \Phi(A) \oplus \Phi(B)$.

Demostración. Como se ha mencionado, los vectores $c_{k-1}^{k-1} \otimes r_0(A)$ y $c_{k-1}^{k-1} \otimes r_0(B)$ tienen sus coordenadas con índice en $I(2^{k-1}m,n)$ y $J(2^{k-1}m,n)$, respectivamente, iguales a cero. Siendo los conjuntos $I(2^{k-1}m,n)$ y $J(2^{k-1}m,n)$ ajenos, se tiene que

$$c_{k-1}^{k-1} \otimes r_0(Z) = c_{k-1}^{k-1} \otimes r_0(A) + c_{k-1}^{k-1} \otimes r_0(B) \in \mathbb{Z}_4^{2^{k-1}nm}.$$

Por otra parte, debido al Corolario 2.3.3 y a la relación (3.4),

$$2\left[\left(c_0^{k-1} \otimes r_0(Z)\right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes r_k(Z)\right)\right] = X + Y,$$

donde

$$X = 2\left[\left(c_0^{k-1} \otimes r_0(A)\right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes r_k(A)\right)\right]$$

y

$$Y = 2\left[\left(c_0^{k-1} \otimes r_0(B)\right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes r_k(B)\right)\right].$$

En consecuencia, $\varphi(Z)$ es la suma de

$$c_{k-1}^{k-1} \otimes r_0(A) + 2[\left(c_0^{k-1} \otimes r_1(A)\right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes r_k(A)\right)] = \varphi(A)$$

y

$$c_{k-1}^{k-1} \otimes r_0(B) + 2[\left(c_0^{k-1} \otimes r_1(B)\right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes r_k(B)\right)] = \varphi(B),$$

lo que finaliza la prueba de (1). De manera similar se demuestra (2). □

Además de las relaciones entre los elementos $\delta_1 = 1+2^{k-1}$, $\delta_2 = 1+2^{k-1}+2^k$ y $\lambda = 1+2^k$ mencionadas al inicio de esta sección, se tienen las siguientes.

Lema 3.3.2. *Sea $k \geq 2$. Entonces $\lambda\delta_1 = \delta_2$ y, en consecuencia, $\lambda\delta_2 = \delta_1$. Además, si $k = 2$, entonces $\delta_1\delta_2 = \lambda$.*

Demostración. La demostración se sigue de realizar un cálculo directo. En efecto, note que

$$\lambda\delta_1 = (1+2^k)(1+2^{k-1}) = 1+2^{k-1}+2^k+2^{2k-1}.$$

Como $k \geq 2$, se tiene que $2k-1 \geq k+1$ y, por lo tanto, 2^{k+1} divide a 2^{2k-1}. Esto implica que $\lambda\delta_1 = 1+2^{k-1}+2^k = \delta_2$. En consecuencia, dado que $\lambda^2 = 1$, multiplicando por λ ambos lados de $\lambda\delta_1 = \delta_2$, obtenemos que $\delta_1 = \lambda\delta_2$. Finalmente, si $k = 2$, entonces δ_1, δ_2 y λ son unidades en $\mathbb{Z}_8$ y, en consecuencia, son de orden 2. Así, multiplicando por δ_2 ambos lados de $\lambda\delta_1 = \delta_2$ obtenemos que $\lambda\delta_1\delta_2 = \delta_2^2 = 1$. Esto implica que $\delta_1\delta_2 = \lambda^{-1} = \lambda$. □

Para finalizar el preámbulo de esta Sección, recuerde que para cualesquiera $y,z \in \mathbb{Z}_{2^{k+1}}$, con representación 2-ádica

$$y = r_0(y) + 2r_1(y) + \cdots + 2^k r_k(y),$$
$$z = r_0(z) + 2r_1(z) + \cdots + 2^k r_k(z),$$

se ha definido la operación $\odot$ como

$$y \odot z = (r_0(y)r_0(z)) + 2(r_1(y)r_1(z)) + \cdots + 2^k(r_k(y)r_k(z)),$$

Esta operación ha sido extendida a $\mathbb{Z}^n_{2^{k+1}}$ de la siguiente manera (ver la relación (2.21)):

$$Y \odot Z = (r_0(Y) * r_0(Z)) + 2(r_1(Y) * r_1(Z)) + \cdots + 2^k(r_k(Y) * r_k(Z)),$$

donde $Y = r_0(Y) + 2r_1(Y) + \cdots + 2^k r_k(Y)$, $Z = r_0(Z) + 2r_1(Z) + \cdots + 2^k r_k(Z)$ están expresados en su representación 2-ádica y "$*$" es la multiplicación coordenada por coordenada.

Teorema 3.3.3. *Sean $k \geq 2$, $n,m \geq 1$ enteros, $\gamma \in \{\delta_1, \delta_2\}$ y $\lambda = 1 + 2^k$. Entonces*

$$\varphi \circ \nu_\gamma^{\otimes m} = \nu^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_{\lambda\gamma}^{\otimes m}. \tag{3.8}$$

Demostración. Observe que es suficiente demostrar la relación (3.8), digamos, para $\gamma = \delta_1$. Esto se debe a que, si probamos la relación

$$\varphi \circ \nu_{\delta_1}^{\otimes m} = \nu^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_{\lambda\delta_1}^{\otimes m},$$

entonces, al aplicar $\eta_\lambda^{\otimes m}$ en cada lado de la igualdad anterior, por la Proposición 3.2.1, obtenemos

$$\varphi \circ \nu_{\delta_2}^{\otimes m} = \nu^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_{\lambda\delta_2}^{\otimes m},$$

la cual corresponde al caso $\gamma = \delta_2$ que faltaba. Por lo tanto, para demostrar el Teorema 3.3.3, únicamente probaremos la relación (3.8) para $\gamma = \delta_1$. Para tal propósito, note que en virtud del Teorema 3.2.5, basta demostrar la siguiente relación:

$$\sigma^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_{\delta_1}^{\otimes m} = \nu^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_{\delta_2}^{\otimes m}. \tag{3.9}$$

Sea $Z = \left(\mathbf{z}^{(1)}|\mathbf{z}^{(2)}|\cdots|\mathbf{z}^{(m)}\right) \in \mathbb{Z}^{mn}_{2^{k+1}}$, donde $\mathbf{z}^{(j)} \in \mathbb{Z}^n_{2^{k+1}}$, $1 \leq j \leq m$, y expresemos a Z como $Z = A + B$, donde A y B son como en (3.3). Entonces, dado que $\eta_{\delta_1}^{\otimes m}$ es un $\mathbb{Z}_{2^{k+1}}$-automorfismo sobre $\mathbb{Z}^{mn}_{2^{k+1}}$,

$$\eta_{\delta_1}^{\otimes m}(Z) = \eta_{\delta_1}^{\otimes m}(A+B) = \eta_{\delta_1}^{\otimes m}(A) + \eta_{\delta_1}^{\otimes m}(B).$$

Por otra parte, note que el vector $A \in \mathbb{Z}_{2^{k+1}}^{mn}$ siempre tiene un cero en aquellas coordenadas con subíndice en el conjunto $I(m,n)$ y, dado que la acción de $\eta_{\delta_1}^{\otimes m}$ es multiplicar por δ_1 a las coordenadas con subíndice en $I(m,n)$, se tiene que

$$\eta_{\delta_1}^{\otimes m}(A) = A.$$

De manera complementaria, note que el vector $B \in \mathbb{Z}_{2^{k+1}}^{mn}$ siempre tiene ceros en las coordenadas con subíndice en el conjunto $J(m,n)$. Por lo tanto,

$$\eta_{\delta_1}^{\otimes m}(B) = \delta_1 B.$$

Por consiguiente,

$$(\sigma^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_{\delta_1}^{\otimes m})(Z) = (\sigma^{\otimes 2^{k-1}m} \circ \varphi)(A + \delta_1 B) = \sigma^{\otimes 2^{k-1}m}(\varphi(A + \delta_1 B)).$$

Por el Lema 3.3.1, $\varphi(A + \delta_1 B) = \varphi(A) + \varphi(\delta_1 B)$ y, dado que $\sigma^{\otimes 2^{k-1}m}$ es un $\mathbb{Z}_4$-automorfismo,

$$(\sigma^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_{\delta_1}^{\otimes m})(Z) = \sigma^{\otimes 2^{k-1}m}(\varphi(A)) + \sigma^{\otimes 2^{k-1}m}(\varphi(\delta_1 B)).$$

Ahora, puesto que el vector $\varphi(A)$ tiene ceros en las coordenadas con subíndice en el conjunto $I(2^{k-1}m,n)$, la siguiente relación es válida

$$\sigma^{\otimes 2^{k-1}m}(\varphi(A)) = \nu^{\otimes 2^{k-1}m}(\varphi(A)).$$

Por otro lado, de la identidad (3) del Corolario 2.3.6, se sigue que

$$\varphi(\delta_1 B) = \varphi(2^{k-1}B) + \varphi(B) + \varphi(2^k B \odot 2B).$$

Como $\varphi(2^{k-1}B)$ y $\varphi(2^k B \odot 2B)$ tienen todas sus coordenadas en el ideal maximal de $\mathbb{Z}_4$, se tienen las siguientes relaciones:

$$\sigma^{\otimes 2^{k-1}m}\left(\varphi(2^{k-1}B)\right) = \nu^{\otimes 2^{k-1}m}\left(\varphi(2^{k-1}B)\right),$$
$$\sigma^{\otimes 2^{k-1}m}\left(\varphi(2^k B \odot 2B)\right) = \nu^{\otimes 2^{k-1}m}\left(\varphi(2^k B \odot 2B)\right).$$

Además, dado que las coordenadas del vector $\varphi(B)$ cuyo subíndice está en $J(2^{k-1}m,n)$ son iguales a cero,

$$\sigma^{\otimes 2^{k-1}m}(\varphi(B)) = \nu^{\otimes 2^{k-1}m}(-\varphi(B)).$$

Consecuentemente,

$$\begin{aligned}\sigma^{\otimes 2^{k-1}m}(\varphi(\delta_1 B)) &= \nu^{\otimes 2^{k-1}m}\left(\varphi(2^{k-1}B) - \varphi(B) + \varphi(2^k B \odot 2B)\right)\\ &= \nu^{\otimes 2^{k-1}m}(\varphi(\delta_2 B)),\end{aligned}$$

donde la última igualdad queda justificada por el Corolario 2.3.6. De este modo,

$$\begin{aligned}\sigma^{\otimes 2^{k-1}m}(\varphi(A)+\varphi(\delta_1 B)) &= \nu^{\otimes 2^{k-1}m}(\varphi(A))+\nu^{\otimes 2^{k-1}m}(\varphi(\delta_2 B))\\ &= \nu^{\otimes 2^{k-1}m}(\varphi(A)+\varphi(\delta_2 B)).\end{aligned}$$

Finalmente, por el Lema 3.3.1, $\varphi(A)+\varphi(\delta_2 B)=\varphi(\eta_{\delta_2}^{\otimes m}(Z))$ y, por lo tanto,

$$\left(\sigma^{\otimes 2^{k-1}m}\circ\varphi\circ\eta_{\delta_1}^{\otimes m}\right)(Z)=\left(\nu^{\otimes 2^{k-1}m}\circ\varphi\circ\eta_{\delta_2}^{\otimes m}\right)(Z),$$

lo que concluye la demostración. □

Recuerde que el principal objetivo de este apartado es especializar la relación (1) del Teorema 3.2.5 para las unidades γ del grupo $1+\langle 2^{k-1}\rangle$, donde $k\geq 2$. El Teorema 3.3.3 satisface este objetivo para las unidades $\gamma\in\{\delta_1,\delta_2\}$, y un caso particular del Teorema 3.2.5 establece la relación cuando $\gamma=1$. Por lo tanto, la unidad que falta contemplar es $\lambda=1+2^k$. A continuación, a partir del Lema 3.2.2, obtendremos una relación particular para la unidad λ. Más aún, deduciremos nuevas relaciones que son equivalentes entre sí y equivalentes al Teorema 3.3.3, en el sentido de que basta conocer alguna de ellas para deducir las otras.

Primero, recuerde que por la Proposición 3.2.1, para cualesquiera enteros $k,m\geq 1$ y toda unidad u de $\mathbb{Z}_{2^{k+1}}$,

$$\nu_u^{\otimes m}=\sigma^{\otimes m}\circ\eta_u^{\otimes m}. \tag{3.10}$$

Por lo tanto, usando (3.10) en la relación (3.8) obtenemos que

$$\varphi\circ\sigma^{\otimes m}\circ\eta_\gamma^{\otimes m}=\sigma^{\otimes 2^{k-1}m}\circ\eta_{-1}^{\otimes 2^{k-1}m}\circ\varphi\circ\eta_{\lambda\gamma}^{\otimes m} \tag{3.11}$$

Además, por la relación (1) del Teorema 3.2.5,

$$\varphi\circ\sigma^{\otimes m}=\sigma^{\otimes 2^{k-1}m}\circ\varphi \tag{3.12}$$

y, en consecuencia,

$$\sigma^{\otimes 2^{k-1}m}\circ\varphi\circ\eta_\gamma^{\otimes m}=\sigma^{\otimes 2^{k-1}m}\circ\eta_{-1}^{\otimes 2^{k-1}m}\circ\varphi\circ\eta_{\lambda\gamma}^{\otimes m}. \tag{3.13}$$

Dado que $\sigma^{\otimes 2^{k-1}m}:\mathbb{Z}_4^{2^{k-1}mn}\to\mathbb{Z}_4^{2^{k-1}mn}$ es una función biyectiva para todo $n\geq 1$, entonces $\sigma^{\otimes 2^{k-1}m}$ es una función invertible y, por lo tanto, es válido cancelarla en la relación (3.13), obteniendo de esta manera

$$\varphi\circ\eta_\gamma^{\otimes m}=\eta_{-1}^{\otimes 2^{k-1}m}\circ\varphi\circ\eta_{\lambda\gamma}^{\otimes m}. \tag{3.14}$$

Consecuentemente, hemos demostrado que el Teorema 3.3.3 implica la relación (3.14).

Recíprocamente, aplicando $\sigma^{\otimes 2^{k-1}m}$ en el lado izquierdo de (3.14) obtenemos la relación (3.13), lo cual, por (3.12) y (3.10), nos conduce a la relación (3.8). Esto quiere decir que la relación establecida en el Teorema 3.3.3 y la relación (3.14) son resultados equivalentes, entendiendo por equivalentes que basta conocer la relación del Teorema 3.3.3 para determinar la relación (3.14), y viceversa.

Por otra parte, recuerde que por la Proposición 3.2.1,

$$\eta_{\lambda\gamma}^{\otimes m} = \eta_{\lambda}^{\otimes m} \circ \eta_{\gamma}^{\otimes m}.$$

Por lo tanto, la relación (3.14) puede ser escrita como:

$$\varphi \circ \eta_{\gamma}^{\otimes m} = \eta_{-1}^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_{\lambda}^{\otimes m} \circ \eta_{\gamma}^{\otimes m}. \tag{3.15}$$

Ya que para todo $k \geq 2$, γ es un elemento del subconjunto $\{\delta_1, \delta_2\}$ de unidades de $\mathbb{Z}_{2^{k+1}}$, entonces la aplicación $\eta_{\gamma^{-1}}^{\otimes m} : \mathbb{Z}_{2^{k+1}}^{mn} \to \mathbb{Z}_{2^{k+1}}^{mn}$ está bien definida y, de hecho, es la función inversa de $\eta_{\gamma}^{\otimes m}$. Por lo tanto, al aplicar $\eta_{\gamma^{-1}}^{\otimes m}$ en el lado derecho de (3.15) obtenemos

$$\varphi = \eta_{-1}^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_{\lambda}^{\otimes m}. \tag{3.16}$$

Dado que la función $\eta_{-1}^{\otimes m}$ es su propio inverso, la identidad anterior puede formularse de la siguiente forma:

$$\eta_{-1}^{\otimes 2^{k-1}m} \circ \varphi = \varphi \circ \eta_{\lambda}^{\otimes m}.$$

Además, como la función $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_4$ es precisamente la función identidad, entonces la relación (3.17) trivialmente se satisface para $k = 1$ y, por lo tanto, hemos demostrado que para todos los enteros $k, m, n \geq 1$ y $\lambda = 1 + 2^k \in \mathbb{Z}_{2^{k+1}}$,

$$\left(\varphi \circ \eta_{\lambda}^{\otimes m}\right)(Z) = \left(\eta_{-1}^{\otimes 2^{k-1}m} \circ \varphi\right)(Z) \qquad \forall Z \in \mathbb{Z}_{2^{k+1}}^{mn}. \tag{3.17}$$

Note que al aplicar la función $\eta_{\gamma}^{\otimes m}$ a ambos lados derechos de la relación (3.16) obtenemos (3.15). Así, la relación (3.17) impica la relación (3.14). En consecuencia, esta relaciones son equivalentes entre sí y, en efecto, al Teorema 3.3.3.

Finalmente, observe que al componer la relación (3.17) con el corrimiento casi-cíclico de índice $2^{k-1}m$, obtenemos que

$$\nu^{\otimes 2^{k-1}m} \circ \varphi = \sigma^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_{\lambda}^{\otimes m},$$

lo que por la relación (3.12) se puede expresar como:

$$\nu^{\otimes 2^{k-1}m} \circ \varphi = \varphi \circ \sigma^{\otimes m} \circ \eta_{\lambda}^{\otimes m} = \varphi \circ \nu_{\lambda}^{\otimes m}. \tag{3.18}$$

Más aún, como antes, note que invirtiendo el sentido de nuestros argumentos, vemos que (3.18) es equivalente la relación (3.17) y, por ende, es equivalente (3.14) y al Teorema 3.3.3.

En resumen hemos demostrado el siguiente resultado, el cual establece que basta demostrar que cualquiera de las siguientes identidades y usar argumentos similares a los que hemos presentado para obtener las otras relaciones.

Teorema 3.3.4. *Sean $n,m \geq 1$ enteros, $\gamma \in \{\delta_1, \delta_2\}$ y $\lambda = 1+2^k$. Entonces:*

1. *Para todo $k \geq 2$,*
$$\varphi \circ \nu_\gamma^{\otimes m} = \nu^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_{\lambda\gamma}^{\otimes m}.$$
2. *Para todo $k \geq 2$,*
$$\varphi \circ \eta_\gamma^{\otimes m} = \eta_{-1}^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_{\lambda\gamma}^{\otimes m}.$$
3. *Para todo $k \geq 1$,*
$$\varphi \circ \eta_\lambda^{\otimes m} = \eta_{-1}^{\otimes 2^{k-1}m} \circ \varphi.$$
4. *Para todo $k \geq 1$,*
$$\varphi \circ \nu_\lambda^{\otimes m} = \nu^{\otimes 2^{k-1}m} \circ \varphi.$$

Vale la pena mencionar que la relación (4) del teorema anterior es una generalización de la identidad $\varphi^k \circ \nu_\lambda = \nu^{\otimes 2^{k-1}} \circ \varphi$ establecida (implícitamente) en la demostración del Teorema 8 de [52], la cual fue la clave para describir propiedades de la imagen bajo φ^k de códigos λ-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$.

Del mismo modo que la relación $\varphi^k \circ \nu_\lambda = \nu^{\otimes 2^{k-1}} \circ \varphi$ fue usada [52] para estudiar propiedades de la imagen bajo φ^k de códigos λ-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, usaremos las relaciones demostradas en esta sección para describir (en los siguientes capítulos) propiedades de la imagen bajo φ^k de códigos λ-casi-cíclicos y γ-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, donde $\gamma \in \{\delta_1, \delta_2\}$.

3.4. Relaciones particulares para la isometría Φ de Gray

En esta sección especializaremos la relación (2) del Teorema 3.2.5 para las unidades $\gamma \neq 1$ del grupo $1 + \langle 2^{k-1} \rangle = \{1, 1+2^{k-1}, 1+2^k, 1+2^{k-1}+2^k\}$, donde $k \geq 2$. Recuerde que en la sección anterior introducimos la siguiente notación: $\delta_1 = 1+2^{k-1}$, $\delta_2 = 1+2^{k-1}+2^k$ y $\lambda = 1+2^k$.

Tomaremos como punto de partida las relaciones que se demostraron en los Teoremas 3.3.3 y 3.3.4. Procediendo con esta idea vemos que lo natural es aplicar la relación $\Phi = \phi \circ \varphi$ a

cada uno de esos resultados (ver la Proposicón 2.2.12). Así, del Teorema 3.3.3 deducimos lo siguiente:

$$\Phi \circ \nu_{\gamma}^{\otimes m} = \phi \circ \nu^{\otimes 2^{k-1}m} \circ \varphi \circ \eta_{\lambda\gamma}^{\otimes m}, \tag{3.19}$$

donde $\gamma \in \{\delta_1, \delta_2\}$, $k \geq 2$. Del mismo modo, del Teorema 3.3.4 se obtienen las siguientes relaciones:

$$\Phi \circ \eta_{\gamma}^{\otimes m} = \phi \circ \eta_{-1}^{\otimes 2^{k-1}m} \circ \varphi \circ \varphi_{\lambda\gamma}^{\otimes m}, \tag{3.20}$$

$$\Phi \circ \eta_{\lambda}^{\otimes m} = \phi \circ \eta_{-1}^{\otimes 2^{k-1}m} \circ \varphi, \tag{3.21}$$

$$\Phi \circ \nu_{\lambda}^{\otimes m} = \phi \circ \nu^{\otimes 2^{k-1}m} \circ \varphi. \tag{3.22}$$

Sin embargo, estas igualdades están incompletas en el sentido de que en el lado derecho de cada una de ellas no aparece la isometría Φ de Gray. Por lo tanto, con el fin de completar cada una de esas identidades, a continuación presentamos expresiones que relacionan a la isometría ϕ de Gray (sobre $\mathbb{Z}_4$) con la aplicación $\eta_{-1}^{\otimes m}$ y el corrimiento casi-negacíclico.

La siguiente permutación será útil.

Sean $m, n \geq 1$ enteros. Sobre $I_{2mn} = \{0, 1, \ldots, 2mn-1\}$ defina la siguiente permutación:

$$\pi := (n-1, (m+1)n-1)\,(2n-1, (m+2)n-1) \cdots (mn-1, 2mn-1)\,. \tag{3.23}$$

Sea $\widetilde{\pi} : \mathbb{F}_2^{2mn} \to \mathbb{F}_2^{2mn}$ la permutacíon inducida por π, es decir, si $Z = (z_0, z_1, \ldots, z_{2mn-1}) \in \mathbb{F}_2^{2mn}$, entonces

$$\widetilde{\pi}(Z) = \left(z_{\pi(0)}, z_{\pi(1)}, \ldots, z_{\pi(2mn-1)}\right).$$

Por ejemplo, si $m = 3$, $n = 2$ y $Z = (z_0, z_1, \ldots, z_{11}) \in \mathbb{F}_2^{12}$, entonces $\pi = (1,7)(3,9)(5,11)$ y, por lo tanto,

$$\begin{aligned}\widetilde{\pi}(Z) &= \left(z_{\pi(0)}, z_{\pi(1)}, z_{\pi(2)}, z_{\pi(3)}, z_{\pi(4)}, z_{\pi(5)}, z_{\pi(6)}, z_{\pi(7)}, z_{\pi(8)}, z_{\pi(9)}, z_{\pi(10)}, z_{\pi(11)}\right) \\ &= \left(z_0, z_7, z_2, z_9, z_4, z_{11}, z_6, z_1, z_8, z_3, z_{10}, z_5\right).\end{aligned}$$

Observe que si escribimos

$$Z = (z_0, z_1 | z_2, z_3 | z_4, z_5 | z_6, z_7 | z_8, z_9 | z_{10}, z_{11})\,,$$

entonces la acción de la permutación $\widetilde{\pi}$ sobre el vector Z consiste en intercambiar las últimas coordenadas de los primeros 3 vectores de longitud 2 con las últimas coordenadas de los siguentes 3 vectores de longitud 2.

En general, si $Z \in \mathbb{F}_2^{2mn}$ y escribimos a Z como la concatenación de $2m$ vectores de longitud n cada uno, entonces $\widetilde{\pi}$ intercambia las últimas coordenadas de los primeros m vectores de longitud n con las últimas coordenadas de los segundos m vectores de longitud n. Por lo tanto, las coordenadas de Z que son permutadas tienen subíndice en el conjunto $I(2m, n)$; mientras que las coordenadas de Z que tienen subíndice en el conjunto $J(2m, n)$ permanecen fijas bajo la acción de $\widetilde{\pi}$.

Proposición 3.4.1. *Sean $m,n \geq 1$ enteros. Entonces*

$$\left(\phi \circ \eta_{-1}^{\otimes m}\right)(Z) = \left(\widetilde{\pi} \circ \phi\right)(Z), \qquad \forall\, Z \in \mathbb{Z}_4^{mn}$$

donde $\widetilde{\pi}$ es la permutación sobre $\mathbb{F}_2^{2mn}$ inducida por la permutación π definida en (3.23)*.*

Demostración. Escriba al vector $Z \in \mathbb{Z}_4^{mn}$ de la forma $Z = A + B$, donde A y B son como en (3.3). Entonces

$$\eta_{-1}^{\otimes m}(Z) = \eta_{-1}^{\otimes m}(A+B) = \eta_{-1}^{\otimes m}(A) + \eta_{-1}^{\otimes m}(B).$$

Dado que A tiene ceros en aquellas coordenadas cuyo subíndice está en el conjunto $I(m,n)$, entonces $\eta_{-1}^{\otimes m}(\phi(A)) = \phi(A)$. Asimismo, ya que B tiene ceros en las coordenadas cuyo subíndice está en el conjunto $J(m,n)$, entonces $\eta_{-1}^{\otimes m}(B) = -B = 3B$. En consecuencia, las representaciones 2-ádicas de $\eta_{-1}^{\otimes m}(A)$ y $\eta_{-1}^{\otimes m}(B)$ son

$$\begin{aligned}
\eta_{-1}^{\otimes m}(A) &= r_0(A) + 2r_1(B), \\
\eta_{-1}^{\otimes m}(B) &= r_0(B) + 2(r_0(B) \oplus r_1(B)).
\end{aligned}$$

Por lo tanto, se sigue del Lema 3.3.1 que

$$\left(\phi \circ \eta_{-1}^{\otimes m}\right)(Z) = \phi\left(\eta_{-1}^{\otimes m}(A) + \eta_{-1}^{\otimes m}(B)\right) = \phi(A) \oplus \phi(3B).$$

Además, por definición, tenemos que

$$\begin{aligned}
\phi(A) &= (r_1(A) | r_1(A) \oplus r_0(A)) \in \mathbb{F}_2^{2mn}, \\
\phi(B) &= (r_0(B) \oplus r_1(B) | r_1(B)) \in \mathbb{F}_2^{2mn}.
\end{aligned}$$

Observe que $\phi(A)$ es un vector que tiene ceros en aquellas coordenadas cuyo subíndice está en $I(2m,n)$ y, por lo tanto, $\widetilde{\pi}(A) = A$. De manera similar, note que $\phi(B)$ es un vector que tiene ceros en las coordenadas con subíndice en $J(2m,n)$. En consecuencia, la acción de $\widetilde{\pi}$ sobre $\phi(B)$ resulta en intercambiar sus dos mitades, es decir,

$$\widetilde{\pi}(\phi(B)) = (r_1(B) \oplus r_0(B) | r_1(B)) = \phi(3B).$$

Así,

$$\begin{aligned}
\left(\phi \circ \eta_{-1}^{\otimes m}\right)(Z) &= \phi(A) \oplus \phi(3B) \\
&= \widetilde{\pi}(\phi(A)) \oplus \widetilde{\pi}(\phi(B)) \\
&= \widetilde{\pi}(\phi(A) \oplus \phi(B)) \\
&= \widetilde{\pi}(\phi(Z)),
\end{aligned}$$

donde la última igualdad se sigue del Lema 3.3.1. □

Como consecuencia inmediata de la Proposición 3.4.1, tenemos el siguiente resultado, el cual es la versión para la isometría Φ de Gray de las relaciones (2) y (4) del Teorema 3.3.4.

Proposición 3.4.2. *Sean $k,m,n \geq 1$ enteros, $\lambda = 1+2^k \in \mathbb{Z}_{2^{k+1}}$ y $\widetilde{\pi}$ la permutación sobre $\mathbb{F}_2^{2^k mn}$ inducida por la permutación*

$$\pi = \begin{pmatrix} n-1 & (2^{k-1}m+1)n-1 \end{pmatrix} \begin{pmatrix} 2n-1 & (2^{k-1}m+2)n-1 \end{pmatrix} \cdots \begin{pmatrix} 2^{k-1}mn-1 & 2^k mn-1 \end{pmatrix}.$$

Entonces

(1) $\Phi \circ \eta_\lambda^{\otimes m} = \widetilde{\pi} \circ \Phi$

(2) *Para todo $k \geq 2$ y $\gamma \in \{\delta_1, \delta_2\}$,*

$$\Phi \circ \eta_\gamma^{\otimes m} = \widetilde{\pi} \circ \Phi \circ \eta_{\lambda\gamma}^{\otimes m}.$$

Demostración. La primera relación se sigue inmediatamente de (3.21) y la Proposicón 3.4.1; la segunda es consecuencia de (3.20) y la Proposición 3.4.1. □

Una expresión que describa la acción de evaluar a la isometría ϕ de Gray en el corrimiento negacíclico fue demostrada en la Proposición 3.4 de [54]. La prueba que aquí daremos de este resultado difiere de la que fue presentada en [54].

Proposición 3.4.3. *Sea ν el corrimiento negacíclico sobre $\mathbb{Z}_4^n$ y σ el corrimiento cíclico sobre $\mathbb{F}_2^{2n}$. Entonces*

$$\phi \circ \nu = \sigma \circ \phi.$$

Demostración. Tomando $k = m = 1$ en la Proposición 3.4.2, obtenemos

$$(\phi \circ \eta_{-1})(Z) = (\widetilde{\pi} \circ \phi)(Z) \qquad \forall Z \in \mathbb{Z}_4^n.$$

Esto implica que

$$\left(\sigma^{\otimes 2} \circ \phi \circ \eta_{-1}\right)(Z) = \left(\sigma^{\otimes 2} \circ \widetilde{\pi} \circ \phi\right)(Z) \qquad \forall Z \in \mathbb{Z}_4^n.$$

Además, por la Proposición 3.2.4, $\sigma^{\otimes 2} \circ \phi = \phi \circ \sigma$ y, por lo tanto,

$$(\phi \circ \nu)(Z) = \left(\sigma^{\otimes 2} \circ \widetilde{\pi} \circ \phi\right)(Z) \qquad \forall Z \in \mathbb{Z}_4^n.$$

De este modo, para finalizar la prueba, es suficiente probar que

$$\left(\sigma^{\otimes 2} \circ \widetilde{\pi}\right)(A) = \sigma(A) \qquad \forall A \in \mathbb{F}_2^{2n}.$$

Sea $A = (a_0, \ldots, a_{n-2}, a_{n-1}, a_n, \ldots, a_{2n-2}, a_{2n-1}) \in \mathbb{F}_2^{2n}$. Entonces

$$\widetilde{\pi}(A) = (a_0, \ldots, a_{n-2}, a_{2n-1}, a_n, \ldots, a_{2n-2}, a_{n-1})$$

y, en consecuencia,

$$\sigma^{\otimes 2}(\widetilde{\pi}(A)) = (a_{2n-1}, a_0, \ldots, a_{n-2}, a_{n-1}, a_n, \ldots, a_{2n-2}),$$

lo cual es precisamente $\sigma(A)$. □

Es natural preguntarnos si el resultado anterior puede generalizarse para el corrimiento casi-negacíclico de la siguiente manera: $\phi \circ \nu^{\otimes m} = \sigma^{\otimes m} \circ \phi$, donde $m \geq 1$ es un entero. Basta un ejemplo para mostrar que, en general, esto no es cierto.

Ejemplo 3.4.4. Sea $m = 2$ y considere al vector $Z = (1,3,1,2,2,1) \in \mathbb{Z}_4^6$. Entonces

$$(\phi \circ \nu^{\otimes 2})(Z) = \phi(3,1,3,3,2,2) = (1,0,1,1,1,1,0,1,0,0,1,1)$$

y

$$\phi(Z) = (0,1,0,1,1,0,1,0,1,1,1,1).$$

Aplicando $\sigma^{\otimes 2}$ a $\phi(Z)$ obtenemos

$$(\sigma^{\otimes 2} \circ \phi)(Z) = (0,0,1,0,1,1,1,1,0,1,1,1),$$

lo cual resulta ser distinto de $(\phi \circ \nu^{\otimes 2})(Z)$. Sin embargo, observe que al aplicar la permutación $\widetilde{\pi}_1 = (0,9)(3,6)$ sobre los subíndices de las coordenadas de $(\sigma^{\otimes 2} \circ \phi)(Z)$ se obtiene $(\phi \circ \nu^{\otimes 2})(Z)$, es decir, para el vector Z dado, la siguiente relación es válida: $(\phi \circ \nu^{\otimes 2})(Z) = (\widetilde{\pi}_1 \circ \sigma^{\otimes 2} \circ \phi)(Z)$.

A continuación presentaremos dos formas de generalizar la igualdad $\phi \circ \nu = \sigma \circ \phi$. La primera forma se sigue de la definición de la función $f^{\otimes m}$ introducida en la sección 1.1 de este manuscrito.

Proposición 3.4.5. *Sean $n, m \geq 1$ enteros, $\nu^{\otimes m}$ el corrimiento negacíclico de índice m sobre $\mathbb{Z}_4^n$ y $\sigma^{\otimes m}$ el corrimiento cíclico de índice m sobre $\mathbb{F}_2^{2n}$. Entonces*

$$\phi^{\otimes m} \circ \nu^{\otimes m} = \sigma^{\otimes m} \circ \phi^{\otimes m}.$$

Demostración. Basta recordar que $(f \circ g)^{\otimes m} = f^{\otimes m} \circ g^{\otimes m}$ para cualesquiera funciones f y g tales que la composición $f \circ g$ esté bien definida. □

En los siguientes capítulos usaremos la identidad establecida en la Proposición 3.4.5 para relacionar de manera adecuada códigos sobre $\mathbb{Z}_4$ con códigos binarios.

La segunda forma de generalizar la relación $\phi \circ \nu = \sigma \circ \phi$ es usando la identidad $\phi \circ \sigma^{\otimes s} = \sigma^{\otimes 2s} \circ \phi$ (Proposición 3.2.4). Además de esto, se requiere de la siguiente permutación. Sea π_1 la permutación sobre el conjunto I_{2mn} definida como

$$\pi_1 = (0,(m+1)n)\,(n,mn)\,(2n,(m+3)n)\,(3n,(m+2)n)\cdots \\ \cdots((m-2)n,(2m-1)n)\,((m-1)n,(2m-2)n)\,. \quad (3.24)$$

Por ejemplo, si $m=2$ y $n=3$, entonces $\pi_1 = (0,9)(3,6)$. Recuerde que en el Ejemplo 3.4.4 notamos que $(\phi \circ \nu^{\otimes 2})(Z) = (\widetilde{\pi}_1 \circ \sigma^{\otimes 2} \circ \phi)(Z)$, donde $Z = (1,3,1,2,2,1) \in \mathbb{Z}_4^6$ y $\widetilde{\pi}_1$ es la permutación sobre $\mathbb{F}_2^{12}$ inducida por π_1. La siguiente afirmación establece que esto no es una mera coincidencia.

Proposición 3.4.6. *Sean $n,m \geq 1$ enteros. Entonces*

$$\phi \circ \nu^{\otimes m} = \widetilde{\pi}_1 \circ \sigma^{\otimes m} \circ \phi,$$

donde $\widetilde{\pi}_1$ es la permutación sobre $\mathbb{F}_2^{2mn}$ inducida por la permutación π_1 definida en (3.24)*.*

Demostración. De la Proposición 3.4.1 sabemos que $\phi \circ \eta_{-1}^{\otimes m} = \widetilde{\pi} \circ \phi$, donde $\widetilde{\pi}$ es la permutación sobre $\mathbb{F}_2^{2mn}$ inducida por la permutación π definida en (3.23). Por lo tanto,

$$\sigma^{\otimes 2m} \circ \phi \circ \eta^{\otimes m} = \sigma^{\otimes m} \circ \widetilde{\pi} \circ \phi,$$

lo cual implica que

$$\phi \circ \nu^{\otimes m} = \sigma^{\otimes 2m} \circ \widetilde{\pi} \circ \phi.$$

Así, solo resta encontrar una expresión en términos de $\sigma^{\otimes m}$ para la permutación $\sigma^{\otimes 2m} \circ \widetilde{\pi}$. Es fácil convencerse de que $\left(\sigma^{\otimes 2m} \circ \widetilde{\pi}\right)(Z) = \left(\widetilde{\pi}_1 \circ \sigma^{\otimes m}\right)(Z)$, donde $Z \in \mathbb{F}_2^{2mn}$ y $\widetilde{\pi}_1$ es la permutación sobre $\mathbb{F}_2^{2mn}$ inducida por la permutación π_1 definida en (3.24). □

Como consecuencia de la Proposición 3.4.6 tenemos la siguiente Proposición, la cual es la versión para la isometría Φ de Gray de los Teoremas 3.3.3 y 3.3.4.

Teorema 3.4.7. *Sean $k,m,n \geq 1$ enteros, $\lambda = 1+2^k \in \mathbb{Z}_{2^{k+1}}$ y $\widetilde{\pi}_1$ la permutación sobre $\mathbb{F}_2^{2^k mn}$ inducida por la permutación π_1 definida como*

$$\pi_1 = \begin{pmatrix} 0 & (2^{k-1}m+1)n \end{pmatrix} \begin{pmatrix} n & 2^{k-1}mn \end{pmatrix} \begin{pmatrix} 2n & (2^{k-1}m+3)n \end{pmatrix} \begin{pmatrix} 3n & (2^{k-1}m+2)n \end{pmatrix} \cdots \\ \cdots \begin{pmatrix} (2^{k-1}-2)n & (2^k m-1)n \end{pmatrix} \begin{pmatrix} (2^{k-1}m-1) & (2^k m-2)n \end{pmatrix} \quad (3.25)$$

Entonces

(1) $\Phi \circ \nu_{\lambda}^{\otimes m} = \widetilde{\pi}_1 \circ \sigma^{\otimes 2^{k-1}m} \circ \Phi$.

(2) *Para todo* $k \geq 2$ *y* $\gamma \in \{\delta_1, \delta_2\}$,

$$\Phi \circ \nu_{\gamma}^{\otimes m} = \widetilde{\pi}_1 \circ \sigma^{\otimes 2^{k-1}m} \circ \Phi \circ \eta_{\lambda\gamma}^{\otimes m}.$$

Demostración. La primera relación es consecuencia de (3.22) y de la Proposición 3.4.6; la segunda se sigue de (3.20) y la Proposición 3.4.6. □

A través de este capítulo hemos estudiado diferentes relaciones en las que se ven involucradas las isometrías φ, Φ de Gray y los distintos corrimientos γ-casi-cíclicos. Asimismo, introducimos el $\mathbb{Z}_{2^{k+1}}$-automorfismo $\eta_\gamma : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}_{2^{k+1}}^n$ y estudiamos sus relaciones con las isometrías φ, Φ y los corrimientos γ-casi-cíclicos. Cada una de estas relaciones formarán parte fundamnetal de los siguientes capítulos, en los que describiremos propiedades de las imágenes bajo φ y Φ de códigos sobre $\mathbb{Z}_{2^{k+1}}$. Estos serán los principales resultados de este trabajo.

Capítulo 4

Imágenes de códigos casi-cíclicos y $(1+2^k)$-casi-cíclicos

En el presente Capítulo investigaremos propiedades de casi-ciclicidad y casi-negaciclicidad de las imágenes, bajo las isometrías φ y Φ de Gray, de códigos casi-cíclicos y $(1+2^k)$-casi-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$. Introduciremos una isometría Φ_1, permutación-equivalente a la isometría Φ de Gray, que nos permitirá definir la isometría de Gray-Nechaev sobre $\mathbb{Z}_{2^{k+1}}$ y estudiar propiedades de casi-ciclicidad de la imagen de Gray de códigos $(1+2^k)$-casi-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$. Incluiremos caracterizaciones de aquellos códigos que son casi-cíclicos y $(1+2^k)$-casi-cíclicos. En este tema, obtendremos resultados más específicos para los códigos que sean cíclicos y $(1+2^k)$-cíclicos lineales de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$. Varios de los resultados presentados en este apartado van en la dirección de los trabajos [51, 52, 54, 55]. En particular, demostraremos que la imagen bajo Φ_1 de un código cíclico lineal de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$ es un código binario casi-cíclico de índice $2^{k-1}n$. Estos resultados generalizan las principales aportaciones de [52] y [54]. Además, como una aplicación de nuestras aportaciones, obtendremos propiedades de casi-ciclicidad y casi-negaciclicidad de los códigos de Reed-Muller $\mathrm{ZRM}(r,s)$ sobre $\mathbb{Z}_4$, donde $s \geq 1$ y $r \in \{0,1,2,s-1,s\}$.

4.1. Introducción

Los códigos consta-cíclicos sobre campos finitos con p elementos (p primo impar), fueron introducidos en [7] como una generalización de los códigos cíclicos. En particular, en [7], para los códigos negacíclicos se diseñó un algortimo capaz de corregir todos los patrones de error con peso de Lee $t \leq \lfloor (p-1)/2 \rfloor$, lo que hace interesante a esta clase de códigos. Sin embargo, dado que la métrica de Lee depende de la estructura del anillo, este algoritmo se restringe a los campos finitos con p elementos. En consecuencia, los códigos negacíclicos sobre anillos finitos, e incluso sobre campos finitos con p^m elementos, no recibieron mucha atención.

No obstante, después de la realización de [23, 40], en [54, 55] los códigos negacíclicos sobre el anillo $\mathbb{Z}_4$ tomaron un papel diferente. En [54, 55], se demostró que la imagen de Gray de un código negacíclico sobre $\mathbb{Z}_4$ es un código binario cíclico. Asimismo, se probó que los códigos negacíclicos lineales de longitud impar sobre $\mathbb{Z}_4$ están en correspondencia biyectiva con los códigos cíclicos lineales de la misma longitud sobre $\mathbb{Z}_4$, lo que estableció una relación entre códigos cíclicos lineales de longitud n impar y códigos cíclicos binarios (no necesariamente lineales) de longitud $2n$, a través de la llamada *isometría de Nechaev-Gray*. Este resultado explicó satisfactoriamente el porqué los códigos de Kerdock, Preparata, entre otros,

están relacionados con códigos cíclicos lineales de longitud impar sobre $\mathbb{Z}_4$. Desde entonces, códigos negacíclicos y, en general, códigos consta-cíclicos sobre anillos finitos, han sido investigados por muchos autores en conexión con códigos casi-cíclicos sobre campos finitos [8,9,13,21,29,33,35,50–52,56,57,59]. En particular, algunos de los resultados presentados en [54,55] fueron generalizados en [51,52] para códigos $(1+2^k)$-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, $k \geq 1$.

El propósito de este capítulo es generalizar algunos de los resultados de [52] y [54] a la familia de códigos $(1+2^k)$-casi-cíclicos de índice $m \geq 1$ y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$. Por supuesto, si $m = 1$, nuestros resultados permiten recuperar las aportaciones de [52] y, si además tomamos $k = 1$, entonces obtendremos algunos de los principales resultados de [54].

El contenido de este capítulo está organizado de la siguiente manera. En la Sección 4.2 investigaremos propiedades de casi-ciclicidad de las imágenes, bajo las isometrías φ y Φ de Gray, de códigos casi-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$. En específico, demostraremos que $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^{mn}$ es un código casi-cíclico de índice m si y sólo si los códigos $\varphi(\mathscr{C}) \subseteq \mathbb{Z}_4^{2^{k-1}mn}$ y $\Phi(\mathscr{C}) \subseteq \mathbb{F}^{2^k mn}$ son códigos casi-cíclicos de índices $2^{k-1}m$ y $2^k m$, respectivamente. En la sección 4.3 aplicaremos los resultados de la Sección 4.2 para obtener propiedades de casi-ciclicidad de los códigos de Reed-Muller $\mathrm{ZRM}(r,s)$ sobre $\mathbb{Z}_4$, donde $s \geq 1$ y r es un elemento del conjunto $\{0,1,2,s-1,s\}$.

En la Sección 4.4 probaremos que un subconjunto $\mathscr{D} \subseteq \mathbb{Z}_{2^{k+1}}^{mn}$ es un código $(1+2^k)$-casi-cíclico de índice m si y sólo si $\varphi(\mathscr{D}) \subseteq \mathbb{Z}_4^{2^{k-1}mn}$ es un código casi-negacíclico de índice $2^{k-1}m$. Además, caracterizaremos aquellos códigos que son casi-cíclicos y $(1+2^k)$-casi-cíclicos. En particular, en la Sección 4.5, enfocaremos nuestra atención a los códigos cíclicos lineales de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$ que son al mismo tiempo $(1+2^k)$-cíclicos y, en consecuencia, la imagen bajo φ de estos códigos será un código casi-negacíclico. Sin embargo, en la búsqueda de resultados más generales, en la Sección 4.6, probaremos que la imagen, con respecto a la isometría φ, de un código cíclico lineal de longitud impar, puede ser transformada a un código casi-negacíclico. En particular, esto generaliza la Proposición 3.7 de [54].

En la Sección 4.7 iniciamos el estudio de las propiedades de la imagen de Gray de los códigos $(1+2^k)$-casi-cíclicos. Veremos que, si $\mathscr{D}$ es un código λ-casi-cíclico, entonces $\Phi(\mathscr{D})$ no tiene propiedades de casi-ciclicidad pero que sí es permutación-equivalente a un código casi-cíclico. Esto nos premite introducir una isometría $\Phi_1 : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{F}_2^{2^k n}$, permutación-equivalente a la isometría Φ de Gray, y demostrar que $\mathscr{D} \subseteq \mathbb{Z}_{2^{k+1}}^{mn}$ es un código $(1+2^k)$-casi-cíclico de índice m si y sólo si $\Phi_1(\mathscr{D}) \subseteq \mathbb{F}^{2^k mn}$ es un código casi-cíclico de índice $2^{k-1}m$. Consecuentemente, probaremos que la imagen bajo Φ_1 de un código cíclico lineal de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$ es un código binario casi-cíclico de índice 2^{k-1}. Esto generaliza el Teorema 3.9 de [54].

Finalmente, en la Sección 4.8, estudiaremos la imagen de Gray-Nechaev de códigos cíclicos lineales de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$. Una nueva caracterización de aquellos códigos cíclicos lineales que son a su vez $(1+2^k)$-cíclicos es obtenida via la permutación de Nechaev.

4.2. Imágenes de códigos casi-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$

En esta sección emplearemos las relaciones del Capítulo 3 para estudiar propiedades de casi-ciclicidad de los códigos $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$, donde $\mathscr{C}$ es un código casi-cíclico de índice $m \geq 1$ y longitud $mn \geq 1$ sobre $\mathbb{Z}_{2^{k+1}}$. Recuerde que un código casi-cíclico es un código γ-casi-cíclico con $\gamma = 1$. Resultados que estudien algunas propiedades de casi-ciclicidad de la imagen con respecto a las isometrías φ y Φ de códigos γ-casi-cíclicos, con $\gamma = \lambda = 1+2^k$, $\gamma = \delta_1 = 1+2^{k-1}$ y $\gamma = \delta_2 = 1+2^{k-1}+2^k$, serán abordados en los siguientes capítulos de este manuscrito.

Como una aplicación del Teorema 3.2.5 se tiene otra aportación de este trabajo, la cual hace una conexión entre códigos casi-cíclicos de cualquier longitud sobre el anillo $\mathbb{Z}_{2^{k+1}}$ y códigos casi-cíclicos de longitud par sobre $\mathbb{Z}_4$ y el campo $\mathbb{F}_2$.

Teorema 4.2.1. *Para cualesquiera enteros $k,m,n \geq 1$ y cualquier código $\mathscr{C}$ de longitud mn sobre $\mathbb{Z}_{2^{k+1}}$, las siguientes afirmaciones son equivalentes:*

(1) *$\mathscr{C}$ es casi-cíclico de índice m.*

(2) *$\varphi(\mathscr{C})$ es un código casi-cíclico de índice $2^{k-1}m$ y longitud $2^{k-1}mn$ sobre $\mathbb{Z}_4$.*

(3) *$\Phi(\mathscr{C})$ es un código binario casi-cíclico de índice $2^k m$ y longitud $2^k mn$.*

Demostración. Observe que tomando $\gamma = 1$ en el Teorema 3.2.5 se obtienen las siguientes relaciones

$$\varphi \circ \sigma^{\otimes m} = \sigma^{\otimes 2^{k-1}m} \circ \varphi \tag{4.1}$$

y

$$\Phi \circ \sigma^{\otimes m} = \sigma^{\otimes 2^k m} \circ \Phi. \tag{4.2}$$

Supongamos que $\mathscr{C}$ es un código casi-cíclico de índice m y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$. Entonces, de acuerdo a la ecuación (4.1), se tiene que

$$\varphi(\mathscr{C}) = \varphi(\sigma^{\otimes m}(\mathscr{C})) = \sigma^{\otimes 2^{k-1}m}(\varphi(\mathscr{C})), \tag{4.3}$$

de donde se concluye que $\varphi(\mathscr{C})$ es un código casi-cíclico de índice $2^{k-1}m$ y longitud $2^{k-1}mn$. Esto prueba que (1) implica (2). Supongamos ahora que $\varphi(\mathscr{C})$ satisface el punto (2) del Teorema 4.2.1. Aplicando la isometría ϕ de Gray (sobre $\mathbb{Z}_4$) en ambos lados de la relación (4.3), y dado que $\Phi = \phi \circ \varphi$ (Proposición 2.2.12), se tiene que $\Phi(\mathscr{C}) = \left(\phi \circ \sigma^{\otimes 2^{k-1}m}\right)(\varphi(\mathscr{C}))$. Como $\phi \circ \sigma^{\otimes 2^{k-1}m} = \sigma^{\otimes 2^k m} \circ \phi$ (Proposición 3.2.4), entonces

$$\Phi(\mathscr{C}) = \sigma^{\otimes 2^k m}(\Phi(\mathscr{C})),$$

es decir, $\Phi(\mathscr{C})$ es un código binario casi-cíclico de índice $2^k m$ y longitud $2^k mn$. Así, (2) implica (3). Finalmente, supongamos que tenemos la condición (3) del Teorema 4.2.1. Entonces

$$\Phi(\mathscr{C}) = \sigma^{\otimes 2^k m}(\Phi(\mathscr{C})).$$

Note que de (4.2) se deduce que

$$\sigma^{\otimes 2^k m}(\Phi(\mathscr{C})) = \Phi(\sigma^{\otimes m}(\mathscr{C})).$$

Así, $\Phi(\mathscr{C}) = \Phi(\sigma^{\otimes m}(\mathscr{C}))$. Dado que la isometría Φ de Gray es inyectiva (Proposición 2.1.9), se concluye que $\mathscr{C} = \sigma^{\otimes m}(\mathscr{C})$. Esto demuestra que (3) implica (1). □

Los siguientes ejemplos ilustran el Teorema 4.2.1 y se aprovechan para revisar algunos aspectos referentes a la linealidad de los códigos $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$, donde $\mathscr{C}$ es un código casi-cíclico (no necesariamente lineal) sobre $\mathbb{Z}_{2^{k+1}}$. Estas cuestiones tienen sentido pues, como se ha mencionado, las aplicaciones φ y Φ no son funciones lineales y, por lo tanto, $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$ pueden ser códigos lineales o no, sin importar si $\mathscr{C}$ es lineal o no.

Para mayor claridad en la presentación de los ejemplos, el vector $(x_0, x_1, \ldots, x_{n-1}) \in R^n$ será escrito como $x_0 x_1 \cdots x_{n-1}$.

Ejemplo 4.2.2. Sean $k = 2$, $n = 3$, $m = 1$ y considérese al código $\mathscr{C} = \{157, 715, 571\} \subseteq \mathbb{Z}_8^3$. Obviamente $\mathscr{C}$ es un código cíclico y, por lo tanto, se sigue del Teorema 4.2.1 que el código $\varphi(\mathscr{C})$ (resp. $\Phi(\mathscr{C})$) es casi-cíclico de índice 2 (resp. 4) y longitud 6 (resp. 12). Para constatar esto, las correspondientes imágenes de los elementos de $\mathscr{C}$ con repecto a φ y Φ son:

$$\begin{array}{ccccc} & \varphi & & \phi & \\ 157 & \longrightarrow & 133\ 131 & \longrightarrow & 011\ 010\ 100\ 101 \\ 715 & \longrightarrow & 313\ 113 & \longrightarrow & 101\ 001\ 010\ 110 \\ 571 & \longrightarrow & 331\ 311 & \longrightarrow & 110\ 100\ 001\ 011 \end{array}$$

Ya que $000 \notin \mathscr{C}$, los códigos $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$ no son lineales. Asimismo, observe que $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$ no son códigos cíclicos. Por lo tanto, en este Ejemplo se presenta un código cíclico no lineal sobre $\mathbb{Z}_8$ cuyas imágenes, con respecto de las isometrías φ y Φ, no son lineales ni cíclicas.

Ejemplo 4.2.3. Sean k, n, m como en el Ejemplo anterior y sea $\mathscr{C} = \{000, 444, 555, 111\}$. Claramente, este código es cíclico. En consecuencia, por el Teorema 4.2.1, $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$ son códigos casi-cíclicos de índices 2 y 4, y longitudes 6 y 12, respectivamente. Los elementos de los códigos $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$ son:

$$\begin{array}{ccccc} & \varphi & & \phi & \\ 000 & \longrightarrow & 000\ 000 & \longrightarrow & 000\ 000\ 000\ 000 \\ 111 & \longrightarrow & 111\ 111 & \longrightarrow & 000\ 000\ 111\ 111 \\ 444 & \longrightarrow & 222\ 222 & \longrightarrow & 111\ 111\ 111\ 111 \\ 555 & \longrightarrow & 333\ 333 & \longrightarrow & 111\ 111\ 000\ 000 \end{array}$$

Como $555, 111 \in \mathscr{C}$ pero $555+111 = 666 \notin \mathscr{C}$, este código no es lineal. Sin embargo, es fácil verificar que los códigos $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$ son códigos lineales. Además de esto, note que $\varphi(\mathscr{C})$ es un código cíclico. Consecuentemente, $\Phi(\mathscr{C})$ también es casi-cíclico de índice 2 y longitud 12. En resumen, este ejemplo presenta un código no lineal sobre $\mathbb{Z}_8$ cuyas imágenes, con respecto a las isometrías φ y Φ, son lineales. En el caso de la imagen bajo φ se tiene un código cíclico y en el caso de Gray se tiene un código casi-cíclico de índice 2.

Los siguientes dos ejemplos son de códigos cíclicos lineales de longitud 3 sobre $\mathbb{Z}_8$. La construcción de estos códigos fue realizada por medio de los resultados presentados en la Sección 1.1.3 de este trabajo. Siendo más específicos, recuerde que si I es un ideal de $\mathbb{Z}_8[x]/\langle x^3-1\rangle$, entonces existe una única colección de polinomios mónicos y coprimos f_0, f_1, f_2, f_3 tales que $f_0 f_1 f_2 f_3 = x^3-1$ e $I = \langle \widehat{F}_1, 2\widehat{F}_2, 2^2\widehat{F}_3\rangle$, donde $\widehat{F}_j = \widehat{f}_j + \langle x^3-1\rangle$ y $\widehat{f}_j = (x^3-1)/f_j$. Asimismo, recuerde que si $\mathscr{C} = P^{-1}(I)$, donde P es la representación polinomial, entonces a los polinomios $\widehat{F}_1, 2\widehat{F}_2, 2^2\widehat{F}_3$ les llamamos los generadores de $\mathscr{C}$, es decir, $\mathscr{C} = \langle \widehat{F}_1, 2\widehat{F}_2, 2^2\widehat{F}_3\rangle$.

Anteriormente se estableció que la factorización de $x^3-1 \in \mathbb{Z}_8[x]$ como un producto de polinomios mónicos, básicos irreducibles y coprimos es $x^3-1 = (x-1)(x^2+x+1)$. Defina $a_1(x) = x-1$ y $a_2(x) = x^2+x+1$.

Ejemplo 4.2.4. Con la notación previa, sean $f_0 = a_1(x), f_1 = 1, f_2 = a_2(x)$ y $f_3 = 1$. Entonces $\widehat{F}_0 = a_2(x), \widehat{F}_1 = 0, \widehat{F}_3 = a_1(x)$ y $\widehat{F}_3 = 0$ y, por lo tanto, $\mathscr{C} = \langle \widehat{F}_1, 2\widehat{F}_2, 2^2\widehat{F}_3\rangle = \langle 2a_1(x)\rangle$ es un código cíclico lineal de longitud 3 sobre $\mathbb{Z}_8$. Los elementos de $\mathscr{C}$ son:

602 404 466 062 620 206 440 044
646 664 000 260 224 422 026 242

Por el Teorema 4.2.1, el código $\varphi(\mathscr{C})$ es casi-cíclico de índice 2 y longitud 6. Los elementos de este código son:

000000 002200 202202 200002 002020 002222 200222 200020
022022 020222 220220 222020 020002 020200 222200 222002

Note que los vectores 222200 y 222002 pertenecen al código $\varphi(\mathscr{C})$ y que su suma sobre $\mathbb{Z}_4^6$ es el vector 000202, el cual no pertence a $\varphi(\mathscr{C})$. Por lo tanto, $\varphi(\mathscr{C})$ no es un código lineal. Asimismo, note que $\sigma(200002) = 220000 \notin \varphi(\mathscr{C})$, lo cual implica que $\varphi(\mathscr{C})$ no es un código cíclico. Por otro lado, sabemos del Teorema 4.2.1 que el código $\Phi(\mathscr{C})$ es casi-cíclico de índice 4 y longitud 12. Los elementos de $\Phi(\mathscr{C})$ son:

000000000000 001100001100 101101101101 100001100001
001010001010 001111001111 100111100111 100010100010
011011011011 010111010111 110110110110 111010111010
010001010001 010100010100 111100111100 111001111001

Como antes, note que los vectores 111100111100 y 111001111001 están en el código $\Phi(\mathscr{C})$ pero su suma binaria, el vector 000101000101, no pertenece a $\Phi(\mathscr{C})$. Por lo tanto, $\Phi(\mathscr{C})$ no es un código lineal. Además, observe que $\Phi(\mathscr{C})$ no es un código cíclico pues $100001100001 \in \Phi(\mathscr{C})$ pero $\sigma(100001100001) = 110000110000 \notin \Phi(\mathscr{C})$. En conclusión, el actual Ejemplo, presenta un código cíclico lineal $\mathscr{C}$ de longitud 3 sobre $\mathbb{Z}_8$ tal que los códigos $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$ no son lineales y tampoco cíclicos.

En los Ejemplos 4.2.2 y 4.2.4 presentamos dos códigos cíclicos sobre $\mathbb{Z}_8$ tales que sus imágenes bajo φ y Φ son códigos que no tienen la propiedad de ser cíclicos. Esto implica que la propiedad de ciclicidad no puede reemplazar a la propiedad de casi-ciclicidad del Teorema 4.2.1.

Ejemplo 4.2.5. Siguiendo con la notación anterior, sean ahora $f_0 = a_2(x), f_1 = 1, f_2 = a_1(x)$ y $f_3 = 1$. Con esta elección de los polinomios f_i, construimos un código cíclico lineal $\mathscr{C}$ de longitud 3 sobre $\mathbb{Z}_8$ generado por $\widehat{F_1} = 0, \widehat{F_2} = a_2(x)$ y $\widehat{F_3} = 0$, es decir,

$$\mathscr{C} = \langle 2a_2(x) \rangle = \langle 2x^2 + 2x + 2 \rangle \subseteq \mathbb{Z}_{2^3}[x]/\langle x^3 - 1 \rangle.$$

Ya que $\mathscr{C}$ es cíclico, se sigue del Teorema 4.2.1 que los códigos $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$ son casi-cíclicos de índices 2 y 4, y longitudes 8 y 16, respectivamente. Los elementos de estos códigos son:

	φ		ϕ	
000	$\longrightarrow$	0000 0000	$\longrightarrow$	0000 0000 0000 0000
222	$\longrightarrow$	0000 2222	$\longrightarrow$	0000 1111 0000 1111
444	$\longrightarrow$	2222 2222	$\longrightarrow$	1111 1111 1111 1111
666	$\longrightarrow$	2222 0000	$\longrightarrow$	1111 0000 1111 0000

De aquí, es fácil convencerse que los códigos $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$ son lineales pero no cíclicos.

Hasta este punto se han presentado algunos códigos cíclicos sobre $\mathbb{Z}_8$ para los que se analiazaron propiedades de linealidad, y en los que también se ilustró que la condición de casi-ciclicidad no puede ser reemplazada por la propiedad de ciclicidad en las afirmaciones (2) y (3) del Teorema 4.2.1. En el Apéndice A, el lector encontrará tablas de códigos cíclicos de longitudes 3, 5 y 7 sobre $\mathbb{Z}_8$, y longitudes 3, 5 sobre $\mathbb{Z}_{16}$, en las que también se calculan sus pesos homogéneos y se señalan cuáles de ellos son *códigos óptimos*. Aquí, *código óptimo* significa que no esxiste otro código de la misma longitud y cardinalidad que tenga mayor distancia mínima.

Por los ejemplos anteriores, tiene sentido preguntarse qué propiedades debe tener un código $\mathscr{C}$ (lineal o no) sobre $\mathbb{Z}_{2^{k+1}}$ para que los códigos $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$ sean lineales. Para el caso de códigos lineales sobre $\mathbb{Z}_4$, el Teorema 5 de [23] presenta una condición necesaria y suficiente para que esto suceda. Una generalización al anillo $\mathbb{Z}_{2^{k+1}}$ del Teorema 5 de [23] es presentada

en [51] y, por lo tanto, en este material no estudiaremos qué condiciones son necesarias o suficientes para que las imágenes bajo φ y Φ sean lineales. Sin embargo, vale la pena mencionar que muy poco se sabe de este problema cuando el anillo es de Galois o finito de cadena. Un reciente trabajo relacionado con este tema es [36], el cual es una continuación de [35]. No obstante, nuestro interés al presentar en los Ejemplos 4.2.2 - 4.2.5 un breve análisis de la linealidad y ciclicidad de los códigos $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$, es para ejemplificar en las futuras secciones que es posible conseguir "buenas propiedades" en los códigos $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$ (tales como la linealidad o ciclicidad) si en lugar de considerar únicamente a los códigos cíclicos, consideramos también a los códigos γ-cíclicos o γ-casi-cíclicos, donde $\gamma \neq 1$ es una unidad en el anillo $\mathbb{Z}_{2^{k+1}}$.

Por otra parte, seguramente el lector ya se percató que no se presentó un ejemplo de un código $\mathscr{C}$ tal que $\varphi(\mathscr{C})$ sea lineal y $\Phi(\mathscr{C})$ no lo sea (o viceversa). Por el Teorema 4.11 de [52], existe un código no lineal que ilustrara este hecho para las isometrías φ^k y de Gray introducidas en ese trabajo. Dado que las isometrías φ^k y de Gray introducidas en [52], y las isometrías φ y Φ que hemos definido en este trabajo son equivalentes, los resultados de [52] también aplican para φ y Φ. Por lo tanto, por el Teorema 4.11 de [52], podemos afirmar que existe un código no lineal $\mathscr{C}$ tal que $\varphi(\mathscr{C})$ sea lineal pero que $\Phi(\mathscr{C})$ no lo sea (o viceversa).

4.2.1. Dos ejemplos especiales

Los Ejemplos 4.2.2 - 4.2.5 ilustran el Teorema 4.2.1 para algunos códigos cíclicos. Sin embargo, la imagen de Gray, así como la imagen con respecto a la isometría φ de estos códigos no son códigos sobresalientes. En esta sección, presentaremos dos códigos lineales sobre $\mathbb{Z}_4$, uno cíclico y el otro casi-cíclico de índice 2, tales que sus imágenes de Gray son, respectivamente, el código extendido de Hamming $\mathscr{H}_e(3)$ y el código binario de Reed-Muller de segundo orden y longitud 16, denotado como $\mathrm{RM}(2,4)$.

Debido a que los códigos que presentaremos están definidos sobre $\mathbb{Z}_4$, únicamente hablaremos de la imagen de Gray de esos códigos, pues la isometría φ es la función identidad sobre $\mathbb{Z}_4^n$. Asimismo, nos referiremos al peso de Lee, ω_L, en lugar del peso homogéneo ya que estas funciones coinciden sobre $\mathbb{Z}_4$.

Ejemplo 4.2.6. Recordemos que el código

$$\mathscr{C}_H = \{\alpha(1111) + \beta(0202) + \gamma(0022) \ : \ \alpha,\beta,\gamma \in \mathbb{Z}_4\}$$

del Ejemplo 1.2.1 es un código cíclico lineal sobre $\mathbb{Z}_4$, de cardinalidad 16 y peso mínimo de Lee $\omega_L(\mathscr{C}_H) = 4$. La imagen de Gray de $\mathscr{C}_H$ es el siguiente código binario de longitud 8, el cual, por el Teorema 4.2.1, es casi-cíclico de índice 2:

$$\phi(\mathscr{C}_H) = \{\phi(Z) \ : \ Z = \alpha(1111) + \beta(0202) + \gamma(0022),\ \alpha,\beta,\gamma \in \mathbb{Z}_4\}.$$

Ya que $\beta(0202) = 2\beta(0101), \gamma(0022) = 2\gamma(0011)$, se sigue del Lema 2.3.4 que

$$\phi(\mathscr{C}_H) = \{\phi(\alpha(1111)) \oplus \phi(\beta(0202)) \oplus \phi(\gamma(0022)) \ : \ \alpha,\beta,\gamma \in \mathbb{Z}_4\}.$$

En otros términos, la relación anterior quiere decir que $\phi(\mathscr{C}_H)$ es el conjunto de todas las combinaciones lineales de los elementos $\phi(\alpha(1011))$, $\phi(\beta(0203))$, $\phi(\gamma(0022))$, $\alpha,\beta,\gamma \in \mathbb{Z}_4$. Obviamante, podemos eliminar los casos $\alpha \in \{0,3\}$ y $\beta,\gamma \in \{0,2,3\}$ ya que $\phi(0000) = 0000\ 0000$ y $\phi(3g) = \phi(g) \oplus \phi(2g)$ (Lema 2.3.4). Con base en estas observaciones, concluimos que $\phi(\mathscr{C}_H)$ es un código binario lineal de longitud 8 generado por los vectores $\phi(1111) = 0000\ 1111$, $\phi(0022) = 0011\ 0011$, $\phi(0202) = 0101\ 0101$ y $\phi(2(1111)) = 1111\ 1111$. Ya que estos vectores son linealmente independientes sobre $\mathbb{F}_2$, tenemos que $\phi(\mathscr{C}_H)$ es un $[8,4,4]$ código binario casi-cíclico de índice 2.

Observe que $\phi(1111) = c_0^3$, $\phi(0022) = c_1^3$, $\phi(0202) = c_2^3$ y $\phi(2(1111)) = c_3^3$. Recuerde que los vectores c_i^k se introdujeron en el Capítulo 2 para definir la isometría de Gray y que éstos forman una base del código binario de Reed-Muller de primer orden $\mathrm{RM}(1,3)$. Así, el Ejemplo 4.2.6, muestra que el código $\mathrm{RM}(1,3)$ es la imagen de Gray de un código cíclico lineal de longitud 4 sobre $\mathbb{Z}_4$. También, recuerde que en la Sección 2.1.1, se definió el código $\mathrm{RM}(1,k)$ de Reed-Muller de primer orden como el código dual del código binario extendido de Hamming $\mathscr{H}_e(k)$, es decir, $\mathrm{RM}(1,k) = \mathscr{H}_e(k)^\perp$. Para el caso $k = 3$, tenemos que el código $\phi(\mathscr{C}_H) = \mathrm{RM}(1,3) = \mathscr{H}_e(3)^\perp$. Esta observación es un caso particular del Teorema 7 de [23]; resultado al cual recurriremos más adelante para obtener propiedades de casi-ciclicidad de algunos códigos definidos sobre $\mathbb{Z}_4$.

Por otro lado, es conocido que el $[8,4,4]$ código binario extendido de Hamming $\mathscr{H}_e(3)$ es auto-dual. Esto implica que $\phi(\mathscr{C}_H) = \mathrm{RM}(1,3) = \mathscr{H}_e(3)$ y, en consecuencia, $\phi(\mathscr{C}_H)$ es un código binario auto-dual y casi-cíclico de índice 2. Es importante señalar que los códigos auto-duales son importantes desde el punto de vista teórico y práctico [42, 43]. En especial, son de particular interés aquellos códigos binarios auto-duales tales que el peso de Hamming de cada vector en el código sea un múltiplo de 4. Estos códigos son conocidos en la literatura como *códigos doblemente pares o de Tipo II* y son difíciles de encontrar. Es notable en la teoría de códigos que el único código binario doblemente par de longitud 8 es el código $\mathscr{H}_e(3)$ (cf. [42]). Finalmente, debemos mencionar que también es conocido que el código $\mathscr{H}_e(3)$ es óptimo, en el sentido de que no existe otro código binario lineal de longitud 8 y dimensión 4 con mejor distancia mínima. Más aún, este código es único, salvo equivalencia. Todas estas características hacen que el código $\phi(\mathscr{C}_H) = \mathrm{RM}(1,3) = \mathscr{H}_e(3)$ sea uno de los códigos más sobresalientes en la teoría de códigos.

Ejemplo 4.2.7. Sea $\mathrm{ZRM}(2,4)$ el código lineal de longitud 8 sobre $\mathbb{Z}_4$ generado por los siguientes vectores: $g_0 = 1111\ 1111$, $g_1 = 0000\ 1111$, $g_2 = 0011\ 0011$, $g_3 = 0101\ 0101$, $g_4 = 0000\ 0022$, $g_5 = 0000\ 0202$ y $g_6 = 0002\ 0002$. Del Ejemplo 1.2.2, sabemos que este código tiene cardinalidad 2^{11} y distancia mínima de Lee $\omega_L(\mathrm{ZRM}(2,4)) = 4$. Asimismo, sabemos que este código no es cíclico pero que sí es casi-cíclico de índice 2 (Ejemplo 1.2.2). Por lo tanto, por el Teorema 4.2.1, la imagen de Gray de $\mathrm{ZRM}(2,4)$ es un código binario casi-cíclico de índice 4 y longitud 16, el cual queda descrito como el siguiente conjunto:

$$\phi(\mathrm{ZRM}(2,4)) = \{\phi(Z) \,:\, Z = a_0g_0 + a_1g_1 + \cdots + a_6g_6,\ a_i \in \mathbb{Z}_4\}.$$

Observe que $g_4 = 2g_1 * g_2$, $g_5 = 2g_1 * g_3$ y $g_6 = g_2 * g_3$, donde "$*$" denota la multiplicación coordenada por coordenada. Usando esta observación y, aplicando sucesivamente el Lema 2.3.4, es posible demostrar que para todo $Z = a_0g_0 + a_1g_1 + \cdots + a_6g_6 \in \mathrm{ZRM}(2,4)$,

$$\phi(Z) = \phi(b_0g_0) \oplus \phi(b_1g_1) \oplus \cdots \oplus \phi(b_6g_6),$$

donde $b_0 = a_0$, $b_i = a_i + 2a_0a_i$ para $1 \leq i \leq 3$, $b_4 = a_4 + a_1a_2$, $b_5 = a_5 + a_1a_3$ y $b_6 = a_6 + a_2a_3$. Note que para a_0 fija, las aplicaciones $a_i \mapsto a_i + 2a_0a_i$ son inyectivas sobre $\mathbb{Z}_4$. De igual modo, note que para escalares $a_1, a_2, a_3 \in \mathbb{Z}_4$ fijos, las aplicaciones $a_4 \mapsto a_4 + a_1a_2$, $a_5 \mapsto a_5 + a_1a_3$ y $a_6 \mapsto a_6 + a_2a_2$ son también permutaciones sobre $\mathbb{Z}_4$. Consecuentemente, si hacemos variar los escalares a_i sobre $\mathbb{Z}_4$, entonces hacemos variar los escalres b_i sobre $\mathbb{Z}_4$. Por lo tanto, cada elemento de $\phi(\mathrm{ZRM}(2,4))$ es una combinación lineal de los vectores $\phi(b_ig_i)$ y, en consecuencia, la imagen de Gray de $\mathrm{ZRM}(2,4)$ es un código binario lineal. Para encontrar una base de $\phi(\mathrm{ZRM}(2,4))$, no es necesario considerar a los vectores $\phi(b_ig_i)$, donde $b_i \in \{0,3\}$, como generadores del código. En consecuencia, $\phi(\mathrm{ZRM}(2,4))$ es el conjunto de todas las combinaciones lineales de los siguientes vectores:

$$\begin{aligned}
\phi(2g_0) &= 1111\ 1111\ 1111\ 1111 & \phi(g_6) &= 0000\ 0011\ 0000\ 0011\\
\phi(2g_1) &= 0101\ 0101\ 0101\ 0101 & \phi(g_0) &= 0000\ 0000\ 1111\ 1111\\
\phi(2g_2) &= 0011\ 0011\ 0011\ 0011 & \phi(g_1) &= 0000\ 0000\ 0101\ 0101\\
\phi(g_3) &= 0001\ 0001\ 0001\ 0001 & \phi(g_2) &= 0000\ 0000\ 0011\ 0011\\
\phi(2g_4) &= 0000\ 1111\ 0000\ 1111 & \phi(g_4) &= 0000\ 0000\ 0000\ 1111\\
\phi(g_5) &= 0000\ 0101\ 0000\ 0101
\end{aligned}$$

Ya que estos vectores son linealmente independientes y $|\mathrm{ZRM}(2,4)| = 2^{11}$, se sigue que el conjunto $\phi(\mathrm{ZRM}(2,4))$ es un $[16,11,4]$ código binario lineal casi-cíclico de índice 4. De acuerdo a las tablas de Markus Grassl [18], este código es óptimo. Más aún, $\phi(\mathrm{ZRM}(2,4))$ es el mejor código binario lineal de longitud 16 y distancia mínima de Hamming igual a 4 que se conoce. Es decir, la cardinalidad de cualquier otro código lineal de longitud 16 y distancia mínima de Hamming igual a 4, es menor o igual a 2^{11}. En la siguiente sección, veremos que $\phi(\mathrm{ZRM}(2,4))$ es precisamente el código de Reed-Muller de segundo orden, el cual, es comunmente denotado por $\mathrm{RM}(2,4)$.

Los Ejemplos 4.2.6 y 4.2.7 dejan en claro que son de interés aquellos códigos que se pueden construir como imágenes de Gray de códigos lineales sobre anillos finitos. En particular, los anteriores ejemplos ilustran la existencia de buenos códigos obtenidos como imágenes de Gray de códigos casi-cíclicos. Así, en la búsqueda de códigos con buenos parámetros obtenidos como la imagen de la isometría de Gray, se deben considerar a los códigos casi-cíclicos. Esto justifica el hecho de proponer una generalización de [51, 52] a la familia de códigos casi-cíclicos.

Otros códigos que han sido construidos como la imagen de Gray de códigos lineales sobre anillos son los códigos binarios (no lineales) de Kerdock, Preparata, Nordstrom-Robinson

Goethals, Delsarte-Goethals, etcétera [23], los cuales tienen mejores parámetros que cualquier otro código comparable con tales códigos. Estos resultados han motivado un amplio estudio en la teoría de códigos sobre anillos finitos y, en particular, en las propiedades de las imágenes de Gray de códigos definidos sobre anillos finitos. Debido a la importancia de estos temas en la Teoría de Códigos, es común encontrar en la literatura la siguiente terminología.

Un código $\mathscr{C}$ de longitud $2^{k-1}n$ sobre $\mathbb{Z}_4$ es llamado $\mathbb{Z}_{2^{k+1}}$-*lineal* si es permutación equivalente al código $\varphi(\mathscr{E})$ para algún código lineal $\mathscr{E}$ de longitud n sobre $\mathbb{Z}_{2^{k+1}}$ [51]. De manera similar, se dice que un código binario $\mathscr{D}$ de longitud $2^k n$ es $\mathbb{Z}_{2^{k+1}}$-*lineal* si es permutación equivalente a la imagen de Gray de un código lineal de longitud n sobre $\mathbb{Z}_{2^{k+1}}$. Por ejemplo, el $[8,4,4]$ código binario extendido de Hamming (Ejemplo 4.2.6) y el código de Reed-Muller de segundo orden $\mathrm{RM}(2,4)$ son $\mathbb{Z}_4$-lineales.

Vale la pena mencionar que encontrar condiciones necesarias y suficientes para que un código (binario o sobre $\mathbb{Z}_4$) sea $\mathbb{Z}_{2^{k+1}}$-lineal es un problema difícil pues, entre otras cosas, las isometrías φ y Φ no son funciones lineales. En esta dirección, el Teorema 6 de [23] da una condición necesaria y suficiente para que un código binario sea $\mathbb{Z}_4$-lineal. Para el caso de códigos sobre $\mathbb{Z}_8$, condiciones necesarias y suficientes para que un código binario sea $\mathbb{Z}_8$-lineal son dadas en la Proposición 4 de [11]. Una generalización a los anillos de enteros módulo 2^{k+1} es dada en [51]. Sin embargo, muy poco se sabe cuando el código está definido sobre un anillo de Galois, o de manera más general, sobre un anillo finito de cadena o de Frobenius.

4.3. Casi-ciclicidad de los códigos de Reed-Muller sobre $\mathbb{Z}_4$

Los códigos binarios de Reed-Muller es una familia de códigos lineales descubiertos por Irvin S. Reed y David. E. Muller en 1954. Aunque estos códigos tienen distancia mínima relativamente pequeña, en la práctica son importantes debido a que pueden ser implementados y decodificados fácilmente. Esto ha originado que algunos de estos códigos hayan sido usados o propuestos para diversas aplicaciones en comunicaciones inalámbricas y del espacio exterior (cf. [4, 41, 53]). Asimismo, estos códigos son de interés matemático ya que están relacionados con geometrías afines y proyectivas (cf. [2, 10]).

Para todo entero $s \geq 0$, existen $s+1$ códigos binarios de Reed-Muller de longitud 2^s. Cada uno de estos códigos es denotado como $\mathrm{RM}(r,s)$, donde $0 \leq r \leq s$, y llamado el *código de Reed-Muller de orden r y longitud* 2^s. Estos códigos se pueden definir de diversas formas. Por conveniencia, en este manuscrito, hemos escogido usar la definición recursiva basada en la construcción $(u|u+v)$ (cf. [7, 27, 38, 45]).

Los códigos $\mathrm{RM}(0,s)$ y $\mathrm{RM}(s,s)$ son definidos, respectivamente, como el código de repetición de longitud 2^s y el espacio $\mathbb{F}_2^{2^s}$, es decir, $\mathrm{RM}(0,s) = \{(0)_{2^s}, (1)_{2^s}\}$ y $\mathrm{RM}(s,s) = \mathbb{F}_2^{2^s}$, donde $(a)_l$ denota al vector cuyas l coordenadas son todas iguales a a. Si $0 < r < s$, entonces el código binario de Reed-Muller $\mathrm{RM}(r,s)$ se define como la construcción $(u|u+v)$ de $\mathrm{RM}(r,s-1)$ y

$\mathrm{RM}(r-1,s-1)$, es decir, $\mathrm{RM}(r,s) = \{(u|u\oplus v) : u \in \mathrm{RM}(r,s-1), v \in \mathrm{RM}(r-1,s-1)\}$. Observe que en la anterior definición hemos usado el símbolo "$\oplus$" en lugar de "$+$". Esto lo hemos hecho para enfatizar que la suma de los vectores en los códigos $\mathrm{RM}(r,s-1)$ y $\mathrm{RM}(r-1,s-1)$ es la suma binaria.

Ya que los códigos $\mathrm{RM}(0,s)$ y $\mathrm{RM}(s,s)$ son códigos lineales, se sigue que para todo $1 \leq r \leq s$, el código $\mathrm{RM}(r,s)$ es lineal. Claramente, la matriz $G(0,s) = (1\ 1\ \cdots\ 1)$ de orden 1×2^s es la única matriz generadora de $\mathrm{RM}(0,s)$. Por otra parte, cualquier matriz $G(s,s)$ de orden $2^s \times 2^s$ cuyos renglones formen una base de $\mathbb{F}_2^{2^s}$ es una matriz generadora de $\mathrm{RM}(s,s)$. Una vez que se han construido matrices generadoras para $\mathrm{RM}(0,s)$ y $\mathrm{RM}(s,s)$, la construcción $(u|u+v)$ permite obtener recursivamente una matriz generadora para el código $\mathrm{RM}(r,s)$ de la siguiente forma:

$$G(r,s) = \begin{pmatrix} G(r,s-1) & G(r,s-1) \\ \mathbf{0} & G(r-1,s-1) \end{pmatrix}, \qquad 1 \leq r < s,$$

donde $\mathbf{0}$ es la matriz de ceros. Por ejemplo, si tomamos $s = 4$ y $r = 2$, entonces

$$G(2,4) = \begin{pmatrix} G(2,3) & G(2,3) \\ \mathbf{0} & G(1,3) \end{pmatrix}.$$

La matriz $G(1,3)$ genera al código $\mathrm{RM}(1,3)$ cuya base es $c_0^3 = 0000\,1111$, $c_1^3 = 0011\,0011$, $c_0^3 = 0101\,0101$ y $c_0^3 = 1111\,1111$. Así, para construir $G(2,4)$, resta conocer la matriz $G(2,3)$. Ésta última es:

$$G(2,3) = \left(\begin{array}{c|c} G(2,2) & G(2,2) \\ \hline \mathbf{0} & G(1,2) \end{array}\right) = \left(\begin{array}{c|c} 1111 & 1111 \\ 0101 & 0101 \\ 0011 & 0011 \\ 0001 & 0001 \\ \hline 0000 & 1111 \\ 0000 & 0101 \\ 0000 & 0011 \end{array}\right).$$

Observe que no hemos elegido a la matriz identidad de orden 4×4 como matriz generadora del código $\mathrm{RM}(2,2)$. La elección ha sido realizada de tal forma que se tenga lo siguiente:

$$G(2,4) = \left(\begin{array}{c|c} 1111\ 1111 & 1111\ 1111 \\ 0101\ 0101 & 0101\ 0101 \\ 0011\ 0011 & 0011\ 0011 \\ 0001\ 0001 & 0001\ 0001 \\ 0000\ 1111 & 0000\ 1111 \\ 0000\ 0101 & 0000\ 0101 \\ 0000\ 0011 & 0000\ 0011 \\ \hline 0000\ 0000 & 1111\ 1111 \\ 0000\ 0000 & 0101\ 0101 \\ 0000\ 0000 & 0011\ 0011 \\ 0000\ 0000 & 0000\ 1111 \end{array}\right) = \begin{pmatrix} \phi(2g_0) \\ \phi(2g_1) \\ \phi(g_3) \\ \phi(g_3) \\ \phi(2g_4) \\ \phi(g_5) \\ \phi(g_6) \\ \phi(g_0) \\ \phi(g_1) \\ \phi(g_2) \\ \phi(g_4) \end{pmatrix},$$

donde ϕ es la isometría de Gray sobre $\mathbb{Z}_4$ y los vectores g_i son aquellos que fueron definidos en los Ejemplos 1.2.2 y 4.2.7. Esto muestra que $\mathrm{RM}(2,4) = \phi(\mathrm{ZRM}(2,4))$, tal como se afirmó en el Ejemplo 4.2.7.

Actualmente, se tienen varios resultados relacionados con estos códigos (cf. [23,27,38,57]). En particular, se conoce que $\mathrm{RM}(s-r-1,s) = \mathrm{RM}(r,s)^{\perp}$. Asimismo, en [23] se prueba que los códigos $\mathrm{RM}(r,s)$, donde $r \in \{0,1,2,s-1,s\}$, son $\mathbb{Z}_4$-lineales. Con el propósito de enunciar formalmente este resultado, necesitamos introducir a la familia $\mathrm{ZRM}(r,s)$ de *códigos de Reed-Muller sobre* $\mathbb{Z}_4$.

Para todo $s \geq 1$, en [23] se definen los códigos de Reed-Muller $\mathrm{ZRM}(0,s)$ y $\mathrm{ZRM}(s,s)$ sobre $\mathbb{Z}_4$ como $\mathrm{ZRM}(0,s) = \{(0)_{2^{s-1}}, (2)_{2^{s-1}}\}$ y $\mathrm{ZRM}(s,s) = \mathbb{Z}_4^{2^{s-1}}$. Si $s \geq 2$ es un entero y $r \in \{1,2,s-1\}$, entonces el código $\mathrm{ZRM}(r,s)$ se define como el código lineal sobre $\mathbb{Z}_4$ generado por los vectores contenidos en el código binario de Reed-Muller $\mathrm{RM}(r-1,s-1)$ y el conjunto $2\mathrm{RM}(r,s-1)$, donde este último denota al código sobre $\mathbb{Z}_4$ que resulta de multiplicar por $2 \in \mathbb{Z}_4$ a cada vector binario en el código $\mathrm{RM}(r,s-1)$. Por ejemplo, si $s = 3$ y $r = 1$, entonces $\mathrm{ZRM}(1,3)$ es el código generado por el código binario de Reed-Muller $\mathrm{RM}(0,2) = \{0000, 1111\}$ y el código

$$\begin{aligned} 2\mathrm{RM}(1,2) &= 2\{0000, 1001, 1100, 0101, 0110, 0011, 1010, 1111\} \\ &= \{0000, 2002, 2200, 0202, 0220, 0022, 2020, 2222\}. \end{aligned}$$

Eliminando los términos redundantes (por ejemplo, 2222 es un múltiplo de 1111) obtenemos que $\mathrm{ZRM}(1,3)$ es generado por los vectores $1111, 0022, 0202$. Los elementos de $\mathrm{ZRM}(1,3)$ son

$$\begin{array}{cccccccc} 0000 & 1111 & 2222 & 3333 & 0202 & 1313 & 2020 & 3131 \\ 0022 & 1133 & 2200 & 3311 & 0220 & 1331 & 2002 & 3113 \end{array}$$

y, por lo tanto, $\mathrm{ZRM}(1,3)$ es el código $\mathscr{C}_H$ de los Ejemplos 1.2.1 y 4.2.6, cuya imagen de Gray es el código de Reed-Muller $\mathrm{RM}(1,3)$.

Por su parte, el código $\mathrm{ZRM}(2,4)$ está generado por los vectores del código de Reed-Muller $\mathrm{RM}(1,3) \subset \mathbb{Z}_4^8$ y los vectores del código $2\mathrm{RM}(1,3) \subset \mathbb{Z}_4^8$. Como una base del código binario $\mathrm{RM}(1,3)$ está formada por los vectores 1111 1111, 0101 0101, 0011 0011 y 0000 1111 y, dado que una base de $\mathrm{RM}(2,3) \subset \mathbb{F}_2^8$ está formada por los vectores que están en la base de $\mathrm{RM}(1,3)$ y los vectores 0001 0001, 0000 0011 y 0000 0101, entonces el código $\mathrm{ZRM}(2,4)$ está generado por $g_0 = 1111\ 1111$, $g_1 = 0000\ 1111$, $g_2 = 0011\ 0011$, $g_3 = 0101\ 0101$, $g_4 = 0000\ 0022$, $g_5 = 0000\ 0202$ y $g_6 = 0002\ 0002$. Como el lector recordará, estos vectores son los generadores del código presentado en los Ejemplos 1.2.2 y 4.2.7, cuya imagen de Gray es el código de Reed-Muller $\mathrm{RM}(2,4)$.

En general, se tiene el siguiente resultado (cf. [23]).

Teorema 4.3.1. *El código de Reed-Muller* $\mathrm{RM}(r,s)$*, donde* $s \geq 1$ *y* $r \in \{0,1,2,s-1,s\}$ *es la imagen de Gray de* $\mathrm{ZRM}(r,s)$*, es decir, para todos los valores de r mencionados, los códigos binarios de Reed-Muller* $\mathrm{RM}(r,s)$ *son* $\mathbb{Z}_4$*-lineales.*

Tal como se observó en los Ejemplos 1.2.1, 1.2.2, 4.2.6 y 4.2.7, los códigos de Reed-Muller sobre $\mathbb{Z}_4$ y los códigos binarios de Reed-Muller tienen propiedades de ciclicidad y casi-ciclicidad. Motivados por estas observaciones, en esta sección estamos interesados en estudiar propiedades de ciclicidad y casi-ciclicidad de los códigos $\mathrm{RM}(r,s) \subseteq \mathbb{F}_2^{2^s}$ y $\mathrm{ZRM}(r,s) \subseteq \mathrm{Z}_4^{s^{s-1}}$, donde $s \geq 1$ y $r \in \{0,1,2,s-1,s\}$. A diferencia de esos ejemplos, ahora estudiaremos propiedades de ciclicidad y casi-ciclicidad de los códigos $\mathrm{RM}(r,s)$ y, como consecuencia de este hecho, obtendremos propiedades de ciclicidad y casi-ciclicidad de los códigos $\mathrm{ZRM}(r,s)$, lo que derivará en una aportación más de este trabajo.

Claramente, por definición, $\mathrm{RM}(0,s)$ es un código casi-cíclico de índice 2^t para cualesquiera enteros s,t tales que $s \geq 1$ y $0 \leq t \leq s-1$. Consecuentemente, por la Proposición 1.2.3, el código $\mathrm{RM}(s-1,s) = \mathrm{RM}(0,s)^{\perp}$, es un código casi-cíclico de índice 2^t para cualesquiera enteros s,t tales que $s \geq 1$ y $0 \leq t \leq s-1$. También, es claro que para todo $s \geq 1$, el código $\mathrm{RM}(s,s) = \mathbb{F}_2^{2^s}$ es casi-cíclico de índice 2^t, $0 \leq t \leq s-1$. Así, los únicos casos que nos quedan por describir son $r = 1,2$ y $s \geq 3$.

Teorema 4.3.2. *Sea $s \geq 3$ un entero. Entonces el código binario de Reed-Muller $\mathrm{RM}(1,s)$ es casi-cíclico de índice 2^{s-2} pero no es casi-cíclico de índice 2^t, para cualquier entero t tal que $0 \leq t \leq s-3$. Si $s \geq 4$, entonces $\mathrm{RM}(2,s)$ es casi-cíclico de índice 2^{s-2} pero no es casi-cíclico de índice 2^t, para cualquier entero t tal que $0 \leq t \leq s-3$.*

Demostración. Demostremos por inducción sobre s la afirmación que se ha hecho para el código $\mathrm{RM}(1,s)$. En el Ejemplo 4.2.6 mostramos que $\mathrm{RM}(1,3)$ es un código casi-cíclico de índice 2^{3-2}. Ahora, note que $\mathrm{RM}(1,3)$ no es un código casi-cíclico de índice 2^0, es decir, no es cíclico pues $0000\ 1111 \in \mathrm{RM}(1,3)$ pero $\sigma(0000\ 1111) = 1000\ 0111 \notin \mathrm{RM}(1,3)$. De aquí que la situación para $s = 3$ queda establecida. Supongamos, ahora, que $s > 3$ y que $\mathrm{RM}(1,s)$ es casi-cíclico de índice 2^{s-2} pero que no es casi-cíclico de índice 2^t, $0 \leq t \leq s-3$. Sea $z = (u|u \oplus v) \in \mathrm{RM}(1,s+1)$, donde $u \in \mathrm{RM}(1,s)$ y $v \in \mathrm{RM}(0,s)$. Entonces

$$\sigma^{\otimes 2^{s-1}}(z) = \left(\sigma^{\otimes 2^{s-2}}(u) \middle| \sigma^{\otimes 2^{s-2}}(u) \oplus \sigma^{\otimes s^{s-1}}(v)\right).$$

Por hipótesis de inducción, $u_1 = \sigma^{\otimes 2^{s-2}}(u) \in \mathrm{RM}(1,s)$ y, como $\mathrm{RM}(0,s)$ es casi-cíclico de índice 2^{s-2}, entonces también se tiene que $v_1 = \sigma^{\otimes s^{s-1}}(v) \in \mathrm{RM}(0,s)$. Por lo tanto,

$$\sigma^{\otimes 2^{s-1}}(z) = (u_1|u_1 \oplus v_1) \in \mathrm{RM}(1,s+1).$$

Esto quiere decir que $\mathrm{RM}(1,s+1)$ es casi-cíclico de índice $2^{s-1} = 2^{(s+1)-2}$. Veamos ahora que $\mathrm{RM}(1,s+1)$ no es casi-cíclico de índice 2^t, donde $0 \leq t \leq s-2$. Supongamos lo contrario, es decir, supongamos que $\mathrm{RM}(1,s+1)$ es casi-cíclico de índice 2^t, para algún $t \in \{0,1,\ldots,s-2\}$. Si $t = 0$, entonces $\mathrm{RM}(1,s+1)$ es cíclico, lo cual implica que el vector $10\cdots0 \in \mathrm{RM}(1,s)$. Pero esto es imposible ya que todo elemento de $\mathrm{RM}(1,s)$, distinto de $(0)_{2^s}$ y $(1)_{2^s}$, tiene peso

de Hamming par (Lema 2.1.3). De este modo, obtenemos que $0 < t \leq s-2$. Ahora, como para todo $u \in \mathrm{RM}(1,s)$ se tiene que $(u|u) \in \mathrm{RM}(1,s+1)$, entonces

$$\sigma^{\otimes 2^t}(u|u) = \left(\sigma^{\otimes 2^{t-1}}(u)|\sigma^{\otimes 2^{t-1}}(u)\right) \in \mathrm{RM}(1,s+1).$$

Pero esto implica que $\sigma^{\otimes 2^{t-1}}(u) \in \mathrm{RM}(1,s)$. Dado que la elección de $u \in \mathrm{RM}(1,s)$ fue arbitraria, se concluye que $\mathrm{RM}(1,s)$ es un código casi-cíclico de índice 2^{t-1}, donde $0 \leq t-1 \leq s-3$ (contradicción). Por lo tanto, $\mathrm{RM}(1,s+1)$ no es casi-cíclico de índice 2^t, donde $0 \leq t \leq s-2$. La demostración de la afirmación del Teorema 4.3.1 para el código $\mathrm{RM}(2,s)$ es similar a la prueba de $\mathrm{RM}(1,s)$ y, por lo tanto, la omitimos. □

Aunque nuestro interés se concentra en los códigos $\mathrm{RM}(r,s)$ donde $r \in \{0,1,2,s-1,s\}$, como otra aplicación directa del Teorema 4.3.1 y la Proposición 1.2.3 (que establece que el código dual de un código casi-cíclico es un código casi-cíclico), obtenemos propiedades de casi-ciclicidad para los códigos duales de $\mathrm{RM}(1,s)$ y $\mathrm{RM}(2,s)$.

Corolario 4.3.3. *Si $s \geq 3$ es un entero, entonces el código binario $\mathrm{RM}(s-2,s) = \mathrm{RM}(1,s)^{\perp}$ es un código casi-cíclico de índice 2^{s-2} pero no es casi-cíclico de índice 2^t, para $0 \leq t \leq s-3$. De igual forma, si $s \geq 4$, entonces el código binario $\mathrm{RM}(s-3,s) = \mathrm{RM}(2,s)^{\perp}$ es un código casi-cíclico de índice 2^{s-2} pero no es casi-cíclico de índice 2^t, para $0 \leq t \leq s-3$.*

Cabe mencionar que en [19] se prueba que, en general, los códigos $\mathrm{RM}(r,s)$ son casi-cíclicos de índice 2^{s-2} pero que no son casi-cíclicos de índice 2^{s-3}. Los Teoremas 4.3.1 y 4.3.3 respaldan ese resultado para los códigos $\mathrm{RM}(r,s)$, donde $s \geq 4$ y $r \in \{1,2,s-2,s-3\}$, y añaden que estos códigos no pueden ser casi-cíclicos para algún otro índice.

Como una aplicación de los Teoremas 4.2.1 y 4.3.1, deducimos algunas propiedades de casi-ciclicidad de los códigos $\mathrm{ZRM}(r,s)$. Obviamente, $\mathrm{ZRM}(0,s)$ y $\mathrm{ZRM}(s,s)$ son cíclicos y casi-cíclicos de cualquier índice.

Teorema 4.3.4. *Sea s un entero.*

(1) *Si $s \geq 2$, entonces $\mathrm{ZRM}(s-1,s)$ es casi-cíclico de índice 2^t y longitud 2^{s-1}, $0 \leq t \leq s-2$. En particular, $\mathrm{ZRM}(s-1,s)$ es un código cíclico sobre $\mathbb{Z}_4$.*

(2) *Si $s \geq 3$, entonces $\mathrm{ZRM}(1,s)$ es casi-cíclico de índice 2^{s-3} y longitud 2^{s-1}. Además, si $s \geq 4$, entonces $\mathrm{ZRM}(1,s)$ no es casi-cíclico de índice 2^t, $0 \leq t \leq s-4$.*

(3) *Si $s \geq 4$, entonces $\mathrm{ZRM}(2,s)$ es casi-cíclico de índice 2^{s-3} y longitud 2^{s-1}, pero no es casi-cíclico de índice 2^t, $0 \leq t \leq s-4$.*

Demostración. (1). Sea $s \geq 2$. Entonces $\mathrm{RM}(s-1,s)$ es un código casi-cíclico de índice 2^l y longitud 2^s sobre $\mathbb{F}_2$, $0 \leq l \leq s-1$. En particular, $\mathrm{RM}(s-1,s)$ es un código casi-cíclico de índice 2^l para $1 \leq l \leq s-1$. Tomando $k=1$, $2m=2^l$ y $2n=2^s$ en el Teorema 4.2.1, obtenemos que $\mathrm{ZRM}(s-1,s)$ es un código casi-cíclico de índice $m=2^{l-1}$ y longitud $n=2^{s-1}$, para $1 \leq l \leq s-1$. Esto es, $\mathrm{ZRM}(s-1,s)$ es un código casi-cíclico de índice 2^t y longitud 2^{s-1}, $0 \leq t \leq s-2$. En particular, tomando $t=0$, obtenemos que $\mathrm{ZRM}(s-1,s)$ es un código cíclico sobre $\mathbb{Z}_4$.
(2). Sea $s \geq 3$. Por el Teorema 4.3.1, $\mathrm{RM}(1,s)$ es un código casi-cíclico de índice $2m=2^{s-2}$ y longitud 2^s sobre $\mathbb{F}_2$. Por lo tanto, por el Teorema 4.2.1, $\mathrm{ZRM}(1,s)$ es un código casi-cíclico de índice $m=2^{s-3}$ y longitud 2^{s-1} sobre $\mathbb{Z}_4$. Además, por el Teorema 4.3.1, $\mathrm{RM}(1,s)$ no es un código casi-cíclico de índice 2^l, donde $0 \leq l \leq s-3$, o bien, donde $1 \leq l \leq s-3$. En consecuencia, si $s \geq 4$, $\mathrm{ZRM}(1,s)$ no es un código casi-cíclico de índice 2^{l-1} para $1 \leq l \leq s-3$, es decir, $\mathrm{ZRM}(1,s)$ no es un código casi-cíclico de índice 2^t, donde $0 \leq t \leq s-4$.
(3). Supongamos que $s \geq 4$, entonces $\mathrm{RM}(2,s)$ es un código casi-cíclico de índice $2m=2^{s-2}$ y longitud 2^s sobre $\mathbb{F}_2$. Como consecuencia del Teorema 4.2.1, se sigue que $\mathrm{ZRM}(2,s)$ es un código casi-cíclico de índice 2^{s-3} y longitud 2^{s-1} sobre $\mathbb{Z}_4$. Más aún, el Teorema 4.3.1 garantiza que $\mathrm{RM}(2,s)$ no es un código casi-cíclico de índice 2^l, donde $1 \leq s \leq s-3$. Por lo tanto, por el Teorema 4.2.1, $\mathrm{ZRM}(2,s)$ no es un código casi-cíclico de índice 2^{l-1}, $0 \leq l \leq s-4$. □

Vale la pena mencionar que los resultados presentados en esta sección, pueden incrementar las posibilidades de que los códigos de Reed-Muller sobre $\mathbb{Z}_4$ tengan más aplicaciones prácticas, o bien, pueden favorecer la búsqueda de nuevos algoritmos de decodificación basados en los *diagramas de Trellis* asociados a los códigos de bloque, tal como se dio para los códigos binarios de Reed-Muller [19]. El lector interesado en conocer más acerca de estos temas, puede consultar por ejemplo, [24, 32].

4.4. Imágenes sobre $\mathbb{Z}_4$ de códigos $(1+2^k)$-casi-cíclicos

En esta sección analizaremos propiedades de casi-negaciclicidad y casi-ciclicidad del código $\varphi(\mathscr{C})$, donde $\mathscr{C}$ es un código $(1+2^k)$-casi-cíclico sobre $\mathbb{Z}_{2^{k+1}}$, $k \geq 1$. Demostramos que $\varphi(\mathscr{C})$ es un código casi-negacíclico de índice $2^{k-1}m$ y logitud $2^{k-1}mn$ sobre $\mathbb{Z}_4$ si y sólo si $\mathscr{C}$ es un código $(1+2^k)$-casi-cíclico de índice m y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$. Este resultado caracteriza a un código $(1+2^k)$-casi-cíclico sobre $\mathbb{Z}_{2^{k+1}}$ en términos de las propiedades de casi-negaciclicidad de su imagen sobre $\mathbb{Z}_4$. Lo anterior generaliza el Teorema 8 de [52].

Continuando con la notación introducida anteriormente, sea $\lambda = 1+2^k$.

Primero investigaremos la propiedad de casi-negaciclicidad del código $\varphi(\mathscr{C})$. Para tal fin, recordemos que por el Teorema 3.3.4, tenemos la siguiente relación

$$\varphi \circ \nu_\lambda^{\otimes m} = \nu^{\otimes 2^{k-1}m} \circ \varphi, \tag{4.4}$$

donde $k \geq 1$, $\nu^{\otimes 2^{k-1}m} : \mathbb{Z}_4^{2^{k-1}mn} \to \mathbb{Z}_4^{2^{k-1}mn}$ es el corrimiento casi-negacíclico de índice $2^{k-1}m$, $\nu_\lambda^{\otimes m}$ es el corrimiento λ-casi-cíclico de índice m y $\varphi : \mathbb{Z}_{2^k+1}^n \to \mathbb{Z}_4^{2^{k-1}n}$ es la isometría introducida en el Capítulo 2 de esta tesis.

Teorema 4.4.1. *Sean $k,m,n \geq 1$ enteros y $\mathscr{C}$ un código de longitud mn sobre $\mathbb{Z}_{2^k+1}$. Entonces $\mathscr{C}$ es λ-casi-cíclico de índice m si y sólo si $\varphi(\mathscr{C})$ es un código casi-negacíclico de índice $2^{k-1}m$ y longitud $2^{k-1}mn$ sobre $\mathbb{Z}_4$.*

Demostración. Si $\mathscr{C}$ es un código λ-casi-cíclico de índice m y longitud mn sobre $\mathbb{Z}_{2^k+1}$, entonces $\nu_\lambda^{\otimes m}(\mathscr{C}) = \mathscr{C}$ y, por lo tanto, de la relación (4.4) se tiene que

$$\varphi(\mathscr{C}) = \varphi(\nu_\lambda^{\otimes m}(\mathscr{C})) = \nu^{\otimes 2^{k-1}m}(\varphi(\mathscr{C})).$$

En otros términos, $\varphi(\mathscr{C})$ es un código casi-negacíclico de índice $2^{k-1}m$ y longitud $2^{k-1}mn$ sobre $\mathbb{Z}_4$. Recíprocamente, supongamos que $\varphi(\mathscr{C}) = \nu^{\otimes 2^{k-1}m}(\varphi(\mathscr{C}))$. Entonces, de la relación (4.4) obtenemos que $\nu^{\otimes 2^{k-1}m}(\varphi(\mathscr{C})) = \varphi(\nu_\lambda^{\otimes m}(\mathscr{C}))$ y, por lo tanto, $\varphi(\mathscr{C}) = \varphi(\nu_\lambda^{\otimes m}(\mathscr{C}))$. Así, debido a la inyectividad de φ, se sigue que $\mathscr{C} = \nu_\lambda^{\otimes m}(\mathscr{C})$, es decir, $\mathscr{C}$ es un código λ-casi-cíclico de índice m y longitud mn sobre $\mathbb{Z}_{2^k+1}$. □

En particular, observe que tomando $m = 1$ en el Teorema 4.4.1, obtenemos que un código $\mathscr{C}$ de longitud n sobre $\mathbb{Z}_{2^k+1}$ es λ-cíclico si y sólo si $\varphi(\mathscr{C})$ es un código casi-negacíclico de índice 2^{k-1} y longitud $2^{k-1}n$ sobre $\mathbb{Z}_4$. Esta observación es tema del Teorema 8 de [52]. Vale la pena mencionar que el Teorema 8 de [52] usa la isometría φ^k, cuya definición fue analizada en las Secciones 2.2.1 y 2.2.2, en lugar de la isometría φ que hemos introducido en este material. Sin embargo, dado que φ^k y φ son equivalentes (Teorema 2.2.6), el Teorema 4.4.1 puede ser considerado como una generalización del Teorema 8 de [52].

Ejemplo 4.4.2. Sean $k = 2$, $\lambda = 1 + 2^2 = 5$ y considere el siguiente código λ-cíclico $\mathscr{C}$ de longitud 4 sobre $\mathbb{Z}_8$:

$$\begin{array}{cccccccc} 1323 & 1744 & 2357 & 2713 & 3235 & 3441 & 3572 & 4174 \\ 4417 & 4453 & 4534 & 5344 & 5727 & 7132 & 7271 & 7445 \end{array}$$

Entonces, por el Teorema 4.4.1, $\varphi(\mathscr{C})$ es un código casi-negacíclico de índice 2 y longitud 8 sobre $\mathbb{Z}_4$. Los elementos de $\varphi(\mathscr{C})$ son:

$$\begin{array}{cccc} 1101\,1323 & 1322\,1122 & 0133\,2331 & 0311\,2113 \\ 1013\,3233 & 1221\,3221 & 1330\,3312 & 2132\,2112 \\ 2213\,2211 & 2231\,2233 & 2312\,2332 & 3122\,3322 \\ 3303\,3121 & 3110\,1132 & 3031\,1211 & 3223\,1223 \end{array}$$

De aquí, es fácil verificar, por inspección directa, que el código $\varphi(\mathscr{C})$ es, en efecto, un código casi-negacíclico de índice 2 y longitud 8 sobre $\mathbb{Z}_4$. Por ejemplo, $11011323 \in \varphi(\mathscr{C})$ (fila 1,

columna 1 del arreglo anterior) implica que $\nu^{\otimes 2}(11011323) = 31101132$ también está en $\varphi(\mathscr{C})$ (fila 4, columna 2 del arreglo anterior). Por el contrario, note que $\sigma^{\otimes 2}(11011323) = 11103132 \notin \varphi(\mathscr{C})$, y por lo tanto, $\varphi(\mathscr{C})$ no es casi-cíclico de índice 2. Más aún, note que $\varphi(\mathscr{C})$ no es cíclico, pues $x = 10133233 \in \varphi(\mathscr{C})$ pero $\sigma(x) = 31013323 \notin \varphi(\mathscr{C})$.

Ejemplo 4.4.3. Sean $k = 2$ y $\lambda = 1 + 2^2 = 5$. Considere ahora el código lineal $\mathscr{C}$ de longitud 4 sobre $\mathbb{Z}_8$ generado por los vectores 2060 y 0206. Ya que $\nu_5(2060) = 0206$ y $\nu_5(0206) = 6020 = 3(2060)$, $\mathscr{C}$ es un código 5-cíclico. Así, por el Teorema 4.4.1, $\varphi(\mathscr{C})$ es un código casi-negacíclico de índice 2 y longitud 8 sobre $\mathbb{Z}_4$. Pero más aún, note que $\mathscr{C}$ también es un código cíclico y, por lo tanto, por el Teorema 4.2.1, $\varphi(\mathscr{C})$ es un código casi-cíclico de índide 2 y longitud 8 sobre $\mathbb{Z}_4$.

En el Ejemplo 4.4.2 notamos que si $\mathscr{C}$ es un código λ-casi-cíclico de índice m y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$, entonces, en general, el código $\varphi(\mathscr{C})$ no es casi-cíclico de índice $2^{k-1}m$ y longitud $2^{k-1}mn$ sobre $\mathbb{Z}_4$. Sin embargo, el Ejemplo 4.4.3 muestra un código sobre $\mathbb{Z}_8$ que tiene la propiedad de ser λ-cíclico y cíclico al mismo tiempo y, por lo tanto, el código $\varphi(\mathscr{C})$ tiene la propiedad de ser casi-negacíclico y casi-cíclico a la vez. De hecho, por los Teoremas 4.2.1 y 4.4.1, el código $\varphi(\mathscr{C})$ es casi-cíclico y λ-casi-cíclico del mismo índice $2^{k-1}m$ y longitud $2^{k-1}mn$ sobre $\mathbb{Z}_4$ si y sólo si $\mathscr{C}$ es un código casi-cíclico y casi-negacíclico del mismo índice m y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$. En consecuencia, es natural preguntarse bajo qué condiciones un código $\mathscr{C}$ de longitud mn sobre $\mathbb{Z}_{2^{k+1}}$ es casi-cíclico y λ-casi-cíclico del mismo índice m. En tal caso, ¿qué otras propiedades poseen los códigos $\mathscr{C}$ y $\varphi(\mathscr{C})$?

Con el propósito de encontrar una respuesta a estas preguntas, recordemos que la aplicación η_γ es el $\mathbb{Z}_{2^{k+1}}$-automorfismo definido sobre $\mathbb{Z}_{2^{k+1}}^n$ como (Sección 3.2 y Proposición 3.2.1)

$$\eta_\gamma : (z_0, \ldots, z_{n-2}, z_{n-1}) \mapsto (z_0, \ldots, z_{n-2}, \gamma z_{n-1}).$$

Consecuentemente, $\eta_\lambda^{\otimes m} : \mathbb{Z}_{2^{k+1}}^{mn} \to \mathbb{Z}_{2^{k+1}}^{mn}$ es el $\mathbb{Z}_{2^{k+1}}$-automorfismo dado por

$$\eta_\gamma^{\otimes m} : \left(\mathbf{z}^{(1)}|\cdots|\mathbf{z}^{(m)}\right) \mapsto \left(\eta_\gamma(\mathbf{z}^{(1)})|\cdots|\eta_\gamma(\mathbf{z}^{(m)})\right), \qquad \mathbf{z}^{(j)} \in \mathbb{Z}_{2^{k+1}}^n,\ 1 \le j \le m.$$

Una respuesta a la primera pregunta la encontramos en el siguiente resultado.

Proposición 4.4.4. *Sea $\mathscr{C}$ un código de longitud mn sobre $\mathbb{Z}_{2^{k+1}}$ y $\lambda = 1 + 2^k$. Cualesquiera de las siguientes dos condiciones implica la tercera.*

(1) *$\mathscr{C}$ un código casi-cíclico de índice m,*

(2) *$\mathscr{C}$ es λ-casi-cíclico de índice m,*

(3) $\eta_\lambda^{\otimes m}(\mathscr{C}) = \mathscr{C}$.

Demostración. (1) y (2) implican (3). Como $\mathscr{C}$ es casi-ccílcio y λ-casi-cíclico de índice m, entonces $\mathscr{C} = \sigma^{\otimes m}(\mathscr{C})$ y $\mathscr{C} = \nu_\lambda^{\otimes m}(\mathscr{C}) = \sigma^{\otimes m}(\eta_\lambda^{\otimes m}(\mathscr{C}))$; de donde obtenemos que $\sigma^{\otimes m}(\mathscr{C}) = \sigma^{\otimes m}(\eta_\lambda^{\otimes m}(\mathscr{C}))$. Siendo $\sigma^{\otimes m}$ una función inyectiva, concluimos que $\mathscr{C} = \eta_\lambda^{\otimes m}(\mathscr{C})$.

(1) y (3) implican (2). Dado que $\mathscr{C}$ es casi-cíclico de índice m y $\eta_\lambda^{\otimes m}(\mathscr{C}) = \mathscr{C}$, entonces $\mathscr{C} = \sigma^{\otimes m}(\mathscr{C}) = \sigma^{\otimes m}(\eta_\lambda^{\otimes m}(\mathscr{C})) = \nu_\lambda^{\otimes m}(\mathscr{C})$. Esto implica que $\mathscr{C}$ es λ-casi-cíclico de índice m.

(2) y (3) implican (1). En este caso, $\mathscr{C}$ λ-casi-cíclico y $\eta_\lambda^{\otimes m}(\mathscr{C}) = \mathscr{C}$. Así, $\mathscr{C} = \nu_\lambda^{\otimes m}(\mathscr{C}) = \sigma^{\otimes m}(\eta_\lambda^{\otimes m}(\mathscr{C})) = \sigma^{\otimes m}(\mathscr{C})$. □

En particular, observe que si $\mathscr{C}$ un código casi-cíclico (o λ-casi-cíclico) de índice m y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$, entonces $\mathscr{C}$ es λ-casi-cíclico (resp. casi-cíclico) si permanece fijo con respecto a la aplicación $\eta_\lambda^{\otimes m}$. Por tal razón, analizaremos con más detalle el significado la propiedad $\eta_\lambda^{\otimes m}(\mathscr{C}) = \mathscr{C}$. Esto quiere decir que para todo $Z \in \mathscr{C}$, se tiene que $\eta_\lambda^{\otimes m}(Z) \in \mathscr{C}$. Si $Z = \left(\mathbf{z}^{(1)} | \cdots | \mathbf{z}^{(m)}\right)$, donde

$$\mathbf{z}^{(j)} = \left(z_0^{(j)}, z_1^{(j)}, \ldots, z_{n-2}^{(j)}, z_{n-1}^{(j)}\right) \in \mathbb{Z}_{2^{k+1}}^n, \qquad 1 \leq j \leq m,$$

entonces $\eta_\lambda^{\otimes m}(Z) \in \mathscr{C}$ si y sólo si

$$\left(\left(z_0^{(1)}, z_1^{(1)}, \ldots, z_{n-2}^{(1)}, \lambda z_{n-1}^{(1)}\right) \middle| \cdots \middle| \left(z_0^{(m)}, z_1^{(m)}, \ldots, z_{n-2}^{(m)}, \lambda z_{n-1}^{(m)}\right)\right) \in \mathscr{C}.$$

Note que la última coordenada de cada $\mathbf{z}^{(j)}$ es la única que se ve afectada por una multiplicación por la unidad $\lambda = 1 + 2^k$. Este producto es fácil de entender puesto que para todo j tal que $1 \leq j \leq m$,

$$\lambda z_{n-1}^{(j)} = (1+2^k) z_{n-1}^{(j)} = \begin{cases} z_{n-1}^{(j)} + 2^k & \text{si } z_{n-1}^{(j)} \in U(\mathbb{Z}_{2^{k+1}}) \\ z_{n-1}^{(j)} & \text{si } z_{n-1}^{(j)} \in \langle 2 \rangle \end{cases} \tag{4.5}$$

Como consecuencia de este análisis, tenemos el siguiente resultado.

Corolario 4.4.5. *Sea $\mathscr{C}$ un código de longitud mn sobre $\mathbb{Z}_{2^{k+1}}$ tal que todas las coordenadas de cualquier vector en $\mathscr{C}$ están en el ideal maximal de $\mathbb{Z}_{2^{k+1}}$, es decir, $\mathscr{C} \subseteq (2\mathbb{Z}_{2^{k+1}})^{mn}$. Entonces, $\mathscr{C}$ es casi-cíclico de índice m si y sólo si $\mathscr{C}$ es λ-casi-cíclico de índice m.*

En particular, ya que un código λ-casi-cíclico de índice $m = 1$ y longitud 4 sobre $\mathbb{Z}_8$ es precisamente un código 5-cíclico de longitud 4 sobre $\mathbb{Z}_8$, el Corolario 4.4.5 justifica el porqué el código del Ejemplo 4.4.3 es también cíclico. Consecuentemente, por los Teoremas 4.2.1 y 4.4.1, esto implica que la imagen bajo φ del código del Ejemplo 4.4.3 tiene la propiedad de ser casi-cíclico y casi-negacíclico de índice 2 y longitud 8 sobre $\mathbb{Z}_8$, lo que coincide con lo que se observó en dicho ejemplo.

En general, por el Teorema 1.3.1, cada código cíclico lineal $\mathscr{C}$ de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$, puede ser expresado como $\mathscr{C} = \langle \widehat{F}_1, 2\widehat{F}_2, \ldots, 2^k\widehat{F}_k \rangle$, donde hemos denominado a los polinomios $\widehat{F}_1, 2\widehat{F}_2, \ldots, 2^k\widehat{F}_k$, los polinomios generadores de $\mathscr{C}$. En consecuencia, se sigue del Corolario 4.4.5, que cualquier código cíclico lineal $\mathscr{C}$ de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$, tal que $\mathscr{C} = \langle 2\widehat{F}_2, \ldots, 2^k\widehat{F}_k \rangle$, es un código λ-cíclico lineal. Por lo tanto, gran parte de los códigos cíclicos lineales de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$ son también códigos λ-cíclicos.

Veamos un ejemplo de un código cíclico y λ-cíclico tal que no todos los vectores contenidos en él tengan todas sus coordenadas en el ideal maximal del anillo $\mathbb{Z}_{2^{k+1}}$. Esto muestra que un código $\mathscr{C}$ puede ser casi-cíclico y λ-casi-cíclico sin que todas las coordenadas de sus elementos estén en el ideal maximal de $\mathbb{Z}_{2^{k+1}}$. Por lo tanto, el recíproco del Corolario 4.4.5 es falso.

Ejemplo 4.4.6. Considere el siguiente código cíclico no lineal $\mathscr{C}$ de longitud 3 sobre $\mathbb{Z}_{16}$, cuyos elementos son:

$$\begin{array}{cccc} (1,12,8) & (5,12,8) & (8,1,12) & (8,5,12) \\ (8,9,12) & (8,13,12) & (9,12,8) & (12,8,1) \\ (12,8,5) & (12,8,9) & (12,8,13) & (13,12,8) \end{array}$$

Usando las relaciones dadas en (4.5), es fácil verificar que $\eta_\lambda(\mathscr{C}) = \mathscr{C}$, donde $\lambda = 1+2^3 = 9$. Por lo tanto, $\mathscr{C}$ es un código cíclico y 9-cíclico. Observe que, por ejemplo, la primera coordenada del vector $(1,12,8) \in \mathscr{C}$ es una unidad y, por lo tanto, no está en el ideal maximal de $\mathbb{Z}_{16}$. Así, no todas las coordenadas de los elementos de $\mathscr{C}$ están en el ideal maximal de $\mathbb{Z}_{16}$.

Por otro lado, la Proposición 4.4.4 establece que si $\mathscr{C}$ es un código casi-cíclico y λ-casi-cíclico del mismo índice m, entonces $\mathscr{C}$ posee la siguiente propiedad adicional: $\eta_\lambda^{\otimes m}(\mathscr{C}) = \mathscr{C}$. Esto atiende a la segunda pregunta que nos hemos planteado acerca de las propiedades adicionales que satisface el código $\mathscr{C}$ cuando éste es casi-cíclico y λ-casi-cíclico. Además, como consecuencia de este hecho y del Teorema 3.3.4 tenemos el siguiente resultado.

Proposición 4.4.7. *Sea $\mathscr{C}$ un código casi-cíclico y λ-casi-cíclico del mismo índice m y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$. Entonces $\eta_{-1}^{\otimes 2^{k-1}m}(\varphi(\mathscr{C})) = \varphi(\mathscr{C})$.*

Demostración. Dado que por hipótesis $\mathscr{C}$ es casi-cíclico y λ-casi-cíclico del mismo índice m, entonces $\eta_\lambda^{\otimes m}(\mathscr{C}) = \mathscr{C}$. Por otro lado, del Teorema 3.3.4, se tiene la siguiente relación:

$$\varphi \circ \eta_\lambda^{\otimes m} = \eta_{-1}^{\otimes 2^{k-1}m} \circ \varphi$$

Por lo tanto, $\eta_{-1}^{\otimes 2^{k-1}m}(\varphi(\mathscr{C})) = \varphi(\eta_\lambda^{\otimes m}(\mathscr{C})) = \varphi(\mathscr{C})$. □

Los códigos de los Ejemplos 4.4.3 y 4.4.6 son códigos cíclicos y λ-cíclicos. Por lo tanto, las imágenes con respecto a φ de estos códigos ilustran la Proposición 4.4.7. Por ejemplo, la

imagen bajo φ del código $\mathscr{C}$ del Ejemplo 4.4.6 consiste de los siguientes vectores:

122 102 122 102	122 302 122 302	212 210 212 210	212 230 212 230
232 230 232 230	232 210 232 210	322 302 322 302	221 021 221 021
221 023 221 023	223 023 223 023	223 021 223 021	322 102 322 102

De aquí, es fácil verificar por inspección directa que $\eta_{-1}^{\otimes 4}(\varphi(\mathscr{C})) = \varphi(\mathscr{C})$. Para ilustrar esto, sea $x = 221\ 023\ 221\ 023 \in \varphi(\mathscr{C})$ (fila 3, columna 1 del arreglo anterior). Aplicando $\eta_{-1}^{\otimes 4}$ a x obtenemos $\eta_{-1}^{\otimes 4}(x) = 223\ 021\ 223\ 021 \in \varphi(\mathscr{C})$ (fila 3, columna 3 del arreglo anterior).

Es natural preguntarse si el recíproco de la Proposición 4.4.7 es también válido, es decir, si $\mathscr{C}$ es un código sobre $\mathbb{Z}_{2^{k+1}}$ tal que $\eta_{-1}^{\otimes 2^{k-1}m}(\varphi(\mathscr{C})) = \varphi(\mathscr{C})$, entonces ¿es $\mathscr{C}$ un código casi-cíclico y λ-casi-cíclico? Debido al Teorema 3.3.4, de existir tal código satisface la propiedad $\eta_{\lambda}^{\otimes m}(\mathscr{C}) = \mathscr{C}$. Desafortunadamente, esta hipótesis no es suficiente para concluir las propiedades de casi-ciclicidad y λ-casi-ciclicidad. El siguiente ejemplo ilustra este hecho.

Ejemplo 4.4.8. Considere el código $\mathscr{C}$ de longitud 3 sobre $\mathbb{Z}_8$ cuyos elementos son

$$155 \quad 151 \quad 133 \quad 137 \quad 144 \quad 122 \quad 111 \quad 115 \quad 116$$

El código $\varphi(\mathscr{C})$ de longitud 6 sobre $\mathbb{Z}_4$ consiste de los siguientes vectores:

133 133	111 133	122 122	111 111	112 110
131 131	113 131	100 122	113 113	

De aquí, es fácil verificar por inspección directa que $\eta_{-1}^{\otimes 2}(\varphi(\mathscr{C})) = \varphi(\mathscr{C})$ y, en consecuencia, $\eta_5(\mathscr{C}) = \mathscr{C}$ (Teorema 3.3.4). Sin embargo, es claro que $\mathscr{C}$ no es un código cíclico ni un código 5-cíclico sobre $\mathbb{Z}_8$.

En resumen, hasta este punto hemos caracterizado a un código λ-casi-cíclico de índice m y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$ como aquel código $\mathscr{C}$ tal que $\varphi(\mathscr{C})$ es un código casi-negacíclico de índice $2^{k-1}m$ y longitud $2^{k-1}mn$ sobre $\mathbb{Z}_4$. También, hemos caracterizado algunos códigos que tienen la propiedad de ser casi-cíclicos y λ-casi-cíclicos del mismo índice. Todos estos resultados son válidos para códigos no necesariamente lineales. El siguiente punto en este trabajo es agregar la condición de linealidad a estos códigos.

Primero recuerde que para cualquier código $\mathscr{C}$ casi-cíclico lineal de índice m y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$, existen $Z_0, Z_1, \ldots, Z_s \in \mathscr{C}$ que *generan a $\mathscr{C}$ como submódulo de* $\mathbb{Z}_{2^{k+1}}^{mn}$, es decir, todo elemento de $\mathscr{C}$ se escribe como combinación lineal (no necesariamente única) de $Z_0, Z_1, \ldots, Z_s$. En este caso, como $\eta_{\lambda}^{\otimes m}$ es un $\mathbb{Z}_{2^{k+1}}$-automorfismo sobre $\mathbb{Z}_{2^{k+1}}^{n}$, no es necesario verificar que $\eta_{\lambda}^{\otimes m}(Z) \in \mathscr{C}$, para todo $Z \in \mathscr{C}$; el problema se simplifica a verificar la condición para los generadores $Z_0, Z_1, \ldots, Z_1$ de $\mathscr{C}$, tal como se establece formalmente a continuación.

Proposición 4.4.9. *Sea $\mathscr{C}$ un código casi-cíclico (λ-casi-cíclico) lineal generado por los vectores $Z_0, Z_1, \ldots, Z_s \in \mathbb{Z}_{2^{k+1}}^{nm}$. Entonces $\mathscr{C}$ es λ-casi-cíclico (resp. casi-cíclico) lineal de índice m y longittud mn sobre $\mathbb{Z}_{2^{k+1}}$ si y sólo si, para todo $0 \leq i \leq s$, se tiene que $\eta_\lambda^{\otimes m}(Z_i) \in \mathscr{C}$.*

Demostración. Supongamos que $\mathscr{C}$ es casi-cíclico y λ-casi-cíclico. Entonces, por la Proposición 4.4.4, para todo $Z \in \mathscr{C}$ se tiene que $\eta_\lambda^{\otimes m}(Z) \in \mathscr{C}$. En particular, esto es cierto para los vectores Z_i, $0 \leq i \leq s$. Recíprocamente, supongamos que $\mathscr{C}$ es casi-cíclico y que $\eta_\lambda^{\otimes m}(Z_i) \in \mathscr{C}$, $0 \leq i \leq s$. Sea $Z \in \mathscr{C}$. Como $Z_0, Z_1, \ldots, Z_s$ generan a $\mathscr{C}$, existen escalares $r_i \in \mathbb{Z}_{2^{k+1}}$ tales que $Z = r_0 Z_0 + \cdots + r_s Z_s$. Consecuentemente, como $\eta_\lambda^{\otimes m}$ es un $\mathbb{Z}_{2^{k+1}}$-automorfismo sobre $\mathbb{Z}_{2^{k+1}}^{nm}$,

$$\eta_\lambda^{\otimes m}(Z) = \eta_\lambda^{\otimes m}(r_0 Z_0 + \cdots + r_s Z_s) = r_0 \eta_\lambda^{\otimes m}(Z_1) + \cdots + r_s \eta_\lambda^{\otimes m}(Z_s).$$

Por lo tanto, ya que $\eta_\lambda^{\otimes m}(Z_i) \in \mathscr{C}$, se sigue que $\eta_\lambda^{\otimes m}(Z) \in \mathscr{C}$, pues $\mathscr{C}$ es un código lineal. □

Veamos un ejemplo en el que se ilustre la proposición anterior.

Ejemplo 4.4.10. Considere el código lineal $\mathscr{C}$ de longitud 4 sobre $\mathbb{Z}_8$ generado por los vectores 1003, 0107, 0013. En otros términos, $\mathscr{C}$ es el conjunto de todas las $\mathbb{Z}_8$-combinaciones lineales de 1003, 0107, 0013. Ya que $\alpha(1,0,0,3) + \beta(0,1,0,7) + \gamma(0,0,1,3) = (0,0,0,0)$ si y sólo si $\alpha = \beta = \gamma = 0$, $\mathscr{C}$ es un código de cardinalidad $8^3 = 512$. Por lo tanto, es impráctico listar todos los elementos de $\mathscr{C}$ para verificar si este código es cíclico y λ-cíclico ($\lambda = 1 + 2^k = 5$.) Sin embargo, como $\mathscr{C}$ está generado por 1003, 0107 y 0013, basta verificar esas propiedades para tales generadores. Como

$$\begin{aligned}
\sigma(1,0,0,3) &= (3,1,0,0) = 3(1,0,0,3) + 1(0,1,0,7) + 0(0,0,1,3),\\
\sigma(0,1,0,7) &= (7,0,1,0) = 7(1,0,0,3) + 0(0,1,0,7) + 1(0,0,1,3),\\
\sigma(0,0,1,3) &= (3,0,0,1) = 3(1,0,0,3) + 0(0,1,0,7) + 0(0,0,1,3),
\end{aligned}$$

se concluye que $\mathscr{C}$ es cíclico lineal. De este modo, por la Proposición 4.4.9, $\mathscr{C}$ es 5-cíclico si y sólo si $\eta_5(1,0,0,3) = (1,0,0,7)$, $\eta_5(0,1,0,7) = (0,1,0,3)$ y $\eta_5(0,0,1,3) = (0,0,1,7)$ están en $\mathscr{C}$. Note que $1007 \in \mathscr{C}$ si y sólo si existen $a,b,c \in \mathbb{Z}_8$ tales que $(1,0,0,7) = a(1,0,0,3) + b(0,1,0,7) + c(0,0,1,3) = (a,b,c,3a+7b+3c)$. De aquí, obtenemos que $a = 1$, $b = c = 0$. Pero al tomar tales valores para a,b,c tenemos que $3a+7b+3c = 3 \neq 7$ como se requiere para la última coordenada. Por lo tanto, $1007 \notin \mathscr{C}$ y, en consecuencia, $\mathscr{C}$ no es un código 5-cíclico.

En esta sección hemos caracterizado a los códigos λ-casi-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, $\lambda = 1 + 2^k$, como aquellos códigos $\mathscr{C}$ tales que $\varphi(\mathscr{C})$ es casi-negacíclico. También, estudiamos condiciones para que un código λ-casi-cíclico sea casi-cíclico del mismo índice (y viceversa). Asimismo, mencionamos otra propiedad que tienen los códigos que son casi-cíclicos y λ-casi-cíclicos (no necesariamente lineales), y también simplificamos las condiciones cuando el código es lineal. En particular, vimos en el Ejemplo 4.4.6, que los vectores en un código que es cíclico y λ-cíclico

no necesariamente tienen todas sus coordenadas en el ideal maximal de $\mathbb{Z}_{2^{k+1}}$. Por lo tanto, es natural preguntarse lo siguiente: ¿cuáles son las condiciones para que un código cíclico lineal $\mathscr{C} = \langle \widehat{F}_1, 2\widehat{F}_2, \ldots, 2^k \widehat{F}_k \rangle$ de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$, sea a su vez λ-cíclico lineal? Este es el tema de la siguiente sección.

4.5. Código cíclicos lineales que son $(1+2^k)$-cíclicos

En esta sección estableceremos condiciones necesarias y suficientes para que un código cíclico lineal de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$ sea $(1+2^k)$-cíclico lineal. Para este propósito usaremos los siguientes hechos que se han descrito con más detalle en la sección 1.3.1.

Recuerde que mediante la representación polinomial $P : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$ identificamos al vector $(a_0, a_1 \ldots, a_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$ con la clase lateral $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle$, y que un código $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ es un código cíclico lineal si y sólo si $P(\mathscr{C})$ es un ideal en el anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$. Asimismo, si I es un ideal de $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$ y n es un entero positivo impar, entonces por el Teorema 1.3.1 existe una colección única de polinomios $f_0, f_1, \ldots, f_{k+1}$ (posiblemente algunos de ellos iguales al polinomio constante 1) tales que $f_0 f_1 \cdots f_{k+1} = x^n - 1$ e $I = \langle \widehat{F}_1, 2\widehat{F}_2, \ldots, 2^k \widehat{F_{k+1}} \rangle$, donde $\widehat{F}_i = \widehat{f}_i + \langle x^n - 1\rangle$ y $\widehat{f}_i = (x^n - 1)/f_i$; más aún, $I = \langle \widehat{F}_1 + 2\widehat{F}_2 + \cdots + 2^k \widehat{F_{k+1}} \rangle$, es decir, $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$ es un anillo de ideales principales. Por último, recuerde que simplificaremos la notación escribiendo $\mathscr{C} = \langle \widehat{F}_1, 2\widehat{F}_2, \ldots, 2^k \widehat{F_{k+1}} \rangle$ y $\mathscr{C} = \langle \widehat{F}_1 + 2\widehat{F}_2 + \cdots + 2^k \widehat{F_{k+1}} \rangle$ para entender que $P(\mathscr{C}) = \langle \widehat{F}_1, 2\widehat{F}_2, \ldots, 2^k \widehat{F_{k+1}} \rangle$, o bien, $P(\mathscr{C}) = \langle \widehat{F}_1 + 2\widehat{F}_2 + \cdots + 2^k \widehat{F_{k+1}} \rangle$, respectivamente.

Sea $n \geq 1$ un entero impar y sea $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ un código cíclico lineal. Ya que $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$ es un anillo de ideales principales, existe $g(x) = g_0 + g_1 x + \cdots + g_{n-1}x^{n-1} + \langle x^n - 1\rangle$ tal que $P(\mathscr{C}) = \langle g(x)\rangle$. Esto implica que $Z \in \mathscr{C}$ si y sólo si existe $r(x) = r_0 + r_1 x + \cdots + r_{n-1}x^{n-1} + \langle x^n - 1\rangle$ tal que

$$P(Z) = r(x)g(x) = \sum_{i=0}^{n-1} \big(r_i x^i g(x)\big) + \langle x^n - 1\rangle.$$

Así, dado que la representación polinomial es un isomorfismo de $\mathbb{Z}_{2^{k+1}}$-módulos, $Z \in \mathscr{C}$ si y sólo si existen escalares $r_i \in \mathbb{Z}_{2^{k+1}}$ tales que

$$Z = P^{-1}\left(\sum_{i=0}^{n-1} \big(r_i x^i g(x)\big) + \langle x^n - 1\rangle\right) = \sum_{i=0}^{n-1} r_i P^{-1}(x^i g(x) + \langle x^n - 1\rangle).$$

Cabe mencionar, si es necesario, que el producto $r(x)g(x)$ es calculado en $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$ y, por lo tanto,

$$P^{-1}(x^i g(x)) = \sigma^i(g_0, g_1, \ldots, g_{n-1}),$$

donde $\sigma^i(g_0, g_1, \ldots, g_{n-1})$ significa que el corrimiento cíclico ha sido aplicado i veces al vector $(g_0, g_1, \ldots, g_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$. Consecuentemente,

$$Z = \sum_{i=0}^{n-1} r_i \sigma^i(g_0, g_1, \ldots, g_{n-1}).$$

Esto implica que $Z \in \mathscr{C}$ si y sólo si Z puede ser expresado como una $\mathbb{Z}_{2^{k+1}}$-combinación lineal (no necesariamente única) de $(g_0, g_1, \ldots, g_{n-1})$, $\sigma(g_0, g_1, \ldots, g_{n-1})$, $\ldots$, $\sigma^{n-1}(g_0, g_1, \ldots, g_{n-1})$. En consecuencia, tenemos el siguiente resultado. Como antes, escribimos $\lambda = 1 + 2^k$.

Proposición 4.5.1. *Sea $\mathscr{C}$ un código cíclico lineal de longitud n impar sobre $\mathbb{Z}_{2^{k+1}}$. Supongamos que $P(\mathscr{C}) = \langle g(x) \rangle$, donde $g(x) = g_0 + g_1 x + \cdots + g_{n-1}x^{n-1} + \langle x^n - 1 \rangle$. Entonces $\mathscr{C}$ es un código λ-cíclico si y sólo si $\eta_\lambda(\sigma^i(g_0, g_1, \ldots, g_{n-1})) = \nu_\lambda^i(g_0, g_1, \ldots, g_{n-1}) \in \mathscr{C}$, donde $1 \leq i \leq n-1$.*

Demostración. Recuerde que un código casi-cíclico de índice $m = 1$ es un código cíclico. Por lo tanto, la demostración es consecuencia inmediata de la Proposición 4.4.9. □

La Proposición 4.5.1 es útil porque basta conocer un polinomio que genere al ideal que corresponde al código cíclico y no es necesario que tal polinomio haya sido construido de una forma especial. Sin embargo, la manera usual de construir un código cíclico $\mathscr{C}$ de longitud n impar sobre $\mathbb{Z}_{2^{k+1}}$ es la siguiente: primero, se encuentra la factorización del polinomio $x^n - 1$ como un producto de polinomios mónicos y básicos irreducibles; segundo, se agrupan esos factores en $k+2$ polinomios $f_0, f_1, \ldots, f_{k+1}$ y, a partir de esta elección, se definen los polinomios $\widehat{F_1}, 2\widehat{F_2}, \cdots, 2^k\widehat{F_{k+1}}$. Finalmente, se considera el ideal en $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1 \rangle$ generado por $\widehat{F_1}, 2\widehat{F_2}, \cdots, 2^k\widehat{F_{k+1}}$. Si la construcción de un código cíclico ha sido realizada de esta forma, entonces podemos identitificar si el código cíclico $\mathscr{C}$ es λ-cíclico o no, analizando únicamente al polinomio generador $\widehat{F_1}$.

Proposición 4.5.2. *Con la notación anterior, si $\mathscr{C} = \langle \widehat{F_1}, 2\widehat{F_2}, \ldots, 2^k\widehat{F_{k+1}} \rangle$, entonces el código cíclico $\mathscr{C}$ es λ-cíclico si y sólo si $\eta_\lambda(\langle \widehat{F_1} \rangle) \subseteq \mathscr{C}$.*

Demostración. Sea $W \in \mathscr{C}$, entonces $W = A + B$, donde $A \in \langle \widehat{F_1} \rangle$ y $B \in \langle 2\widehat{F_2}, \ldots, 2^k\widehat{F_{k+1}} \rangle$. Como todo elemento de $\langle 2\widehat{F_2}, \ldots, 2^k\widehat{F_{k+1}} \rangle$ permanece fijo bajo la acción de η_λ, se sigue que $\eta_\lambda(W) = \eta_\lambda(A) + B \in \mathscr{C}$ si y si sólo si $\eta_\lambda(A) \in \mathscr{C}$. □

Corolario 4.5.3. *Con la notación anterior, $\eta_\lambda(\langle \widehat{F_1} \rangle) \subseteq \mathscr{C}$ si y sólo si $\nu_\lambda^i(f_0, f_1, \ldots, f_{n-1}) \in \mathscr{C}$ para todo $1 \leq i \leq n-1$, donde $\widehat{F_1} = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} + \langle x^n - 1 \rangle$.*

Como consecuencia de la Proposición 4.5.2 y del Corolario 4.5.3 , cualquier código cíclico lineal $\mathscr{C} = \langle \widehat{F_1}, 2\widehat{F_2}, \ldots, 2^k\widehat{F_{k+1}} \rangle$ tal que $\widehat{F_1} = 0 + \langle x^n - 1 \rangle$, es un código λ-cíclico, pues $f_0 = f_1 = \cdots = f_{n-1} = 0$ y, en consecuencia, $\nu_\lambda^i(0, \ldots, 0) = (0 \ldots, 0) \in \mathscr{C}$ para todo $1 \leq i \leq n-1$, puesto que $\mathscr{C}$ es lineal. Esto reafirma lo que observamos en el Corolario 4.4.5.

Veamos algunos ejemplos concretos.

Ejemplo 4.5.4. Sea $k=2$ y $n=3$ y recuerde que $x^3-1=a_1(x)a_2(x)=(x-1)(x^2+x+1)$ es la factorización de x^3-1 como un producto de polinomios mónicos, coprimos y básicos irreducibles sobre $\mathbb{Z}_8$. Sean $f_0=a_1(x)$, $f_1=a_2(x)$, $f_2=1$ y $f_3=1$. Entonces $\widehat{f_0}=a_2(x)$, $\widehat{f_1}=a_1(x)$, $\widehat{f_2}=x^3-1$ y $\widehat{f_3}=x^3-1$ y, por lo tanto, en el anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^3-1\rangle$, $\widehat{F_0}=a_2(x)$, $\widehat{F_1}=a_1(x)$, $\widehat{F_2}=0$ y $\widehat{F_3}=0$. Así, por el Teorema 1.3.1, $\mathscr{C}=\langle\widehat{F_1}\rangle=\langle x-1\rangle$ es un código cíclico lineal de longitud 3 sobre $\mathbb{Z}_8$, y cardinalidad 2^6. Ya que $x-1$ es el polinomio generador de $\mathscr{C}$ y $P^{-1}(x-1)=(-1,1,0)=(7,1,0)\in\mathbb{Z}_8^3$, se sigue que $\mathscr{C}$ es $(1+2^2)$-cíclico si y sólo si los vectores

$$\nu_5(7,1,0)=(0,7,1) \qquad\qquad \nu_5^2(7,1,0)=\nu_5(0,7,1)=(5,0,7)$$

son elementos de $\mathscr{C}$. Esto es muy fácil verificarlo puesto que $(a,b,c)\in\mathscr{C}$ si y sólo si existe un polinomio $h(x)$ tal que $a_0+a_1x+a_2x^2+\langle x^3-1\rangle=h(x)(x-1)+\langle x^3-1\rangle$, lo que ocurre si y sólo si $x=1$ es una raíz del polinomio $a_0+a_1x+a_2x^2\in\mathbb{Z}_8[x]$. Entonces, es claro que $x=1$ es un raíz de $7x+x^2$ pero que no es raíz de $5+7x^2$ y, por lo tanto, $(5,0,7)\notin\mathscr{C}$. Esto nos permite concluir que $\mathscr{C}$ no es 5-cíclico.

Note que si $\mathscr{C}\subseteq\mathbb{Z}_8^3$ es un código cíclico lineal tal que $\mathscr{C}=\langle x-1,2\widehat{F_2},2^2\widehat{F_3}\rangle$, entonces el código cíclico lineal $\mathscr{D}=\langle x-1\rangle$ (Ejemplo 4.5.4) está contenido en $\mathscr{C}$, es decir, $\mathscr{D}$ es un subcódigo de $\mathscr{C}$. Ya que $\mathscr{D}$ no es un código λ-cíclico, es natural pensar que $\mathscr{C}$ no es λ-cíclico. Sin embargo, los polinomios $2\widehat{F_2},2^2\widehat{F_3}$ pueden ayudar a que $\mathscr{C}$ sea λ-cíclico, sin importar que $\mathscr{D}$ no sea λ-cíclico. Para ilustrar esto, presentamos el siguiente ejemplo.

Ejemplo 4.5.5. Sean $a_1(x)$ y $a_2(x)$ como en el ejemplo anterior. Considere ahora que $f_0=1$, $f_1=a_2(x)$, $f_2=1$ y $f_3=a_1(x)$. Entonces se sigue que $\widehat{F_0}=0$, $\widehat{F_1}=a_1(x)$, $\widehat{F_2}=0$ y $\widehat{F_3}=a_2(x)$. Por lo tanto, $\mathscr{C}=\langle\widehat{F_1},2^2\widehat{F_3}\rangle=\langle a_1(x),2^2a_2(x)\rangle=\langle a_1(x)+2^2a_2(x)\rangle=\langle 3+5x+4x^2\rangle$ es un código cíclico de longitud 3 sobre $\mathbb{Z}_8$ y cardinalidad $2^7=128$. De este modo, por la Proposición 4.5.2 y el Corolario 4.5.3, $\mathscr{C}$ es un código λ-cíclico si y sólo si los vectores $\nu_\lambda^i(7,1,0)$, con $1\leq i\leq 2$, pertenecen a $\mathscr{C}$. Dicho de otra forma, $\mathscr{C}$ es λ-cíclico si y sólo si $\nu_\lambda(7,1,0)=(0,7,1)$ y $\nu_\lambda^2(0,7,1)=(5,0,7)$ pueden ser expresados como $\mathbb{Z}_8$-combinaciones lineales de $(3,5,4)$, $(4,3,5)$ y $(5,4,3)$. Ya que el código es cíclico, $\nu_\lambda(7,1,0)=(0,7,1)\in\mathscr{C}$. Así, resta verificar si $\nu_\lambda^2(0,7,1)=(5,0,7)$ está o no en $\mathscr{C}$. Como

$$(5,0,7)=0(3,5,4)+4(4,3,5)+1(5,4,3),$$

concluimos que $(5,0,7)\in\mathscr{C}$ y, por lo tanto, $\mathscr{C}$ es λ-cíclico.

Los Cuadros 4.1 y 4.2 contienen una lista de todos los códigos cíclicos lineales (no triviales) de longitud 3 sobre $\mathbb{Z}_8$ y $\mathbb{Z}_{16}$, respectivamente escritos de la forma $\langle\widehat{F_1},2\widehat{F_2},2^2\widehat{F_3}\rangle$ y $\langle\widehat{G_1},2\widehat{G_2},2^2\widehat{G_3},2^3\widehat{G_4}\rangle$. Hemos señalado con una ✓ aquellos códigos cíclicos que son también λ-cíclicos, con $\lambda=1+2^k$. Consecuentemente, aquellos códigos $\mathscr{C}$ señalado con ✓, son tales que $\varphi(\mathscr{C})$ es un código casi-negacíclico, casi-cíclico y, en virtud de la Proposición 4.4.7, son invariantes con respecto a la aplicación $\eta_{-1}^{\otimes 2^{k-1}}$.

Generadores	Cardinalidad	5-cíclico	Generadores	Cardinalidad	5-cíclico
$\langle 2\rangle$	2^6	✓	$\langle 2^2a_2\rangle$	2	✓
$\langle 2^2\rangle$	2^3	✓	$\langle a_1, 2a_2\rangle$	2^8	✓
$\langle a_1\rangle$	2^6	–	$\langle a_1, 2^2a_2\rangle$	2^7	✓
$\langle 2a_1\rangle$	2^4	✓	$\langle a_2, 2a_1\rangle$	2^7	✓
$\langle 2^2a_1\rangle$	2^2	✓	$\langle a_2, 2^2a_1\rangle$	2^5	✓
$\langle a_2\rangle$	2^3	–	$\langle 2a_1, 2^2a_2\rangle$	2^5	✓
$\langle 2a_2\rangle$	2^2	✓	$\langle 2a_2, 2^2a_1\rangle$	2^4	✓

$x^3-1=a_1a_2, \quad a_1=x+7, \quad a_2=x^2+x+1$

✓: código cíclico y 5-cíclico

–: código cíclico pero no 5-cíclico

Cuadro 4.1: Códigos cíclicos lineales de longitud 3 sobre $\mathbb{Z}_8$ que son 5-cíclicos.

Observe que 12 de los 14 códigos cíclicos lineales (no triviales) de longitud 3 sobre $\mathbb{Z}_8$ son también códigos 5-cíclicos, es decir, solamente 2 códigos cíclicos no son 5-cíclicos. Asimismo, 20 de los 22 códigos códigos cíclicos lineales (no triviales) de longitud 3 sobre $\mathbb{Z}_{16}$ son códigos 9-cíclicos. Esto implica que la mayoría de los códigos cíclicos tienen como imagen bajo φ a un código casi-negacíclico. Sin embargo, como no todos los códigos cíclicos son λ-cíclicos, tenemos algunos códigos cuya imagen bajo φ no es un código casi-negacíclico. El propósito de la siguiente sección es obtener códigos casi-negacíclicos sobre $\mathbb{Z}_4$ a partir de cualquier código cíclico lineal de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$.

Antes de inciar una nueva sección, presentaremos otro resultado que caracteriza a aquellos códigos cíclicos que son λ-cíclicos. Dicho resultado, será usado más adelante para caracterizar códigos que son cíclicos y λ-cíclicos a través de sus imágenes binarias (Teorema 4.8.4). Para tal propósito, recuerde que se ha definido la aplicación $\widetilde{\mu}_\lambda : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}_{2^{k+1}}^n$ como (sección 1.4)

$$(a_0, a_1, a_2, \ldots, a_i, \ldots, a_{n-1}) \mapsto (a_0, \lambda a_1, \lambda^2 a_2, \ldots, \lambda^i a_i, \ldots, \lambda^{n-1} a_{n-1}).$$

Asimismo, recuerde que si n es impar, entonces la aplicación μ_λ con dominio $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n-1\rangle$ y contradominio $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n-\lambda\rangle$, definida como $A(x)+\langle x^n-1\rangle \mapsto A(\lambda x)+\langle x^n-\lambda\rangle$, es un isomorfismo de anillos (Lema 1.3.6) tal que $\mu_\lambda \circ P = P \circ \widetilde{\mu}_\lambda$. En particular, este hecho implica que un código $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ es cíclico lineal si y sólo si $\widetilde{\mu_\lambda}(\mathscr{C})$ es λ-cíclico lineal (Lema 1.4.1).

Proposición 4.5.6. *Sea $\mathscr{C}$ un código cíclico lineal de longitud n impar sobre $\mathbb{Z}_{2^{k+1}}$. Entonces, $\widetilde{\mu}_\lambda(\mathscr{C}) = \mathscr{C}$ si y sólo si $\mathscr{C}$ es un código λ-cíclico lineal.*

Demostración. Supongamos que $\widetilde{\mu}_\lambda(\mathscr{C}) = \mathscr{C}$. Como $\mu_\lambda \circ P = P \circ \widetilde{\mu}_\lambda$, se sigue que $\mu_\lambda(P(\mathscr{C})) = P(\widetilde{\mu}_\lambda(\mathscr{C})) = P(\mathscr{C})$. Por otro lado, como $\mathscr{C}$ es cíclico lineal de longitud impar, $P(\mathscr{C})$ es un ideal

Generadores	Cardinalidad	9-cíclico	Generadores	Cardinalidad	9-cíclico
$\langle 2\rangle$	2^9	✓	$\langle a_1, 2^2a_2\rangle$	2^{10}	✓
$\langle 2^2\rangle$	2^6	✓	$\langle a_1, 2^3a_2\rangle$	2^9	✓
$\langle a_1\rangle$	2^8	–	$\langle a_2, 2a_1\rangle$	2^{10}	✓
$\langle 2a_1\rangle$	2^6	✓	$\langle a_2, 2^2a_1\rangle$	2^8	✓
$\langle 2^2a_1\rangle$	2^4	✓	$\langle a_2, 2^3a_1\rangle$	2^6	✓
$\langle 2^3a_1\rangle$	2^2	✓	$\langle 2a_1, 2^2a_2\rangle$	2^8	✓
$\langle a_2\rangle$	2^4	–	$\langle 2a_1, 2^3a_2\rangle$	2^7	✓
$\langle 2a_2\rangle$	2^3	✓	$\langle 2^2a_1, 2^3a_2\rangle$	2^5	✓
$\langle 2^2a_2\rangle$	2^2	✓	$\langle 2a_2, 2^2a_1\rangle$	2^7	✓
$\langle 2^3a_2\rangle$	2	✓	$\langle 2a_2, 2^3a_1\rangle$	2^5	✓
$\langle a_1, 2a_2\rangle$	2^{11}	✓	$\langle 2^2a_2, 2^3a_1\rangle$	2^4	✓

$x^3-1=a_1a_2, \quad a_1=x+15, \quad a_2=x^2+x+1$

✓: código cíclico y 9-cíclico

–: código cíclico pero no 9-cíclico

Cuadro 4.2: Códigos cíclicos lineales de longitud 3 sobre $\mathbb{Z}_{16}$ que son 9-cíclicos.

en $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n-1\rangle$ y, por lo tanto, $\mu_\lambda(P(\mathscr{C}))=P(\mathscr{C})$ es un ideal en $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n-\lambda\rangle$. Esto implica que $\mathscr{C}$ es un código λ-cíclico lineal.
Recíprocamente, sea $Z=(z_0,z_1,\ldots,z_i,\ldots,z_{n-1})\in\mathscr{C}$. Entonces, dado que por hipótesis $\mathscr{C}$ es cíclico y λ-cíclico lineal, los siguientes vectores son elementos del código $\mathscr{C}$:

$$\begin{aligned}
\sigma^{n-i-1}(Z) &= (z_{i+1},\ldots,z_{n-i-1},z_i),\\
\sigma^{n-i}(Z) &= (z_i,z_{i+1},\ldots,z_{n-i-1}),\\
\nu_\lambda(\sigma^{n-i-1}(Z)) &= (\lambda z_i,z_{i+1},\ldots,z_{n-i-1}),\\
\sigma^{n-i}(Z)-\nu_\lambda(\sigma^{n-i-1}(Z)) &= (2^kz_i,0,\ldots,0),\\
\sigma^{i}(\sigma^{n-i}(Z)-\nu_\lambda(\sigma^{n-i-1}(Z))) &= (0,\ldots,0,2^kz_i,0,\ldots,0),
\end{aligned}$$

donde $0\le i\le n-1$. Por lo tanto, $\mathscr{C}$ contiene a todos los vectores de la forma

$$x_i=(0,\ldots,0,2^kz_i,0,\ldots,0),$$

donde 2^kz_i aparece en la coordenada i, $0\le i\le n-1$ e i es un número impar. Como consecuencia de este hecho, y de que $\mathscr{C}$ es lineal, $\widetilde{\mu}_\lambda(Z)=Z+x_1+x_3+\cdots+x_{n-2}\in\mathscr{C}$, tal como queríamos demostrar. □

Ya que el código cíclico $\mathscr{C}$ de la Proposición anterior es lineal, la Proposición 4.5.6 se puede enunciar para los generadores del código $\mathscr{C}$.

4.6. Códigos cíclicos lineales y códigos casi-negacíclicos

En esta sección mostraremos una manera conveniente de obtener códigos casi-negacíclicos como imágenes bajo φ de códigos cíclicos lineales de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$. Nuestro punto de partida es el siguiente diagrama conmutativo, el cual implica que un código $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ es cíclico lineal si y sólo si $\widetilde{\mu}_\lambda(\mathscr{C})$ es λ-cíclico lineal (Lema 1.4.1), donde $\lambda = 1+2^k$.

$$\begin{array}{ccc} \mathbb{Z}_{2^{k+1}}^n & \xrightarrow{P} & \mathbb{Z}_{2^{k+1}}[x]/\langle x^n-1\rangle \\ \downarrow{\scriptstyle \widetilde{\mu}_\lambda} & & \downarrow{\scriptstyle \mu_\lambda} \\ \mathbb{Z}_{2^{k+1}}^n & \xrightarrow{P} & \mathbb{Z}_{2^{k+1}}[x]/\langle x^n-\lambda\rangle \end{array}$$

Del Teorema 4.2.1, sabemos que la imagen bajo φ de un código cíclico (lineal o no) de longitud n sobre $\mathbb{Z}_{2^{k+1}}$ es un código casi-cíclico de índice 2^{k-1} y longitud $2^{k-1}n$ sobre $\mathbb{Z}_4$. Igualmente, del Teorema 4.4.1, la imagen de un código λ-cíclico (lineal o no) de longitud n sobre $\mathbb{Z}_{2^{k+1}}$ es un código casi-negacíclico de índice 2^{k-1} y longitud $2^{k-1}n$ sobre $\mathbb{Z}_4$. Ya que por un lado tenemos códigos casi-cíclicos y, por otro, códigos casi-negacíclicos, es natural preguntarse si es posible agregar una aplicación en el lado derecho del siguiente diagrama de tal forma que éste conmute.

$$\begin{array}{ccccc} \mathbb{Z}_{2^{k+1}}[x]/\langle x^n-1\rangle & \xrightarrow{P^{-1}} & \mathbb{Z}_{2^{k+1}}^n & \xrightarrow{\varphi} & \mathbb{Z}_4^{2^{k-1}n} \\ \downarrow{\scriptstyle \mu_\lambda} & & \downarrow{\scriptstyle \widetilde{\mu}_\lambda} & & \vdots\,? \\ \mathbb{Z}_{2^{k+1}}[x]/\langle x^n-\gamma\rangle & \xrightarrow{P^{-1}} & \mathbb{Z}_{2^{k+1}}^n & \xrightarrow{\varphi} & \mathbb{Z}_4^{2^{k-1}n} \end{array}$$

De ser posible esto, se tendría que la imagen bajo φ de códigos cíclicos lineales de longitud n, n impar, sobre $\mathbb{Z}_{2^{k+1}}$, está relacionada con la imagen bajo φ de códigos λ-cíclicos lineales de longitud n sobre $\mathbb{Z}_{2^{k+1}}$. Para responder esta pregunta, estudiamos la composición $\varphi \circ \widetilde{\mu}_\lambda$.

Proposición 4.6.1. *Sean $\lambda = 1+2^k$, $k \geq 1$ y $n \geq 1$ un entero. Entonces, para todo $Z \in \mathbb{Z}_{2^{k+1}}^n$,*

$$(\varphi \circ \widetilde{\mu}_\lambda)(Z) = (\widetilde{\mu}_{-1}^{\otimes 2^{k-1}} \circ \varphi)(Z).$$

Demostración. Primero, recordemos que para todo $Z \in \mathbb{Z}_{2^{k+1}}^n$,

$$\varphi(Z) = c_{k-1}^{k-1} \otimes r_0(Z) + 2\left[c_0^{k-1} \otimes r_1(Z) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes r_k(Z)\right].$$

En consecuencia,

$$\varphi\left(\widetilde{\mu}_\lambda(Z)\right) = c_{k-1}^{k-1} \otimes r_0(\widetilde{\mu}_\lambda(Z)) + 2\left[c_0^{k-1} \otimes r_1(\widetilde{\mu}_\lambda(Z)) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes r_k(\widetilde{\mu}_\lambda(Z))\right].$$

Por lo tanto, con el propósito de obtener la identidad que establece esta Proposición, calculamos la representación 2-ádica del vector $\widetilde{\mu}_\lambda(Z)$. Ya que $\lambda = 1 + 2^k$ es una unidad de orden 2, la coordenada z_j del vector Z, con j impar, aparece multiplicada por λ en $\widetilde{\mu}_\lambda(Z)$; mientras que, si j es par, z_j aparce sin modificar en el vector $\widetilde{\mu}_\lambda(Z)$. Por otra parte, recuerde que la representación 2-ádica de λz_j es

$$\lambda z_j = r_0(z_j) + 2r_1(z_j) + \cdots + 2^{k-1} r_{k-1}(z_j) + 2^k(r_0(z_j) \oplus r_k(z_j)).$$

Por lo tanto, si $e = (e_0, e_1, \ldots, e_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$ es el vector tal que $e_j = 0$ si j es par, y $e_j = 1$ si j es impar, entonces la representación 2-ádica de $\widetilde{\mu}_\lambda(Z)$ puede ser expresada como sigue:

$$\widetilde{\mu}_\lambda(Z) = r_0(Z) + 2r_1(Z) + \cdots + 2^{k-1} r_k(Z) + 2^k(r_k(Z) \oplus e * r_0(Z)),$$

donde $e * r_0(Z)$ es la multiplicación coordenada a coordenada de e y $r_0(Z)$. Sustituyendo esta última relación en la expresión de $\varphi\left(\widetilde{\mu}_\lambda(Z)\right)$ obtenemos que

$$\varphi\left(\widetilde{\mu}_\lambda(Z)\right) = c_{k-1}^{k-1} \otimes r_0(Z) + 2\left[c_0^{k-1} \otimes r_1(Z) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes (r_k(Z) \oplus e * r_0(Z))\right].$$

De aquí, por la propiedad de distributividad del producto de Kronecker y por el Corolario 2.3.3, se sigue que

$$\varphi\left(\widetilde{\mu}_\lambda(Z)\right) = c_{k-1}^{k-1} \otimes (r_0(Z) + 2e * r_0(Z)) + 2\left[c_0^{k-1} \otimes r_1(Z) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes r_k(Z)\right].$$

Ahora, por la definición de e, tenemos que $r_0(Z) + 2e * r_0(Z) = \widetilde{\mu}_{-1}(r_0(Z))$ y, por lo tanto,

$$c_{k-1}^{k-1} \otimes (r_0(Z) \oplus 2e * r_0(Z) = \widetilde{\mu}_{-1}^{\otimes 2^{k-1}}(r_0(Z)).$$

Además, ya que el vector $2\left[c_0^{k-1} \otimes r_1(Z) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes r_k(Z)\right]$ tiene todas sus coordenadas en el ideal maximal, éste permanece invariante bajo $\widetilde{\mu}_{-1}^{\otimes 2^{k-1}}$. Por lo tanto,

$$\varphi\left(\widetilde{\mu}_\lambda(Z)\right) = \widetilde{\mu}_{-1}^{\otimes 2^{k-1}}(r_0(Z)) + \widetilde{\mu}_{-1}^{\otimes 2^{k-1}}\left(2\left[c_0^{k-1} \otimes r_1(Z) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes r_k(Z)\right]\right),$$

de donde conluimos que $\varphi\left(\widetilde{\mu}_\lambda(Z)\right) = \widetilde{\mu}_{-1}^{\otimes 2^{k-1}}(\varphi(Z))$. □

La Proposición 4.6.1 establece que la aplicación $\widetilde{\mu}_{-1}^{\otimes 2^{k-1}} : \mathbb{Z}_4^{2^{k-1}n} \to \mathbb{Z}_4^{2^{k-1}n}$ hace conmutar el siguiente diagrama, sin importar si n es par o impar.

$$\begin{array}{ccc} \mathbb{Z}_{2^{k+1}}^n & \xrightarrow{\varphi} & \mathbb{Z}_4^{2^{k-1}n} \\ \downarrow{\scriptstyle \widetilde{\mu}_\lambda} & & \downarrow{\scriptstyle \widetilde{\mu}_{-1}^{\otimes 2^{k-1}}} \\ \mathbb{Z}_{2^{k+1}}^n & \xrightarrow{\varphi} & \mathbb{Z}_4^{2^{k-1}n} \end{array}$$

En particular, si n es impar, entonces tenemos el siguiente resultado.

Teorema 4.6.2. *Sean $k \geq 1$, $\lambda = 1+2^k$ y $n \geq 1$ un entero impar. Entonces, el siguiente diagrama conmuta*

$$\begin{array}{ccccc} \mathbb{Z}_{2^{k+1}}[x]/\langle x^n-1\rangle & \xrightarrow{P^{-1}} & \mathbb{Z}_{2^{k+1}}^n & \xrightarrow{\varphi} & \mathbb{Z}_4^{2^{k-1}n} \\ \downarrow{\scriptstyle \mu_\lambda} & & \downarrow{\scriptstyle \widetilde{\mu}_\lambda} & & \downarrow{\scriptstyle \widetilde{\mu}_{-1}^{\otimes 2^{k-1}}} \\ \mathbb{Z}_{2^{k+1}}[x]/\langle x^n-\gamma\rangle & \xrightarrow{P^{-1}} & \mathbb{Z}_{2^{k+1}}^n & \xrightarrow{\varphi} & \mathbb{Z}_4^{2^{k-1}n} \end{array}$$

Consecuentemente, si $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ es un código cíclico lineal, entonces $\widetilde{\mu}_{-1}^{\otimes 2^{k-1}}(\varphi(\mathscr{C}))$ es un código casi-negacíclico (no necesariamente lineal) de índice 2^{k-1} y longitud $2^{k-1}n$ sobre $\mathbb{Z}_4$.

Demostración. La conmutatividad del diagrama es consecuencia inmediata de la Proposición 4.6.1. Supongamos que $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ es un código cíclico lineal, con n impar. Entonces, por el Lema 1.4.1, $\widetilde{\mu}_\lambda(\mathscr{C})$ es un código λ-cíclico lineal de longitud n y, por lo tanto, $\varphi(\widetilde{\mu}_\lambda(\mathscr{C}))$ es un código casi-negacíclico de índice 2^{k-1} y longitud $2^{k-1}n$ sobre $\mathbb{Z}_4$. Ya que $\varphi(\widetilde{\mu}_\lambda(\mathscr{C})) = \widetilde{\mu}_{-1}^{\otimes 2^{k-1}}(\varphi(\mathscr{C}))$, el resultado se sigue. □

Recuerde que si $\mathscr{C}$ es un código cíclico lineal de longitud $n \geq 1$ (impar) sobre $\mathbb{Z}_4$, entonces $\widetilde{\mu}_{-1}(\mathscr{C})$ es un código negacíclico de longitud $n \geq 1$ sobre $\mathbb{Z}_4$ (Corolario 2.5 de [54]). Asimismo, recuerde que un código $\mathscr{D} \subseteq \mathbb{Z}_4^{2^{k-1}n}$ es llamado $\mathbb{Z}_{2^{k+1}}$-lineal si existe un código lineal $\mathscr{E} \subseteq \mathbb{Z}_{2^{k+1}}^n$ tal que $\varphi(\mathscr{E})$ es permutación equivalente a $\mathscr{D}$. Así, en estos términos, el Teorema 4.6.2, establece que si $\mathscr{D}$ es un código $\mathbb{Z}_{2^{k+1}}$-lineal y casi-cíclico de índice 2^{k-1} y longitud $2^{k-1}n$ (n impar) sobre $\mathbb{Z}_4$, entonces $\widetilde{\mu}_{-1}^{\otimes 2^{k-1}}(\mathscr{D})$ es un código casi-negacíclico. Más aún, observe que $\widetilde{\mu}_{-1}^{\otimes 2^{k-1}}(\mathscr{D})$, es un código $\mathbb{Z}_{2^{k+1}}$-lineal. En este sentido, el Teorema 4.6.2 ofrece una generalización del Corolario 2.5 de [54].

Veamos un ejemplo

Ejemplo 4.6.3. Sea $\mathscr{C}$ el código lineal de longitud 3 sobre $\mathbb{Z}_8$ generado por el polinomio $a_2(x) = 1+x+x^2$. En otros términos,

$$P(\mathscr{C}) = \{a_2(x)r(x) + \langle x^3-1\rangle \ : \ r(x) + \langle x^3-1\rangle \in \mathbb{Z}_8[x]/\langle x^3-1\rangle\}.$$

Si $r(x) = r_0 + r_1x + r_2x^2 + \langle x^3-1\rangle$, entonces

$$a_2(x)r(x) + \langle x^3-1\rangle = \sum_{i=0}^{2} r_i x^i a_2(x) + \langle x^3-1\rangle.$$

Ya que $x^i a_2(x) + \langle x^3-1\rangle = a_2(x) + \langle x^3-1\rangle$, se sigue que

$$P^{-1}(a_2(x)r(x) + \langle x^3-1\rangle) = \sum_{i=0}^{2} r_i P^{-1}(x^i a_2(x) + \langle x^3-1\rangle) = \alpha(111),$$

donde $\alpha = \sum_{i=0}^{2} r_i$. Consecuentemente,

$$\mathscr{C} = \{\alpha(111) \ : \ \alpha \in \mathbb{Z}_8\} = \{000, 111, 222, 333, 444, 555, 666, 777\},$$

es decir, $\mathscr{C}$ es el código de repetición de longitud 3 sobre $\mathbb{Z}_8$. Claramente este código no es 5-cíclico y, por lo tanto, $\varphi(\mathscr{C})$ no es un código casi-negacíclcico de índice 2. Sin embargo, en virtud del Teorema 4.6.2, el código $\widetilde{\mu}_{-1}^{\otimes 2}(\varphi(\mathscr{C}))$ sí es un código casi-negacíclico de índice 2; tal como se muestra en el siguiente Cuadro:

	φ		$\widetilde{\mu}_{-1}^{\otimes 2}$	
000	$\to$	000 000	$\to$	000 000
111	$\to$	111 111	$\to$	131 131
222	$\to$	000 222	$\to$	000 222
333	$\to$	111 333	$\to$	131 313
444	$\to$	222 222	$\to$	222 222
555	$\to$	333 333	$\to$	313 313
666	$\to$	222 000	$\to$	222 000
777	$\to$	333 111	$\to$	313 131

4.7. Imágenes binarias de códigos $(1+2^k)$-casi-cíclicos

En esta sección estudiaremos propiedades de casi-ciclícidad de la imagen de Gray de un código $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ (no necesariamente lineal) que tiene la propiedad de ser $(1+2^k)$-casi-cíclico. Por medio de ejemplos veremos que el código $\Phi(\mathscr{C})$, donde $\Phi : (\mathbb{Z}_{2^{k+1}}^n, \delta_h) \to (\mathbb{F}_2^{2^{kn}}, \delta_H)$ es la isometría de Gray, no siempre es casi-cíclico, lo cual es natural en virtud del Teorema 4.2.1. Sin

embargo, mostraremos que $\Phi(\mathscr{C})$ es permutación equivalente a un código casi-cíclico, lo que conlleva a la definición de una isometría $\Phi_1 : (\mathbb{Z}_{2^{k+1}}^n, \delta_h) \to (\mathbb{F}_2^{2^{kn}}, \delta_H)$ permutación equivalente a la isometría de Gray Φ. Con la introducción de la isometría Φ_1, se demuestra lo siguiente: el código $\Phi_1(\mathscr{C})$ es casi-cíclico de índice $2^{k-1}m$ si y sólo si $\mathscr{C}$ es un código $(1+2^k)$-casi-cíclico de índice m y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$.

Iniciamos este apartado presentando algunos ejemplos que ilustran que, en general, la imagen de Gray de un código $(1+2^k)$-casi-cíclico no es un código casi-cíclico de algún índice pero que sí es equivalente a un código casi-cíclico. Para ser consistentes con la notación introducida en las secciones previas, sea $\lambda = 1+2^k$, $k \geq 1$.

Ejemplo 4.7.1. Considere el código $\mathscr{C}$ de longitud 3 sobre $\mathbb{Z}_8$ con elementos

$$000 \quad 151 \quad 222 \quad 373 \quad 444 \quad 515 \quad 666 \quad 737.$$

Este código es λ-cíclico lineal, con $\lambda = 1+2^k = 5$. La imagen de $\mathscr{C}$ con respecto a la isometría Φ de Gray es un código binario de longitud 12 cuyos elementos son:

$$\begin{array}{cccc} 000000000000 & 010010101101 & 000111000111 & 010101101010 \\ 111111111111 & 101101010010 & 111000111000 & 101010010101 \end{array}$$

Observe que si $z = 010010101101$, entonces los vectores $\sigma^{\otimes 6}(z)$, $\sigma^{\otimes 4}(z)$, $\sigma^{\otimes 3}(z)$, $\sigma^{\otimes 2}(z)$ y $\sigma^{\otimes 1}(z) = \sigma(z)$ no pertenecen al código $\Phi(\mathscr{C})$. Por lo tanto, $\Phi(\mathscr{C})$ no tiene alguna propiedad de casi-ciclicidad. Sin embargo, si definimos la permutación $\varepsilon : I_{12} \to I_{12}$ como $\varepsilon = (3 \quad 6)(4 \quad 7)(5 \quad 8)$ y consideramos la permutación $\widetilde{\varepsilon}$ sobre $\mathbb{F}_2^{12}$ inducida por ε, entonces afirmamos que el código $\widetilde{\varepsilon}(\Phi(\mathscr{C}))$ es casi-cíclico de índice 2 y longitud 12 sobre $\mathbb{F}_2$. Para demostrar esto, observe que los elementos de $\widetilde{\varepsilon}(\Phi(\mathscr{C}))$ son:

$$\begin{array}{cccc} 000000000000 & 010101010101 & 000000111111 & 010101101010 \\ 111111111111 & 101010101010 & 111111000000 & 101010010101 \end{array}$$

Entonces, es claro que los vectores de la primera y tercera columna permanecen invariantes con respecto a $\sigma^{\otimes 2}$. Asimismo, es claro que $\sigma^{\otimes 2}$ intercambia los vectores de la segunda y cuarta columna. De aquí, concluimos que $\widetilde{\varepsilon}(\Phi(\mathscr{C}))$ es casi-cíclico de índice 2 y longitud 12 sobre $\mathbb{F}_2$, tal como se afirmó.

Ejemplo 4.7.2. Considere el siguiente código $\mathscr{C}$ no lineal de longitud 3 sobre $\mathbb{Z}_{16}$:

$$(1,14,5) \quad (5,9,14) \quad (9,14,13) \quad (13,1,14) \quad (14,5,9) \quad (14,13,1).$$

Es fácil verificar, por inspección directa, que $\mathscr{C}$ es λ-cíclico, con $\lambda = 1+2^3 = 9$. La imagen de Gray de $\mathscr{C}$ es un código binario de longitud 24 cuyos elementos son:

$$\begin{array}{ccc} 010001000011111100101110 & 011110010111101000100001 & 111100101110010001000011 \\ 101000100001011110010111 & 101011001111110000010100 & 110000010100101011001111 \end{array}$$

Sea $z = 010001000011111100101110$ (fila 1 y columna 1 del arreglo anterior) y $d > 1$ cualquier divisor de 24. Entonces es fácil verificar, mediante cálculos directos, que $\sigma^{\otimes d}(z) \notin \mathscr{C}$. Por lo tanto, el código $\mathscr{C}$ no es casi-cíclico para algún índice. No obstante, de igual modo que en el Ejemplo 4.7.1, permutando las coordenadas de $\Phi(\mathscr{C})$ es posible obtener un código que sí sea casi-cíclico. Para demostrar esto, sea $\varepsilon : I_8 \to I_8$ la permutación definida como

$$\varepsilon = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 2 & 4 & 6 & 1 & 3 & 5 & 7 \end{pmatrix} = (1 \quad 2 \quad 4)(3 \quad 6 \quad 5).$$

Entonces afirmamos que $\widetilde{\varepsilon}(\Phi(\mathscr{C}))$ es un código casi-cíclico de índice 4 y longitud 24, donde $\widetilde{\varepsilon}$ es la permutación sobre $\mathbb{F}_2^{24} = (\mathbb{F}_2^3)^8$ inducida por ε de la siguiente manera:

$$\widetilde{\varepsilon} : (Z_0|Z_1|\cdots|Z_7) \mapsto \left(Z_{\varepsilon(0)}|Z_{\varepsilon(1)}|\cdots|Z_{\varepsilon(7)}\right), \qquad Z_i \in \mathbb{F}_2^3$$

Esto puede constatarse teniendo en cuenta que los elementos del código $\widetilde{\varepsilon}(\Phi(\mathscr{C}))$ son:

010111001100000101011110	011101110000010100111001	111010100001101000110011
101011000110100010001111	101110011000001010111100	110101000011010001100111

Ejemplo 4.7.3. Sea $\mathscr{C}$ el código de longitud 6 sobre $\mathbb{Z}_8$ que consta de los elementos dados a continuación:

062 100	062 243	062 247	062 500	062 674	062 634	206 324	206 467	206 463
206 724	206 010	206 050	602 720	602 063	602 067	602 320	602 414	602 454

Por inspección directa, es fácil verificar que $\mathscr{C}$ es un código λ-casi-cíclico de índice 2, donde $\lambda = 1+2^k = 5$. La imagen de Gray de $\mathscr{C}$ es el siguiente código binario de longitud 24:

010000001000010100001100	010010001111010011001110	010011001110010010001111
010100001100010000001000	010111001001010101001011	010101001011010111001001
001001100111001101100011	001111100100001110100101	001110100101001111100100
001101100011001001100111	001000100000001010100010	001010100010001000100000
100100001010100000001110	100010001001100011001000	100011001000100010001001
100000001110100100001010	100101001101100111001111	100111001111100101001101

De igual modo que en los ejemplos anteriores, $\Phi(\mathscr{C})$ no es casi-cíclico para algún índice. Pero, siguiendo con la misma filosofía, permutamos las coordenadas de $\Phi(\mathscr{C})$ para inducir alguna propiedad de casi-ciclicidad en $\Phi(\mathscr{C})$. Con la notación del Ejemplo 4.7.2, es posible, aunque tedioso, verificar que en efecto $\widetilde{\varepsilon}(\Phi(\mathscr{C}))$ es un código casi-cíclico de índice 4 y longitud 24 sobre $\mathbb{F}_2$.

En los Ejemplos 4.7.1, 4.7.2 y 4.7.3 se definió una permutación, denotada por $\widetilde{\varepsilon}$ de tal forma que el código $\widetilde{\varepsilon}(\Phi(\mathscr{C}))$ resultó, en todo los casos, ser casi-cíclico. En lo sucesivo definiremos de forma general la permutación $\widetilde{\varepsilon}$ y demostraremos que el código $\widetilde{\varepsilon}(\Phi(\mathscr{C}))$ es casi-cíclico.

Para cualesquiera enteros $k,m \geq 1$, definimos la permutación $\varepsilon : I_{2^k m} \to I_{2^k m}$ de la siguiente forma: por medio del algoritmo de la división en los enteros, podemos expresar a $l \in I_{2^k m}$ como $l = (2^{k-1}m)i + j$, donde $0 \leq j \leq 2^{k-1}m - 1$ es el residuo de la división. Entonces definimos $\varepsilon(l) = 2j + i$.

Observe que si $0 \leq l \leq 2^{k-1}m - 1$, entonces $l = (2^{k-1}m)(0) + l$ y, en consecuencia, $\varepsilon(l) = 2l + 0 = 2l$. Esto quiere decir que la imagen con respecto a ε de los primeros $2^{k-1}m$ números del conjunto $I_{2^k m}$ (con el orden de los naturales) son todos los números pares de $I_{2^k m}$. De manera similar, si $2^{k-1}m \leq l \leq 2^k m - 1$, entonces $l = (2^{k-1}m)(1) + (j)$, donde $0 \leq j \leq 2^{k-1}m - 1$. Por lo tanto, $\varepsilon(l) = 2j + 1$ y, consecuentemente, la imagen bajo ε de la segunda mitad de $I_{2^k m}$, son todos lo números impares de $I_{2^k m}$.

A través de la aplicación ε, inducimos la permutación $\widetilde{\varepsilon}$ sobre $\mathbb{F}_2^{2^k mn} = (\mathbb{F}_2^n)^{2^k m}$ de la siguiente forma:

$$Z = \left(Z_0 | Z_1 | \cdots | Z_{2^k m - 1}\right) \mapsto \widetilde{\varepsilon}(Z) = \left(Z_{\varepsilon(0)} | Z_{\varepsilon(1)} | \cdots | Z_{\varepsilon(2^k m - 1)}\right), \tag{4.6}$$

donde $Z_0, Z_1, \ldots, Z_{2^k m - 1} \in \mathbb{F}_2^n$. Ilustremos estas definiciones con algunos ejemplos.

Ejemplo 4.7.4. Sean $k = 1$, $m = 1$, y $n \geq 1$. Entonces $2^{k-1}m = 1$ y, por lo tanto, para definir ε, dividimos cada elemento de $I_2 = \{0, 1\}$ entre 1, obteniendo:

$$0 = 1(0) + 0, \qquad 1 = 1(1) + 0.$$

En consecuencia, ε es la permutación sobre I_2 dada por:

$$\varepsilon(0) = 2(0) + 0 = 0, \qquad \varepsilon(1) = 2(0) + 1 = 1,$$

es decir, ε es la permutación identidad sobre I_2 y, por consiguiente, $\widetilde{\varepsilon} : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$ es la permutación identidad. Observe que para este caso, la primera (resp. segunda) mitad del conjunto I_2 consta sólo del cero (resp. uno), que es el único número par (resp. impar) de I_2.

Ejemplo 4.7.5. Sean $k = 2$, $m = 1$ y $n = 3$. Entonces $2^{k-1}m = 2$ y, por lo tanto, dividimos cada elemento de I_4 entre 2, obteniendo de este modo:

$$\begin{aligned} 0 &= 2(0) + 0, & 2 &= 2(1) + 0, \\ 1 &= 2(0) + 1, & 3 &= 2(1) + 1. \end{aligned}$$

Consecuentemente, $\varepsilon : I_4 \to I_4$ es tal que

$$\begin{aligned} \varepsilon(0) &= 2(0) + 0 = 0, & \varepsilon(2) &= 2(0) + 1 = 1, \\ \varepsilon(1) &= 2(1) + 0 = 2, & \varepsilon(3) &= 2(1) + 1 = 3. \end{aligned}$$

Observe que ahora, la primera (resp. segunda) mitad del conjunto I_4, es el conjunto $\{0, 1\}$ (resp. $\{2, 3\}$), y que la imagen del conjunto $\{0, 1\}$ (resp. $\{2, 3\}$) bajo ε es precisamente el conjunto de

todos los números pares (resp. impares) de I_4. Por otra parte, note que si $Z = (Z_0|Z_1|Z_2|Z_3) = (z_0,z_1,z_2|z_3,z_4,z_5|z_6,z_7,z_8|z_9,z_{10},z_{11}) \in \mathbb{F}_2^{12}$, entonces

$$\begin{aligned}\widetilde{\varepsilon}(Z) &= (\underbrace{z_0,z_1,z_2}_{Z_{\varepsilon(0)}}|\underbrace{z_3,z_4,z_5}_{Z_{\varepsilon(1)}}|\underbrace{z_6,z_7,z_8}_{Z_{\varepsilon(2)}}|\underbrace{z_9,z_{10},z_{11}}_{Z_{\varepsilon(3)}}) \\ &= (\underbrace{z_0,z_1,z_2}_{Z_0}|\underbrace{z_6,z_7,z_8}_{Z_2}|\underbrace{z_3,z_4,z_5}_{Z_1}|\underbrace{z_9,z_{10},z_{11}}_{Z_3}).\end{aligned}$$

De aquí, podemos ver que, en términos de ciclos, $\widetilde{\varepsilon} = (3,6)(4,7)(5,8)$, lo cual coincide con la permutación empleada en el Ejemplo 4.7.1.

Ejemplo 4.7.6. Sean $k = n = 3$ y $m = 1$. Entonces $2^k m = 8$ y $2^{k-1}m = 4$. Por lo tanto,

$$\varepsilon = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 2 & 4 & 6 & 1 & 3 & 5 & 7 \end{pmatrix}.$$

Siendo $n = 3$, ε induce la permutación $\widetilde{\varepsilon}$ sobre $\mathbb{F}_2^{24}$ dada por la regla de asignación

$$(Z_0|Z_1|\cdots|Z_7) \mapsto \left(Z_{\varepsilon(0)}|Z_{\varepsilon(1)}|\cdots|Z_{\varepsilon(7)}\right),$$

donde $Z_i \in \mathbb{F}_2^3$. Consecuentemente, ε coincide con la permutación del Ejemplo 4.7.2.

Dado que la defínción de ε es similar a la de la permutación τ, introducida en la relación (2.9) para demostrar que las isometrías Φ y Φ' del Teorema 2.1.13 son (permutación) equivalentes, vale la pena comparar estas definiciones para ver en qué casos son las mismas funciones. Este es el propósito del siguiente ejemplo. Antes, recordemos que para cualesquiera enteros $n \geq 1$y $k \geq 0$, $\tau : I_{2^k n} \to I_{2^k n}$ está definida como $\tau(l) = 2^k j + i$, donde $l = in + j$, $0 \leq j \leq n-1$.

Ejemplo 4.7.7. Sean $m \geq 1$ y $k = n = 1$. Entonces $\varepsilon : I_{2m} \to I_{2m}$ y, por lo tanto, $\varepsilon(l) = 2j + i$, donde $l = mi + j$, $0 \leq j \leq m-1$. Analizando con más detalle la acción de ε, vemos que si $0 \leq l \leq m-1$, entonces $\varepsilon(l) = 2l$. Asimismo, note que si $l \geq m$, entonces $l = m(1) + j$ y, en consecuencia, $\varepsilon(l) = 2j+1$, donde $0 \leq j \leq m-1$. De aquí obtenemos

$$\varepsilon = \begin{pmatrix} 0 & 1 & 2 & \cdots & i & \cdots & m-1 & m & m+1 & m+2 & \cdots & m+i & \cdots & 2m-1 \\ 0 & 2 & 4 & \cdots & 2i & \cdots & 2m-2 & 1 & 3 & 5 & \cdots & 2i+1 & \cdots & 2m-1 \end{pmatrix}.$$

Esta permutación es precisamente la permutación τ de la relación (2.9). Sin embargo, si elegimos $m = 1$ y $k \geq 1$ y $n \geq 1$, entonces $\varepsilon : I_{2^k} \to I_{2^k}$ mientras que $\tau : I_{2^k n} \to I_{2^k n}$ y, por lo tanto, ε es distinta a la permutación τ. Asimismo, si tomamos $m,k \geq 1$ y $n = 1$, vemos que $\varepsilon : I_{2^k m} \to I_{2^k m}$ y $\tau : I_{2^k} \to I_{2^k}$ no tienen los mismos dominios. De este modo, hemos mostrado que, las permutaciones ε y τ son las mismas únicamente para $m \geq 1$ y $k = n = 1$.

Sean $k,m,n \geq 1$ enteros y $\Phi : \mathbb{Z}_{2^{k+1}}^{mn} \to \mathbb{F}_2^{2^k mn}$ la isometría de Gray. Por medio de la permutación $\widetilde{\varepsilon}$ sobre $\mathbb{F}_2^{2^k nm}$ definimos la isometría $\Phi_1 : \left(\mathbb{Z}_{2^{k+1}}^{mn}, \delta_h\right) \to \left(\mathbb{F}^{2^k mn}, \delta_H\right)$ dada por la relación

$$\Phi_1 = \widetilde{\varepsilon} \circ \Phi \tag{4.7}$$

donde δ_h y δ_H son, respectivamente, la distancia homogénea sobre $\mathbb{Z}_{2^{k+1}}^n$ y la distancia de Hamming sobre $\mathbb{F}_2^{2^k mn}$.

Como se vio en los Ejemplos 4.7.1, 4.7.2 y 4.7.3, el código $\Phi_1(\mathscr{C})$ es casi-cíclcico, siempre que $\mathscr{C}$ sea un código λ-casi-cíclico de índice m y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$, donde $\lambda = 1 + 2^k$. Nuestra siguiente labor es demostrar que este resultado es válido en general. Para tal fin, necesitamos entender con más detalle la permutación $\widetilde{\varepsilon}$. Una forma sencilla de interpretar la permutación $\widetilde{\varepsilon}$ es mediante la transposición de matrices.

Sea $Z = (Z_0|Z_1|\cdots|Z_{2^k m-1}) \in (\mathbb{F}_2^n)^{2^k m}$, es decir, Z es la concatenación de $2^k m$ vectores binarios de longitud n cada uno. Dado que $k \geq 1$, el número de vectores de longitud n es par y, por lo tanto, podemos agrupar a estos vectores en dos grupos. El primer grupo consiste precisamente de la primera mitad del vector Z y el segundo grupo de la segunda mitad. Para distinguir entre el primero y el segundo grupo, cambiamos la forma de escribir los subíndices de Z a la siguiente:

$$Z = \left(Z_{0,0}|Z_{0,1}|\cdots|Z_{0,2^{k-1}m-1}|Z_{1,0}|Z_{1,1}|Z_{1,2^{k-1}m-1}\right).$$

Observe que los elementos de la primera mitad tienen su primer subíndice igual a cero y su segundo subíndice variando entre 0 y $2^{k-1}m-1$. De manera similar, los vectores del segundo grupo tienen su primer subíndice igual a 1 y su segundo subíndice variando entre 0 y $2^{k-1}m-1$.

Con la introducción de esa notación, a Z le hacemos correponder la siguiente matriz de tamaño $2 \times 2^{k-1}m$ cuyas entradas son elementos de $\mathbb{F}_2^n$:

$$M_Z = \begin{pmatrix} Z_{0,0} & Z_{0,1} & \cdots & Z_{0,2^{k-1}m-1} \\ Z_{1,0} & Z_{1,1} & \cdots & Z_{1,2^{k-1}m-1} \end{pmatrix}.$$

Considere, ahora, un bloque Z_l de Z, donde $0 \leq l \leq 2^k m-1$, es decir, el subíndice l es el usual. Queremos determinar en qué renglón y en qué columna de la matriz M_Z se encuentra Z_l. Dado que M_Z tiene $2^{k-1}m$ columnas, el residuo de la división de l entre $2^{k-1}m$ indica en qué columna de M_Z se encuentra Z_l, mientras que la parte entera indica en qué renglón de M_Z se ubica Z_l. Es decir, si $l = (2^{k-1}m)i + j$, donde $0 \leq j \leq 2^{k-1}m-1$, entonces Z_l se sitúa en el renglón i y la columna j. En consecuencia, Z_l se encuentra en la fila j y la columna i de la matriz transpuesta de M_Z.

Para relacionar lo anterior con la permutación $\widetilde{\varepsilon}$, note que M_Z^t es una matriz de tamaño $2^{k-1}m \times 2$ y que, concatenando (en orden) sus renglones, obtenemos un vector $Z^t \in (\mathbb{F}_2^n)^{2^k m}$. Así, se sigue de las dimensiones de M^t, que Z_l se encuentra en la posición $2j+i = \varepsilon(l)$, donde $l = (2^{k-1}m)i + j$, $0 \leq j \leq 2^{k-1}m-1$. Por lo tanto, podemos concluir que $Z^t = \widetilde{\varepsilon}(Z)$.

Con base a las observaciones anteriores, el siguiente resultado es fácil de probar.

Teorema 4.7.8. *Sean $k,m,n \geq 1$, enteros y $Z \in \mathbb{Z}_{2^{k+1}}^{nm}$. Entonces $\Phi_1(Z) = (\phi^{\otimes 2^{k-1}m} \circ \varphi)(Z)$.*

Demostración. Recordemos que por definición

$$\varphi(Z) = c_{k-1}^{k-1} \otimes r_0(Z) + 2[c_0^{k-1} \otimes r_1(Z) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes r_k(Z)],$$

donde $c_{k-1}^{k-1} \otimes r_0(Z)$, $c_0^{k-1} \otimes r_0(Z) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes r_k(Z) \in (\mathbb{F}_2^n)^{2^k m}$. Por lo tanto, es posible escribir

$$c_{k-1}^{k-1} \otimes r_0(Z) = \left(A_0|A_1|\cdots|A_{2^k m-1}\right)$$

y

$$c_0^{k-1} \otimes r_0(Z) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes r_k(Z) = \left(B_0|B_1|\cdots|B_{2^k m-1}\right),$$

donde $A_i, B_i \in \mathbb{F}_2^n$, $0 \leq i \leq 2^k m - 1$. Consecuentemente,

$$\begin{aligned} \varphi(Z) &= \left(A_0|A_1|\cdots|A_{2^k m-1}\right) + 2\left(B_0|B_1|\cdots|B_{2^k m-1}\right) \\ &= \left(A_0 + 2B_0|A_1 + 2B_1|\cdots|A_{2^k m-1} + 2B_{2^k m-1}\right). \end{aligned}$$

Ahora, calculamos $\Phi(Z)$ usando la relación $\Phi(Z) = (\phi \circ \varphi)(Z)$. Así,

$$\begin{aligned} \Phi(Z) &= \phi\left(A_0 + 2B_0|A_1 + 2B_1|\cdots|A_{2^k m-1} + 2B_{2^k m-1}\right) \\ &= \left(B_0|B_1|\cdots|B_{2^k m-1}|A_0 \oplus B_0|A_1 \oplus B_1|\cdots|A_{2^k m-1} \oplus B_{2^k m-1}\right). \end{aligned}$$

Por otra parte, aplicamos $\phi^{\otimes 2^{k-1}m}$ a $\varphi(Z)$ (dado que $\varphi(Z) \in \left(\mathbb{Z}_4^n\right)^{2^{k-1}m}$, la isometría ϕ de Gray se aplica a los vectores $A_i + 2B_i \in \mathbb{F}_2^n$):

$$\begin{aligned} (\phi^{\otimes 2^{k-1}m} \circ \varphi)(Z) &= \left(\phi(A_0 + 2B_0)|\phi(A_1 + 2B_1)|\cdots|\phi(A_{2^k m-1} + 2B_{2^k m-1})\right) \\ &= \left(B_0|A_0 \oplus B_0|A_1|A_1 \oplus B_1|\cdots|B_{2^k m-1}|A_{2^k m-1} \oplus B_{2^k m-1}\right). \end{aligned}$$

Con el fin de relacionar a $\Phi(Z)$ con $(\phi^{\otimes 2^{k-1}m} \circ \varphi)(Z)$, considere la matriz $M_{\Phi(Z)}$, asociada al vector $\Phi(Z) \in \left(\mathbb{F}_2^n\right)^{2^k m}$:

$$M_{\Phi(Z)} = \begin{pmatrix} B_0 & B_1 & \cdots & B_{2^k m-1} \\ A_0 \oplus B_0 & A_1 \oplus B_1 & \cdots & A_{2^k m-1} \oplus B_{2^k m-1} \end{pmatrix}.$$

Note que el primer renglón de $M_{\Phi(Z)}$ es la primera mitad de $\Phi(Z)$, y que su segundo renglón es la segunda mitad de $\Phi(Z)$. Asimismo, observe que concatenando los renglones de la matriz $M_{\Phi(Z)}^t$ obtenemos el vector $\Phi(Z)^t$, el cual coincide con $(\phi^{\otimes 2^{k-1}m} \circ \varphi)(Z)$. Ya que la permutación que envía $\Phi(Z)$ a $\Phi(Z)^t$ es $\widetilde{\varepsilon}$, el resultado se sigue. □

Recuerde que por la Proposición 3.4.5, para todo $s \geq 1$, se tiene que $\phi^{\otimes s} \circ \nu^{\otimes s} = \sigma^{\otimes s} \circ \phi^{\otimes s}$, donde $\nu^{\otimes s}$ es el corrimiento casi-negacíclico sobre $\mathbb{Z}_4^{sn}$, $\sigma^{\otimes s}$ es el corrimiento casi-cíclico sobre $\mathbb{F}^{2n}$ y ϕ es la isometría de Gray de $\mathbb{Z}_4^{sn}$ a $\mathbb{F}_2^{2sn}$. Combinando el Teorema 4.7.8 con la Proposición 3.4.5, obtenemos el siguiente resultado.

Teorema 4.7.9. *Con la notación anterior,* $\Phi_1 \circ \nu_\lambda^{\otimes m} = \sigma^{\otimes 2^{k-1}m} \circ \Phi_1$.

Demostración. Aplicando $\nu_\lambda^{\otimes m}$ a la derecha de la relación $\Phi_1 = \phi^{\otimes 2^{k-1}m} \circ \varphi$ obtenemos que

$$\Phi_1 \circ \nu_\lambda^{\otimes m} = \phi^{\otimes 2^{k-1}m} \circ \varphi \circ \nu_\lambda^{\otimes m}.$$

Usando el hecho de que $\varphi \circ \nu_\lambda^{\otimes m} = \nu^{\otimes 2^{k-1}m} \circ \varphi$ (Teorema 3.3.4), tenemos que

$$\Phi_1 \circ \nu_\lambda^{\otimes m} = \phi^{\otimes 2^{k-1}m} \circ \nu^{\otimes 2^{k-1}m} \circ \varphi.$$

Ahora, por la Proposición 3.4.5, $\phi^{\otimes 2^{k-1}m} \circ \nu^{\otimes 2^{k-1}m} = \sigma^{\otimes 2^{k-1}m} \circ \phi^{\otimes 2^{k-1}m}$ y, por lo tanto,

$$\Phi_1 \circ \nu_\lambda^{\otimes m} = \sigma^{\otimes 2^{k-1}m} \circ \phi^{\otimes 2^{k-1}m} \circ \varphi,$$

de donde el resultado se sigue al reemplazar $\phi^{\otimes 2^{k-1}m} \circ \varphi$ por Φ_1 (Teorema 4.7.8). □

Como consecuencia del Teorema 4.7.9, a continuación caracterizamos a los códigos λ-casi-cíclicos, donde $\lambda = 1 + 2^k$, en términos de las propiedades de casi-ciclicidad de sus imágenes con respecto a la isometría Φ_1.

Teorema 4.7.10. *Sea $\mathscr{C}$ un código sobre $\mathbb{Z}_{2^{k+1}}$ y $\lambda = 1 + 2^k$. Entonces $\mathscr{C}$ es un código λ-casi-cíclico de índice m y longitud mn si y sólo si $\Phi_1(\mathscr{C})$ es un código casi-cíclico de índice $2^{k-1}m$ y longitud $2^k mn$ sobre $\mathbb{F}_2$.*

Demostración. Supongamos que $\mathscr{C}$ es un código λ-casi-cíclico de índice m y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$. Entonces $\nu_\lambda^{\otimes m}(\mathscr{C}) = \mathscr{C}$ y, por lo tanto, del Teorema 4.7.9 se tiene que

$$\Phi_1(\mathscr{C}) = \Phi_1(\nu_\lambda^{\otimes m}(\mathscr{C})) = \sigma^{\otimes 2^{k-1}m}(\Phi_1(\mathscr{C})).$$

En consecuencia, $\Phi_1(\mathscr{C}) = \sigma^{\otimes 2^{k-1}m}(\Phi_1(\mathscr{C}))$. Esto es, $\Phi_1(\mathscr{C})$ es un código casi-cíclico de índice $2^{k-1}m$ y longitud $2^k mn$ sobre $\mathbb{F}_2$. Recíprocamente, si $\Phi_1(\mathscr{C}) = \sigma^{\otimes 2^{k-1}m}(\Phi_1(\mathscr{C}))$, entonces $\Phi_1(\mathscr{C}) = \Phi_1(\nu_\lambda^{\otimes m}(\mathscr{C}))$ pues, por el Teorema 4.7.9, $\sigma^{\otimes 2^{k-1}m}(\Phi_1(\mathscr{C})) = \Phi_1(\nu_\lambda^{\otimes m}(\mathscr{C}))$. Como la isometría de Gray Φ y la permutación $\widetilde{\varepsilon}$ son funciones inyectivas, se tiene que $\Phi_1 = \widetilde{\varepsilon} \circ \Phi$ es también una función inyectiva. Consecuentemente, $\mathscr{C} = \nu_\lambda^{\otimes m}(\mathscr{C})$. □

A modo de ejemplo, recuerde que el código $\mathscr{C}$ del Ejemplo 4.7.3 es un código λ-casi-cíclcico de índice 2 y longitud 6 sobre $\mathbb{Z}_8$, donde $\lambda = 5$. Por lo tanto, se sigue del Teorema 4.7.10 que $(\widetilde{\varepsilon} \circ \Phi)(\mathscr{C}) = \Phi_1(\mathscr{C})$ es un código casi-cíclico de índice 4 y longitud 24 sobre $\mathbb{F}_2$, tal como afirmamos sin demostración en dicho ejemplo.

Otra aplicación del resultado anterior es la siguiente Proposición que establece algunas propiedades del código de Reed-Muller $ZRM(s-1,s)$ sobre $\mathbb{Z}_4$.

Proposición 4.7.11. *Sea $s \geq 2$ un entero y $ZRM(s-1,s)$ el código de Reed-Muller sobre $\mathbb{Z}_4$ de longitud 2^{s-1}. Entonces*

(1) *El código $ZRM(s-1,s)$ es negacíclico.*

(2) *$ZRM(s-1,s)$ es invariante con respecto al automorfismo η_3 sobre $\mathbb{Z}_4^{2^{s-1}}$, el cual multiplica la última coordenada de cada vector de $\mathbb{Z}_4^{2^{s-1}}$ por 3.*

Demostración. (1) Sea $k = 1$ y observe que $\Phi_1 = \phi^{\otimes m}$, pues φ es la función identidad sobre $\mathbb{Z}_4$. Asimismo, siendo $\mathrm{RM}(s-1,s)$ un código cíclico (casi-cíclico de índice $2^0 = 1$), con la notación del Teorema 4.7.10, la única posibilidad para el entero m es $m = 1$. Consecuentemente, $\Phi_1 = \phi$. Ya que $\Phi_1(ZRM(s-1,s)) = \phi(ZRM(s-1,s)) = \mathrm{RM}(s-1,s)$, se sigue, del Teorema 4.7.10, que $ZRM(s-1,s)$ es un código negacíclico de longitud 2^{s-1} sobre $\mathbb{Z}_4$.
(2) Recuerde que por el Teorema 4.3.4, $ZRM(s-1,s)$ es un código cíclico. Así, $ZRM(s-1,s)$ es un código cíclico y negacíclico. Por lo tanto, en virtud de la Proposición 4.4.4, $ZRM(s-1,s)$ es invariante con respecto al automorfismo η_3 sobre $\mathbb{Z}_4^{2^{s-1}}$. □

Es importante señalar que si $\mathscr{C}$ es un código λ-casi-cíclico de índice m y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$, entonces el índice de casi-ciclicidad del código $\Phi_1(\mathscr{C})$ es menor que el índice de casi-ciclicidad del código $\Phi(\mathscr{D})$, donde $\mathscr{D}$ es un código casi-cíclico de índice m y longitud mn sobre $\mathbb{Z}_{2^{k+1}}$. De manera más específica, por el Teorema 4.7.10, el índice de casi-ciclicidad de $\Phi_1(\mathscr{C})$ es $2^{k-1}m$ mientras que, por el Teorema 4.2.1, el índice de casi-ciclicidad de $\Phi(\mathscr{D})$ es $2^k m$ (el doble de índice de $\Phi_1(\mathscr{C})$). Esto quiere decir que el código $\Phi_1(\mathscr{C})$ está más "cerca" de ser un código cíclico y, por lo tanto, en este sentido, $\Phi_1(\mathscr{C})$ tiene mejor propiedad de casi-ciclícidad que el código $\Phi(\mathscr{D})$.

Debido a las observaciones previas, si $\mathscr{C}$ es un código casi-cíclico y λ-casi-cíclico a la vez, entonces puede ser preferible calcular $\Phi_1(\mathscr{C})$ en lugar de $\Phi(\mathscr{C})$. Si lo anterior es preferible, entonces para el caso de códigos cíclicos lineales de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$, puede ser más conveniente usar la isometría Φ_1 que la isometría Φ pues la mayoría de estos códigos son λ-cíclicos. Sin embargo, no todos los códigos cíclicos lineales de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$ son λ-cíclicos. Así, es importante investigar si existe una forma de obtener códigos casi-cíclicos de índice 2^{k-1} y longitud $2^{k-1}n$ sobre $\mathbb{F}_2$, como imagenes de Gray de cualquier código cíclico lineal de longitud n (impar) sobre $\mathbb{Z}_{2^{k+1}}$. Esto es lo que investigaremos en la siguiente sección.

4.8. Imágenes de Nechaev-Gray de códigos cíclicos lineales

En esta sección investigaremos una forma de obtener códigos casi-cíclicos de índice 2^{k-1} y longitud $2^k n$ sobre $\mathbb{F}_2$, como imágenes de Gray de cualquier código cíclico lineal de longitud n (impar) sobre $\mathbb{Z}_{2^{k+1}}$. Note que esta clase de códigos casi-cíclicos han sido obtenidos como imágenes, con respecto a la isometría Φ_1, de códigos λ-cíclicos (Teorema 4.7.10).

Sean $k \geq 1$, $n \geq 1$ un entero impar y $\lambda = 1+2^k$. Recuerde que el Teorema 4.6.2 establece que $\varphi \circ \widetilde{\mu}_\lambda = \widetilde{\mu}_{-1}^{\otimes 2^{k-1}} \circ \varphi$ y, por lo tanto,

$$\phi^{\otimes 2^{k-1}} \circ \varphi \circ \widetilde{\mu}_\lambda = \phi^{\otimes 2^{k-1}} \circ \widetilde{\mu}_\lambda^{\otimes 2^{k-1}} \circ \varphi.$$

Ya que por el Teorema 4.7.8, $\Phi_1 = \phi^{\otimes 2^{k-1}} \circ \varphi$, obtenemos que

$$\begin{aligned} \Phi_1 \circ \widetilde{\mu}_\lambda &= \phi^{\otimes 2^{k-1}} \circ \widetilde{\mu}_{-1}^{\otimes 2^{k-1}} \circ \varphi \\ &= (\phi \circ \widetilde{\mu}_{-1})^{\otimes 2^{k-1}} \circ \varphi, \end{aligned} \tag{4.8}$$

donde la última igualdad se debe a que $(f \circ g)^{\otimes s} = f^{\otimes s} \circ g^{\otimes s}$, para cualesquiera funciones f, g tales que la composición $f \circ g$ esté definida.

Una bella descripción de la aplicación $\phi \circ \widetilde{\mu}_{-1}$ fue econtrada en [54]. Con el propósito de enunciar formalmente tal descripción, necesitamos definir la *permutación de Nechaev*.

Para cualquier entero $n \geq 1$ impar, en [54] se define la permutación $\mathscr{N} : I_{2n} \to I_{2n}$ como

$$\mathscr{N} = (1, n+1)(3, n+3) \cdots (2i+1, n+2i+1) \cdots (n-2, 2n-2).$$

Continuando la terminología introducida en [54], definimos la *permutación de Nechaev* sobre $\mathbb{F}_2^{2n}$ como la permutación $\widetilde{\mathscr{N}}$ inducida por $\mathscr{N}$, es decir, si $Z = (z_0, z_1, \ldots, z_{2n-1}) \in \mathbb{F}_2^{2n}$, entonces

$$\widetilde{\mathscr{N}}(Z) = \left(z_{\mathscr{N}(0)}, z_{\mathscr{N}(1)}, \ldots, z_{\mathscr{N}(2n-1)}\right).$$

Proposición 4.8.1. *Sea $n \geq 1$ un entero impar y $\widetilde{\mu}_{-1}$ la permutación sobre $\mathbb{Z}_4^n$ definida como*

$$\widetilde{\mu}_{-1}(z_0, z_1, \ldots, z_i, \ldots, z_{n-1}) = (z_0, -z_1, \ldots, (-1)^i z_i, \ldots, (-1)^{n-1} z_{n-1}).$$

Entonces

$$\phi \circ \mu_{-1} = \widetilde{\mathscr{N}} \circ \phi.$$

Como $\widetilde{\mathscr{N}}$ es una permutación sobre $\mathbb{F}_2^{2n}$, se sigue que la función $\Psi = \widetilde{\mathscr{N}} \circ \phi$ es una isometría, la cual ha sido denominada en [54, 55] la *isometría de Nechaev-Gray*.

Por otra parte, aplicando la Proposición 4.8.1 a la relación (4.8), obtenemos que

$$\Phi_1 \circ \widetilde{\mu}_\lambda = \left(\widetilde{\mathscr{N}} \circ \phi\right)^{\otimes 2^{k-1}} \circ \varphi = \widetilde{\mathscr{N}}^{\otimes 2^{k-1}} \circ \phi^{\otimes 2^{k-1}} \circ \varphi = \widetilde{\mathscr{N}}^{\otimes 2^{k-1}} \circ \Phi_1.$$

Ya que $\widetilde{\mathscr{N}}$ es una permutación sobre $\mathbb{F}_2^{2n}$, entonces $\widetilde{\mathscr{N}}^{\otimes 2^{k-1}}$ es una permutación sobre $\mathbb{F}_2^{2^k n}$ y, por lo tanto, $\Psi = \widetilde{\mathscr{N}}^{\otimes 2^{k-1}} \circ \Phi$ es una isometría. Observe que si $k = 1$, entonces $\Phi_1 = \phi$ y, por lo tanto,

$$\widetilde{\mathscr{N}}^{\otimes 2^{k-1}} \circ \Phi_1 = \widetilde{\mathscr{N}} \circ \phi.$$

Por tal razón, llamaremos a la aplicación

$$\Psi = \widetilde{\mathscr{N}}^{\otimes 2^{k-1}} \circ \Phi_1$$

la *isometría de Nechaev-Gray* (sobre $\mathbb{Z}_{2^{k+1}}$). El siguiente resultado generaliza el Corolario 3.8 de [54], el Teorema 14 de [55] y es análogo al Corolario 17 de [52].

Teorema 4.8.2. *Sea $\mathscr{C}$ un código lineal de longitud n impar sobre $\mathbb{Z}_{2^{k+1}}$. Las siguientes son equivalentes:*

(1) *$\mathscr{C}$ es un código cíclico,*

(2) *$\Phi(\mathscr{C})$ es un código casi-cíclico de índice 2^k y longitud $2^k n$ sobre $\mathbb{F}_2$,*

(3) *$\Psi(\mathscr{C})$ es un código casi-cíclico de índice 2^{k-1} y longitud $2^k n$ sobre $\mathbb{F}_2$.*

Demostración. Ya que un código casi-cíclico de índice $m = 1$ es precisamente un código cíclico, del Teorema 4.2.1 obtenemos que (1) implica (2).
(2) implica (3). Sea $\Phi(\mathscr{C})$ es un código casi-cíclico de índice 2^k y longitud n sobre $\mathbb{F}_2$. Entonces, en virtud del Teorema 4.2.1, $\mathscr{C}$ es un código cíclico de longitud n sobre $\mathbb{Z}_{2^{k+1}}$, el cual por hipótesis es lineal. Por el Lema 1.4.2, $\widetilde{\mu}_\lambda(\mathscr{C})$ es un código λ-cíclico lineal de longitud n sobre $\mathbb{Z}_{2^{k+1}}$. Así, por el Teorema 4.7.10, $\Phi_1(\widetilde{\mu}_\lambda(\mathscr{C}))$ es un código casi-cíclico de longitud n sobre $\mathbb{F}_2$. Por definición, se tiene que $\Psi(\mathscr{C}) = \mathscr{N}^{\otimes 2^{k-1}}(\Phi_1(\mathscr{C})) = \Phi_1(\widetilde{\mu}_\lambda(\mathscr{C}))$, de donde el resultado se sigue.
(3) implica (1). Por definición $\Psi(\mathscr{C}) = \mathscr{N}^{\otimes 2^{k-1}}(\Phi_1(\mathscr{C})) = \Phi_1(\widetilde{\mu}_\lambda(\mathscr{C}))$. Esto quiere decir que $\Phi_1(\widetilde{\mu}_\lambda(\mathscr{C}))$ es un código casi-cíclico de índice 2^{k-1} y longitud $2^{k-1}n$ sobre $\mathbb{F}_2$. Como n es impar y $\mathscr{C}$ es lineal, el Lema 1.4.1 establece que $\mathscr{C}$ es un código cíclico de longitud n sobre $\mathbb{Z}_{2^{k+1}}$. □

Ejemplo 4.8.3. Sea $\mathscr{C}$ el código cíclico lineal de repetición de longitud 3 sobre $\mathbb{Z}_8$ (Ejemplo 4.6.3). Ya que $\nu_5(111) = 511 \notin \mathscr{C}$, $\mathscr{C}$ no es un código 5-cíclico y, en consecuencia, $\Phi_1(\mathscr{C})$ no es código casi-cíclico de índice 2 y longitud 12 sobre $\mathbb{F}_2$. Sin embargo, por el Teorema 4.8.2 la imagen de $\mathscr{C}$ con respecto a la isometría de Nechaev-Gray, sí es un código casi-cíclico de índice

2 y longitud 12. Para ilustrar este hecho, primero calculamos la imagen de $\mathscr{C}$ con respecto a φ y luego aplicamos $\phi^{\otimes 2}$ para obtener Φ_1:

	φ		$\phi^{\otimes 2}$	
000	$\longrightarrow$	000 000	$\longrightarrow$	000000 000000
111	$\longrightarrow$	111 111	$\longrightarrow$	000111 000111
222	$\longrightarrow$	000 222	$\longrightarrow$	000000 111111
333	$\longrightarrow$	111 333	$\longrightarrow$	111111 111111
444	$\longrightarrow$	222 222	$\longrightarrow$	000111 111000
555	$\longrightarrow$	333 333	$\longrightarrow$	111000 111000
666	$\longrightarrow$	222 000	$\longrightarrow$	111111 000000
777	$\longrightarrow$	333 111	$\longrightarrow$	111000 111111

Dado que en este Ejemplo $n = 3$, se sigue que $\mathscr{N} = (1,4)$. Por lo tanto, la permutación de Nechaev sobre $\mathbb{F}_2^6$ es tal que $\widetilde{\mathscr{N}}(z_0,z_1,z_2,z_3,z_4,z_5) = (z_0,z_4,z_2,z_3,z_1,z_5)$. Siendo $k = 2$, la isometría de Nechaev-Gray $\mathbb{Z}_8^{12}$ es precisamente $\Psi = \widetilde{\mathscr{N}}^{\otimes 2} \circ \Phi_1$. Por lo tanto la imagen de Nechaev-Gray del código $\mathscr{C}$ es la siguiente:

	Ψ		
000	$\longrightarrow$	000000	000000
111	$\longrightarrow$	010101	010101
222	$\longrightarrow$	000000	111111
333	$\longrightarrow$	111111	111111
444	$\longrightarrow$	010101	101010
555	$\longrightarrow$	101010	101010
666	$\longrightarrow$	111111	000000
777	$\longrightarrow$	101010	101010

De este arreglo podemos verificar que en efecto $\Psi(\mathscr{C})$ es un código casi-cíclico de índice 2 y longitud 12 sobre $\mathbb{F}_2$.

En la Proposición 4.5.6 caracterizamos a los códigos lineales de longitud n (impar) sobre $\mathbb{Z}_{2^{k+1}}$ que tienen la propiedad de ser cíclicos y λ-cíclicos al mismo tiempo, como aquellos códigos para los cuales $\mathscr{C} = \widetilde{\mu}_\lambda(\mathscr{C})$. Usando esta caracterización y la relación $\Phi_1 \circ \widetilde{\mu}_\lambda = \widetilde{\mathscr{N}}^{\otimes 2^{k-1}} \circ \Phi_1$, caracterizamos, ahora, a estos códigos en términos de su imagen bajo Φ_1.

Teorema 4.8.4. *Sea $\mathscr{C}$ un código lineal de longitud n (impar) sobre $\mathbb{Z}_{2^{k+1}}$ y $\lambda = 1+2^k$, $k \geq 1$. Entonces $\mathscr{C}$ es un código cíclico y λ-cíclico si y sólo si $\Phi_1(\mathscr{C})$ es invariante con recpecto a la permutación $\widetilde{\mathscr{N}}^{\otimes 2^{k-1}}$, donde $\widetilde{\mathscr{N}}$ es la permutación de Nechaev.*

Demostración. Sea $\mathscr{C}$ un código cíclico y λ-cíclico de longitud n (impar) sobre $\mathbb{Z}_{2^{k+1}}$. Entonces, $\widetilde{\mu}_\lambda(\mathscr{C}) = \mathscr{C}$ y, por lo tanto,

$$\Phi_1(\mathscr{C}) = \Phi_1\left(\widetilde{\mu}_\lambda(\mathscr{C})\right) = \widetilde{\mathscr{N}}^{\otimes 2^{k-1}}\left(\Phi_1(\mathscr{C})\right).$$

Esto quiere decir, que $\Phi_1(\mathscr{C})$ es invariante con respecto a $\widetilde{\mathscr{N}}^{\otimes 2^{k-1}}$.
Recíprocamente, supongamos que $\Phi_1(\mathscr{C}) = \widetilde{\mathscr{N}}^{\otimes 2^{k-1}}(\Phi_1(\mathscr{C}))$. Ya que $\left(\widetilde{\mathscr{N}}^{\otimes 2^{k-1}} \circ \Phi_1\right)(\mathscr{C}) = (\Phi_1 \circ \widetilde{\mu}_\lambda)(\mathscr{C})$, se tiene que $\Phi_1(\mathscr{C}) = \Phi_1(\widetilde{\mu}_\lambda(\mathscr{C}))$. Como Φ_1 es inyectiva, se concluye que $\mathscr{C} = \widetilde{\mu}_\lambda(\mathscr{C})$, es decir, $\mathscr{C}$ es λ-cíclico. □

Enunciado de otra forma, el Teorema 4.8.4 dice que si un código binario $\mathscr{D}$ es $\mathbb{Z}_{2^{k+1}}$-lineal y casi-cíclico de índice 2^{k-1} y longitud $2^k n$, donde n es impar, entonces este código es equivalente a la imagen de un código cíclico y λ-cíclico si y sólo si $\mathscr{D}$ es invariante con respecto a la permutación $\widetilde{\mathscr{N}}^{\otimes 2^{k-1}}$, donde $\widetilde{\mathscr{N}}$ es la permutación de Nechaev.

De los Cuadros 4.1 y 4.2, notamos que la mayoría de los códigos cíclicos lineales de longitud 3 sobre $\mathbb{Z}_8$ y $\mathbb{Z}_{16}$ son λ-cíclicos. Como consecuencia de este hecho, obtenemos que la imagen con respecto a la isometría Φ_1 de estos códigos son invariantes con respecto a la permutación $\widetilde{\mathscr{N}}^{\otimes 2^{k-1}}$, donde $k = 2, 3$. En general, como la mayoría de los códigos cíclicos lineales de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$ son cíclicos y λ-cíclicos, entonces varios de esos códigos tienen como imagen con respecto a Φ_1 un código que es invariante bajo la acción de $\widetilde{\mathscr{N}}^{\otimes 2^{k-1}}$.

Capítulo 5

Imágenes de códigos $(1+2^{k-1})$-cíclicos y $(1+2^{k-1}+2^k)$-cíclicos

En este capítulo describiremos algunas propiedades de las imágenes, con respecto a las isometrías φ y Φ de Gray, de códigos $(1+2^{k-1})$-cíciclos y $(1+2^{k-1}+2^k)$-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, donde $k \geq 3$. Demostraremos que un código $\mathscr{C}$ es $(1+2^{k-1})$-cíclico si y sólo si $\widetilde{\pi}(\sigma \otimes \nu)^{\otimes 2^{k-2}}(c) + \widehat{c} \in \varphi(\mathscr{C})$, donde $c \in \varphi(\mathscr{C})$ y $\widehat{c} = c_{k-1}^{k-1} \otimes (2,0,\ldots,0) \in \mathbb{Z}_4^{2^{k-1}n}$ siempre que el vector $t \in \mathbb{Z}_4^{2^{k-1}}$, obtenido al concatenar en orden las coordenadas de c con subíndice en el conjunto $\{n-1, 2n-1, \ldots, 2^{k-1}n-1\}$, satisface que $t \in (1,3,\ldots,1,3) + \langle 2c_0^{k-1}, \ldots, 2c_{k-3}^{k-1}, 2c_{k-1}^{k-1}\rangle$; en caso contrario, $\widehat{c} = (0)_{2^{k-1}n}$. La permutación $\widetilde{\pi}$ es la permutación sobre $\mathbb{Z}_4^{2^{k-1}n}$ inducida por la permutación π definida en la relación (5.3). Usando la misma notación, también demostraremos que un código $\mathscr{C}$ es $(1+2^{k-1}+2^k)$-cíclico si y sólo si para todo $c \in \varphi(\mathscr{C})$ obtenemos que $\widetilde{\pi}(\nu \otimes \sigma)^{\otimes 2^{k-2}}(c) + \widehat{c} \in \varphi(\mathscr{C})$.

5.1. Introducción

El estudio de propiedades como linealidad, casi-ciclicidad y casi-negaciclicidad de códigos obtenidos como imágenes de Gray de códigos consta-cíclicos sobre anillos, es una reciente y atractiva línea de investigación impulsada por los trabajos de Hammons et. al [23], A. Nechaev [40] y J. Wolfmann [54, 55]; siendo [54, 55] los primeros trabajos que analizan la relación entre códigos consta-cíclicos sobre anillos y códigos casi-cíclicos sobre campos finitos.

En específico, en [54, 55] se demostró que la imagen de Gray de un código negacíclico de longitud n sobre $\mathbb{Z}_4$ es un código cíclico binario (no necesariamente lineal) de longitud $2n$. Asimismo, se probó que la imagen de Nechaev-Gray de un código cíclico lineal de longitud n impar sobre $\mathbb{Z}_4$ es un código cíclico binario de longitud $2n$. Entre otras cosas, estos resultados dieron una explicación satisfactoria al por qué los códigos de Kerdock, Preparata, etc. están relacionados con códigos cíclicos binarios no lineales; hecho que fue descubierto en [23, 40].

Hoy en día existen varios trabajos que generalizan algunos de los resultados alcanzados en [54, 55] a los anillos $\mathbb{Z}_{p^{k+1}}$ de enteros módulo p^{k+1} (cf. [33, 51, 52, 59]); a los anillos de Galois $GR(p^{k+1}, s)$ (cf. [35, 36, 50]) y, de manera más general, a los anillos de cadena finita (cf. [29]). Aunque originalmente, el estudio de estos temas se plantea sobre anillos de cadena finita, recientemente algunas investigaciones han encontrado resultados interesantes en otras

familias de anillos finitos que no son de cadena finita (cf. [17, 57] y las referencias citadas en este trabajo).

Para ser más claros con respecto a clase de códigos consta-cíclicos (o γ-cíclicos para ser más específicos) contemplados en [29, 33, 35, 36, 50–52, 54, 55], recuerde que un anillo de cadena finita es un anillo local de ideales principales y, en consecuencia, la retícula de ideales de un anillo de cadena finita R es (cf. [14]):

$$R \supset \langle \theta \rangle \supset \langle \theta^2 \rangle \supset \cdots \supset \langle \theta^{t-1} \rangle \supset \langle \theta^t \rangle \supset \langle 0 \rangle.$$

Entonces, en los trabajos antes mencionados, se estudian propiedades de casi-ciclicidad de la imagen de Gray de códigos γ-cíclicos, donde $\gamma = 1 - \theta^t$. En gran medida esto se debe a que si $R = \mathbb{Z}_4$, entonces $\theta = 2$, $t = 1$ y, por lo tanto, $\gamma = 1 + 2^1 = 3$; unidad que fue considera en [54, 55] para definir a los códigos negacíclicos sobre $\mathbb{Z}_4$.

El propósito del presente apartado es investigar algunas propiedades de casi-negaciclicidad y casi-ciclicidad de los códigos $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C})$, donde φ y Φ son las isometrías introducidas en el Capítulo 2 de esta tesis, $\mathscr{C}$ es un código γ-cíclico sobre $\mathbb{Z}_{2^{k+1}}$ y γ es una de las siguientes unidades en $\mathbb{Z}_{2^{k+1}}$:

$$\delta_1 = 1 + 2^{k-1}, \qquad \delta_2 = 1 + 2^{k-1} + 2^k, \qquad \text{con } k \geq 3.$$

Observe que los códigos que ahora consideraremos están definidos sobre el anillo $\mathbb{Z}_{2^{k+1}}$, donde $k \geq 3$, el cual es un anillo de cadena finita en el que $\theta = 2$ y $t = k$. Así, nuestro trabajo continúa en la línea de investigación de códigos definidos sobre la clase de anillos de cadena finita. Sin embargo, note que las unidades que estaremos considerando no son de la forma $1 - \theta^t$, unidad que fue considerada en [29, 33, 35, 36, 50–52, 54, 55]. Desde el punto de vista de la retícula de ideales del anillo $\mathbb{Z}_{2^{k+1}}$, las unidades δ_1 y δ_2 provienen de sumar 1 a los elementos 2^{k-1} y $2^{k-1} + 2^k$, los cuales pertenecen al ideal $\langle 2^{k-1} \rangle \subseteq \mathbb{Z}_{2^{k+1}}$; mientras que la unidad $\gamma = 1 + 2^k$ resulta de sumar 1 al generador del ideal $\langle 2^k \rangle$ de $\mathbb{Z}_{2^{k+1}}$. Por lo tanto, con este trabajo proponemos ir un paso a la izquierda en la retícula de ideales del anillo $\mathbb{Z}_{2^{k+1}}$:

$$\mathbb{Z}_{2^{k+1}} \supset \langle 2 \rangle \supset \langle 2^2 \rangle \supset \cdots \supset \langle 2^{k-1} \rangle \supset \langle 2^k \rangle \supset \langle 0 \rangle.$$

En la Sección 5.2 caracterizamos a los códigos δ_1-cíclicos en términos de sus imágenes con respecto a la isometría φ (cf. Teorema 5.2.17), y en la Sección 5.3 caracterizaremos a la familia de códigos δ_2-cíclicos a través de sus imágenes con respecto a la isometría φ (cf. Teorema 5.3.3). Algunos casos especiales de códigos δ_1-cíclicos así como de códigos δ_2-cíclicos serán tratados con mayor detalle.

Aunque algunos resultados presentados en este apartado serán válidos también para $k = 2$, se ha pospuesto el estudio de códigos sobre $\mathbb{Z}_8$ para el siguiente capítulo. Esto se debe a que en $\mathbb{Z}_8$ las unidades $\delta_1 = 1 + 2^{k-1} = 3$ y $\delta_2 = 1 + 2^{k-1} + 2^k = 7$ son de orden 2 y, en consecuencia, las propiedades de sus imágenes se ven alteradas por esta particularidad.

5.2. Imágenes sobre $\mathbb{Z}_4$ de códigos $(1+2^{k-1})$-cíclicos

En esta sección estudiaremos algunas propiedades del código $\varphi(\mathscr{C})$, donde $\mathscr{C}$ es un código δ_1-cíclico, $\delta_1 = 1+2^{k-1}$, $k \geq 3$ y φ es la isometría introducida en la Sección 2.2. A diferencia de los capítulos anteriores, el código $\mathscr{C}$ tiene únicamente la característica de ser δ_1-cíclico, en lugar de ser δ_1-casi-cíclico. Futuros trabajos pueden considerar la posibilidad de generalizar los resultados que aquí presentamos a la familia de códigos δ_1-casi-cíclicos.

Veamos un ejemplo de un código δ_1-cíclico de longitud 3 sobre $\mathbb{Z}_{16}$.

Ejemplo 5.2.1. Sean $k = 3$, $n = 3$ y $\mathscr{D}$ el código (no lineal) de longitud 3 sobre $\mathbb{Z}_{16}$ cuyos elementos son:

$$\begin{array}{cccc} (1,6,7) & (3,1,6) & (14,3,1) & (5,14,3) \\ (15,5,14) & (6,15,5) & (9,6,15) & (11,9,6) \\ (14,11,9) & (13,14,11) & (7,13,14) & (6,7,3) \end{array}$$

Es fácil verificar que este código es δ_1-cíclico, con $\delta_1 = 1+2^{k-1} = 5$. La imagen de $\mathscr{D}$ con respecto a la isometría φ es el siguiente código de longitud 12 sobre $\mathbb{Z}_4$:

$$\begin{array}{cccc} 101\ 123\ 123\ 101 & 110\ 112\ 312\ 310 & 211\ 011\ 031\ 231 & 121\ 301\ 103\ 323 \\ 312\ 130\ 110\ 332 & 031\ 213\ 211\ 033 & 303\ 321\ 321\ 303 & 330\ 332\ 132\ 130 \\ 233\ 033\ 013\ 213 & 323\ 103\ 301\ 121 & 132\ 310\ 330\ 112 & 013\ 231\ 233\ 011 \end{array}$$

Note que $\varphi(\mathscr{D})$ no es un código casi-cíclico ni un código casi-negacíclico para ningún índice d, donde d es un divisor de 12, con $1 \leq d < 12$. Sin embargo, $\varphi(\mathscr{D})$ tiene la siguiente propiedad:

Sean σ y ν, respectivamente, el corrimiento cíclcio y negacíclico sobre $\mathbb{Z}_4$. Considere la permutación $\pi = (0 \quad 6)(3 \quad 9)$ sobre el conjunto $I_{12} = \{0,1,\ldots,11\}$ y sea $\widetilde{\pi}$ la permutación sobre $\mathbb{Z}_4^{12}$ inducida por π. Entonces

$$\widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2}\right)\left(\varphi(Z) + \varphi(2^3\mathbf{b}_Z \odot 2\mathbf{b}_Z)\right) \in \varphi(\mathscr{D}) \tag{5.1}$$

donde $2^3\mathbf{b}_Z \odot 2\mathbf{b}_Z = (0,0,2^3 r_0(z_2) r_2(z_2))$ y $Z = (z_0,z_1,z_2) \in \mathscr{C}$.

Por ejemplo, sea $Z = (3,1,6)$. Entonces $\varphi(Z) = 110\ 112\ 312\ 310$ y $2^3 Z \odot 2Z = (0,0,0)$. En consecuencia, $\varphi(2^3 Z \odot 2Z) = (0)_{12}$ y, por lo tanto,

$$\begin{aligned} \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2}\right)\left(\varphi(Z) + \varphi(2^3 Z \odot 2Z)\right) &= \widetilde{\pi}((\sigma(110)|\nu(112)|\sigma(312)|\nu(310))) \\ &= \widetilde{\pi}(011|211|231|031) \\ &= 211\ 011\ 031\ 231, \end{aligned}$$

el cual es un vector que está en el código $\varphi(\mathscr{D})$. De manera similar, si $Z = (9,6,15)$, entonces

$\varphi(Z) = 303\ 321\ 321\ 303$, $\varphi(2^3Z \odot 2Z) = 002\ 002\ 002\ 002$ y, por lo tanto,

$$\begin{aligned}\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2}\right)\left(\varphi(Z)+\varphi(2^3Z\odot 2Z)\right) &= \widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2}\right)(301\ 323\ 323\ 301)\\ &= \widetilde{\pi}((\sigma(301)|\nu(323)|\sigma(323)|\nu(301)))\\ &= \widetilde{\pi}(130|132|132|130)\\ &= 330\ 332\ 132\ 130,\end{aligned}$$

obteniendo de nuevo un vector que se encuentra en $\varphi(\mathscr{D})$. Para finalizar este ejemplo, observe que el siguiente vector no pertence a $\varphi(\mathscr{D})$:

$$\begin{aligned}\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2}\right)(\varphi(Z)) &= \widetilde{\pi}(\sigma(303)|\nu(321)|\sigma(321)|\nu(303))\\ &= \widetilde{\pi}(130|132|332|330)\\ &= 330\ 332\ 132\ 130.\end{aligned}$$

De este último hecho concluimos que la propiedad

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2}\right)(\varphi(Z)) \in \varphi(\mathscr{D}), \quad \varphi(Z) \in \varphi(\mathscr{D}) \tag{5.2}$$

no es satisfecha por el código $\varphi(\mathscr{D})$ y, por lo tanto, el término $\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2}\right)\left(\varphi(2^3Z\odot 2Z)\right)$ debe considerarse (aunque más adelante investigaremos qué condiciones debe satisfacer un código $\mathscr{C}$ para que $\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-1}}\right)\left(\varphi(2^kZ\odot 2Z)\right)$ pueda ser omitido).

Demostrar la propiedad (5.2) que se observó en el ejemplo anterior es el principal propósito de esta sección. De este modo, demostraremos que todos los códigos $(1+2^{k-1})$-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, con $k \geq 3$, tienen como imagen con respecto a φ un código sobre $\mathbb{Z}_4$ que cumple con la propiedad (5.1) del Ejemplo 5.2.1. De hecho, demostraremos que esta propiedad caracteriza a tales códigos.

Aunque en este capítulo nos interesa estudiar las imágenes de códigos δ_1-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, con $k \geq 3$, algunas definiciones y resultados que presentaremos aquí serán enunciados para $k \geq 2$. Esto lo hacemos con el fin ser lo más general posible y de dar una pauta de algunas de las diferencias que encontraremos cuando analicemos las imágenes de códigos 3-cíclicos y negacíclicos en $\mathbb{Z}_8$.

Iniciamos dando una definición de la permutación π que se usó en el Ejemplo 5.2.1.

Sean $k \geq 2$, $n \geq 1$ enteros y $l = 2^{k-2}n$. Sobre el conjunto

$$I_{2^{k-1}n} = \{0, 1, 2, \ldots, n2^{k-1} - 1\}$$

definimos la permutación π como

$$\pi = (0 \quad l)(n \quad l+n)(2n \quad l+2n)\cdots((2^{k-2}-1)n \quad l+(2^{k-2}-1)n). \tag{5.3}$$

Veamos algunos ejemplos de esta permutación.

Ejemplo 5.2.2. Sean $k = n = 3$. Entonces $l = 2^{k-2}n = 6$ y $(2^{k-2}-1)n = 3$. Así, π es una permutación sobre el conjunto I_{12} definida como $\pi = (0 \quad l)(n \quad l+n) = (0 \quad 6)(3 \quad 9)$. Note que esta permutación es precisamente la permutación π del Ejemplo 5.2.1.

Ejemplo 5.2.3. Un caso particular de la permutación π es cuando tomamos cualquier entero $k \geq 2$ y fijamos $n = 1$. Para esta situación, $l = 2^{k-2}n = 2^{k-2}$ y, por lo tanto, π es la permutación sobre el conjunto $I_{2^{k-1}}$ dada por la expresión

$$\pi = (0 \quad 2^{k-2})(1 \quad 2^{k-2}+1)(2 \quad 2^{k-2}+2)\cdots(2^{k-2}-1 \quad 2^{k-2}-1, 2^{k-1}-1).$$

Observe que si $Z = (A|B)$ es un vector de longitud $2^{k-1}n$ sobre algún alfabeto, en el que A y B son de la misma longitud, entonces $\widetilde{\pi}(Z) = (B|A)$, donde $\widetilde{\pi}$ es la permutación inducida por π.

Ejemplo 5.2.4. Otro caso de particular interés resulta al considerar $k = 2$ y $n \geq 1$. En este caso, $l = 2^{k-2}n = n$ y $(2^{k-2}-1)n = 0$. En consecuencia, π es la permutación sobre el conjunto I_{2n} definida por el ciclo $\pi = (0, n)$. Como veremos, este hecho es una de las causas del porqué es necesario distinguir entre los casos $k \geq 3$ y $k = 2$.

Sea $n \geq 1$ un entero y $Z = (z_0, z_1, \ldots, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$. Recuerde que en la Sección 1.3 de esta tesis definimos los siguientes vectores de $\mathbb{Z}_{2^{k+1}}^n$:

$$\mathbf{a} = (z_0, z_1, \ldots, z_{n-2}, 0), \qquad \mathbf{b} = (0, \ldots, 0, z_{n-1}),$$

en donde acordamos que si $n = 1$, entonces $\mathbf{a} = 0$ y $\mathbf{b} = z_0$. Con base en lo anterior, es claro que para todo $n \geq 1$ y $Z \in \mathbb{Z}_{2^{k+1}}^n$, tenemos la expresión $Z = \mathbf{a} + \mathbf{b}$.

Lema 5.2.5. *Sean $k \geq 2$ y $n \geq 1$ enteros. Siguiendo con la notación anterior, se tienen las siguientes relaciones:*

(1) $\sigma(\varphi(\mathbf{a})) = \sigma^{\otimes 2}(\varphi(\mathbf{a})) = \cdots = \sigma^{\otimes 2^{k-1}}(\varphi(\mathbf{a}))$.

(2) $\nu(\varphi(\mathbf{a})) = \nu^{\otimes 2}(\varphi(\mathbf{a})) = \cdots = \nu^{\otimes 2^{k-1}}(\varphi(\mathbf{a}))$.

(3) $\sigma(\varphi(\mathbf{a})) = \nu(\varphi(\mathbf{a}))$.

(4) $\nu^{\otimes 2^{k-1}}(\varphi(\mathbf{a})) = (\sigma \otimes \nu)^{\otimes 2^{k-2}}(\varphi(\mathbf{a})) = (\nu \otimes \sigma)^{\otimes 2^{k-2}}(\varphi(\mathbf{a}))$.

(5) Si $\widetilde{\pi}$ es la permutación sobre $\mathbb{Z}_4^{2^{k-1}n}$ inducida por la permutación π definida en la relación (5.3)*, entonces*

$$\nu^{\otimes 2^{k-1}}(\varphi(\mathbf{a})) = \widetilde{\pi}\left(\nu^{\otimes 2^{k-1}}(\varphi(\mathbf{a}))\right).$$

En particular, se tiene que

$$\nu^{\otimes 2^{k-1}}(\varphi(\mathbf{a})) = \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}(\varphi(\mathbf{a}))\right) = \widetilde{\pi}\left((\nu \otimes \sigma)^{\otimes 2^{k-2}}(\varphi(\mathbf{a}))\right).$$

Demostración. Dado que $\mathbf{a}$ tiene un cero en la coordenada con subíndice $n-1$, se tiene que el vector $\varphi(\mathbf{a}) \in \mathbb{Z}_4^{2^{k-1}}$ tiene un cero en aquellas coordenadas con subíndice en el conjunto (ver la relación (3.6))

$$I(2^{k-1},n) = \{n-1, 2n-1, 3n-1, \ldots, 2^{k-1}n-1\}.$$

Consecuentemente, $\varphi(\mathbf{a})$ puede ser expresado como la concatenación de 2^{k-1} vectores de longitud n sobre $\mathbb{Z}_4$, los cuales tienen su última coordenada igual a cero, digamos $(A^i,0) \in \mathbb{Z}_4^{n-1} \times \{0\}$. Entonces

$$\varphi(\mathbf{a}) = \big(\underbrace{A^0,0}_{n}|\underbrace{A^1,0}_{n}|\cdots|\underbrace{A^{2^{k-1}-2},0}_{n}|\underbrace{A^{2^{k-1}-1},0}_{n}\big).$$

A partir de aquí es fácil convencerse de que las relaciones (1)-(4) del Lema son ciertas. En efecto,

$$\begin{aligned}\sigma^{\otimes 2^{k-1}}(\varphi(\mathbf{a})) &= \big(\sigma(A^0,0)|\sigma(A^1,0)|\cdots|\sigma(A^{2^{k-1}-2})|\sigma(A^{2^{k-1}-1},0)\big)\\ &= \big(0,A^0|0,A^1|\cdots|0,A^{2^{k-1}-2}|0,A^{2^{k-1}-1}\big).\end{aligned}$$

Pero esta expresión es la misma si calculamos $\sigma(\varphi(\mathbf{a}))$, $\sigma^{\otimes 2}(\varphi(\mathbf{a}))$, etcétera. Esto verifica la reclación (1) del Lema. Además, note que

$$\sigma(A^i,0) = (0,A^i) = \nu(A^i,0), \qquad \forall\, i = 0,1,\ldots,2^{k-1}-1,$$

y, por lo tanto, (2)-(4) se siguen inmediatamente. Para demostrar (5), observe que el vector $\nu^{\otimes 2^{k-1}}(\varphi(\mathbf{a})) = \sigma^{\otimes 2^{k-1}}(\varphi(\mathbf{a}))$ tiene ceros en las coordenadas con subíndice en el conjunto

$$\{0,n,2n,\ldots,(2^{k-1}-1)n\},$$

y que la permutación $\widetilde{\pi}$ intercambia precisamente aquellas coordenas cuyo subíndice está en tal conjunto. En consecuencia (5) se sigue. □

Observe que en virtud del Lema 5.2.5, el vector

$$\nu^{\otimes 2^{k-1}}(\varphi(\mathbf{a})) = (\sigma\otimes\nu)^{\otimes 2^{k-2}}(\varphi(\mathbf{a})) = (\nu\otimes\sigma)^{\otimes 2^{k-1}}(\varphi(\mathbf{a}))$$

permanece fijo bajo la permutación $\widetilde{\pi}$.

Lema 5.2.6. *Sean $k \geq 2$, $n \geq 1$ y $\widetilde{\pi}$ la permutación sobre $\mathbb{Z}_4^{2^{k-1}}$ inducida por la permutación π definida en* (5.3)*. Entonces, para todo $Z \in \mathbb{Z}_{2^{k+1}}$, se tiene que*

$$\nu^{\otimes 2^{k-1}}(\varphi(2^kZ \odot 2Z)) = \widetilde{\pi}(\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(\varphi(2^kZ\odot 2Z)\right) = \widetilde{\pi}(\nu\otimes\sigma)^{\otimes 2^{k-2}}\left(\varphi(2^kZ\odot 2Z)\right).$$

Demostración. Si $Z = r_0(Z)+2r_1(Z)+\cdots+2^k r_k(Z)$ es la representación 2-ádica de Z, entonces

$$\begin{aligned}\varphi(2^kZ\odot 2Z) &= 2c_{k-1}^{k-1}\otimes r_0(Z)*r_{k-1}(Z) = c_{k-1}^{k-1}\otimes 2A\\ &= c_{k-2}^{k-2}\otimes(1,1)\otimes 2A = c_{k-2}^{k-2}\otimes(2A|2A),\end{aligned}$$

donde $A = r_0(Z)*r_{k-1}(Z)\in\{0,1\}^n\subseteq\mathbb{Z}_4^n$ y "$*$" es la multiplicación coordenada por coordenada de los vectores $r_0(Z)$ y $r_{k-1}(Z)$. En consecuencia, por el Lema 3.2.3, se tiene que

$$\nu^{\otimes 2^{k-1}}(\varphi(2^kZ\otimes 2Z)) = \nu^{\otimes 2^{k-1}}(c_{k-2}^{k-2}\otimes(2A|2A)) = c_{k-2}^{k-2}\otimes\nu^{\otimes 2}(2A|2A).$$

Ya que $2A$ es un vector cuyas coordenadas están en el ideal maximal de $\mathbb{Z}_4$, se sigue que

$$\nu^{\otimes 2}(2A|2A) = (\nu(2A)|\nu(2A)) = (\sigma(2A)|\nu(2A)) = (\nu(2A)|\sigma(2A)).$$

De acuerdo a la defínción del operador "$\otimes$", tenemos que $(\sigma(2A)|\nu(2A)) = (\sigma\otimes\nu)(2A|2A)$. Por lo tanto,

$$\nu^{\otimes 2^{k-1}}(\varphi(2^kZ\otimes 2Z)) = c_{k-2}^{k-2}\otimes(\sigma\otimes\nu)(2A|2A) = (\sigma\otimes\nu)^{\otimes 2^{k-2}}(c_{k-2}^{k-2}\otimes(2A|2A)).$$

Reintegrando el proceso, obtenemos la relación $c_{k-2}^{k-2}\otimes(2A|2A) = c_{k-1}^{k-1}\otimes 2A$, de donde concluimos que $\nu^{\otimes 2^{k-1}}(\varphi(2^kZ\odot 2Z)) = (\sigma\otimes\nu)^{\otimes 2^{k-2}}\big(\varphi(2^kZ\odot 2Z)\big)$. Para demostrar la segunda relación, basta observar que $\nu^{\otimes 2^{k-1}}(\varphi(2^kZ\odot 2Z))$ es la concatenación de 2^{k-1} vectores de longitud n cada uno, a saber, los vectores $\nu(2A)$:

$$\nu^{\otimes 2^{k-1}}(\varphi(2^kZ\odot 2Z)) = (\nu(2A)|\nu(2A)|\cdots|\nu(2A)|\nu(2A))\in(\mathbb{Z}_4^n)^{2^{k-1}}.$$

Recuerde que la definición de la permutación π es

$$\pi = (0\quad l)(n\quad l+n)(2n\quad l+2n)\cdots((2^{k-2}-1)n\quad l+(2^{k-2}-1)n),$$

donde $l = 2^{k-2}n$. Por lo tanto, la permutación $\widetilde{\pi}$ intercambia la primera coordenada del vector $\nu(2A)$ ubicado en el bloque i con la primera coordenada del vector $\nu(2A)$ del bloque $l+i$, donde $0\le i\le(2^{k-2}-1)n$. En consecuencia, se sigue que

$$\nu^{\otimes 2^{k-1}}(\varphi(2^kZ\odot 2Z)) = \widetilde{\pi}(\nu^{\otimes 2^{k-1}}(\varphi(2^kZ\odot 2Z))),$$

lo que finaliza la prueba. □

Del mismo modo que en el Lema 5.2.5, observemos que el vector $\nu^{\otimes 2^{k-1}}(\varphi(2^kZ\odot 2Z))$ queda invariante bajo la acción de permutación $\widetilde{\pi}$. Así, esta permutación puede o no ser considerada como parte de escritura de dicho vector. Haremos uso de esta ventaja en el Teorema 5.2.10 que enunciaremos más adelante.

Lema 5.2.7. *Sea $n \geq 1$ un entero y $\mathbf{b} = (0,\ldots,0,b) \in \mathbb{Z}_4^n$.*

(1) Si $k \geq 2$, entonces $\nu^{\otimes 2^{k-1}}\left(3c_{k-1}^{k-1}\otimes\mathbf{b} + 2c_{k-2}^{k-1}\otimes\mathbf{b}\right) = (\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(c_{k-1}^{k-1}\otimes\mathbf{b}\right)$.

(2) Si $k \geq 3$, entonces $\left(\widetilde{\pi}\circ(\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)\left(c_{k-1}^{k-1}\otimes\mathbf{b}\right) = (\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(c_{k-1}^{k-1}\otimes\mathbf{b}\right)$.

Demostración. Primero note que

$$3c_{k-1}^{k-1}\otimes\mathbf{b} + 2c_{k-2}^{k-1}\otimes\mathbf{b} = \left(3c_{k-1}^{k-1} + 2c_{k-2}^{k-1}\right)\otimes\mathbf{b}.$$

Además, de la definición recursiva de los vectores c_i^{k-1}, sabemos que $c_{k-1}^{k-1} = c_{k-2}^{k-2}\otimes(1,1)$ y $c_{k-2}^{k-1} = c_{k-2}^{k-1}\otimes(0,1)$. En consecuencia,

$$3c_{k-1}^{k-1} + 2c_{k-2}^{k-1} = c_{k-2}^{k-2}\otimes(3,1).$$

Por otra parte, del Lema 3.2.3 se obtiene que

$$\begin{aligned}\nu^{\otimes 2^{k-1}}\left(\left(3c_{k-1}^{k-1} + 2c_{k-2}^{k-1}\right)\otimes\mathbf{b}\right) &= (\nu\otimes\nu)^{\otimes 2^{k-2}}\left(\left(3c_{k-1}^{k-1} + 2c_{k-2}^{k-1}\right)\otimes\mathbf{b}\right)\\ &= (\nu\otimes\nu)^{\otimes 2^{k-2}}\left(c_{k-2}^{k-2}\otimes(3,1)\otimes\mathbf{b}\right)\\ &= (\nu\otimes\nu)^{\otimes 2^{k-2}}\left(c_{k-2}^{k-2}\otimes(3\mathbf{b}|\mathbf{b})\right).\end{aligned}$$

Dado que la longitud del vector c_{k-2}^{k-2} es 2^{k-2}, aplicamos el Lema 3.2.3 para obtener:

$$(\nu\otimes\nu)^{\otimes 2^{k-2}}\left(c_{k-2}^{k-2}\otimes(3\mathbf{b}|\mathbf{b})\right) = c_{k-2}^{k-2}\otimes(\nu(3\mathbf{b})|\nu(\mathbf{b})).$$

Como $\mathbf{b} = (0,\ldots,0,b) \in \mathbf{Z}_4^n$, entonces $\nu(3\mathbf{b}) = \nu(0,\ldots,0,3b) = (b,0,\ldots,0) = \sigma(\mathbf{b})$. Así,

$$\begin{aligned}c_{k-2}^{k-2}\otimes(\nu(3\mathbf{b})|\nu(\mathbf{b})) &= c_{k-2}^{k-2}\otimes(\sigma(\mathbf{b})|\nu(\mathbf{b}))\\ &= c_{k-2}^{k-2}\otimes(\sigma\otimes\nu)(\mathbf{b}|\mathbf{b})\\ &= (\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(c_{k-2}^{k-2}\otimes(\mathbf{b}|\mathbf{b})\right)\\ &= (\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(c_{k-2}^{k-2}\otimes(1|1)\otimes\mathbf{b}\right)\\ &= (\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(c_{k-1}^{k-1}\otimes\mathbf{b}\right).\end{aligned}$$

Esto finaliza la prueba de (1). Para demostrar (2), observe que

$$(\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(c_{k-1}^{k-1}\otimes\mathbf{b}\right) = (\sigma(\mathbf{b})|\nu(\mathbf{b})|\sigma(\mathbf{b})|\nu(\mathbf{b})|\cdots|\sigma(\mathbf{b})|\nu(\mathbf{b})).$$

En consecuencia, las coordenadas con subíndice en el conjunto

$$P = \{0, 2n, 4n, \ldots, 2^{k-2}n, (2^{k-2}+2)n, \ldots, (2^{k-1}-2)n\},$$

son todas iguales a b; mientras que las coordenadas con subíndice en el conjunto

$$I = \{n, 3n, 5n, \ldots, (2^{k-2}+1)n, (2^{k-2}+3)n, \ldots, (2^{k-1}-1)n\}$$

son todas iguales a $-b$. Por otro lado, recuérdese que la permutación π está definida como

$$\pi = (0 \quad l)(n \quad n+l)\cdots((2^{k-2}-2)n \quad l+(2^{k-2}-2)n)((2^{k-2}-1)n \quad l+(2^{k-2}-1)n),$$

donde $l = 2^{k-2}n$. Como $k \geq 3$, la permutación π es distinta de la permutación $(0,n)$ y, por lo tanto, $\pi(P) = P$ y $\pi(I) = I$; de donde (2) se sigue. □

Vale la pena observar que si $k = 2$, entonces $P = \{0\}$, $I = \{n\}$ y $\pi = (0 \quad n)$. Por lo tanto, $\pi(P) = I$ y $\pi(I) = P$, de este modo, si $k = 2$ la relación (2) del Lema 5.2.7 es falsa. Por otro lado, obsérvese que en la relación (1) del Lema 5.2.7 la permutación $\widetilde{\pi}$ no figura mientras que ésta es la clave para establecer la relación (2) del Lema 5.2.7.

Lema 5.2.8. *Sean $k \geq 2$, $n \geq 1$ enteros y $\mathbf{b} = (0, \ldots, 0, b) \in \mathbb{Z}_4^n$. Entonces en $\mathbb{Z}_4^{2^{k-1}n}$:*

(1) $\nu^{\otimes 2^{k-1}}\left(2c_{k-1}^{k-1} \otimes \mathbf{b} + 2c_0^{k-1} \otimes \mathbf{b}\right) = \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}(2c_0^{k-1} \otimes \mathbf{b})\right)$.

(2) $\nu^{\otimes 2^{k-1}}\left(2c_{k-1}^{k-1} \otimes \mathbf{b} + 2c_0^{k-1} \otimes \mathbf{b}\right) = \widetilde{\pi}\left((\nu \otimes \sigma)^{\otimes 2^{k-2}}(2c_0^{k-1} \otimes \mathbf{b})\right)$.

Demostración. Dado que $c_{k-1}^{k-1} = (1,1) \otimes c_{k-2}^{k-2}$ y $c_0^{k-1} = (0,1) \otimes c_{k-2}^{k-2}$, tenemos que

$$2c_{k-1}^{k-1} \otimes \mathbf{b} + 2c_0^{k-1} \otimes \mathbf{b} = \left(2c_{k-1}^{k-1} + 2c_0^{k-1}\right) \otimes \mathbf{b} = \left((2,0) \otimes c_{k-2}^{k-2}\right) \otimes \mathbf{b}.$$

Por lo tanto,

$$\nu^{\otimes 2^{k-1}}\left(2c_{k-1}^{k-1} \otimes \mathbf{b} + 2c_0^{k-1} \otimes \mathbf{b}\right) = \nu^{\otimes 2^{k-1}}\left(\left((2,0) \otimes c_{k-2}^{k-2}\right) \otimes \mathbf{b}\right) = \left((2,0) \otimes c_{k-2}^{k-2}\right) \otimes \nu(\mathbf{b}).$$

En consecuencia, en este último vector, se puede observar que las coordenadas cuyo subíndice está en el conjunto $F = \{0, n, 2n, \ldots, (2^{k-2}-1)n\}$ son iguales a $2b$; mientras que las coordenadas cuyo subíndice está en el conjunto $G = \{2^{k-2}n, (2^{k-2}+1)n, \ldots, (2^{k-1}-1)n\} = \{l, l+n, \ldots, l+(2^{k-2}-1)n\}$, donde $l = 2^{k-2}n$, son iguales a cero. De acuerdo a la definición de la permutación π, es fácil ver que $\pi(F) = G$ y $\pi(G) = F$. Por lo tanto,

$$\begin{aligned}
(2,0) \otimes c_{k-2}^{k-2} \otimes \nu(\mathbf{b}) &= \widetilde{\pi}\left((0,2) \otimes c_{k-2}^{k-2} \otimes \nu(\mathbf{b})\right) \\
&= \widetilde{\pi}\left(2(0,1) \otimes c_{k-2}^{k-2} \otimes \nu(\mathbf{b})\right) \\
&= \widetilde{\pi}\left(2c_0^{k-1} \otimes \nu(\mathbf{b})\right) \\
&= \left(\widetilde{\pi} \circ \nu^{\otimes 2^{k-1}}\right)(2c_0^{k-1} \otimes \mathbf{b}),
\end{aligned}$$

donde la última igualdad es debida al Lema 3.2.3. Finalmente, como las coordenadas del vector $2c_0^{k-1} \otimes \mathbf{b}$ están en el ideal maximal de $\mathbb{Z}_4$, se sigue que

$$\nu^{\otimes 2^{k-1}}\left(2c_0^{k-1} \otimes \mathbf{b}\right) = (\sigma \otimes \nu)^{\otimes 2^{k-2}}\left(2c_0^{k-1} \otimes \mathbf{b}\right) = (\nu \otimes \sigma)^{\otimes 2^{k-2}}\left(2c_0^{k-1} \otimes \mathbf{b}\right).$$

De estos últimos hechos, se concluyen (1) y (2). □

Vale la pena notar que la permutación $\widetilde{\pi}$ es necesaria para establecer el punto (2) de éste último Lema. En consecuencia, debe tenerse cuidado cuando se vea involucrado el vector $\nu^{\otimes 2^{k-1}}\left(2c_{k-1}^{k-1} \otimes \mathbf{b} + 2c_0^{k-1} \otimes \mathbf{b}\right)$.

A contiunuación damos un último lema antes de enunciar uno de los resultados más importantes de este apartado.

Lema 5.2.9. *Sean $k \geq 2, n \geq 1$ enteros, $\mathbf{b} = (0,\ldots,0,b) \in \mathbb{Z}_4^n$ y $1 \leq i \leq k-1$. Entonces*

(1) $\nu^{\otimes 2^{k-1}}\left(2c_i^{k-1} \otimes \mathbf{b}\right) = (\sigma \otimes \nu)^{\otimes 2^{k-2}}\left(2c_i^{k-1} \otimes \mathbf{b}\right) = \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\left(2c_i^{k-1} \otimes \mathbf{b}\right)\right).$

(2) $\nu^{\otimes 2^{k-1}}\left(2c_i^{k-1} \otimes \mathbf{b}\right) = (\nu \otimes \sigma)^{\otimes 2^{k-2}}\left(2c_i^{k-1} \otimes \mathbf{b}\right) = \widetilde{\pi}\left((\nu \otimes \sigma)^{\otimes 2^{k-2}}\left(2c_i^{k-1} \otimes \mathbf{b}\right)\right).$

Demostración. Dado que las coordenadas del vector $2c_i^{k-1} \otimes \mathbf{b}$ están en el ideal maximal de $\mathbb{Z}_4^n$, es claro que:

$$\nu^{\otimes 2^{k-1}}\left(2c_i^{k-1} \otimes \mathbf{b}\right) = (\sigma \otimes \nu)^{\otimes 2^{k-2}}\left(2c_i^{k-1} \otimes \mathbf{b}\right) = (\nu \otimes \sigma)^{\otimes 2^{k-2}}\left(2c_i^{k-1} \otimes \mathbf{b}\right).$$

De este modo, sólo tenemos que desmostrar que el vector $\nu^{\otimes 2^{k-1}}\left(2c_i^{k-1} \otimes \mathbf{b}\right)$ permanece invariante con respecto a la permutación $\widetilde{\pi}$, es decir,

$$\nu^{\otimes 2^{k-1}}\left(2c_i^{k-1} \otimes \mathbf{b}\right) = \widetilde{\pi}\left(\nu^{\otimes 2^{k-1}}\left(2c_i^{k-1} \otimes \mathbf{b}\right)\right).$$

Recuerde que para todo i, $1 \leq i \leq k-1$, se tiene que $c_i^{k-1} = (1,1) \otimes c_{i-1}^{k-2}$. Por lo tanto,

$$\begin{aligned} \nu_i^{\otimes 2^{k-1}} \otimes \mathbf{b} &= 2c_i^{k-1} \otimes \nu(\mathbf{b}) \\ &= 2\left((1,1) \otimes c_{i-1}^{k-2}\right) \otimes \nu(\mathbf{b}) \\ &= 2(1,1) \otimes \left(c_{i-1}^{k-2} \otimes \nu(\mathbf{b})\right). \end{aligned}$$

Esto implica que la primera y segunda mitad del vector $(1,1) \otimes c_i^{k-1} \otimes \nu(\mathbf{b})$ son iguales, de donde el resultado se establece. □

Teorema 5.2.10. *Sean $n \geq 1$, $k \geq 3$ enteros y $\widetilde{\pi}$ la permutación sobre $\mathbb{Z}_4^{2^{k-1}n}$ inducida por la permutación π definida en la relación* (5.1)*. Entonces para todo $Z = (z_0, z_1, \ldots, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$*

$$\begin{aligned}(\varphi \circ \nu_{\delta_1})(Z) &= \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\left(\varphi(Z) + \varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z)\right)\right) \\ &= \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}(\varphi(Z))\right) + \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\left(\varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z)\right)\right) \\ &= \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}(\varphi(Z))\right) + (\sigma \otimes \nu)^{\otimes 2^{k-2}}\left(\varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z)\right),\end{aligned}$$

donde $\mathbf{b}_Z = (0, \ldots, 0, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$.

Demostración. La idea de la demostración será desarrollar el lado derecho de la siguiente relación (Teorema 3.3.3)

$$\varphi \circ \nu_{\delta_1} = \nu^{\otimes 2^{k-1}} \circ \varphi \circ \eta_{\delta_2},$$

donde $\delta_1 = 1 + 2^{k-1}$, $\delta_2 = 1 + 2^{k-1} + 2^k$ y $k \geq 3$. Para este propósito, sea $Z = \mathbf{a} + \mathbf{b}_Z$, con $\mathbf{a} = (z_0, z_1, \ldots, z_{n-2}, 0)$ y $\mathbf{b}_Z = Z - \mathbf{a}$ (teniendo en cuenta que si $n = 1$, entonces $\mathbf{a} = 0$). Siendo η_{δ_2} un $\mathbf{Z}_{2^{k+1}}$-automorfismo sobre el módulo $\mathbb{Z}_{2^{k+1}}^n$, esta forma de expresar a Z implica que

$$\begin{aligned}(\varphi \circ \nu_{\delta_1})(Z) &= \left(\nu^{\otimes 2^{k-1}} \circ \varphi \circ \eta_{\delta_2}\right)(\mathbf{a} + \mathbf{b}_Z) \\ &= (\nu^{\otimes 2^{k-1}} \circ \varphi)(\eta_{\delta_2}(\mathbf{a}) + \eta_{\delta_2}(\mathbf{b}_Z)).\end{aligned}$$

Por definición, la acción de η_{δ_2} consiste en multiplicar la última coordenada de su argumento por la unidad δ_2. En consecuencia,

$$\begin{aligned}\eta_{\delta_2}(\mathbf{a}) &= (z_0, z_1, \ldots, z_{n-2}, \delta_2 \cdot 0) = (z_0, z_1, \ldots, z_{n-2}, 0) = \mathbf{b}_Z, \\ \eta_{\delta_2}(\mathbf{b}_Z) &= (0, 0, \ldots, 0, \delta_2 \cdot z_{n-2}) = \delta_2(0, \ldots, 0, z_{n-1}) = \delta_2 \mathbf{b}_Z.\end{aligned}$$

Así, $(\varphi \circ \nu_{\delta_2})(Z) = (\nu^{\otimes 2^{k-1}} \circ \varphi)(\mathbf{a} + \delta_2 \mathbf{b}_Z)$. Debido al Lema 3.3.1, la función φ es lineal en la suma $\mathbf{a} + \delta_2 \mathbf{b}_Z$, es decir, $\varphi(\mathbf{a} + \delta_2 \mathbf{b}_Z) = \varphi(\mathbf{a}) + \varphi(\delta_2 \mathbf{b}_Z)$. Además, por el Corolario 2.3.6,

$$\varphi(\delta_2 \mathbf{b}_Z) = \varphi(2^{k-1} \mathbf{b}_Z) - \varphi(\mathbf{b}_Z) + \varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z).$$

Por lo tanto,

$$(\varphi \circ \nu_{\delta_1})(Z) = \nu^{\otimes 2^{k-1}}(\varphi(\mathbf{a})) + \nu^{\otimes 2^{k-1}}(\varphi(2^{k-1} \mathbf{b}_Z) - \varphi(\mathbf{b}_Z)) + \nu^{\otimes 2^{k-1}}(\varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z)).$$

De los Lemas 5.2.5 y 5.2.6 se sigue que

$$\begin{aligned}\nu^{\otimes 2^{k-1}}(\varphi(\mathbf{a})) &= \left(\widetilde{\pi} \circ (\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)(\varphi(\mathbf{a})) \\ \nu^{\otimes 2^{k-1}}\left(\varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z)\right) &= \left(\widetilde{\pi} \circ (\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)\left(\varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z)\right)\end{aligned}$$

Así, centramos nuestra atención en el término $v^{\otimes 2^{k-1}}(\varphi(2^{k-1}\mathbf{b}_Z)-\varphi(\mathbf{b}_Z))$. Expresando a $\mathbf{b}_Z$ en su representación 2-ádica se tiene que

$$\begin{aligned}-\varphi(\mathbf{b}_Z) &= 3c_{k-1}^{k-1}\otimes r_0(\mathbf{b}_Z)+2\left[\left(c_0^{k-1}\otimes r_1(\mathbf{b}_Z)\right)\oplus\cdots\oplus\left(c_{k-1}^{k-1}\otimes r_k(\mathbf{b}_Z)\right)\right],\\ \varphi(2^{k-1}\mathbf{b}_Z) &= 2\left[\left(c_{k-2}^{k-1}\otimes r_0(\mathbf{b}_Z)\right)\oplus\left(c_{k-1}^{k-1}\otimes r_1(\mathbf{b}_Z)\right)\right].\end{aligned}$$

Debido al Coroloario 2.3.3, es posible escribir

$$\begin{aligned}-\varphi(\mathbf{b}_Z) &= 3c_{k-1}^{k-1}\otimes r_0(\mathbf{b}_Z)+2c_0^{k-1}\otimes r_1(\mathbf{b}_Z)+2\left[\left(c_1^{k-1}\otimes r_2(\mathbf{b}_Z)\right)\oplus\cdots\oplus\left(c_{k-1}^{k-1}\otimes r_k(\mathbf{b}_Z)\right)\right],\\ \varphi(2^{k-1}\mathbf{b}_Z) &= 2c_{k-2}^{k-1}\otimes r_0(\mathbf{b}_Z)+2c_{k-1}^{k-1}\otimes r_1(\mathbf{b}_Z).\end{aligned}$$

Sumando las dos expresiones anteriores obtenemos

$$\begin{aligned}\varphi(2^{k-1}\mathbf{b}_Z)-\varphi(\mathbf{b}_Z) = {} & 3c_{k-1}^{k-1}\otimes r_0(\mathbf{b}_Z)+2c_{k-2}^{k-1}\otimes r_0(\mathbf{b}_Z)\\ & +2c_0^{k-1}\otimes r_1(\mathbf{b}_Z)+2c_{k-1}^{k-1}\otimes r_1(\mathbf{b}_Z)\\ & +2\left[\left(c_1^{k-1}\otimes r_2(\mathbf{b}_Z)\right)\oplus\cdots\oplus\left(c_{k-1}^{k-1}\otimes r_k(\mathbf{b}_Z)\right)\right].\end{aligned}$$

Por lo tanto, $v^{\otimes 2^{k-1}}(\varphi(2^{k-1}\mathbf{b}_Z)-\varphi(\mathbf{b}_Z))$ es la suma de las siguientes tres expresiones:

$$\begin{aligned}&v^{\otimes 2^{k-1}}\left(3c_{k-1}^{k-1}\otimes r_0(\mathbf{b}_Z)+2c_{k-2}^{k-1}\otimes r_0(\mathbf{b}_Z)\right),\\ &v^{\otimes 2^{k-1}}\left(2c_0^{k-1}\otimes r_1(\mathbf{b}_Z)+2c_{k-1}^{k-1}\otimes r_1(\mathbf{b}_Z)\right),\\ &v^{\otimes 2^{k-1}}\left(2\left[\left(c_1^{k-1}\otimes r_2(\mathbf{b}_Z)\right)\oplus\cdots\oplus\left(c_{k-1}^{k-1}\otimes r_k(\mathbf{b}_Z)\right)\right]\right).\end{aligned}\tag{5.4}$$

Siendo $k\geq 3$, de los Lemas 5.2.7-5.2.9 se sigue que cada una de las 3 expresiones anteriores puede ser sustituida, respectivamente, por las siguientes:

$$\begin{aligned}&\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\ (c_{k-1}^{k-1}\otimes\mathbf{b}_Z)\right),\\ &\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\ (2c_0^{k-1}\otimes\mathbf{b}_Z)\right),\\ &\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\ \left(2\left[\left(c_1^{k-1}\otimes r_2(\mathbf{b}_Z)\right)\oplus\cdots\oplus\left(c_{k-1}^{k-1}\otimes r_k(\mathbf{b}_Z)\right)\right]\right)\right).\end{aligned}\tag{5.5}$$

Consecuentemente, al reunir todos estos elementos obtenemos que

$$v^{\otimes 2^{k-1}}(\varphi(2^{k-1}\mathbf{b}_Z)-\varphi(\mathbf{b}_Z))=\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(\varphi(\mathbf{b}_Z)\right)\right).$$

Por lo tanto,

$$\begin{aligned}\left(\varphi\circ\nu_{\delta_2}\right)(Z) = {} & \widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(\varphi(\mathbf{a})\right)\right)+\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(\varphi(\mathbf{b}_Z)\right)\right)\\ & +\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)\right)\right).\end{aligned}$$

Dado que la aplicación $\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)$ es un $\mathbb{Z}_4$-automorfismo, se tiene que

$$\left(\varphi\circ\nu_{\delta_2}\right)(Z)=\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(\varphi(\mathbf{a})+\varphi(\mathbf{b}_Z)+\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)\right)\right).$$

Al aplicar el Lema 3.3.1 a esta última relación y del hecho que $\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)$ es un $\mathbb{Z}_4$-automorfismo, obtenemos las primeras dos identidades establecidas en este teorema. La última relación se sigue del Lema 5.2.6. □

En el Ejemplo 5.2.1 presentamos un código de longitud 3 sobre $\mathbb{Z}_{16}$, denotado como $\mathscr{D}$, el cual tiene la propiedad de ser δ_1-cíclico. Al calcular su imagen con respecto a φ, observamos que $\varphi(\mathscr{D})$ tiene la siguiente propiedad:

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2}\right)(\varphi(Z)+\varphi(2^2\mathbf{b}_Z\odot 2\mathbf{b}_Z))\in\varphi(\mathscr{D}),\qquad \varphi(Z)\in\varphi(\mathscr{D}),$$

donde $\widetilde{\pi}$ es la permutación sobre $\mathbb{Z}_4^{12}$ inducida por la permutación $\pi=(0,6)(3,9)$.

A continuación, como una aplicación inmediata del Teorema 5.2.10, introducimos el siguiente resultado, el cual afirma que la propiedad anterior da una primera caracterización de los códigos δ_1-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, donde $k\geq 3$.

Teorema 5.2.11. *Sean $k\geq 3$, $n\geq 1$ enteros, π la permutación definida en* (5.3)*, y $\widetilde{\pi}$ la permutación sobre $\mathbb{Z}_4^{2^{k-1}n}$ inducida por π. Entonces las siguientes afirmaciones son equivalentes:*

(1) $\mathscr{C}\subseteq\mathbb{Z}_{2^{k+1}}^n$ un código δ_1-cíclico (no necesariamente lineal).

(2) $\varphi(\mathscr{C})$ es un código (no necesariamente lineal) de longitud $2^{k-1}n$ sobre $\mathbb{Z}_4$ tal que:

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(Z)+\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z))\in\varphi(\mathscr{C}),\tag{5.6}$$

donde $Z=(z_0,\ldots,z_{n-2},z_{n-1})\in\mathscr{C}$ y $\mathbf{b}_Z=(0,\ldots,0,z_{n-1})\in\mathbb{Z}_{2^{k+1}}^n$.

Demostración. Supongamos que $\mathscr{C}\subseteq\mathbb{Z}_{2^{k+1}}^n$ es un código δ_1-cíclico (no necesariamente lineal). Entonces $\nu_{\delta_1}(\mathscr{C})=\mathscr{C}$ y, por lo tanto, $(\varphi\circ\nu_{\delta_1})(\mathscr{C})=\varphi(\mathscr{C})$. Por otra parte, como $k\geq 3$, por el Teorema 5.2.10 se tiene que

$$\begin{aligned}(\varphi\circ\nu_{\delta_1})(\mathscr{C})&=\left\{(\varphi\circ\nu_{\delta_1})(Z)\ :\ Z\in\mathscr{C}\right\}\\&=\left\{\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2}\right)(\varphi(Z)+\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z))\ :\ Z\in\mathscr{C}\right\},\end{aligned}$$

donde $Z=(z_0,\ldots,z_{n-2},z_{n-1})\in\mathscr{C}$ y $\mathbf{b}_Z=(0,\ldots,0,z_{n-1})\in\mathbb{Z}_{2^{k+1}}^n$. De este modo, dado que $\mathscr{C}$ es δ_1-cíclico y la isometría φ es inyectiva,

$$\varphi(\mathscr{C})=\left\{\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2}\right)(\varphi(Z)+\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z))\ :\ \varphi(Z)\in\mathscr{C}\right\}.$$

Esto demuestra que (1) implica (2). Veamos ahora que (2) implica (1). Sea Z un vector en el código $\mathscr{C}$. Entonces $\varphi(Z) \in \varphi(\mathscr{C})$ y, por lo tanto,

$$\widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2}\right)(\varphi(Z) + \varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z)) \in \varphi(\mathscr{C}).$$

A razón del Teorema 5.2.10,

$$\widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2}\right)(\varphi(Z) + \varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z)) = \varphi(\nu_{\delta_1}(Z)),$$

de donde se sigue que $\varphi(\nu_{\delta_1}(Z)) \in \varphi(\mathscr{C})$. Más aún, debido a la inyectividad de la isometría φ, la expresión $\varphi(\nu_{\delta_1}(Z)) \in \varphi(\mathscr{C})$ implica que $\nu_{\delta_1}(Z) \in \mathscr{C}$. En consecuencia, hemos demostrado que si $Z \in \mathscr{C}$, entonces $\nu_{\delta_1}(Z) \in \mathscr{C}$, es decir, hemos probado que $\mathscr{C}$ es δ_1-cíclico. □

Veamos un ejemplo de un código δ_1-cíclico lineal sobre $\mathbb{Z}_{16}$.

Ejemplo 5.2.12. Sean $k = n = 3$ y considere el siguiente código lineal $\mathscr{R}$ de repetición de longitud 3 sobre $\mathbb{Z}_{16}$. Dado que $n \equiv 3 \pmod 4$, por la Proposición 1.3.14 y el Lema 1.4.1, al tomar $\beta = 1 + 2^{k-1} = 3$, obtenemos que el conjunto $\mu_3(\mathscr{R})$ es un código 3-cíclico lineal de longitud 3 sobre $\mathbb{Z}_{16}$, donde $\mu_3(z_0, z_1, z_2) = (z_0, 3z_1, 9z_2)$. Explícitamente, los elementos de $\mu_3(\mathscr{R})$ son:

$(0,0,0)$	$(1,5,9)$	$(2,10,2)$	$(3,15,11)$
$(4,4,4)$	$(5,9,13)$	$(6,14,6)$	$(7,3,15)$
$(8,8,8)$	$(9,13,1)$	$(10,2,10)$	$(11,7,3)$
$(12,12,12)$	$(13,1,5)$	$(14,6,14)$	$(15,11,7)$

Preservando el orden, la imagen del código $\mu_3(\mathscr{R})$ con respecto a la isometría φ consta de los siguientes elementos:

000 000 000 000	113 133 113 133	020 020 202 202	133 113 311 331
000 222 000 222	133 331 133 331	020 202 202 020	113 311 331 133
222 222 222 222	331 311 331 311	202 202 020 020	311 331 133 113
222 000 222 000	311 133 311 113	202 020 020 202	331 133 113 311

Veamos paso a paso que, en efecto, $\varphi(\mu_3(\mathscr{R}))$ satisface la afirmación (2) del Teorema 5.2.11. En todos los casos conservaremos el orden en el que aparecen los elementos.

Primero, a cada elemento de $\varphi(\mu_3(\mathscr{R}))$ le aplicamos la transformación $(\sigma \otimes \nu)^{\otimes 2}$, obteniendo lo siguiente:

000 000 000 000	311 113 311 113	002 002 220 220	313 111 131 333
000 222 000 222	313 333 313 333	002 220 220 002	311 331 133 113
222 222 222 222	133 331 133 331	220 220 002 002	131 333 313 111
222 000 222 000	131 111 131 111	220 002 002 220	133 113 311 331

Segundo, a cada uno de estos nuevos vectores, les aplicamos la permutación $\widetilde{\pi}$ sobre $\mathbb{Z}_4^{12}$ inducida por la permutación $\pi = (0 \quad 6)(3 \quad 9)$:

000 000 000 000	311 113 311 113	202 202 020 020	113 311 331 133
000 222 000 222	313 333 313 333	202 020 020 202	111 131 333 313
222 222 222 222	133 331 133 331	020 020 202 202	331 133 113 311
222 000 222 000	131 111 131 111	020 202 202 020	333 313 111 131

Tercero, calculamos los vectores $2^3\mathbf{b}_Z \odot 2\mathbf{b}_Z$, para lo cual es *importante tener conocimiento de las últimas coordenadas de los vectores del código* $\mu_3(\mathscr{R})$*:*

$(0,0,0)$	$(0,0,0)$	$(0,0,0)$	$(0,0,0)$
$(0,0,0)$	$(0,0,8)$	$(0,0,0)$	$(0,0,8)$
$(0,0,0)$	$(0,0,0)$	$(0,0,0)$	$(0,0,0)$
$(0,0,0)$	$(0,0,8)$	$(0,0,0)$	$(0,0,8)$

Si $2^3\mathbf{b}_Z \odot 2\mathbf{b}_Z = (0,0,8)$, entonces

$$(\sigma \otimes \nu)^{\otimes 2}(\varphi(2^3\mathbf{b}_Z \odot 2\mathbf{b}_Z)) = 200\ 200\ 200\ 200.$$

En cualquier otro caso, tenemos que

$$(\sigma \otimes \nu)^{\otimes 2}(\varphi(2^3\mathbf{b}_Z \odot 2\mathbf{b}_Z)) = 000\ 000\ 000\ 000.$$

De este modo, al sumar el vector $(\sigma \otimes \nu)^{\otimes 2}(\varphi(2^3\mathbf{b}_Z \odot 2\mathbf{b}_Z))$ a cada uno de los elementos calculados previamente, obtenemos el siguiente código sobre $\mathbb{Z}_{16}$.

000 000 000 000	311 113 311 113	202 202 020 020	113 311 331 133
000 222 000 222	113 133 113 133	202 020 020 202	311 331 133 113
222 222 222 222	133 331 133 331	020 020 202 202	331 133 113 311
222 000 222 000	331 311 331 311	020 202 202 020	133 113 311 331

Claramente este código es nuevamente $\varphi(\mu_3(\mathscr{R}))$ con los elementos registrados en otro orden y, por lo tanto, hemos ilustrado con este código que en efecto se tiene la propiedad (2) establecida en el Teorema 5.2.11.

Sea $\mathscr{C}$ un código de longitud n sobre $\mathbb{Z}_{2^{k+1}}$. En virtud del Teorema 5.2.11, una forma de determinar si $\mathscr{C}$ es un código δ_1-cíclico o no, es a través del código $\varphi(\mathscr{C}) \subseteq \mathbb{Z}_4^{2^{k-1}n}$. Para tal fin, debe verificarce la condición (5.6), es decir, por el Teorema 5.2.11 debe comprobarse que para cada $\varphi(Z) \in \varphi(\mathscr{C})$ el vector

$$\widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2}\right)(\varphi(Z) + \varphi(2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z)) = \\ \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}(\varphi(Z))\right) + (\sigma \otimes \nu)^{\otimes 2^{k-2}}\left(\varphi(2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z)\right)$$

es un elemento de $\varphi(\mathscr{C})$; para lo cual, es necesario conocer el sumando

$$(\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)\right).$$

Claramente, debido a la inyectividad de las aplicaciones φ y $(\sigma\otimes\nu)^{\otimes 2^{k-2}}$, el anterior sumando está determinado de manera única por el vector $2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z$, el cual a su vez depende (aunque no de manera única) del elemento $Z=(z_0,\ldots,z_{n-1})\in\mathscr{C}$, o bien, del vector $\mathbf{b}_Z=(0,\ldots,0,z_{n-1})\in\mathbb{Z}_{2^{k+1}}^n$, cuya única coordenada significativa es z_{n-1}. En otros términos, esto quiere decir que hasta el momento no es suficiente conocer al código $\varphi(\mathscr{C})$ para determinar si $\mathscr{C}$ es un código δ_1-cíclico o no. Basados en esto, afirmamos que la condición (2) del Teorema 5.2.11 ofrece una caracterización parcial de la familia de códigos δ_1-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$ (compárece con el Teorema 5.2.17).

Por los motivos antes expuestos, en los siguientes párrafos analizaremos una forma de llevar la condición (2) del Teorema 5.2.11 al punto que sea sólo necesario conocer al código $\varphi(\mathscr{C})$ para precisar si $\mathscr{C}$ es δ_1-cíclico o no. Claramente, como se ha mencionado, el problema recae en el vector $\mathbf{b}_Z=(0,\ldots,0,z_{n-1})$, el cual se usa para calcular $2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z$ y $\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)$. Por lo tanto, nuestro análisis se concentra en estudiar al vector $\mathbf{b}_Z$. Por el momento, y hasta que no se especifíque lo contrario, supongamos que $k\geq 3$.

Sea $\mathbf{b}_Z=(0,\ldots,0,z_{n-1})\in\mathbb{Z}_{2^{k+1}}^n$. Escribiendo a $\mathbf{b}_Z$ en su representación 2-ádica,

$$\mathbf{b}_Z=r_0(\mathbf{b}_Z)+2r_1(\mathbf{b}_Z)+\cdots+2^k r_k(\mathbf{b}_Z),$$

obtenemos que

$$\begin{aligned}2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z&=2^k r_0(\mathbf{b}_Z)*2r_{k-1}(\mathbf{b}_Z)\\&=(0,\ldots,0,2^k r_0(z_{n-1})r_{k-1}(z_{n-1}))\\&=(0,\ldots,0,2^k z_{n-1}\odot 2z_{n-1}),\end{aligned}$$

donde "$*$" denota la multiplicación coordenada por coordenada. Por una parte, observe que las relaciones anteriores implican que $2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z\neq(0)_n$ si y sólo si $2^k z_{n-1}\odot 2z_{n-1}\neq 0$; hecho al cual haremos mención más adelante. Por otra parte, dado que $r_0(z_{n-1})$ y $r_{k-1}(z_{n-1})$ están en el conjunto $\{0,1\}$, tenemos que $2^k r_0(z_{n-1})r_{k-1}(z_{n-1})\in\{0,2^k\}$; por lo que sólo existen dos posibilidades para el vector $2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z$:

1) $2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z=(0,\ldots,0)\in\mathbb{Z}_{2^{k+1}}^n$, y

2) $2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z=(0,\ldots,0,2^k)\in\mathbb{Z}_{2^{k+1}}^n$.

El primer caso se tiene si y sólo si una de las siguientes condiciones equivalentes ocurre:

1.a) $2^k z_{n-1} \odot 2z_{n-1} = 0$,

1.b) $r_0(z_{n-1})r_{k-1}(z_{n-1}) = 0$,

1.c) $r_0(z_{n-1}) = 0$, o bien, $r_{k-1}(z_{n-1}) = 0$,

1.d) $\varphi(2^k z_{n-1} \odot 2z_{n-1}) = (0)_{2^{k-1}}$,

1.e) $\varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z) = (0)_{2^{k-1}n} \in \mathbf{Z}_4^{2^{k-1}n}$,

1.f) $\varphi(\nu_{\delta_1}(Z)) = \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)(\varphi(Z))$.

Note que en particular, del punto 1.c) se sigue que para todo $z_{n-1} \in \langle 2 \rangle \subseteq \mathbb{Z}_{2^{k+1}}$, $2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z = (0,\ldots,0) \in \mathbb{Z}_{2^{k+1}}^n$ y, por lo tanto, todo elemento z_{n-1} que pertenezca al ideal maximal del anillo $\mathbb{Z}_{2^{k+1}}$, satisface la siguiente relación

$$\varphi(\nu_{\delta_1}(Z)) = \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)(\varphi(Z)).$$

Como consecuencia de este breve análisis tenemos el siguiente resultado.

Proposición 5.2.13. *Sean $k \geq 3, n \geq 1$ enteros, π la permtación definida en* (5.3)*, y $\widetilde{\pi}$ la permutación sobre $\mathbb{Z}_4^{2^{k-1}n}$ inducida por π. Sea $\mathscr{C} \subseteq (2\mathbb{Z}_{2^{k+1}})^n$ un código. Entonces $\mathscr{C}$ es δ_1-cíclico si y sólo si*

$$\widetilde{\pi}\left(\nu^{\otimes 2^{k-1}}(\varphi(\mathscr{C}))\right) = \widetilde{\pi}\left(\sigma^{\otimes 2^{k-1}}(\varphi(\mathscr{C}))\right) = \varphi(\mathscr{C}).$$

Demostración. Por definición, $\varphi(Z) = c_{k-1}^{k-1} \otimes r_0(Z) + 2\left[c_0^{k-1} \otimes r_1(Z) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes r_k(Z)\right]$, donde $Z \in \mathbb{Z}_{2^{k+1}}^n$. En consecuencia, si $Z \in (2\mathbb{Z}_{2^{k+1}})^n$, todas las coordenadas del vector $\varphi(Z)$ están en el ideal maximal de $\mathbb{Z}_4$. Así $\widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)(\varphi(Z)) = \widetilde{\pi}\left((\nu \otimes \nu)^{\otimes 2^{k-2}}\right)(\varphi(Z))$ y $\widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)(\varphi(Z)) = \widetilde{\pi}\left((\sigma \otimes \sigma)^{\otimes 2^{k-2}}\right)(\varphi(Z))$. Por lo tanto,

$$\widetilde{\pi}\left(\nu^{\otimes 2^{k-1}}\right)(\varphi(Z)) = \widetilde{\pi}\left(\sigma^{\otimes 2^{k-1}}\right)(\varphi(Z)).$$

En consecuencia, si $\mathscr{C} \subseteq (2\mathbb{Z}_{2^{k+1}})^n$ es un código δ_1-cíclico, entonces

$$\widetilde{\pi}\left(\nu^{\otimes 2^{k-1}}(\varphi(\mathscr{C}))\right) = \widetilde{\pi}\left(\sigma^{\otimes 2^{k-1}}(\varphi(\mathscr{C}))\right) = \varphi(\mathscr{C}).$$

Para la implicación recírpoca, supongamos que $Z \in \mathscr{C}$ y probemos que $\nu_{\delta_1}(Z) \in \mathscr{C}$. Como $Z \in (2\mathbb{Z}_{2^{k+1}})^n$,

$$\varphi(\nu_{\delta_1}(Z)) = \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)(\varphi(Z)).$$

Además, ya que $\varphi(Z) \in (2\mathbb{Z}_4)^{2^{k-1}n}$, entonces

$$\varphi(\nu_{\delta_1}(Z)) = \widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(Z)) = \widetilde{\pi}\left(\nu)^{\otimes 2^{k-1}}\right)(\varphi(Z)).$$

Debido a la inyectividad de φ, de lo anterior obtenmos que $\nu_{\delta_1}(Z) \in \mathscr{C}$. □

De la descripción de los códigos γ-cíclicos dada en la sección 1.3.2, obtenemos que existen varios códigos δ_1-cíclicos lineales sobre $\mathbb{Z}_{2^{k+1}}$ que satisfacen las hipótesis de la Proposición anterior.

Continuando con el análisis central, observe que el segundo caso sucede si y sólo si una de las siguientes condiciones equivalentes resulta:

2.a) $2^k z_{n-1} \odot 2z_{n-1} = 2^k$,

2.b) $r_0(z_{n-1})r_{k-1}(z_{n-1}) = 1$,

2.c) $r_0(z_{n-1}) = r_{k-1}(z_{n-1}) = 1$,

2.d) $\varphi(2^k z_{n-1} \odot 2z_{n-1}) = (2)_{2^{k-1}}$,

2.e) $\varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z) = c_{k-1}^{k-1} \otimes (0,\ldots,0,2) = (0,\ldots,0,2|0,\ldots,0,2|\cdots|0,\ldots,0,2) \in (\mathbb{Z}_4^n)^{2^{k-1}}$,

2.f) $\varphi(\nu_{\delta_1}(Z)) = \widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(Z) + c_{k-1}^{k-1} \otimes (0,\ldots,0,2))$.

A diferencia del caso 1, en esta segunda instancia el vector $\varphi(Z)$ se ve afectado por el sumando $c_{k-1}^{k-1} \otimes (0,\ldots,0,2)$. A raíz de esta observación, analizaremos con más detalle este caso.

Primero observemos que del punto 2.e) se tiene que las únicas coordenadas del vector $\varphi(Z)$ que se ven alteradas por el sumando $c_{k-1}^{k-1} \otimes (0,\ldots,0,2)$ son aquellas con subíndice en el conjunto $I(2^{k-1},n) = \{n-1, 2n-1, \ldots, 2^{k-1}n-1\}$.

Por otro lado, recuerde que si expresamos al vector $Z = (z_0,\ldots,z_{n-2},z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$ de la forma $Z = \mathbf{a} + \mathbf{b}_Z$, donde $\mathbf{a} = (z_0,\ldots,z_{n-2},0)$ y $\mathbf{b}_Z = (0,\ldots,0,z_{n-1})$, entonces (cf. Lema 3.3.1)

$$\varphi(Z) = \varphi(\mathbf{a}) + \varphi(\mathbf{b}_Z).$$

Asimismo, recuerde que $\varphi(\mathbf{a})$ tiene ceros en las coordenas con subíndice en $I(2^{k-1},n)$ y, por lo tanto, las coordenadas del vector $\varphi(Z)$ con subíndice en $I(2^{k-1},n)$ son precisamente las coordenas del vector $\varphi(\mathbf{b}_Z)$ con subíndice en ese mismo conjunto. Dado que $\varphi(\mathbf{b}_Z)$ tiene ceros en el conjunto $J(2^{k-1},n)$ (ver la relación 3.7), las coordenadas significativas de $\varphi(\mathbf{b}_Z)$ son aquellas con subíndice en $I(2^{k-1},n)$. Note que al concatenar en orden esas coordenadas, obtenemos el vector $\varphi(z_{n-1})$ y, por lo tanto, los vectores $\varphi(z_{n-1})$ y $\varphi(\mathbf{b}_Z)$ quedan completamente descritos

por las coordenadas del vector $\varphi(Z)$ con subíndice en $I(2^{k-1},n)$. De este modo, si conocemos $\varphi(Z)$, entonces también conocemos $\varphi(z_{n-1})$ y $\varphi(\mathbf{b}_Z)$.

Dado que φ es inyectiva, basta tener conocimiento del vector $\varphi(z_{n-1})$ para comprender al elemento z_{n-1}, y recíprocamente. En particular, queremos usar esta información para entender qué propiedades tiene el vector $\varphi(z_{n-1})$ cuando $2^k z_{n-1} \odot 2z_{n-1} \neq 0$.

Ya que $\varphi(2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z) \neq (0)_{2^{k-1}n}$ si y sólo si $\varphi(2^{k-1}z_{n-1} \odot 2z_{n-1}) \neq (0)_{2^{k-1}}$ (pues φ es inyectiva y $2^k z_{n-1} \odot 2z_{n-1} \neq 0$ si y sólo si $2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z \neq (0)_n$), en lo subsecuente analizaremos a los vectores $\varphi(x)$, donde $x \in \mathbb{Z}_{2^{k+1}}^n$, y para los cuales $2^k x \odot 2x \neq 0$.

Es importante observar que hasta este momento no se ha hecho uso explícito de la hipótesis general de que $k \geq 3$. De hecho es fácil ver que las observaciones previas son válidas también cuando $k = 2$. Sin embargo, para que las siguientes expresiones tengan sentido, a partir de este punto haremos uso de tal hipótesis.

Sea $k \geq 3$ y $x = r_0(x) + 2r_1(x) + \cdots + 2^k r_k(x)$ un elemento del anillo $\mathbb{Z}_{2^{k+1}}$ expresado en su representación 2-ádica. En virtud de la definición de φ,

$$\begin{aligned}\varphi(x) &= c_{k-1}^{k-1} \otimes r_0(x) + 2\left[c_0^{k-1} \otimes r_1(x) \oplus \cdots \oplus c_{k-2}^{k-1} \otimes r_{k-1}(x) \oplus c_{k-1}^{k-1} \otimes r_k(x)\right] \\ &= r_0(x)c_{k-1}^{k-1} + 2\left[r_0(x)c_0^{k-1} \oplus \cdots \oplus r_{k-1}(x)c_{k-2}^{k-1} \oplus r_k(x)c_{k-1}^{k-1}\right].\end{aligned}$$

Supongamos primero que $2^k x \odot 2x \neq 0$. Entonces $r_0(x) = r_{k-1}(x) = 1$ y, por lo tanto,

$$\varphi(x) = c_{k-1}^{k-1} + 2\left[r_1(x)c_0^{k-1} \oplus \cdots \oplus r_{k-2}(x)c_{k-3}^{k-1} \oplus c_{k-2}^{k-1} \oplus r_k(x)c_{k-1}^{k-1}\right].$$

Dado que $k \geq 3$, una forma equivalente de escribir la relación anterior es (ver el Corolario 2.3.3):

$$\varphi(x) - c_{k-1}^{k-1} + 2c_{k-2}^{k-1} = 2\left[r_1(x)c_0^{k-1} \oplus \cdots \oplus r_{k-2}(x)c_{k-3}^{k-1} \oplus r_k(x)c_{k-1}^{k-1}\right].$$

Recuerde que por definición,

$$c_{k-1}^{k-1} = c_{k-2}^{k-2} \otimes (1,1), \qquad c_{k-2}^{k-1} = c_{k-2}^{k-2} \otimes (0,1).$$

En consecuencia,

$$-c_{k-1}^{k-1} + 2c_{k-2}^{k-1} = c_{k-2}^{k-2} \otimes (3,1) = (3,1,3,1,\ldots,3,1) \in \mathbb{Z}_4^{2^{k-1}} \tag{5.7}$$

De este modo, si $2^k x \odot 2x \neq 0$, obtenemos

$$\varphi(x) + (3,1,3,1,\ldots,3,1) = 2\left[r_1(x)c_0^{k-1} \oplus \cdots \oplus r_{k-2}(x)c_{k-3}^{k-1} \oplus r_k(x)c_{k-1}^{k-1}\right].$$

Recíprocamente, supongamos que

$$\varphi(x) + (3,1,3,1,\ldots,3,1) = 2\left[\alpha_1 c_0^{k-1} \oplus \cdots \oplus \alpha_{k-2}c_{k-3}^{k-1} \oplus \alpha_k c_{k-1}^{k-1}\right],$$

donde $\alpha_k, \alpha_i \in \{0,1\}$, $1 \leq i \leq k-2$. Entonces, usando la relación (5.7) y el Corolario 2.3.3, obtenemos:

$$\varphi(x) = c_{k-1}^{k-1} + 2\left[\alpha_1 c_0^{k-1} \oplus \cdots \oplus \alpha_{k-2} c_{k-3}^{k-1} \oplus c_{k-2}^{k-1} \oplus \alpha_k c_{k-1}^{k-1}\right].$$

Debido a que la función φ es inyectiva,

$$x = 1 + 2\alpha_1 + \cdots + 2^{k-2}\alpha_{k-2} + 2^{k-1} + 2^k\alpha_k. \tag{5.8}$$

Además, como $\alpha_k, \alpha_i \in \{0,1\}$, $1 \leq i \leq k-2$, la relación (5.8) resulta ser la representación 2-ádica de x. En particular, esto implica que $r_0(x) = r_{k-1}(x) = 1$ y, por lo tanto, $2^k x \odot 2x \neq 0$. Consecuentemente, se ha demostrado que $2^k x \odot 2x \neq 0$ si y sólo si

$$\varphi(x) + (3,1,3,1,\ldots,3,1) = 2\left[\alpha_1 c_0^{k-1} \oplus \cdots \oplus \alpha_{k-2} c_{k-3}^{k-1} \oplus \alpha_k c_{k-1}^{k-1}\right], \tag{5.9}$$

para algunos escalares $\alpha_1, \alpha_2, \ldots, \alpha_{k-2}, \alpha_k \in \{0,1\}$. Pero podemos decir más aún.

A razón del Corolario 2.3.3, el término del lado derecho de la relación (5.9) puede expresarse como

$$\alpha_1\left(2c_0^{k-1}\right) + \cdots + \alpha_{k-2}\left(2c_{k-3}^{k-1}\right) + \alpha_k\left(2c_{k-1}^{k-1}\right).$$

Este punto de vista permite escribir al vector $\varphi(x)+(3,1,3,1,\ldots,3,1)$ como combinación lineal (en $\mathbb{Z}_4$) de los vectores

$$2c_0^{k-1},\ 2c_1^{k-1},\ \ldots\ ,\ 2c_{k-3}^{k-1},\ 2c_{k-1}^{k-1}.$$

Por otra parte, recuerde que por definición, el submódulo de $\mathbb{Z}_4^{2^{k-1}}$ generado por los vectores $2c_0^{k-1}, 2c_1^{k-1}, \ldots, 2c_{k-3}^{k-1}, 2c_{k-1}^{k-1}$ es el conjunto

$$\langle 2c_0^{k-1}, \ldots, 2c_{k-3}^{k-1}, 2c_{k-1}^{k-1}\rangle = \left\{\alpha_1\left(2c_0^{k-1}\right) + \cdots + \alpha_{k-2}\left(2c_{k-3}^{k-1}\right) + \alpha_k\left(2c_{k-1}^{k-1}\right) : \alpha_i \in \mathbb{Z}_4\right\}.$$

Así, los escalares α_i de la relación anterior varían en $\mathbb{Z}_4$. Sin embargo, ya que $2c_i^{k-1} \in \{0,2\}^{2^{k-1}}$, es suficiente elegir a los escalares α_i en el conjunto $\{0,1\} \subseteq \mathbb{Z}_4$. Esto demuestra que para cada vector $v \in \langle 2c_0^{k-1}, \ldots, 2c_{k-3}^{k-1}, 2c_{k-1}^{k-1}\rangle$, existe $x \in \mathbb{Z}_{2^{k+1}}$ tal que $\varphi(x) + (3,1,3,1,\ldots,3,1) = v$, o de forma equivalente, para cada $v \in \langle 2c_0^{k-1}, \ldots, 2c_{k-3}^{k-1}, 2c_{k-1}^{k-1}\rangle$ existe $x \in \mathbb{Z}_{2^{k+1}}$ tal que $2^k x \odot 2x \neq 0$.

Todo lo anterior nos conlleva a enunciar el siguiente resultado.

Proposición 5.2.14. *Sea $k \geq 3$ un entero y $x \in \mathbb{Z}_{2^{k+1}}$. Entonces $2^k x \odot 2x \neq 0$ si y sólo si*

$$\varphi(x) + (3,1,3,1,\ldots,3,1) \in \langle 2c_0^{k-1}, \ldots, 2c_{k-3}^{k-1}, 2c_{k-1}^{k-1}\rangle \subseteq \mathbb{Z}_4^{2^{k-1}}.$$

Además, existe una biyección entre el conjunto $X = \{x \in \mathbb{Z}_{2^{k+1}} : 2^k x \odot 2x \neq 0\}$ y el submódulo $\langle 2c_0^{k-1}, \ldots, 2c_{k-3}^{k-1}, 2c_{k-1}^{k-1}\rangle$ de $\mathbb{Z}_4^{2^{k-1}}$ dada por

$$\alpha_1\left(2c_0^{k-1}\right) + \cdots + \alpha_{k-2}\left(2c_{k-3}^{k-1}\right) + \alpha_k\left(2c_{k-1}^{k-1}\right) \mapsto 1 + 2\alpha_1 + \cdots + 2^{k-2}\alpha_{k-2} + 2^{k-1} + 2^k\alpha_k.$$

En consecuencia, $|X| = |\langle 2c_0^{k-1}, \ldots, 2c_{k-3}^{k-1}, 2c_{k-1}^{k-1}\rangle| = 2^{k-1}$.

Vale la pena observar que el submódulo $\langle 2c_0^{k-1},\ldots,2c_{k-3}^{k-1},2c_{k-1}^{k-1}\rangle$ de $\mathbb{Z}_4^{2^{k-1}}$ es un código lineal de longitud 2^{k-1} sobre $\mathbb{Z}_4$ que está contenido en el código de Reed-Muller $\mathrm{ZRM}(1,k-1)$ sobre $\mathbb{Z}_4$, y cuyos elementos tienen todas sus coordenadas en el ideal maximal de $\mathbb{Z}_4$. Para ser más específicos con esta observación, recuerde que por definición, el código $\mathrm{ZRM}(1,k-1)$ es el código de longitud 2^{k-1} sobre $\mathbb{Z}_4$ generado por $\mathrm{RM}(0,k-1)$ y $2\mathrm{RM}(1,s-1)$, donde el código binario $\mathrm{RM}(0,k-1)$ es el código de repetición de longitud 2^{k-1} y el código binario $\mathrm{RM}(1,k-1)$ es el de Reed-Muller de primer orden de longitud 2^{k-1} (ver la sección 2.1.1). De hecho, dado que una base del código $\mathrm{RM}(1,k-1)$ está formada por los vectores $c_0^{k-1},c_1^{k-1},\ldots,c_{k-1}^{k-1}$ (cf. Lema 2.1.3), se sigue que

$$\langle 2c_0^{k-1},\ldots,2c_{k-3}^{k-1},2c_{k-1}^{k-1}\rangle \subset 2\mathrm{RM}(1,k-1)\subset \mathrm{ZRM}(1,k-1).$$

Cabe mencionar que en todos los casos, estamos considerando que el conjunto $\mathbb{F}_2=\{0,1\}$ está incluido en el conjunto $\mathbb{Z}_4=\{0,1,2,3\}$.

Además de lo anterior, observe que también la Proposición 5.2.14 da una explicación alternativa al por qué todo $x\in\langle 2\rangle\subseteq\mathbb{Z}_{2^{k+1}}$ satisface que $2^k x\odot 2x=0$. En efecto, note que a través de este resultado tenemos que demostrar que el vector $\varphi(x)+(3,1,\ldots,3,1)$ no pertenece al módulo $\langle 2c_0^{k-1},\ldots,2c_{k-3}^{k-1},2c_{k-1}^{k-1}\rangle$. Pero dado que para todo $x\in\langle 2\rangle$, el vector $\varphi(x)$ tiene todas sus coordenadas en el ideal maximal de $\mathbb{Z}_4$, se sigue que todas las coordenadas del vector $\varphi(x)+(3,1,\ldots,3,1)$ son unidades de $\mathbb{Z}_4$ y, por lo tanto, no puede pertenecer al submódulo $\langle 2c_0^{k-1},\ldots,2c_{k-3}^{k-1},2c_{k-1}^{k-1}\rangle$.

Por otra parte, la relación

$$2\left(\alpha_1 c_0^{k-1}+\cdots+\alpha_{k-2}c_{k-3}^{k-1}+\alpha_k c_{k-1}^{k-1}\right)=(0)_{2^{k-1}}\in\mathbb{Z}_4^{2^{k-1}}$$

implica que

$$\alpha_1 c_0^{k-1}+\cdots+\alpha_{k-2}c_{k-3}^{k-1}+\alpha_k c_{k-1}^{k-1}=(0)_{2^{k-1}}\in\mathbb{Z}_4^{2^{k-1}},$$

pues $\alpha_i,\alpha_k\in\{0,1\}$, $0\leq i\leq k-2$, y $c_0^{k-1},\ldots,c_{k-2}^{k-1},c_{k-1}^{k-1}\in\{0,1\}^{2^{k-1}}$. Como resultado de este hecho,

$$2c_{k-2}^{k-1}\notin\langle 2c_0^{k-1},\ldots,2c_{k-3}^{k-1},2c_{k-1}^{k-1}\rangle,$$

a razón de que los vectores $c_0^{k-1},\ldots,c_{k-3}^{k-1},c_{k-2}^{k-1},c_{k-1}^{k-1}$ son linealmente independientes sobre $\mathbb{F}_2$.

Veamos algunos ejemplos para esclarecer todo lo que se ha anotado hasta este momento.

Ejemplo 5.2.15. Sea $k=3$. Entonces el submódulo $\langle 2c_0^{k-1},\ldots,2c_{k-3}^{k-1},2c_{k-1}^{k-1}\rangle$ es:

$$\langle 2c_0^2,2c_2^2\rangle=\{0022,2222,0000,2200\}.$$

Por lo tanto, por la Proposición 5.2.13, en $\mathbb{Z}_{16}$ se tienen 4 elementos x tales que $2^3x\odot 2x\neq 0$ y, más aún, sabemos que la representación 2-ádica de estos elementos es de la forma

$$1+2\alpha_1+2^2+2^3\alpha_3,\qquad \alpha_1,\alpha_3\in\{0,1\}.$$

$x \in U(\mathbb{Z}_{16})$	$r_0(x)$	$r_1(x)$	$r_2(x)$	$r_3(x)$	$2^3x \odot 2x$	$\varphi(x)$	$\varphi(x)+3131$
1	1	0	0	0	0	1111	0202
3	1	1	0	0	0	1133	0220
5	1	0	1	0	8	1313	0000
7	1	1	1	0	8	1331	0022
9	1	0	0	1	0	3333	2020
11	1	1	0	1	0	3311	2002
13	1	0	1	1	8	3131	2222
15	1	1	1	1	8	3113	2200

$x = r_0(x) + 2r_1(x) + 2^2r_2(x) + 2^3r_3(x)$ es la representación 2-ádica de $x \in \mathbb{Z}_{16}$.

Cuadro 5.1: Elementos de $x \in \mathbb{Z}_{16}$ tales que $2^3x \odot 2x \neq 0$

En consecuencia, $x = 5$, $x = 7$, $x = 13$ y $x = 15$ son tales que $2^3x \odot 2x \neq 2^3$. Para constatar esto, en el Cuadro 5.1 presentamos un esquema en el que analizamos la representación 2-ádica de los elementos $x \in U(\mathbb{Z}_{16})$ y la verificación de la Proposición 5.2.14. Dado que para todo $x \in \langle 2 \rangle \subseteq \mathbb{Z}_{16}$ tenemos que $2^3x \odot 2x = 0$ y $\varphi(x) + (3,1,3,1) \notin \langle 2c_0^2, 2c_2^2 \rangle$, se han omitido tales elementos en dicho cuadro. Por otra parte, queremos aprovechar este ejemplo para ilustar que en efecto el submódulo $\langle 2c_0^{k-1}, \ldots, 2c_{k-3}^{k-1}, 2c_{k-1}^{k-1} \rangle$ está contenido en el código de Reed-Muller $\mathrm{ZRM}(1, k-1)$. Siendo $k = 3$, $\mathrm{ZRM}(1,3)$ es el código generado por $\mathrm{RM}(0,2) = \{0000, 1111\}$ y $2\mathrm{RM}(1,2) = \{0000, 2002, 2200, 0202, 0220, 0022, 2020, 2222\}$. En la Sección 4.3 de este material, mostramos que los elementos de $\mathrm{ZRM}(1,3)$ son

$$\begin{array}{cccccccc} 0000 & 1111 & 2222 & 3333 & 0202 & 1313 & 2020 & 3131 \\ 0022 & 1133 & 2200 & 3311 & 0220 & 1331 & 2002 & 3113. \end{array}$$

De lo anterior vemos que $\langle 2c_0^2, 2c_2^2 \rangle = \{0022, 2222, 0000, 2200\} \subset 2\mathrm{RM}(1,2) \subset \mathrm{ZRM}(1,3)$, concluyendo de este modo el ejemplo.

Ejemplo 5.2.16. Sea $k = 4$. Entonces el submódulo $\langle 2c_0^{k-1}, \ldots, 2c_{k-3}^{k-1}, 2c_{k-1}^{k-1} \rangle$ es

$$\langle 2c_0^3, 2c_1^3, 2c_3^3 \rangle = \langle 2(0000\,1111), 2(0011\,0011), 2(1111\,1111) \rangle,$$

el cual consiste de los siguientes elementos:

$$00002222, 00220022, 2222\,2222, 0022\,2200, 2222\,0000, 2200\,0022, 2200\,2200, 0000\,0000.$$

Por la Proposición 5.2.14, la representación 2-ádica de los elementos $x \in \mathbb{Z}_{32}$ tales que $2^4x \odot 2x \neq 0$ es de la forma

$$1 + 2\alpha_1 + 2^2\alpha_2 + 2^3 + 2^4\alpha_4, \quad \alpha_i \in \{0,1\}.$$

$x \in U(\mathbb{Z}_{32})$	$a_0a_1a_2a_3a_4$	$2^4x \odot 2x$	$\varphi(x)$	$\varphi(x)+31313131$
1	10000	0	1111 1111	0202 0202
3	11000	0	1111 3333	0202 2020
5	10100	0	1133 1133	0220 0220
7	11100	0	1133 3311	0220 2002
9	10010	16	1212 1313	0000 0000
11	11010	16	1313 3131	0000 2222
13	10110	16	1331 1331	0022 0022
15	11110	16	1331 3113	0022 2200
17	10001	0	3333 3333	2020 2020
19	11001	0	3333 1111	2020 0202
21	10101	0	3311 3311	2002 2002
23	11101	0	3311 1133	2002 0220
25	10011	16	3131 3131	2222 2222
27	11011	16	3131 1313	2222 0000
29	10111	16	3113 3113	2200 2200
31	11111	16	3113 1331	2200 0022

$x = a_0 + 2a_1 + 2^2a_2 + 2^3a_3 + 2^4a_4$ es la representación 2-ádica de $x \in U(\mathbb{Z}_{32})$

Cuadro 5.2: Elementos de $x \in U(\mathbb{Z}_{32})$ tales que $2^4x \odot 2x \neq 0$

En consecuencia, estos elementos son 9,11,13,15,25,27,29,31. Como en el ejemplo anterior, creamos el Cuadro 5.2 para analizar la representación 2-ádica de las unidades en $\mathbb{Z}_{32}$ y constatar que en efecto $\varphi(x)+31313131 \in \langle 2c_0^3, 2c_1^3, 2c_3^3\rangle$ si y sólo si $x \in \{9,11,13,15,25,27,29,31\}$. Asimismo, como antes sólo hemos considerado a las unidades pues los divisores de cero en $\mathbb{Z}_{32}$ son tales que $2^4x \odot 2x = 0$.

Veamos ahora cómo aplicar la Proposición 5.2.14 para determinar si un código $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ es δ_1-cíclico o no, conociendo únicamente su imagen con respecto a la isometría φ.

Por el Teorema 5.2.11 debemos verificar que para cada $\varphi(Z) \in \varphi(\mathscr{C})$, el vector

$$\widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)(\varphi(Z)) + (\sigma \otimes \nu)^{\otimes 2^{k-2}}\left(\varphi(2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z)\right)$$

es un elemento del código $\varphi(\mathscr{C})$; para lo cual es necesario conocer al vector

$$(\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)\right).$$

Tal como se ha demostrado,

$$\begin{aligned}\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z) &= c_{k-1}^{k-1}\otimes(0,\ldots,0,2)\\ &= (0,\ldots,0,2|0,\ldots,0,2|\cdots|0,\ldots,0,2)\in(\mathbb{Z}_4^n)^{2^{k-1}}\end{aligned}$$

si y sólo si $2^k z_{n-1}\odot 2z_{n-1}\neq 0$, donde $\mathbf{b}_Z=(0,\ldots,0,z_{n-1})\in\mathbb{Z}_{2^{k+1}}^n$. Por la Proposición 5.2.14, $2^k z_{n-1}\odot 2z_{n-1}\neq 0$ si y sólo si

$$\varphi(z_{n-1})+(3,1,\ldots,3,1)\in\langle 2c_0^{k-1},\ldots,2c_3^{k-1},2c_{k-1}^{k-1}\rangle\subset\mathbb{Z}_4^{2^{k-1}}.$$

Ahora recuerde que el vector $\varphi(z_{n-1})$ se obtiene al concatenar en orden las coordenadas de $\varphi(Z)$ con subíndice en el conjunto $I(2^{k-1},n)$. Por lo tanto, $\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)=c_{k-1}^{k-1}\otimes(0,\ldots,0,2)$ si y sólo si el vector $\varphi(z_{n-1})$, obtenido al concatenar en orden las coordenadas de $\varphi(Z)$ con subíndice en el conjunto $I(2^{k-1},n)$, satisface

$$\varphi(z_{n-1})+(3,1,\ldots,3,1)\in\langle 2c_0^{k-1},\ldots,2c_3^{k-1},2c_{k-1}^{k-1}\rangle.$$

Si esta última relación no se satisface, por la Proposición 5.2.14, $2^k z_{n-1}\odot 2z_{n-1}=0$ y, por lo tanto, $\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)=(0)_{2^{k-1}n}$. De este modo, si $c=\varphi(Z)$ y

$$\widehat{c}=(\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)\right),\tag{5.10}$$

entonces $\widehat{c}=c_{k-1}^{k-1}\otimes(2,0,\ldots,0)$ si y sólo si el vector $t\in\mathbb{Z}_4^{2^{k-1}}$, obtenido al concatenar en orden las coordenadas de c con subíndice en el conjunto $I(2^{k-1},n)$, satisface

$$t+(3,1,\ldots,3,1)\in\langle 2c_0^{k-1},\ldots,2c_3^{k-1},2c_{k-1}^{k-1}\rangle,$$

o equivalentemente, $t\in(1,3,\ldots,1,3)+\langle 2c_0^{k-1},\ldots,2c_3^{k-1},2c_{k-1}^{k-1}\rangle$. En consecuencia, hemos demostrado el siguiente resultado:

Teorema 5.2.17. *Sean $k\geq 3$ y $n\geq 1$ enteros, π la permutación definida en la relación* (5.3) *y $\widetilde{\pi}$ la permutación sobre $\mathbb{Z}_4^{2^{k-1}n}$ inducida por π. Entonces las siguientes afirmaciones son equivalentes:*

(1) $\mathscr{C}\subseteq\mathbb{Z}_{2^{k+1}}^n$ es un código δ_1-cíclico (no necesariamente lineal);

(2) $\varphi(\mathscr{C}) \subseteq \mathbb{Z}_4^{2^{k-1}n}$ *es un código (no necesariamente lineal) tal que*

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(c)+\widehat{c}\in\varphi(\mathscr{C}),\qquad \forall\, c\in\varphi(\mathscr{C})$$

donde $\widehat{c}=c_{k-1}^{k-1}\otimes(2,0,\ldots,0)$ *si y sólo si el vector* $t\in\mathbb{Z}_4^{2^{k-1}}$*, obtenido al concatenar en orden las coordenadas de c con subíndice en el conjunto* $I(2^{k-1},n)$*, satisface*

$$t\in(1,3,\ldots,1,3)+\langle 2c_0^{k-1},\ldots,2c_3^{k-1},2c_{k-1}^{k-1}\rangle.$$

En caso contrario, $\widehat{c}=(0)_{2^{k-1}n}\in\mathbb{Z}_4^{2^{k-1}n}$.

Observe que la afirmación (2) del Teorema 5.2.17 depende únicamente del conocimiento del código $\varphi(\mathscr{C})$. En este sentido, el Teorema 5.2.17 ofrece una caraterización completa de los códigos δ_1-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, con respecto a su imagen $\varphi(\mathscr{C})$.

Ejemplo 5.2.18. Retomemos el Ejemplo 5.2.12 en el que analizamos la imagen del código δ_1-cíclico lineal $\mu_3(\mathscr{R})\subseteq\mathbb{Z}_{16}^3$, donde $\delta_1=1+2^{k-1}=5$. En dicho ejemplo establecimos que la imagen del código $\mu_3(\mathscr{R})$ con respecto a la isometría φ es:

000 000 000 000	113 133 113 133	020 020 202 202	133 113 311 331
000 222 000 222	133 331 133 331	020 202 202 020	113 311 331 133
222 222 222 222	331 311 331 311	202 202 020 020	311 331 133 113
222 000 222 000	311 133 311 113	202 020 020 202	331 133 113 311

También, vereficamos paso a paso que $\varphi(\mu_3(\mathscr{R}))$ satisface la afirmación (2) del Teorema 5.2.11, y en el proceso hicimos uso del conocimiento de los vectores $2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z$, donde $Z\in\mu_3(\mathscr{R})$. Ahora, comprobaremos que en efecto $\mu_3(\mathscr{R})$ es δ_1-cíclico únicamente con el conocimiento del código $\varphi(\mu_3(\mathscr{R}))$. En virtud del punto (2) del Teorema 5.2.17, debemos probar que

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2}\right)(c)+\widehat{c}\in\varphi(\mu_3(\mathscr{R})),\qquad \forall\, c\in\varphi(\mu_3(\mathscr{R}))$$

donde $\widetilde{\pi}$ es la permutación sobre $\mathbb{Z}_4^{12}$ inducida por $\pi=(0,6)(3,9)$ y $\widehat{c}=(1111)\otimes(200)$ si y sólo si el vector $t\in\mathbb{Z}_4^4$, obtenido al concatenar en orden las coordenadas de c con subíndice en el conjunto $I(2^3,3)=\{2,5,8,11\}$, satisface que $t\in(1313)+\langle 2c_0^2,2c_2^2\rangle=\{1313,1331,3131,3113\}$. En caso contrario, se toma $\widehat{c}=(0)_{12}\in\mathbb{Z}_4^{12}$. Conservando el orden en el que aparecen los elementos de $\varphi(\mu_3(\mathscr{R}))$, tenemos que los vectores t son:

0000	3333	0022	3311
0202	3131	0220	3113
2222	1111	2200	1133
2020	1313	2002	1331

En consecuencia, los vectores $\widehat{c}$ son:

$$\begin{array}{cccc} 000\,000\,000\,000 & 000\,000\,000\,000 & 000\,000\,000\,000 & 000\,000\,000\,000 \\ 000\,000\,000\,000 & 200\,200\,200\,200 & 000\,000\,000\,000 & 200\,200\,200\,200 \\ 000\,000\,000\,000 & 000\,000\,000\,000 & 000\,000\,000\,000 & 000\,000\,000\,000 \\ 000\,000\,000\,000 & 200\,200\,200\,200 & 000\,000\,000\,000 & 200\,200\,200\,200 \end{array}$$

Por lo tanto, el código que se obtiene al aplicar a cada elemento $c \in \varphi(\mu_3(\mathscr{R}))$ la transformación $\left(\widetilde{\pi} \circ (\sigma \otimes \nu)^{\otimes 2}\right)(c) + \widehat{c}$, es:

$$\begin{array}{cccc} 000\ 000\ 000\ 000 & 311\ 113\ 311\ 113 & 202\ 202\ 020\ 020 & 113\ 311\ 331\ 133 \\ 000\ 222\ 000\ 222 & 113\ 133\ 113\ 133 & 202\ 020\ 020\ 202 & 311\ 331\ 133\ 113 \\ 222\ 222\ 222\ 222 & 133\ 331\ 133\ 331 & 020\ 020\ 202\ 202 & 331\ 133\ 113\ 311 \\ 222\ 000\ 222\ 000 & 331\ 311\ 331\ 311 & 020\ 202\ 202\ 020 & 133\ 113\ 311\ 331 \end{array}$$

Dado que este último código es $\varphi(\mu_3(\mathscr{R}))$, se sigue del Teorema 5.2.17 que $\mu_3(\mathscr{R})$ es δ_1-cíclico.

Observe que el código $\mu_3(\mathscr{R})$ del Ejemplo 5.2.12 es lineal pero $\varphi(\mu_3(\mathscr{R}))$ no es lineal puesto que, por ejemplo, $133\,133\,113\,133 + 311\,113\,311\,113 = 020\,202\,020\,202 \notin \varphi(\mu_3(\mathscr{R}))$. En el siguiente ejemplo, veremos un código lineal sobre $\mathbb{Z}_{16}$ cuya imagen con respecto a φ es un código lineal sobre $\mathbb{Z}_4$. Será de particular interés lo que observaremos al respecto.

Ejemplo 5.2.19. Sean $k = 3$, $n = 3$ y $\mathscr{C}_1$ el siguiente código lineal de longitud 3 sobre $\mathbb{Z}_{16}$:

$$\mathscr{C}_1 = \{a(151) + b(080) + c(008) : a,b,c \in \mathbb{Z}_{16}\}.$$

Dado que es suficiente tomar $b,c \in \{0,1\}$, se tiene que $\mathscr{C}_1$ contiene 64 elementos. Además, observe que

$$\begin{aligned} \nu_5(151) &= 515 = 5(151) + 1(080) + 0(008), \\ \nu_5(080) &= 008 = 0(151) + 0(080) + 1(008), \\ \nu_5(008) &= 800 = 8(151) + 1(080) + 1(008). \end{aligned}$$

En consecuencia $\mathscr{C}_1$ es un código δ_1-cíclico lineal, donde $\delta_1 = 1 + 2^{k-1} = 5$. (En términos de polinomios e ideales, el código $\mathscr{C}_1$ corresponde, mediante la representación polinomial P, al ideal $\langle 1 + 5x + x^2 \rangle$ del anillo $\mathbb{Z}_{16}[x]/\langle x^3 - 5 \rangle$). Con la ayuda del Programa Computacional MAGMA V2.15-13 (Student Version), obtuvimos que la imagen de $\mathscr{C}_1$ bajo φ es un código lineal generado por los siguientes vectores en $\mathbb{Z}_4^{12}$:

$$\begin{aligned} &g_1 = 111\ 131\ 111\ 131, \quad g_2 = 020\ 020\ 020\ 020, \quad g_3 = 002\ 002\ 002\ 002, \\ &g_4 = 000\ 222\ 000\ 222, \quad g_5 = 000\ 000\ 222\ 222. \end{aligned}$$

Por otra parte, como $\mathscr{C}_1$ es δ_1-cíclico, se sigue del Teorema 5.2.17 que para cada $c \in \varphi(\mathscr{C}_1)$

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2}\right)(c)+\widehat{c}\in\varphi(\mathscr{C}_1),$$

donde $\widehat{c}=1111\otimes 200=200\,200\,200\,200$ si y sólo si el vector $t\in\mathbb{Z}_4^{2^2}$, obtenido al concatenar en orden las coordenadas de c con subíndice en el conjunto $I(2^2,3)=\{0,3,6,9\}$, satisface

$$t\in(1313)+\langle 2c_0^2,2c_2^2\rangle=\{1313,1331,3131,3113\}.$$

En caso contrario, $\widehat{c}=(0)_{12}$. En particular, tomando $c=g_3$, tenemos que $\widehat{c}=\widehat{g_3}=(0)_{12}$ y, por lo tanto,

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2}\right)(g_3)+\widehat{g_3}=200\,200\,200\,200\in\varphi(\mathscr{C}_1).$$

En consecuencia, las dos posibilidades para el vector $\widehat{c}$ pertenecen al código $\varphi(\mathscr{C}_1)$. Recordando que $\varphi(\mathscr{C}_1)$ es un código lineal, concluimos que para todo $c\in\varphi(\mathscr{C}_1)$, $\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2}\right)(c)\in\varphi(\mathscr{C}_1)$.

El anterior ejemplo presenta un código $\mathscr{C}$ tal que $\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(\mathscr{C}))=\varphi(\mathscr{C})$. Esta propiedad apareció implícitamente en la Proposición 5.2.13 en la que se demostró que un código $\mathscr{C}\subseteq(2\mathbb{Z}_{2^{k+1}})^n$ es δ_1-cíclico si y sólo si $\widetilde{\pi}\left(\nu^{\otimes 2^{k-2}}\right)(\varphi(\mathscr{C}))=\widetilde{\pi}\left(\sigma^{\otimes 2^{k-2}}\right)(\varphi(\mathscr{C}))=\varphi(\mathscr{C})$. Observe que en este resultado no se requiere que los códigos $\mathscr{C}$ o $\varphi(\mathscr{C})$ sean lineales, pero se restringe a códigos δ_1-cíclicos tales que $\mathscr{C}\subseteq(2\mathbb{Z}_{2^{k+1}})^n$. Desde este punto de vista, el ejemplo 5.2.19 muestra que existen códigos δ_1-cíclicos tales que $\mathscr{D}\nsubseteq(2\mathbb{Z}_{2^{k+1}})^n$ y

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(\mathscr{D}))=\varphi(\mathscr{D}).$$

El propósito del siguiente resultado es dar algunas condiciones para que lo anterior suceda.

Proposición 5.2.20. *Sean $n\geq 1$, $k\geq 3$ enteros y $\mathscr{C}\subseteq\mathbb{Z}_{2^{k+1}}^n$ un código tal que $2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z\in\mathscr{C}$ para todo $Z\in\mathscr{C}$, y $\varphi(\mathscr{C})\subseteq\mathbb{Z}_4^{2^{k-1}n}$ es un código lineal. Entonces $\mathscr{C}$ es δ_1-cíclico si y sólo si*

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(\mathscr{C}))=\varphi(\mathscr{C}).$$

Demostración. Supongamos que $\mathscr{C}$ es un código δ_1-cíclico y sea $c\in\varphi(\mathscr{C})$. Entonces, con la notación del Teorema 5.2.17, $\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(c)+\widehat{c}\in\varphi(\mathscr{C})$. En particular, si tomamos $x=\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)$, donde $Z\in\mathscr{C}$, entonces

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(x)+\widehat{x}\in\varphi(\mathscr{C}).$$

Pero dado que $x=\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)$ tiene todas sus coordenadas en el ideal maximal de $\mathbb{Z}_4$, se sigue que $\widehat{x}=(0)_{2^{k-1}n}$. En consecuencia esto muestra que si $x=\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)$, entonces

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(x)=(\sigma\otimes\nu)^{\otimes 2^{k-2}}(x)\in\varphi(\mathscr{C}),$$

donde la igualdad se debe al Lema 5.2.6. Ahora recuerde que para todo $c=\varphi(Z)\in\varphi(\mathscr{C})$ se ha definido $\widehat{c}=(\sigma\otimes\nu)^{\otimes 2^{k-2}}(x)$ (cf. relación (5.10)). Por lo tanto, dado que por hipótesis $\varphi(\mathscr{C})$ es lineal, tenemos que

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(c)\in\varphi(\mathscr{C})\qquad\forall\, c\in\varphi(\mathscr{C}).$$

Recíprocamente, supongamos que $\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(\mathscr{C}))=\varphi(\mathscr{C})$ y sea $Z\in\mathscr{C}$. Entonces $\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(Z))$ y $\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(2^k\mathbf{b}_Z\otimes 2\mathbf{b}_Z))$ son elementos de $\varphi(\mathscr{C})$. Consecuentemente, del Teorema 5.2.10 y de la linealidad de $\varphi(\mathscr{C})$ concluimos que

$$\varphi(\nu_{\delta_1}(Z))=\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(Z))+\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z))\in\varphi(\mathscr{C}),$$

de donde el resultado se sigue pues φ es inyectiva. □

5.3. Imágenes sobre $\mathbb{Z}_4$ de códigos $(1+2^{k-1}+2^k)$-cíclicos

En la sección anterior describimos a los códigos $(1+2^{k-1})$-cíclicos en términos de sus respectivas imágenes bajo la isometría $\varphi:\mathbb{Z}_{2^{k+1}}^n\to\mathbb{Z}_4^{2^{k-1}n}$, introducida en el Capítulo 2 de esta tesis. En este apartado, caracterizaremos a la familia de códigos $(1+2^{k-1}+2^k)$-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, $k\geq 3$, por medio de un enunciando similar al Teorema 5.2.17. Esto es natural pues las unidades $\delta_1=1+2^{k-1}$ y $\delta_2=1+2^{k-1}+2^k$ son inversas una de la otra en $\mathbb{Z}_{2^{k+1}}$.

Como introducción, veamos un ejemplo de un código δ_2-cíclico sobre $\mathbb{Z}_{16}$, y analicemos algunas de sus propiedades.

Ejemplo 5.3.1. Sean $k=3$, $n=3$ y $\mathscr{C}$ el siguiente código (no lineal) de longitud 3 sobre $\mathbb{Z}_{16}$ con elementos:

$(14,13,1)$	$(13,14,13)$	$(9,13,14)$	$(6,9,13)$
$(9,6,9)$	$(5,9,6)$	$(14,5,9)$	$(5,14,5)$
$(1,5,14)$	$(6,1,5)$	$(1,6,1)$	$(13,1,6)$

Por inspección directa, es fácil verificar que $\mathscr{C}$ es δ_2-cíclico, donde $\delta_2=13$. Conservando el orden en el que hemos enumerado los elementos de $\mathscr{C}$, el código $\varphi(\mathscr{C})$ es:

231 011 031 211	323 101 303 121	332 310 330 312	033 231 233 031
303 323 323 303	130 332 132 330	213 033 013 233	121 303 101 323
112 130 110 132	011 213 211 013	101 121 121 101	310 112 312 110

Al igual que el código $\varphi(\mathscr{D})$ del Ejemplo 5.2.1, $\varphi(\mathscr{C})$ no es casi-cíclico ni casi-negacíclico de índice d, donde $1\leq d<12$ es un divisor de 12. Por otra parte, siendo $\delta_1=5$ y $\delta_2=13$ inversos

uno del otro en $\mathbb{Z}_{16}$, es natural pensar que el código $\varphi(\mathscr{C})$ posee una propiedad similar a la de los códigos δ_1-cíclicos. Pero antes, observe que no es posible que satisfaga el Teorema 5.2.17 pues el código $\mathscr{C}$ no es δ_1-cíclico y, por lo tanto, la propiedad debe ser diferente, aunque muy similar. Para examinar tal situación, sea $\widetilde{\pi}$ la permutación sobre $\mathbb{Z}_4^{12}$, inducida por la biyección $\pi=(0,6)(3,9)$ que actúa sobre el conjunto $I_{12}=\{0,1,\ldots,11\}$. Entonces *afirmamos que*

$$\widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2}\right)(c)+\widehat{c}\in\varphi(\mathscr{C})\qquad\forall\, c\in\varphi(\mathscr{C})$$

donde $\widehat{c}=(1111)\otimes(200)$ *si y sólo si el vector* $t\in\mathbb{Z}_4^4$*, obtenido al concatenar en orden las coordenadas de c con subíndice en el conjunto* $\{0,3,6,9\}$ *satisface que*

$$t\in 1313+\langle 2c_0^2,2c_2^2\rangle=\{1313,1331,3131,3113\}.$$

Comprobemos que en efecto esto así es. Conservando el orden en el que hemos enumerado los elementos de $\varphi(\mathscr{C})$, calculamos primero los vectores t:

1111	3131	2002	3131
3333	0202	3333	2313
2002	1313	1111	0220

En consecuencia, los correspondientes vectores $\widehat{c}$ son:

000 000 000 000	200 200 200 200	000 000 000 000	200 200 200 200
000 000 000 000	000 000 000 000	000 000 000 000	000 000 000 000
000 000 000 000	200 200 200 200	000 000 000 000	000 000 000 000

Cada uno de estos vectores $\widehat{c}$ serán sumados a los correspondientes vectores $\widetilde{\pi}(\nu\otimes\sigma)^{\otimes 2}(c)$ que a continuación calculamos en dos etapas. Primero calculamos $(\nu\otimes\sigma)^{\otimes 2}(c)$:

323 101 303 121	132 110 130 112	233 031 033 231	103 123 123 103
130 332 132 330	013 233 213 033	121 303 101 323	312 330 310 332
211 013 011 213	301 321 321 301	301 112 312 101	031 211 231 011

entonces los vectores $\widetilde{\pi}(\nu\otimes\sigma)^{\otimes 2}(c)$ son:

323 101 303 121	132 110 130 112	033 231 233 031	103 123 123 103
130 332 132 330	213 033 013 233	121 303 101 323	312 330 310 332
011 213 211 013	301 321 321 301	301 112 312 101	231 011 031 211

En consecuencia, los elementos $\widetilde{\pi}(\nu\otimes\sigma)^{\otimes 2}(c)+\widehat{c}$ son:

323 101 303 121	132 110 130 112	033 231 233 031	103 123 123 103
130 332 132 330	213 033 013 233	121 303 101 323	312 330 310 332
011 213 211 013	301 321 321 301	301 112 312 101	231 011 031 211

Como podemos observar, éstos últimos son precisamente los elementos de $\varphi(\mathscr{C})$ dispuestos en otro orden y, por lo tanto, la afirmación anterior es satisfecha.

Con el fin de establecer formalmente que cualquier código δ_2-cíclico sobre $\mathbb{Z}_{2^{k+1}}$ puede ser caraterizado por la propiedad descrita en el ejemplo anterior, requerimos del siguiente resultado.

Teorema 5.3.2. *Sean $n \geq 1$, $k \geq 3$ enteros y $\widetilde{\pi}$ la permutación sobre $\mathbb{Z}_4^{2^{k-1}n}$ inducida por la permutación π definida en la relación* (5.1)*. Entonces para todo $Z = (z_0, z_1, \ldots, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$*

$$\begin{aligned}(\varphi \circ \nu_{\delta_2})(Z) &= \widetilde{\pi}\left((\nu \otimes \sigma)^{\otimes 2^{k-2}}\left(\varphi(Z) + \varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z)\right)\right) \\ &= \widetilde{\pi}\left((\nu \otimes \sigma)^{\otimes 2^{k-2}}(\varphi(Z))\right) + \widetilde{\pi}\left((\nu \otimes \sigma)^{\otimes 2^{k-2}}\left(\varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z)\right)\right) \\ &= \widetilde{\pi}\left((\nu \otimes \sigma)^{\otimes 2^{k-2}}(\varphi(Z))\right) + (\nu \otimes \sigma)^{\otimes 2^{k-2}}\left(\varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z)\right),\end{aligned}$$

donde $\mathbf{b}_Z = (0, \ldots, 0, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$.

Demostración. Sean $\delta_2 = 1 + 2^{k-1} + 2^k$ y $Z = (z_0, \ldots, z_{n-2}, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$, con $k \geq 3$. Primero observe que

$$\begin{aligned}\nu_{\delta_2}(Z) &= \left((1+2^{k-1}+2^k)z_{n-1}, z_0, \ldots, z_{n-2}\right) = \left((1+2^{k-1})z_{n-1} + 2^k z_{n-1}, z_0, \ldots, z_{n-2}\right) \\ &= \left((1+2^{k-1})z_{n-1}, z_0, \ldots, z_{n-2}\right) + \left(2^k z_{n-1}, 0, \ldots, 0\right) = \nu_{\delta_1}(Z) + 2^k \sigma(\mathbf{b}_Z).\end{aligned}$$

En consecuencia, por el Corolario 2.3.6,

$$\varphi\left(\nu_{\delta_2}(Z)\right) = \varphi\left(\nu_{\delta_1}(Z) + 2^k \sigma(\mathbf{b}_Z\right) = \varphi\left(\nu_{\delta_1}(Z)\right) + \varphi\left(2^k \sigma(\mathbf{b}_Z)\right).$$

Así, por el Teorema 5.2.10,

$$\begin{aligned}\left(\varphi \circ \nu_{\delta_2}\right)(Z) = \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)(\varphi(Z)) + \left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)(\varphi(2^k \mathbf{b}_Z \odot 2\mathbf{b}_Z)) \\ + \varphi\left(2^k \sigma(\mathbf{b}_Z)\right).\end{aligned}$$

Por definición de la isometría φ, tenemos que $\varphi(2^k \sigma(\mathbf{b}_Z)) = 2c_{k-1}^{k-1} \otimes r_0(\sigma(\mathbf{b}_Z))$, de donde concluimos que

$$\varphi\left(2^k \sigma(\mathbf{b}_Z)\right) = \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)\left(c_{k-1}^{k-1} \otimes 2r_0(\mathbf{b}_Z)\right).$$

Asimismo, de la definición de φ, tenemos que

$$\begin{aligned}&\widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)(\varphi(Z)) = \\ &\qquad \widetilde{\pi}\left((\sigma \otimes \nu)^{\otimes 2^{k-2}}\right)\left(c_0^{k-1} \otimes r_0(Z) + 2\left[c_0^{k-1} \otimes r_1(Z) \oplus \cdots \oplus c_{k-1}^{k-1} \otimes r_k(Z)\right]\right).\end{aligned}$$

Además, dado que $\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)$ es un $\mathbb{Z}_4$-automorfismo del módulo $\mathbb{Z}_4^{2^{k-1}n}$,

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(Z)) = \widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)\left(c_0^{k-1}\otimes r_0(Z)\right) + \widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)\left(2\left[c_0^{k-1}\otimes r_1(Z)\oplus\cdots\oplus c_{k-1}^{k-1}\otimes r_k(Z)\right]\right).$$

En consecuencia,

$$\left(\varphi\circ\nu_{\delta_2}\right)(Z) = \widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)\left(c_0^{k-1}\otimes r_0(Z)+c_{k-1}^{k-1}\otimes 2r_0(\mathbf{b}_Z)\right) + \widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)\left(2\left[c_0^{k-1}\otimes r_1(Z)\oplus\cdots\oplus c_{k-1}^{k-1}\otimes r_k(Z)\right]\right).$$

Analizando el primer sumando del lado derecho de la relación anterior vemos que

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)\left(c_0^{k-1}\otimes r_0(Z)+c_{k-1}^{k-1}\otimes 2r_0(\mathbf{b}_Z)\right) = \widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2^{k-2}}\right)\left(c_0^{k-1}\otimes r_0(Z)\right).$$

Ahora el resultado se sigue de los Lemas 5.2.6, 5.2.8 y 5.2.9, y de invertir el sentido de los argumentos dados en esta demostración. □

Es importante señalar que el Teorema 5.3.2 puede ser demostrado con argumentos similares a los dados en la prueba del Teorema 5.2.10. También, observe que en la demostración se ha hecho uso de la relación $\delta_2 = \delta_1 + 2^k$. Por otro lado, de la parte multiplicativa sabemos que $\delta_1\lambda = \delta_2$, lo cual nos permite ofrecer otra demostración del Teorema 5.3.2.

Segunda demostración del Teorema 5.3.2. Sean $k\geq 3$, $\delta_1 = 1+2^{k-1}$ y $\delta_2 = 1+2^{k-1}+2^k$. Dado que $\delta_1\lambda = \delta_2$, entonces $\nu_{\delta_2} = \nu_{\delta_1}\circ\eta_\lambda$, donde η_λ es el $\mathbb{Z}_{2^{k+1}}$-automorfismo del módulo $\mathbb{Z}_{2^{k+1}}^n$ dado por (ver la Sección 3.2 y la Proposición 3.2.1 para más detallles)

$$\eta_\gamma : (z_0,\ldots,z_{n-2},z_{n-2}) \mapsto (z_0,\ldots,z_{n-2},\gamma z_{n-2}).$$

Sean $Z = (z_0,\ldots,z_{n-2},z_{n-1}), \mathbf{b}_Z = (0,\ldots,0,z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$. Entonces, por el Teorema 5.2.10,

$$\begin{aligned}\varphi(\nu_{\delta_2}(Z)) &= \varphi(\nu_{\delta_1}(\eta_\lambda(Z)))\\ &= \widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(\varphi(\eta_\gamma(Z))\right)\right) + (\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(\varphi(2^k\mathbf{b}_{\eta_\lambda(Z)}\odot 2\mathbf{b}_{\eta_\lambda(Z)})\right) \quad (5.11)\end{aligned}$$

Debido al Teorema 3.3.4,

$$\varphi(\eta_\lambda(Z)) = \eta_{-1}^{\otimes 2^{k-1}}(\varphi(Z)) = (\eta_{-1}\otimes\eta_{-1})^{\otimes 2^{k-1}}(\varphi(Z)).$$

Así,

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\left(\varphi(\eta_\gamma(Z))\right)\right) = \left(\widetilde{\pi}\circ(\sigma\otimes\nu)^{\otimes 2^{k-2}}\circ(\eta_{-1}\otimes\eta_{-1})^{\otimes 2^{k-2}}\right)(\varphi(Z)).$$

Ahora, recuerde que $(f\otimes g)^{\otimes N} = f^{\otimes N}\circ g^{\otimes N}$, donde $N\geq 1$ es un entero y f,g son funciones para las cuales la composición $f\circ g$ esté bien definida. Como consecuencia de este hecho, tenemos que

$$\begin{aligned}(\sigma\otimes\nu)^{\otimes 2^{k-2}}\circ(\eta_{-1}\circ\eta_{-1})^{\otimes 2^{k-2}} &= ((\sigma\otimes\nu)\circ(\eta_{-1}\circ\eta_{-1}))^{\otimes 2^{k-2}}\\ &= ((\sigma\circ\eta_{-1})\otimes(\nu\circ\eta_{-1})))^{\otimes 2^{k-2}}\\ &= (\nu\otimes\sigma)^{\otimes 2^{k-2}}\end{aligned}$$

Sustituyendo, obtenemos:

$$\widetilde{\pi}(\sigma\otimes\nu)^{\otimes 2^{k-2}}(\varphi(\eta_\lambda(Z))) = \widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2^{k-2}}\right)(\varphi(Z)).$$

Por otro lado, $\mathbf{b}_{\eta_\lambda(Z)} = (0,\ldots,0,\lambda z_{n-1})$, donde $\lambda = 1+2^k$. Así,

$$2^k\mathbf{b}_{\eta_\lambda(Z)} = (0,\ldots,0,2^k\lambda z_{n-1}) = (0,\ldots,0,2^k z_{n-1}) = 2^k\mathbf{b}_Z.$$

Similarmente, se prueba que $2\mathbf{b}_{\eta_\lambda(Z)} = 2\mathbf{b}_Z$. Por lo tanto, $2^k\mathbf{b}_{\eta_\lambda(Z)}\odot 2\mathbf{b}_{\eta_\lambda(Z)} = 2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z$. De este modo, al reunir todos elementos expuestos, obtenemos una segunda demostración del Teorema 5.3.2. □

Como consecuencia del Teorema 5.3.2 se tiene el siguiente resultado, el cual caracteriza a los códigos δ_2-cíclicos en términos de sus respectivas imágenes bajo la isometría φ. Este resultado es análogo al Teorema 5.2.17 y, por lo tanto, omitimos su demostración.

Teorema 5.3.3. *Sean $k\geq 3$ y $n\geq 1$ enteros, π la permutación definida en la relación* (5.3) *y $\widetilde{\pi}$ la permutación sobre $\mathbb{Z}_4^{2^{k-1}n}$ inducida por π. Entonces las siguientes afirmaciones son equivalentes:*

(1) $\mathscr{C}\subseteq\mathbb{Z}_{2^{k+1}}^n$ es un código δ_2-cíclico (no necesariamente lineal).

(2) $\varphi(\mathscr{C})\subseteq\mathbb{Z}_4^{2^{k-1}}$ es un código (no necesariamente lineal) tal que

$$\widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2^{k-2}}\right)(c)+\widehat{c}\in\varphi(\mathscr{C})\qquad\forall\, c\in\varphi(\mathscr{C})$$

donde $\widehat{c} = c_{k-1}^{k-1}\otimes(2,0,\ldots,0)$ si y sólo si el vector $t\in\mathbb{Z}_4^{2^{k-1}}$, obtenido al concatenar en orden las coordenadas de c con subíndice en el conjunto $I(2^{k-1},n)$, satisface

$$t+(3,1,\ldots,3,1)\in\langle 2c_0^{k-1},\ldots,2c_3^{k-1},2c_{k-1}^{k-1}\rangle.$$

En caso contrario, $\widehat{c} = (0)_{2^{k-1}n}\in\mathbb{Z}_4^{2^{k-1}n}$.

Los correspondientes resultados a las Proposiciones 5.2.13 y 5.2.20 para códigos δ_2-cíclicos son enunciados e ilustrados a continuación.

Proposición 5.3.4. *Sean $k \geq 3, n \geq 1$ enteros, π la permtación definida en* (5.3)*, y $\widetilde{\pi}$ la permutación sobre $\mathbb{Z}_4^{2^{k-1}n}$ inducida por π. Sea $\mathscr{C} \subseteq (2\mathbb{Z}_{2^{k+1}})^n$ un código. Entonces $\mathscr{C}$ es δ_2-cíclico si y sólo si*

$$\widetilde{\pi}\left(\nu^{\otimes 2^{k-1}}\right)(\varphi(\mathscr{C})) = \widetilde{\pi}\left(\sigma^{\otimes 2^{k-1}}\right)(\varphi(\mathscr{C})) = \varphi(\mathscr{C}).$$

Consecuentemente, un código $\mathscr{C} \subseteq (2\mathbb{Z}_{2^{k+1}})^n$ es δ_1-cíclico si y sólo si es δ_2-cíclico.

Observe que en este resultado, así como en la Proposición 5.2.13, la condición de linealidad no es impuesta al código sobre $\mathbb{Z}_{2^{k+1}}$. A modo de ejemplo, sea $\mathscr{C}$ el código (no lineal) de longitud 3 sobre $\mathbb{Z}_{16}$ cuyos elementos son:

$$\begin{array}{cccc} (2,2,6) & (2,6,10) & (6,10,10) & (6,12,8) \\ (8,6,12) & (8,14,12) & (10,10,14) & (10,14,2) \\ (12,8,6) & (12,8,14) & (14,2,2) & (14,12,8). \end{array}$$

Una forma de verificar que este código es δ_1-cíclico y, por lo tanto, δ_2-cíclico, donde $\delta_1 = 5$ y $\delta_2 = 13$, es calcular $\nu_{\delta_1}(\mathscr{C})$ y verificar si $\nu_{\delta_1}(\mathscr{C}) = \mathscr{C}$. Otra forma es aplicar la Proposición 5.3.4, para lo cual debemos calcular $\varphi(\mathscr{C})$ y comprobar si $\widetilde{\pi}\left(\sigma^{\otimes 2^2}\right)(\varphi(\mathscr{C})) = \varphi(\mathscr{C})$. Con el fin de ilustrar dicho resultado, con la ayuda del Programa Computacional MAGMA V12-15.13 (Student Version), obtuvimos el código $\varphi(\mathscr{C})$:

$$\begin{array}{ccc} 000\ 002\ 222\ 220 & 002\ 022\ 220\ 200 & 022\ 222\ 200\ 000 \\ 022\ 202\ 222\ 002 & 202\ 220\ 222\ 200 & 222\ 200\ 202\ 220 \\ 222\ 220\ 000\ 002 & 220\ 200\ 002\ 022 & 220\ 022\ 222\ 020 \\ 222\ 020\ 220\ 022 & 200\ 000\ 022\ 222 & 222\ 002\ 022\ 202. \end{array}$$

Ahora calculamos $\sigma^{\otimes 2^2}(\varphi(\mathscr{C}))$:

$$\begin{array}{ccc} 000\ 200\ 222\ 022 & 200\ 202\ 022\ 020 & 202\ 222\ 020\ 000 \\ 202\ 220\ 222\ 200 & 220\ 022\ 222\ 020 & 222\ 020\ 220\ 022 \\ 222\ 022\ 000\ 200 & 022\ 020\ 200\ 202 & 022\ 202\ 222\ 002 \\ 222\ 002\ 022\ 202 & 020\ 000\ 202\ 222 & 222\ 200\ 202\ 220. \end{array}$$

Finalmente, aplicamos la permutación $\widetilde{\pi}$, la cual actúa sobre un vector en $\mathbb{Z}_4^{12}$ como sigue:

$$A = a_0a_1a_2\ \ b_0b_1b_2\ \ c_0c_1c_2\ \ d_0d_1d_2 \mapsto \widetilde{\pi}(A) = c_0a_1a_2\ \ d_0b_1b_2\ \ a_0b_1c_2\ \ b_0d_1d_2.$$

De este modo, el código $\widetilde{\pi}\left(\sigma^{\otimes 2^2}\right)(\varphi(\mathscr{C}))$ es:

$$\begin{array}{ccc} 200\ 000\ 022\ 222 & 000\ 002\ 222\ 220 & 002\ 022\ 220\ 200 \\ 202\ 220\ 222\ 200 & 220\ 022\ 222\ 020 & 222\ 020\ 220\ 022 \\ 022\ 222\ 200\ 000 & 222\ 220\ 000\ 002 & 222\ 002\ 022\ 202 \\ 022\ 202\ 222\ 002 & 220\ 200\ 002\ 022 & 222\ 200\ 202\ 220. \end{array}$$

Dado que este último código es $\varphi(\mathscr{C})$, por la Proposición 5.3.4, concluimos que $\mathscr{C}$ es δ_1-cíclico y, por lo tanto, δ_2-cíclico.

Vale la pena observar que $\mathscr{C}$ no es código λ-cíclico ni cíclico, donde $\lambda = 1+2^k = 9$. Por lo tanto, $\varphi(\mathscr{C})$ no satisface las relaciones $\sigma^{\otimes 2^2}(\varphi(\mathscr{C})) = \varphi(\mathscr{C})$ y $\nu^{\otimes 2^2}(\varphi(\mathscr{C})) = \varphi(\mathscr{C})$. De este modo, la permutación $\widetilde{\pi}$ debe considerarse para establecer la Proposición 5.3.4.

El siguiente resultado es análogo a la Proposición 5.2.20.

Proposición 5.3.5. *Sea $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$, con $k \geq 3$, un código (no necesariamente lineal) tal que $2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z \in \mathscr{C}$ para todo $Z \in \mathscr{C}$, y $\varphi(\mathscr{C})$ es un código lineal $\mathbb{Z}_4$. Entonces $\mathscr{C}$ es un código δ_2-cíclico si y sólo si*

$$\widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2^{k-2}}\right)(\varphi(\mathscr{C})) = \varphi(\mathscr{C}).$$

Veamos un ejemplo.

Ejemplo 5.3.6. Sean $k = n = 3$ y $\mathscr{C}_2 \subseteq \mathbb{Z}_{16}^3$ el código lineal generado por los vectores $(1,13,9)$, $(0,8,0)$ y $(0,0,8)$, es decir,

$$\mathscr{C}_2 = \{a(1,13,9)+b(0,8,0)+c(0,0,8) \ : \ a,b,c \in \mathbb{Z}_{16}\}.$$

Dado que es suficiente considerar $b,c \in \{0,1\}$, el código $\mathscr{C}_2$ contiene 64 elementos. Note que

$$\begin{aligned}
\nu_{13}(g_1) &= (5,1,13) = 5(1,13,9)+0(0,8,0)+0(0,0,8),\\
\nu_{13}(g_2) &= (0,0,8) = 0(1,13,9)+0(0,8,0)+1(0,0,8),\\
\nu_{13}(g_3) &= (8,0,0) = 8(1,13,9)+1(0,8,0)+1(0,0,8).
\end{aligned}$$

Por lo tanto, $\mathscr{C}_2$ es un código δ_2-cíclico lineal, donde $\delta_2 = 1+2^{k-1}+2^k = 13$. Además, ya que $(0,0,0)$, $(0,0,8) \in \mathscr{C}_2$, el vector $2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z$ pertenece al código $\mathscr{C}_2$ para todo $Z \in \mathscr{C}_2$. Por otra parte, con la ayuda del Programa Computacional MAGMA V12.15-13 (Student Version) obtuvimos que $\varphi(\mathscr{C}_2)$ es un código lineal generado por los vectores:

$$\begin{aligned}
&g_1 = 111\ 131\ 111\ 131, \quad g_2 = 020\ 020\ 020\ 020, \quad g_3 = 002\ 002\ 002\ 002,\\
&g_4 = 000\ 222\ 000\ 222, \quad g_5 = 000\ 000\ 222\ 222.
\end{aligned}$$

Consecuentemente, $\mathscr{C}_2$ es un código que satisface las hipótesis de la Proposición 5.3.5 y, por lo tanto, $\varphi(\mathscr{C}_2)$ satisface la relación

$$\widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2}\right)(\varphi(\mathscr{C}_2)) = \varphi(\mathscr{C}_2),$$

con lo cual concluimos el ejemplo.

Recuerde que en el Ejemplo 5.2.19 presentamos un código δ_1-cíclico lineal $\mathscr{C}_1 \subseteq \mathbb{Z}_{16}^3$, de cardinalidad 64, generado por los elementos $(1,5,1)$, $(0,8,0)$ y $(0,0,8)$. En el ejemplo anterior vimos un código δ_2-cíclico lineal $\mathscr{C}_2 \subseteq \mathbb{Z}_{16}^3$ generado por los vectores $(1,13,1)$, $(0,8,0)$ y $(0,0,8)$, y de cardinalidad 64. Ahora observe que $(1,13,1) = (1,5,1)+(0,8,0) \in \mathscr{C}_1$. De este modo, por cuestiones de cardinalidad, tenemos que $\mathscr{C}_1 = \mathscr{C}_2$ y, por lo tanto, este código es δ_1-cíclico y δ_2-cíclico a la vez. El propósito de la siguiente sección es estudiar esta clase de códigos.

5.4. Códigos consta-cíclicos lineales

En este apartado estudiaremos códigos lineales que tienen la propiedad de ser al mismo tiempo δ_1-cíclicos y δ_2-cíclicos, donde $k \geq 3$, $\delta_1 = 1+2^{k-1}$ y $\delta_2 = 1+2^{k-1}+2^k$; notación que preservaremos a lo largo de esta sección. A modo de ejemplo, podemos considerar el código lineal $\mathscr{C}_1 = \mathscr{C}_2 \subseteq \mathbb{Z}_{16}^3$ de los ejemplos 5.2.19 y 5.3.6. De este modo, la familia de códigos que estudiaremos contiene códigos distintos del código cero $\{(0)_n\} \subseteq \mathbb{Z}_{2^{k+1}}^n$.

Primero recuerde que si $\gamma \in U(\mathbb{Z}_{2^{k+1}})$, entonces η_γ es el $\mathbb{Z}_{2^{k+1}}$-automorfismo definido sobre $\mathbb{Z}_{2^{k+1}}^n$ como

$$\eta_\gamma : (z_0, \ldots, z_{n-2}, z_{n-1}) \mapsto (z_0, \ldots, z_{n-2}, \gamma z_{n-1}).$$

(ver la sección 3.2 y la Proposición 3.2.1 para más detalles). Asimismo, debido al Lema 3.3.2 tenemos que $\lambda\delta_1 = \delta_2$ y $\lambda\delta_2 = \delta_1$, donde $\lambda = 1+2^k$.

Proposición 5.4.1. *Sea $\mathscr{C}$ un código de longitud $n \geq 1$ sobre $\mathbb{Z}_{2^{k+1}}$ y $\gamma \in \{\delta_1, \delta_2\}$. Si $\mathscr{C}$ es un código γ-cíclico, entonces $\mathscr{C}$ es $\lambda\gamma$-cíclico si y sólo si $\eta_\lambda(\mathscr{C}) = \mathscr{C}$.*

Demostración. Observe que $\nu_{\delta_1} = \nu_{\delta_2} \circ \eta_\lambda$ y $\nu_{\delta_2} = \nu_{\delta_1} \circ \eta_\lambda$. de este modo, el resultado se sigue de la inyectividad de las aplicaciones $\nu_{\delta_1}, \nu_{\delta_2}$ y η_λ. □

En la Proposición 4.4.4 se enunció un resultado similar a la Proposición 5.4.1, en el cual se establece que un código cíclico $\mathscr{C}$ (casi-cíclico de índice $m = 1$) es a su vez un código λ-cíclico si y sólo si $\eta_\lambda(\mathscr{C}) = \mathscr{C}$. De este modo, podría pensarse que un código $\mathscr{C}$ que es δ_1-cíclico y δ_2-cíclico a la vez, es también un código cíclico y λ-cíclico. Esto no siempre es cierto, y para ilustrarlo nos apoyamos en el código del Ejemplo 5.3.6.

Por otra parte, observe que debido al Teorema 3.3.4,

$$\varphi \circ \eta_\lambda = \eta_{-1}^{\otimes 2^{k-1}} \circ \varphi.$$

Por lo tanto, de la Proposición 5.4.1 concluimos que si un código $\mathscr{C}$ es δ_1-cíclico y δ_2-cíclico a la vez, entonces $\varphi(\mathscr{C})$ queda invariante bajo la acción de $\eta_{-1}^{\otimes 2^{k-1}}$, es decir, $\eta_{-1}^{\otimes 2^{k-1}}(\varphi(\mathscr{C})) = \varphi(\mathscr{C})$. De este modo, si un código $\mathscr{C}$ es δ_1-cíclico y δ_2-cíclico al mismo tiempo, entonces el código $\varphi(\mathscr{C})$ satisface lo siguiente:

1) $\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(c)+\widehat{c}\in\varphi(\mathscr{C})$, para todo $c\in\varphi(\mathscr{C})$,

2) $\widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2^{k-2}}\right)(c)+\widehat{c}\in\varphi(\mathscr{C})$, para todo $c\in\varphi(\mathscr{C})$, y

3) $\eta_{-1}^{\otimes 2^{k-1}}(\varphi(\mathscr{C}))=\varphi(\mathscr{C})$.

Más aún, observe que cualesquiera dos de estas tres relaciones caracteriza a tales códigos, pero ninguna por sí sola.

Si además suponemos que $\varphi(\mathscr{C})$ es lineal y que $2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z\in\mathscr{C}$ para todo $Z\in\mathscr{C}$, entonces obtenemos el siguiente resultado.

Corolario 5.4.2. *Sea $\mathscr{C}\subseteq\mathbb{Z}_{2^{k+1}}^n$ un código (no necesariamente lineal) tal que $\varphi(\mathscr{C})$ es lineal y $2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z\in\mathscr{C}$ para todo $Z\in\mathscr{C}$. Entonces $\mathscr{C}$ es δ_1-cíclico y δ_2-cíclico si y sólo si*

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(\mathscr{C}))=\widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2^{k-2}}\right)(\varphi(\mathscr{C}))=\varphi(\mathscr{C}).$$

Demostración. Se sigue de las Proposiciones 5.2.20 y 5.3.5. □

Para ilustrar este último hecho, consideremos el código lineal $\mathscr{C}\subseteq\mathbb{Z}_{16}^3$ generado por los vectores $(1,5,1)$, $(0,8,0)$ y $(0,0,8)$. En los ejemplos 5.2.19 y 5.3.6 se probó que $\mathscr{C}$ es un código δ_1-cíclico y δ_2-cíclico lineal, tal que $\varphi(\mathscr{C})$ es lineal y $2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z\in\mathscr{C}$ para todo $Z\in\mathscr{C}$. Así, el código $\mathscr{C}$ satisface las hipótesis de la Proposición 5.4.2 y, por lo tanto, $\varphi(\mathscr{C})$ permanece invariante bajo las aplicaciones

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right),\qquad\widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2^{k-2}}\right).$$

El siguiente resultado describe la situación cuando añadimos la condición de linealidad a $\mathscr{C}$.

Proposición 5.4.3. *Sea $\mathscr{C}$ un código lineal de longitud $n\geq 1$ sobre $\mathbb{Z}_{2^{k+1}}$. Sea $\gamma\in\{\delta_1,\delta_2\}$ y $\lambda=1+2^k$. Si $\mathscr{C}$ es γ-cíclico, entonces $\mathscr{C}$ es $\lambda\gamma$-cíclico si y sólo si $2^k\mathbf{b}_Z\in\mathscr{C}$, para todo $Z\in\mathscr{C}$.*

Demostración. Supongamos que $\mathscr{C}$ es un código γ-cíclico y $\lambda\gamma$-cíclico lineal. Entonces, por la Proposición 5.4.1, $\eta_\lambda(\mathscr{C})=\mathscr{C}$, es decir, para todo $Z=(z_0,\ldots,z_{n-2},z_{n-1})\in\mathscr{C}$, se tiene que $\eta_\lambda(Z)=(z_0,\ldots,z_{n-2},\lambda z_{n-1})\in\mathscr{C}$. Como $\lambda=1+2^k$, entonces

$$\eta_\lambda(Z)=(z_0,\ldots,z_{n-2},z_{n-1})+(0,\ldots,0,2^kz_{n-1})\in\mathscr{C}$$

Debido a que $\mathscr{C}$ es lineal, $\eta_\lambda(Z)-Z=(0,\ldots,0,2^kz_{n-1})=2^k\mathbf{b}_Z\in\mathscr{C}$.
Recíprocamente, supongamos que $\mathscr{C}$ es un código γ-cíclico lineal tal que $2^k\mathbf{b}_Z\in\mathscr{C}$, para todo $Z\in\mathscr{C}$. Entonces $2^k\mathbf{b}_Z+Z=\eta_\lambda(Z)\in\mathscr{C}$. Por lo tanto, de la Proposición 5.4.1 se sigue que $\mathscr{C}$ es $\lambda\gamma$-cíclico. □

Observe que $2^k\mathbf{b}_Z = (0,\ldots,0,2^k z_{n-1})$, donde $Z = (z_0,\ldots,z_{n-2},z_{n-1})$, puede ser solamente el vector cero o el vector $(0,\ldots,0,2^k)$. La primera situación pasa si y sólo si $z_{n-1} \in \langle 2\rangle \subset \mathbb{Z}_{2^{k+1}}$. De este modo, si $\mathscr{C}$ es un código γ-cíclico lineal, donde $\gamma \in \{\delta_1,\delta_2\}$, y tal que todas las coordenadas de los vectores contenidos en él están en él ideal maximal de $\mathbb{Z}_{2^{k+1}}$, entonces $2^k\mathbf{b}_Z = (0,\ldots,0) \in \mathscr{C}$ para todo $Z \in \mathscr{C}$. Por lo tanto, $\mathscr{C}$ es también un código λ γ-cíclico lineal. Así, todo código γ-cíclico lineal, tal que todas las coordenadas de los vectores contenidos en el están en el ideal maximal de $\mathbb{Z}_{2^{k+1}}$, es también un código $\lambda\gamma$-cíclico lineal. Sin embargo, debe tenerse cuidado pues esto no implica que el código sea λ-cíclico y, en consecuencia, cíclico. Esto es, existen códigos que son δ_1-cíclicos y δ_2-cíclicos pero que no son códigos cíclicos ni λ-cíclicos. Por ejemplo, considere el código lineal $\mathscr{C} \subseteq \mathbb{Z}_{16}^3$ generado por el vector $(2,10,2)$. Los elementos de $\mathscr{C}$ son:

$$(14,6,14),\ (6,14,6),\ (4,4,4),\ (12,12,12),\ (2,10,2),\ (10,2,10),\ (0,0,0),\ (8,8,8).$$

De aquí, podemos verificar fácilmente que $\mathscr{C}$ es un código δ_1-cíclico, donde $\delta_1 = 5$. Además, dado que las coordenadas de cualquier vector en $\mathscr{C}$ están en el ideal maximal de $\mathbb{Z}_{16}$, $\mathscr{C}$ es también un código δ_2-cíclico. Sin embargo, este código no es cíclico ni λ-cíclico, con $\lambda = 9$, tal como se puede verificar fácilmente por inspección directa.

Por otra parte, $2^k\mathbf{b}_Z = (0,\ldots,0,2^k)$ si y sólo si z_{n-1} es una unidad en $\mathbb{Z}_{2^{k+1}}$. De este modo, si $\mathscr{C}$ es un código que contiene vectores cuya última coordenada sean unidades, basta verificar si para uno de esos vectores $2^k\mathbf{b}_Z = (0,\ldots,0,2^k) \in \mathscr{C}$. Esto quiere decir, que aunque la condición de la Proposición 5.4.1 establezca que "$2^k\mathbf{b}_Z \in \mathscr{C}$ para todo $Z \in \mathscr{C}$", no es necesario verificar esta propiedad para todo $Z \in \mathscr{C}$ cuya última coordenada sea una unidad, sino que basta fijarnos en uno sólo.

El análisis del párrafo anterior nos trae a la mente el vector

$$2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z = (0,\ldots,0,2^k r_0(z_{n-1})r_{k-1}(z_{n-1})),$$

el cual también sólo puede tomar dos posibilidades: el vector cero y el vector $(0,\ldots,0,2^k)$. Si $2^k\mathbf{b}_Z = (0,\ldots,0)$, entonces $2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z = (0,\ldots,0)$. Si $2^k\mathbf{b}_Z = (0,\ldots,0,2^k z_{n-1})$, entonces $2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z$ todavía puede tomar sus dos posibilidades, dependiendo del término $r_{k-1}(z_{n-1})$. En cualquier caso, lo anterior implica que si $2^k\mathbf{b}_Z \in \mathscr{C}$ para todo vector Z en un código $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$, entonces $2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z \in \mathscr{C}$ para todo $Z \in \mathscr{C}$. Sin embargo, el recíproco de esta observación no es en general cierto. Por ejemplo, considere el código $\mathscr{C} = \{0000,1111\} \subseteq \mathbb{Z}_{16}^3$. Entonces $2^k\mathbf{b}_Z \odot \mathbf{b}_Z = 0000$ para todo $Z \in \mathscr{C}$ y, por lo tanto, $2^k\mathbf{b}_Z \odot \mathbf{b}_Z \in \mathscr{C}$. Pero $2^k\mathbf{b}_Z = 0000$ si $Z = 0000$, y $2^3\mathbf{b}_Z = 0008$ si $Z = 1111$. De este modo, $2^k\mathbf{b}_Z$ no siempre está en el código $\mathscr{C}$ para todo $Z \in \mathscr{C}$.

No obstante, es posible tener el siguiente resultado.

Teorema 5.4.4. *Sea $\mathscr{C}$ un código lineal de longitud n sobre $\mathbb{Z}_{2^{k+1}}$ tal que $\varphi(\mathscr{C})$ es lineal. Entonces $\mathscr{C}$ es δ_1-cíclico y δ_2-cíclico si y sólo si*

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(\mathscr{C})) = \widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2^{k-2}}\right)(\varphi(\mathscr{C})) = \varphi(\mathscr{C}).$$

Demostración. Si $\mathscr{C}$ es δ_1-cíclico y δ_2-cíclico lineal, entonces $2^k\mathbf{b}_Z \in \mathscr{C}$ para todo $Z \in \mathscr{C}$. Consecuentemente, $2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z \in \mathscr{C}$ para todo $Z \in \mathscr{C}$. De este modo, por la Proposición 5.4.2,

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(\mathscr{C})) = \widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2^{k-2}}\right)(\varphi(\mathscr{C})) = \varphi(\mathscr{C}).$$

Supongamos ahora que $\varphi(\mathscr{C})$ satisface la relación anterior y demostremos que $\mathscr{C}$ es δ_1-cíclico y δ_2-cíclico. Sea $Z \in \mathscr{C}$. Debido a los Teoremas 5.2.10 y 5.3.2,

$$\begin{aligned}\varphi(\nu_{\delta_1}(Z)) &= \widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(Z)) + (\sigma\otimes\nu)^{\otimes 2^{k-2}}(\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)),\\ \varphi(\nu_{\delta_2}(Z)) &= \widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2^{k-2}}\right)(\varphi(Z)) + (\nu\otimes\sigma)^{\otimes 2^{k-2}}(\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)).\end{aligned}$$

Si $2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z$ es igual al vector cero, entonces $\nu_{\delta_1}(Z)$ y $\nu_{\delta_2}(Z)$ están en $\mathscr{C}$. Si $2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z = (0,\ldots,0,2^k) \in \mathbb{Z}_{2^{k+1}}^n$, entonces se sigue de los Teoremas 5.2.17, 5.3.3 y de la Proposición 5.2.14 que las las coordenadas de $\varphi(Z)$ con subíndice en el conjunto $I(2^{k-1},n)$ son unidades. Por lo tanto, como $\varphi(\mathscr{C})$ es lineal y $(\sigma\otimes\nu)^{\otimes 2^{k-2}}(\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)) = (\nu\otimes\sigma)^{\otimes 2^{k-2}}(\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z))$, tenemos que

$$\widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(Z)) - \widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2^{k-2}}\right)(\varphi(Z)) = c_{k-1}^{k-1}\otimes(2,0\ldots,0) = \widehat{c} \in \varphi(\mathscr{C}).$$

Dado que $\widehat{c} = (\sigma\otimes\nu)^{\otimes 2^{k-2}}(\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z)) = (\nu\otimes\sigma)^{\otimes 2^{k-2}}(\varphi(2^k\mathbf{b}_Z\odot 2\mathbf{b}_Z))$, obtenemos que los vectores

$$\begin{aligned}\varphi(\nu_{\delta_1}(Z)) - \widehat{c} &= \widetilde{\pi}\left((\sigma\otimes\nu)^{\otimes 2^{k-2}}\right)(\varphi(Z)),\\ \varphi(\nu_{\delta_2}(Z)) - \widehat{c} &= \widetilde{\pi}\left((\nu\otimes\sigma)^{\otimes 2^{k-2}}\right)(\varphi(Z)),\end{aligned}$$

pertencen al cdóigo $\varphi(\mathscr{C})$. Consecuentemente, $\nu_{\delta_1}(Z)$ y $\nu_{\delta_2}(Z)$ están en $\mathscr{C}$. □

Continuamos nuestro análisis de las propiedades de los códigos δ_1-cíclicos y δ_2-cíclicos lineales sobre $\mathbb{Z}_{2^{k+1}}$ pero ahora con la hipótesis de que la longitud n es impar. Esto lo hacemos con la finalidad de aprovechar la estructura de dichos códigos, la cual ha sido desarrollada en el Capítulo 1 de este material.

En virtud de los Lemas 1.3.6 y 1.4.1, recordemos los códigos cíclicos y δ_1-cíclicos están relacionados mediante el siguiente diagrama conmutativo

$$\begin{array}{ccc}\mathbb{Z}_{2^{k+1}}^n & \xrightarrow{\quad P \quad} & \mathbb{Z}_{2^{k+1}}[x]/\langle x^n-1\rangle\\ \Big\downarrow{\scriptstyle \widetilde{\mu}_\beta} & & \Big\downarrow{\scriptstyle \mu_\beta}\\ \mathbb{Z}_{2^{k+1}}^n & \xrightarrow{\quad P \quad} & \mathbb{Z}_{2^{k+1}}[x]/\langle x^n-\delta_1\rangle\end{array}$$

donde $\beta^n = \delta_2$, μ_β y $\widetilde{\mu}_\beta$ son los isomorfismos de $\mathbb{Z}_{2^{k+1}}$-módulos dados por:

$$\mu_\beta : a(x) + \langle x^n - 1\rangle \mapsto a(\beta x) + \langle x^n - \delta_1\rangle$$

y

$$\widetilde{\mu}_\beta : (a_0, a_1, \ldots, a_{n-1}) \mapsto (a_0, \beta a_1, \ldots, \beta^{n-1} a_{n-1}).$$

Asimismo, códigos cíclicos y δ_2-cíclicos están conectados por medio del siguiente diagrama conmutativo

$$\begin{array}{ccc} \mathbb{Z}_{2^{k+1}}^n & \xrightarrow{\quad P \quad} & \mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle \\ \Big\downarrow \widetilde{\mu}_\xi & & \Big\downarrow \mu_\xi \\ \mathbb{Z}_{2^{k+1}}^n & \xrightarrow{\quad P \quad} & \mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \delta_2\rangle \end{array}$$

donde $\xi^n = \delta_1$ y μ_ξ y $\widetilde{\mu}_\xi$ son definidos de manera similar a μ_β y $\widetilde{\mu}_\beta$. Dado que todas las aplicaciones involucradas en estos diagramas son isomorfismos, se tiene que los $\mathbb{Z}_{2^{k+1}}$-módulos $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \delta_1\rangle$ y $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \delta_2\rangle$ son isomorfos. Es posible dar explícitamente un isomorfismo, para lo cual recordemos que si n es impar y $u \in U(\mathbb{Z}_{2^{k+1}})$, entonces existe una única raíz n-ésima de u. Esto es, existe un único $v \in U(\mathbb{Z}_{2^{k+1}})$ tal que $v^n = u$. Como antes, sea $\lambda = 1 + 2^k$.

Lema 5.4.5. *Sea $n \geq 1$ impar. Entonces la aplicación*

$$\mu_\lambda : \mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \delta_1\rangle \to \mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \delta_2\rangle$$

definida como

$$a(x) + \langle x^n - \delta_1\rangle \mapsto a(\beta x) + \langle x^n - \delta_2\rangle$$

es un isomorfismo de $\mathbb{Z}_{2^{k+1}}$-módulos. Por lo tanto, un conjunto I es un ideal de $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \delta_1\rangle$ si y sólo si $\mu_\lambda(I)$ es un ideal de $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \delta_2\rangle$.

Demostración. Observe que

$$(\mu_\lambda \circ \mu_\beta)(a(x) + \langle x^n - 1\rangle) = \mu_\lambda(a(\beta x) + \langle x^n - \delta_1\rangle) = a(\lambda\beta x) + \langle x^n - \delta_2\rangle$$

donde $\beta^n = \delta_2$. Entonces $(\lambda\beta)^n = \lambda^n\beta^n = \lambda^n\delta_2$. Siendo n impar, $\lambda^n = \lambda$ pues λ es de orden 2. Así, $(\lambda\beta)^n = \lambda\delta_2 = \delta_1$. Esto implica que $\lambda\beta = \xi$ puesto que la raíz n-ésima de δ_1 es única. De este modo, $\mu_\lambda \circ \mu_\beta = \mu_\xi$ y, por lo tanto, μ_λ es un isomorfismo. □

Como consecuencia inmediata del Lema 5.4.5 tenemos la siguiente resultado análogo al Lema 1.4.1, el cual generaliza la Proposición 3.7 de [54].

Proposición 5.4.6. *Sea n un entero impar. Entonces, un código $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ es δ_1-cíclico si y sólo si $\widetilde{\mu}_\lambda(\mathscr{C})$ es un código δ_2-cíclico, donde $\widetilde{\mu}_\lambda : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}_{2^{k+1}}^n$ está dado por*

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto (a_0, \lambda a_1, \ldots, \lambda^{n-1} a_{n-1}).$$

Demostración. El resultado se sigue de la relación $\mu_\lambda \circ P = P \circ \widetilde{\mu}_\lambda$, donde P es la representación polinomial, y del hecho de que un código $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ es γ-cíclico si y sólo si $P(\mathscr{C})$ es un ideal de $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \gamma \rangle$, con $\gamma \in \{\delta_1, \delta_1\}$ (cf. Proposición 1.2.6). □

En otros términos, la Proposición 5.4.6 permite construir un código δ_2-cíclico lineal de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$, a partir de un código δ_2-cíclico lineal de la misma longitud, y viceversa.

Por otro lado, en la Proposición 4.6.1 mostramos que $\varphi \circ \mu_\lambda = \mu_{-1}^{\otimes 2^{k-1}} \circ \varphi$. De este modo, este resultado junto con la Proposición 5.4.6, nos dan ahora la posibilidad de pasar de un código δ_1-cíclico a un código δ_2-cíclico (y viceversa) por medio de sus imagenes con respecto a la isometría φ.

Proposición 5.4.7. *Sea $n \geq 1$ un entero impar. Entonces el siguiente diagrama conmuta.*

$$\begin{array}{ccccc}
\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \delta_1 \rangle & \xrightarrow{P^{-1}} & \mathbb{Z}_{2^{k+1}}^n & \xrightarrow{\varphi} & \mathbb{Z}_4^{2^{k-1}n} \\
\downarrow{\scriptstyle \mu_\lambda} & & \downarrow{\scriptstyle \widetilde{\mu}_\lambda} & & \downarrow{\scriptstyle \widetilde{\mu}_{-1}^{\otimes 2^{k-1}}} \\
\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \delta_2 \rangle & \xrightarrow{P^{-1}} & \mathbb{Z}_{2^{k+1}}^n & \xrightarrow{\varphi} & \mathbb{Z}_4^{2^{k-1}n}
\end{array}$$

Además, la función inversa de $\widetilde{\mu}_\lambda$ es ella misma.

Habiendo estudiado las relaciones entre los códigos δ_1-cíclicos y δ_2-cíclicos lineales de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$, somos ahora capaces de dar condiciones necesarias y suficientes para que dichos códigos coincidan. El siguiente resultado es análogo a la Proposición 4.5.6.

Proposición 5.4.8. *Sea $\mathscr{C}$ un código δ_1-cíclico lineal de longitud n impar sobre $\mathbb{Z}_{2^{k+1}}$. Entonces $\mathscr{C}$ es δ_2-cíclico si y sólo si $\widetilde{\mu}_\lambda(\mathscr{C}) = \mathscr{C}$.*

Demostración. Supongamos que $\mathscr{C}$ es δ_1-cíclico y δ_2-cíclico lineal de longitud n impar sobre $\mathbb{Z}_{2^{k+1}}$. Entonces, por la Proposición 5.4.3,

$$2^k \mathbf{b}_Z = (0, \ldots, 0, 2^k z_{n-1}) \in \mathscr{C}, \qquad \forall\, Z = (z_0, \ldots, z_{n-2}, z_{n-1}) \in \mathscr{C}.$$

Además, $W = \nu_{\delta_1}(Z) = (\delta_1 z_{n-1}, \ldots, z_0, \ldots, z_{n-2}) \in \mathscr{C}$ y, por lo tanto,

$$2^k \mathbf{b}_W = (0, \ldots, 0, 2^k z_{n-2}) \in \mathscr{C}.$$

Continuando de esta manera vemos que $(0,\ldots,0,2^k z_i) \in \mathscr{C}$, donde $0 \leq i \leq n-1$ y z_i es la coordenada i de un vector $Z \in \mathscr{C}$. Consecuentemente, dado $Z = (z_0,\ldots,z_i,\ldots,z_{n-1}) \in \mathscr{C}$, el vector $x_i = (0,\ldots,0,2^k z_i,0,\ldots,0) \in \mathscr{C}$. Por lo tanto, dado que $\mathscr{C}$ es lineal,

$$\widetilde{\mu}_\lambda(Z) = Z + x_1 + x_3 + \cdots + x_{n-2} \in \mathscr{C}.$$

Recíprocamente, supongamos que $\widetilde{\mu}_\lambda(\mathscr{C}) = \mathscr{C}$. Como $\mu_\lambda \circ P = P \circ \widetilde{\mu}_\lambda$, tenemos que

$$\mu_\lambda(P(\mathscr{C})) = P(\widetilde{\mu}_\lambda(C)) = P(\mathscr{C}).$$

Por otra parte, como $\mathscr{C}$ es δ_1-cíclico lineal, $P(\mathscr{C})$ es un ideal en el anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \delta_1\rangle$ y, por lo tanto, $P(\mathscr{C})$ es un ideal en $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - \delta_2\rangle$. Esto implica que $\mathscr{C}$ es un código δ_2-cíclico. □

El resultado anterior nos permite dar otra propiedad de la imagen bajo φ de un código que es δ_1-cíclico y δ_2-cíclico lineal de longitud impar sobre $\mathbb{Z}_{2^{k+1}}$.

Corolario 5.4.9. *Si $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$ es un código δ_1-cíclico y δ_2-cíclico lineal de longitud impar, entonces $\mu_{-1}^{\otimes 2^{k-1}}(\varphi(\mathscr{C})) = \varphi(\mathscr{C})$.*

Vale la pena señalar que en virtud del Teorema 4.6.2, el recíproco de la Proposición 5.4.9 es falso. Esto es, si un código lineal $\mathscr{C} \subseteq \mathbb{Z}_{2^{k+1}}^n$, con n impar, es tal que $\mu_{-1}^{\otimes 2^{k-1}}(\varphi(\mathscr{C})) = \varphi(\mathscr{C})$, entonces no necesariamente $\mathscr{C}$ es δ_1-cíclico y δ_2-cíclico.

A modo de ejemplo, hemos elaborado el Cuadro 5.3, el cual contiene una lista de todos los códigos lineales δ_1-cíclicos de longitud 3 sobre $\mathbb{Z}_{16}$, donde $\delta_1 = 1+2^{k-1} = 5$. Hemos señalado con el símbolo ✓aquellos códigos que son también δ_2-cíclicos, con $\delta_2 = 1+2^{k-1}+2^k = 13$. Asimismo, se ha calculado la imagen con respecto a φ de dichos códigos, y se ha especificado cuáles de ellos tienen imagen lineal. De este modo, el Cuadro 5.3 ofrece una gama de ejemplos que ilustran los resultados descritos en esta sección. Todos los cálculos han sido realizados con el programa computacional MAGMA® V2.15-13 (Student Version). Otros cuadros similares se encuentran en el Apéndice A.

Generadores	$\#\mathscr{C}$	δ_2-cíclico	$\varphi(\mathscr{C})$ lineal	Generadores	$\#\mathscr{C}$	δ_2-cíclico	$\varphi(\mathscr{C})$ lineal
$\langle 2\rangle$	8^3	✓	✓	$\langle d_1, 2^2 d_2\rangle$	$16^2\cdot 4$	✓	–
$\langle 2^2\rangle$	4^3	✓	✓	$\langle d_1, 2^3 d_2\rangle$	$16^2\cdot 2$	✓	–
$\langle 2^3\rangle$	2^3	✓	✓	$\langle d_2, 2d_1\rangle$	$16\cdot 8^2$	✓	✓
$\langle d_1\rangle$	16^2	–	–	$\langle d_2, 2^2 d_1\rangle$	$16\cdot 4^2$	✓	✓
$\langle 2d_1\rangle$	8^2	✓	–	$\langle d_2, 2^3 d_1\rangle$	$16\cdot 2^2$	✓	✓
$\langle 2^2 d_1\rangle$	4^2	✓	–	$\langle 2d_1, 2^2 d_2\rangle$	$8^2\cdot 4$	✓	✓
$\langle 2^3 d_1\rangle$	2^2	✓	✓	$\langle 2d_1, 2^3 d_2\rangle$	$8^2\cdot 2$	✓	✓
$\langle d_2\rangle$	16	–	–	$\langle 2d_2, 2^2 d_1\rangle$	$8\cdot 4^2$	✓	✓
$\langle 2d_2\rangle$	8	✓	✓	$\langle 2d_2, 2^3 d_1\rangle$	$8\cdot 2^2$	✓	✓
$\langle 2^2 d_2\rangle$	4	✓	✓	$\langle 2^2 d_1, 2^3 d_2\rangle$	$4^2\cdot 2$	✓	✓
$\langle 2^3 d_3\rangle$	2	✓	✓	$\langle 2^2 d_2, 2^3 d_1\rangle$	$4\cdot 2^2$	✓	✓
$\langle d_1, 2d_2\rangle$	$16^2\cdot 8$	✓	✓				

$x^3-\delta_1 = d_1 d_2$, $\quad d_1 = x+3$, $\quad d_2 = x^2+13x+9$, $\quad \delta_1 = 1+2^{k-1} = 5$, $\quad \delta_2 = 1+2^{k-1}+2^k = 13$, $\quad k = 3$.
✓: El código tiene la propiedad señalada por la columna.
–: El código no tiene la propiedad señalada por la columna.

Cuadro 5.3: Códigos δ_1-cíclicos lineales de longitud 3 sobre $\mathbb{Z}_{16}$.

Capítulo 6

Imágenes de códigos 3-cíclicos y negacíclicos sobre $\mathbb{Z}_8$

En el presente capítulo analizaremos propiedades de ciclícidad y negaciclícidad de las imágenes, bajo las isometrías φ y Φ de Gray, de códigos 3-cíclicos y negacíclicos sobre $\mathbb{Z}_8$. Daremos varias propiedades de las imagen bajo φ de estos códigos y, en particular, demostraremos que la imagen de un código 3-cíclico o negacíclico sobre $\mathbb{Z}_8$ es un código negacíclico, módulo una traslación, sobre $\mathbb{Z}_4$. A raíz de este hecho, demostraremos que la imagen de Gray de un código 3-cíclico o negacíclico sobre $\mathbb{Z}_8$ es un código cíclico binario, módulo una traslación. Asimismo, estableceremos que un código $\mathscr{C} \subseteq \mathbb{Z}_8^n$ es 3-cíclico y negacíclico a la vez si y sólo si $\varphi(\mathscr{C})$ es un código negacíclico sobre $\mathbb{Z}_4$, o equivalentemente, si y sólo si $\Phi(\mathscr{C})$ es un código cíclico binario. Estos resultados son parte de las aportaciones más relevantes de este trabajo y, además, generalizan las contribuciones más importantes de [54].

6.1. Introducción

Los códigos negacíclicos fueron estudiados por primera vez en el contexto de campos finitos por E. R. Berlekamp en [7]. Años más tarde, el estudio de esta clase de códigos fue extendida al ámbito del anillo $\mathbb{Z}_4$ por J. Wolfman en [54, 55]. En esos trabajos se desmostró que la imagen de Gray de un código negacíclico de longitud n sobre $\mathbb{Z}_4$, es un código cíclico binario de longitud $2n$. Más aún, se probó que si la longitud n es impar, entonces la imagen de Gray de un código cíclico lineal $\mathscr{C} \subseteq \mathbb{Z}_4^n$ es permutación-equivalente a un código cíclico binario (no necesariamente lineal); de hecho la equivalencia está dada por la permutación de Nechaev. Con los resultados alcanzados en [54, 55] se dió una explicación satisfactoria al porqué los códigos de Kerdock y Preparata están relacionados con códigos cíclicos doblemente extendidos; hecho que fue anunciado en [23, 40]. Más aún, se encontró una manera de construir códigos cíclicos de longitud $2n$, con n impar, a partir de códigos cíclicos de longitud n sobre $\mathbb{Z}_4$.

Después de esos trabajos algunos autores han investigado las propiedades de ciclícidad de la imagen de Gray de algunas familias de códigos γ-cíclicos sobre algunas familias de anillos finitos. En particular, cuando el anillo es $\mathbb{Z}_{2^{k+1}}$, en [51, 52] se estudiaron las propiedades de la imagen de Gray de códigos λ-cíclicos donde $\lambda = 1 + 2^k$, probando que la imagen de Gray de uno de tales códigos es un código casi-cíclico de índice 2^{k-1} y longitud $2^k n$ sobre $\mathbb{F}_2$. Observe que si $k = 2$, entonces $\lambda = 5$ y, por lo tanto, la imagen de Gray de un 5-código cíclico de longitud n sobre $\mathbb{Z}_8$ es un código casi-cíclico de índice 2 y longitud $4n$ sobre $\mathbb{F}_2$. En particular, observe que la imagen de Gray de un código 5-cíclico sobre $\mathbb{Z}_8$ no es en general un código cíclico, sino

un código casi-cíclico. Por otra parte, note que $5 \neq -1$ en $\mathbb{Z}_8$ y, en consecuencia, los códigos que se consideraron en [51, 52] no corresponden a los códigos negacíclicos sobre ese anillo.

En este capítulo estudiaremos propiedades de la imagen bajo las funciones φ y Φ de Gray de códigos negacíclicos sobre $\mathbb{Z}_8$. Ya que $7 = -1$ en $\mathbb{Z}_8$, y la representación 2-ádica de 7 es $7 = 1 + 2 + 2^2 = 1 + 2^{k-1} + 2^k$, con $k = 2$, entonces estudiar propiedades de las imágenes de códigos negacíclicos sobre $\mathbb{Z}_8$ corresponde a estudiar propiedades de las imágenes de códigos δ_2-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$ para el caso $k = 2$, el cual no fue considerado en los principales resultados del Capítulo 5. Continuando con el espíritu de este trabajo, también estudiaremos propiedades de las imágenes de los códigos 3-cíclicos sobre $\mathbb{Z}_8$, lo que corresponde al caso de códigos δ_1-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$ con $k = 2$; situación que tampoco formó parte del Capítulo 5.

Varias propiedades de la imagen de códigos 3-cíclicos y negacíclicos son establecidas. En particular, demostraremos que un código $\mathscr{C} \subseteq \mathbb{Z}_8$ es un código 3-cíclico si y sólo $\varphi(\mathscr{C})$ es un código negacíclico, módulo una traslación (Teorema 6.3.9), equivalentemente, si y sólo si su imagen de Gray es un código cíclico binario, módulo una traslación (Teorema 6.3.10). Similarmente, probaremos que un código $\mathscr{C} \subseteq \mathbb{Z}_8$ es un código negacíclico si y sólo $\varphi(\mathscr{C})$ es un código negacíclico, módulo una traslación (Teorema 6.4.1), o equivalentemente, si y sólo si su imagen de Gray es un código cíclico binario, módulo una traslación (Teorema 6.4.2).

Observe que los códigos que se obtienen como imágenes de Gray de códigos 3-cíclicos o negacíclicos no son códigos cíclicos. De este modo los códigos negacíclicos sobre $\mathbb{Z}_8$ no tienen imagen de Gray cíclica; hecho que generalizaría plenamente los resultados mencionados de [54, 55]. Sin embargo, demostraremos que la manera correcta de obtener códigos cíclicos a partir de códigos sobre $\mathbb{Z}_8$, es por medio de códigos que tienen la propiedad de ser 3-cíclicos y negacíclicos a la vez. En específico, demostraremos que la imagen bajo φ de un código $\mathscr{C}$ sobre $\mathbb{Z}_8$ es un código negacíclico sobre $\mathbb{Z}_8$ si y sólo si $\mathscr{C}$ es un código 3-cíclico y negacíclico a la vez, o equivalentemente, la imagen de Gray de un código $\mathscr{C}$ sobre $\mathbb{Z}_8$ es un código cíclico binario si y sólo si $\mathscr{C}$ es un código 3-cíclico y negacíclico a la vez. Estos resultados son quizás las aportaciones más importantes de esta tesis.

6.2. Un ejemplo particular

Antes de iniciar el análisis de las propiedades de casi-ciclicidad y casi-negaciclicidad de las imágenes de códigos 3-cíclicos y 7-cíclicos definidos sobre $\mathbb{Z}_8$, veamos un ejemplo particular. Para tal propósito, recordemos los siguientes hechos generales, los cuales han sido descritos con más detalles en el Capítulo 1. Para todo entero $n \geq 1$ impar, el polinomio $x^n - 1$ tiene una factorización única en $\mathbb{Z}_8[x]$ como un producto de polinomios mónicos, básicos irreducibles y coprimos. Asimismo, si γ es una unidad en $\mathbb{Z}_8$, entonces existe un único β en $U(\mathbb{Z}_8)$ tal que $\beta^n = \gamma^{-1}$ (Corolario 1.3.5). La unidad β es llamada la raíz n-ésima de γ^{-1}. De hecho, ya que todas las unidades en $\mathbb{Z}_8$ son de orden 2, para todo entero $n \geq 1$ impar, la raíz n-ésima β coincide

con la unidad γ.

En el Lema 1.3.8 se demostró que si $x^n-1=a_1(x)a_2(x)\cdots a_r(x)$, donde los polinomios $a_i(x)$ son mónicos, básicos irreducibles y coprimos, entonces una tal factorización de $x^n-\gamma$ es $x^n-\gamma=b_1(x)b_2(x)\cdots b_r(x)$, donde

$$b_i(x)=\beta^{-gr(a_i(x))}a_i(\beta x), \qquad 1\leq i\leq r.$$

Por ejemplo, sean $k=2$ y $n=3$. Entonces la factorización de $x^3-1\in\mathbb{Z}_8$ como un producto de polinomios mónicos, básicos irreducibles y coprimos es:

$$x^3-1=(x+7)(x^2+x+1)=a_1(x)a_2(x),$$

donde $a_1(x)=x+7$ y $a_2(x)=1+x+x^2$. Ahora, considere la unidad $\delta_1=1+2^{k-1}=3$ en $\mathbb{Z}_8$. Entonces la factorización de $x^3-\delta_1$ en $\mathbb{Z}_8[x]$ como un producto de polinomios básicos irreducibles y coprimos es $x^3-\delta_1=b_1(x)b_2(x)$, donde

$$\begin{aligned} b_1(x)&=\beta^{-1}a_1(x)=3^{-1}a_1(x)=3^{-1}(7+3x)=5+x,\\ b_2(x)&=\beta^{-2}a_2(x)=3^{-2}a_2(x)=3^{-2}(1+3x+3^2x^2)=1+3x+x^2. \end{aligned}$$

Por otra parte, si I es un ideal del anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n-1\rangle$, entonces existe una única colección $f_0,f_1,\ldots,f_{k+1}$ de polinomios mónicos y coprimos, tales que $f_0f_1\cdots f_{k+1}=x^n-1$ e $I=\langle\widehat{F_1},2\widehat{F_2},\ldots,2^k\widehat{F_{k+1}}\rangle$, donde $\widehat{F_i}=\widehat{f_i}+\langle x^n-1\rangle$ y $\widehat{f_i}=(x^n-1)/f_i$ (Teorema 1.3.1). Como consecuencia de este hecho, en el Teorema 1.3.9 y el Corolario 1.3.10, se demostró que si γ es una unidad de $\mathbb{Z}_{2^{k+1}}$ y

$$\mu_\beta:\mathbb{Z}_{2^{k+1}}[x]/\langle x^n-1\rangle\to\mathbb{Z}_{2^{k+1}}[x]/\langle x^n-\gamma\rangle$$

es el isomorfismo de anillos definido como $a(x)+\langle x^n-1\rangle\mapsto a(\beta x)+\langle x^n-\gamma\rangle$, donde $\beta^n=\gamma^{-1}$, entonces

$$J=\mu_\beta(I)=\langle\widehat{G_1},2\widehat{G_2},\ldots,2^k\widehat{G_{K+1}}\rangle,$$

donde los generadores $\widehat{G_i}$ se calculan reemplazando los factores $f_i+\langle x^n-1\rangle$ por $g_i+\langle x^n-\gamma\rangle$ en la expresión de $\widehat{F_i}$. El polinomio g_i está definido por la relación $g_i=\beta^{-gr(f_i)}f_i(\beta x)$.

Por ejemplo, consideremos nuevamente los casos $k=2$, $n=3$, y sean

$$f_0=1, \qquad f_1=a_1(x), \qquad f_2=1, \qquad f_3=a_2(x),$$

donde $a_1(x)=7+x$ y $a_2(x)=1+x+x^2$. Entonces es claro que los polinomios f_0,f_1,f_2 y f_3 son mónicos, coprimos y $f_0f_1f_2f_3=x^3-1$. Esta elección de los polinomios f_i implica que

$$\widehat{f_0}=x^3-1, \qquad \widehat{f_1}=a_2(x), \qquad \widehat{f_2}=x^3-1, \qquad \widehat{f_3}=a_1(x).$$

Por lo tanto, en $\mathbb{Z}_8[x]/\langle x^3-1\rangle$, tenemos que

$$\widehat{F_0}=0, \qquad \widehat{F_1}=a_2(x), \qquad \widehat{F_2}=0, \qquad \widehat{F_3}=a_1(x).$$

En consecuencia, $I=\langle \widehat{F_1}, 2\widehat{F_2}, 2^2\widehat{F_3}\rangle = \langle 1+x+x^2, 4(7+x)\rangle$ es un ideal en $\mathbb{Z}_8[x]/\langle x^3-1\rangle$ de cardinalidad 2^S, donde $S=\sum_{i=0}^{k}(k+1-i)gr(f_{i+1})=5$. Así, el conjunto

$$J=\mu_3(I)=\langle \widehat{G_1}, 2\widehat{G_2}, 2^2\widehat{G_3}\rangle = \langle 1+3x+x^2, 4(5+x)\rangle$$

es un ideal en $\mathbb{Z}_8[x]/\langle x^3-\delta_1\rangle$ de la misma cardinalidad que I.

Sea $P:\mathbb{Z}_8^3\to\mathbb{Z}_8[x]/\langle x^3-1\rangle$, $\gamma\in U(\mathbb{Z}_8)$, la representación polinomial, entonces de la Proposición 1.2.6 se sigue que los conjuntos

$$\begin{aligned}\mathscr{C}&=P^{-1}(I)=\{(z_0,z_1,z_2)\in\mathbb{Z}_8^3 \,:\, z_0+z_1x+z_2x^2+\langle x^3-1\rangle\in I\},\\ \mathscr{C}_{\delta_1}&=P^{-1}(J)=\{(z_0,z_1,z_2)\in\mathbb{Z}_8^3 \,:\, z_0+z_1x+z_2x^2+\langle x^3-\delta_1\rangle\in J\},\end{aligned}$$

son códigos cíclicos y δ_1-cíclicos, respectivamente, ambos lineales. En lo siguiente estudiaremos la imagen de estos códigos con respecto a las isometrías φ, Φ y Φ_1. Para este objetivo, haremos uso de las propiedades de estas isometrías, las cuales fueron estudiadas en los Capítulos 2, 3 y 4 de esta tesis.

Primero analicemos los códigos $\varphi(\mathscr{C})$, $\Phi(\mathscr{C})$ y $\Phi_1(\mathscr{C})$. Como $I=\langle 1+x+x^2, 4(7+x)\rangle$, entonces I tiene como polinomio generador a $1+x+x^2+4(7+x)$, esto es,

$$I=\langle 1+x+x^2+4(7+x)\rangle=\langle 5+5x+x^2\rangle,$$

De aquí se sigue que $Z\in\mathscr{C}$ si y sólo si existen $r_0,r_1,r_2\in\mathbb{Z}_8$ tales que

$$Z=r_0(5,5,1)+r_1(1,5,5)+r_2(5,1,5).$$

En otros términos, $\mathscr{C}$ es en el submódulo de $\mathbb{Z}_8^3$ generado por $g_0=(5,5,1)$, $g_1=(1,5,5)$ y $g_2=(5,1,5)$. Observe que con el propósito de calcular explícitamente los códigos $\varphi(\mathscr{C})$, $\Phi(\mathscr{C})$ y $\Phi_1(\mathscr{C})$, los generadores g_0, g_1 y g_2 no son del todo adecuados. Sin embargo, realizando operaciones elementales renglón a la matriz cuyos renglones son los vectores g_0, g_1 y g_2 en $\mathbb{Z}_8$, obtenemos que $g_0'=(1,1,1)$, $g_1'=(0,4,0)$ y $g_2'=(0,0,4)$ forman un conjunto de generadores del código $\mathscr{C}$. Así,

$$\mathscr{C}=\{r_0(1,1,1)+r_1(0,4,0)+r_2(0,0,4) \,:\, r_0,r_1,r_2\in\mathbb{Z}_8\}.$$

Por lo tanto,

$$\varphi(\mathscr{C})=\{\varphi(Z) \,:\, Z=r_0(1,1,1)+r_1(0,4,0)+r_2(0,0,4), r_0,r_1,r_2\in\mathbb{Z}_8\}.$$

De este modo, si $Z \in \mathscr{C}$, se sigue del Corolario 2.3.6 que

$$\varphi(Z) = \varphi(r_0(1,1,1)) + \varphi(r_1(0,4,0)) + \varphi(r_2(0,0,4)).$$

Note que formalmente $r_1, r_2 \in \mathbb{Z}_8$ pero ya que las coordenadas de $r_1(0,4,0)$ y $r_2(0,0,4)$ están en el ideal maximal de $\mathbb{Z}_8$, es suficiente considerar los casos $r_0, r_1 \in \{0,1\}$. Esto implica que

$$\varphi(r_1(0,4,0)) = r_1\varphi(0,4,0), \quad \varphi(r_2(0,0,4)) = r_2\varphi((0,0,4)), \quad r_1, r_2 \in \{0,1\}.$$

Asimismo, ya que $2^2(1,1,1) \odot 2(1,1,1) = (0,0,0)$, del Corolario 2.3.6 se obtiene que

$$\varphi(r_0(1,1,1)) = (a_0 + 2a_2)\varphi(1,1,1) + a_1\varphi(2(1,1,1)),$$

donde $r_0 = a_0 + 2a_1 + 2^2a_2$ está expresado en su representación 2-ádica. Por su parte, como r_0 varía sobre $\mathbb{Z}_8$, el elemento $a_0 + 2a_2$ varía sobre todo $\mathbb{Z}_4$. En consecuencia,

$$\varphi(\mathscr{C}) = \{a\varphi(1,1,1) + b\varphi(2(1,1,1)) + c\varphi(0,4,0) + d\varphi(0,0,4) \ : \ a \in \mathbb{Z}_4, b,c,d \in \mathbb{F}_2\}.$$

Ahora, como $\varphi(2(1,1,1))$, $\varphi(0,4,0)$ y $\varphi(0,0,4)$ tienen sus coordenadas en el ideal maximal de $\mathbb{Z}_4$, podemos considerar que b,c y d toman valores en $\mathbb{Z}_4$, lo cual implica que $\varphi(\mathscr{C})$ es un código lineal de longitud 6 sobre $\mathbb{Z}_4$. A raíz de lo anterior, y a que es suficiente tomar $a \in \mathbb{Z}_4$ y $b,c,d \in \mathbb{F}_2$, se dice que $\varphi(\mathscr{C})$ es un código lineal de tipo $4 \cdot 2^3$. Explícitamente, $\varphi(\mathscr{C})$ es generado por los vectores:

$$\varphi(1,1,1) = 111\,111, \quad \varphi(2(1,1,1)) = 000\,111, \quad \varphi(0,4,0) = 020\,020, \quad \varphi(0,0,4) = 002\,002.$$

Observe que este código no es negacíclico pues $\nu(\varphi(1,1,1)) = 311\,111 \notin \varphi(\mathscr{C})$.

Por su parte, la imagen de Gray del código $\mathscr{C}$ queda descrita como

$$\Phi(\mathscr{C}) = \{\Phi(Z) \ : \ Z = r_0(1,1,1) + r_1(0,4,0) + r_2(0,0,4), r_0, r_1, r_2 \in \mathbb{Z}_8\}.$$

Debido al Corolario 2.3.8, si $Z \in \mathscr{C}$, entonces

$$\begin{aligned}\Phi(Z) &= \Phi(r_0(1,1,1)) \oplus \Phi(r_1(0,4,0)) \oplus \Phi(r_2(0,0,4)) \\ &= \Phi(r_0(1,1,1)) \oplus r_1\Phi(0,4,0) \oplus r_2\Phi(0,0,4).\end{aligned}$$

Además, como $2^2(1,1,1) \odot 2(1,1,1) = (0,0,0)$ se sigue que

$$\Phi(r_0(1,1,1)) = \alpha_0\Phi(1,1,1) \oplus \alpha_1\Phi(2(1,1,1)) \oplus \alpha_2\Phi(4(1,1,1)),$$

donde $r_0 = \alpha_0 + 2\alpha_1 + 2^2\alpha_2$ está expresado en su representación 2-ádica. En consecuencia, $\Phi(\mathscr{C})$ es el conjunto de todas la combinaciones lineales de los siguientes vectores en $\mathbb{F}_2^{12}$:

$$\Phi(1,1,1) = 000\,000\,111\,111, \quad \Phi(2,2,2) = 000\,111\,000\,111, \quad \Phi(4,4,4) = 111\,111\,111\,111,$$
$$\Phi(0,4,0) = 010\,010\,010\,010, \quad \Phi(0,0,4) = 001\,001\,001\,001.$$

Ya que estos vectores son linealmente independientes, $\Phi(\mathscr{C})$ es un $[12,5]$-código binario. Además, como el peso de Hamming de $\Phi(0,4,0)$ es 4, se sigue que $\omega_H(\Phi(\mathscr{C})) \leq 4$. De hecho, es fácil verificar que cualquier $\mathbb{F}_2$-combinación lineal de la base de $\Phi(\mathscr{C})$ descrita anteriormente tiene peso de Hamming mayor o igual a 4 y, por lo tanto, $\omega_H(\Phi(\mathscr{C})) = 4$. Consecuentemente, $\Phi(\mathscr{C})$ es un $[12,5,4]$-código lineal binario. Para finalizar el análisis del código $\Phi(\mathscr{C})$, note que éste no es cíclico pues $\sigma(\Phi(0,0,4)) \notin \Phi(\mathscr{C})$.

Ahora, la isometría $\Phi_1 : \mathbb{Z}_8^3 \to \mathbb{F}_2^{12}$ está definida como $\Phi_1 = \widetilde{\varepsilon} \circ \Phi$, donde $\widetilde{\varepsilon}$ es la permutación sobre $\mathbb{F}_3^{12}$ inducida por la permutación $\varepsilon = (3,6)(4,7)(5,8)$ (ver el Ejemplo 4.7.5). Consecuentemente, $\Phi_1(\mathscr{C})$ es también un $[12,5,4]$-código lineal binario con base

$$\begin{aligned}
&(\widetilde{\varepsilon} \circ \Phi)(1,1,1) = 000\,000\,111\,111, && (\widetilde{\varepsilon} \circ \Phi)(2,2,2) = 000\,111\,000\,111,\\
&(\widetilde{\varepsilon} \circ \Phi)(4,4,4) = 111\,111\,111\,111, && (\widetilde{\varepsilon} \circ \Phi)(0,4,0) = 010\,010\,010\,010,\\
&(\widetilde{\varepsilon} \circ \Phi)(0,0,4) = 001\,001\,001\,001.
\end{aligned}$$

Ya que esta base es la misma que la del código $\Phi(\mathscr{C})$, inferimos que $\Phi_1(\mathscr{C}) = \Phi(\mathscr{C})$ y, en particular, esto quiere decir que $\Phi_1(\mathscr{C})$ no es un código cíclico. Sin embargo, de los Teoremas 4.4.1 sabemos que $\varphi(\mathscr{C})$ y $\Phi(\mathscr{C}) = \Phi_1(\mathscr{C})$ tienen las siguientes propiedades de casi-negaciclicidad y casi-ciclicidad:

1. $\varphi(\mathscr{C})$ es un código casi-cíclico y casi-negacíclico de índice 2, longitud 6 y tipo $4 \cdot 2^3$.
2. $\Phi(\mathscr{C})$ es un $[12,5,4]$-código binario lineal y casi-cíclico de índices 2 y 4.

Vale la pena observar que de acuerdo a la base de datos [18] el código binario $\Phi(\mathscr{C})$ es óptimo. Esto es, $\Phi(\mathscr{C})$ es un código lineal con la máxima distancia mínima de Hamming posible entre todos los $[12,5]$-códigos lineales binarios. Asimismo, encontramos que $\varphi(\mathscr{C})$ es un código que no está registrado en [3] y que $\Phi(\mathscr{C})$ es código que no está registrado en [58].

Ahora analizaremos los códigos $\varphi(\mathscr{C}_{\delta_1})$ y $\Phi(\mathscr{C}_{\delta_1})$. Recuerde que $\mathscr{C}_{\delta_1}$ es el código δ_1-cíclico lineal sobre $\mathbb{Z}_8$ definido como

$$\mathscr{C}_{\delta_1} = P^{-1}(J) = \{(z_0,z_1,z_2) \in \mathbb{Z}_8^3 \,:\, z_0 + z_1 x + z_2 x^2 + \langle x^3 - \delta_1 \rangle \in J\},$$

donde $J = \langle 1 + 3x + x^2, 4(5+x) \rangle = \langle 1 + 7x + x^2 \rangle \subseteq \mathbb{Z}_8[x]/\langle x^3 - \delta_1 \rangle$. Por lo tanto, $Z \in \mathscr{C}_{\delta_1}$ si y sólo si existen $r_0, r_1, r_2 \in \mathbb{Z}_8$ tales que

$$Z = r_0(5,7,1) + r_1(3,5,7) + r_2(5,3,5).$$

Al realizar operaciones elementales renglón a la matriz con entradas en $\mathbb{Z}_8$ y cuyos renglones son los vectores $(5,7,1)$, $(3,5,7)$ y $(5,3,5)$, obtenemos que $(1,3,1)$, $(0,4,0)$ y $(0,0,4)$ generan a $\mathscr{C}_{\delta_1}$. De este modo, bajo argumentos similares a los anteriores, es posible demostrar que

$$\varphi(\mathscr{C}_{\delta_1}) = \{a\,\varphi(1,3,1) + b\,\varphi(2(1,3,1)) + c\,\varphi(0,4,0) + d\,\varphi(0,0,4) \,:\, a \in \mathbb{Z}_8, b,c,d \in \mathbb{F}_2\}$$

es un código lineal de longitud 6 sobre $\mathbb{Z}_4$ y tipo $4\cdot 2^3$. Los generadores del código $\varphi(\mathscr{C}_{\delta_1})$ son:

$$\varphi(131) = 111\,131, \quad \varphi(222) = 020\,202, \quad \varphi(040) = 020\,020, \quad \varphi(004) = 002\,002.$$

Observe que:

$$\begin{aligned}
\nu(111\,131) &= 311\,113 = 3\varphi(131) + \varphi(2(131)) + \varphi(004),\\
\nu(020\,202) &= 202\,020 = 2\varphi(131) + \varphi(2(131)),\\
\nu(020\,020) &= 002\,002 = \varphi(004),\\
\nu(002\,002) &= 200\,200 = 2\varphi(131) + \varphi(040) + \varphi(004).
\end{aligned}$$

Por lo tanto, $\varphi(\mathscr{C})$ es un código negacíclico lineal. En consecuencia, $\Phi(\mathscr{C}_{\delta_1})$ es un código cíclico binario. No es difícil convencerse de que

$$\Phi(Z) = \alpha_0\Phi(131) \oplus \alpha_1\Phi(2(131)) \oplus \alpha_2\Phi(4(131)) \oplus (\alpha_0\alpha_1 \oplus r_1)\Phi(040) \oplus r_2\Phi(004),$$

donde $Z = r_0(131) + r_1(040) + r_2(004)$, $r_0 \in \mathbb{Z}_8$, $r_1, r_2 \in \mathbb{F}_2$ y $r_0 = \alpha_0 + 2\alpha_1 + 2^2\alpha_2$ está expresado en su representación 2-ádica. A partir de esta relación, es claro que $\Phi(\mathscr{C}_{\delta_1})$ es el conjunto de todas las $\mathbb{F}_2$-combinaciones lineales de

$$\begin{aligned}
&\Phi(131) = 000\,000\,111\,111, \quad \Phi(262) = 010\,101\,010\,101, \quad \Phi(444) = 111\,111\,111\,111,\\
&\Phi(131) = 010\,010\,010\,010, \quad \Phi(131) = 001\,001\,001\,001.
\end{aligned}$$

Dado que estos vectores son linealmente independientes, $\Phi(\mathscr{C}_{\delta_1})$ es un $[12,5]$-código cíclico binario. Además, como $\omega_H(\mathscr{C}_{\delta_1}) = \omega_H(\mathscr{C}) = 4$, se sigue que $\Phi(\mathscr{C}_{\delta_1})$ es un $[12,5,4]$-código cíclico binario, el cual es óptimo según la base de datos [18].

Finalmente, veamos qué propiedad tiene el código $\Phi_1(\mathscr{C})$. Permutando las coordenadas de los generadores de $\Phi(\mathscr{C})$, obtenemos los generadores del código $\Phi_1(\mathscr{C})$. Esto resulta en lo siguiente:

$$\begin{aligned}
&(\widetilde{\varepsilon}\circ\Phi)(131) = 000\,111\,000\,111, && (\widetilde{\varepsilon}\circ\Phi)(262) = 010\,010\,101\,101,\\
&(\widetilde{\varepsilon}\circ\Phi)(444) = 111\,111\,111\,111, && (\widetilde{\varepsilon}\circ\Phi)(131) = 010\,010\,010\,010,\\
&(\widetilde{\varepsilon}\circ\Phi)(131) = 001\,001\,001\,001.
\end{aligned}$$

Ya que $\sigma((\widetilde{\varepsilon}\circ\Phi)(131)) \notin \Phi_1(\mathscr{C})$, el código $\Phi_1(\mathscr{C})$ no es cíclico.

Es importante resaltar que la propiedad de negaciclícidad no apareció en el código $\varphi(\mathscr{C})$, pero que sí es parte del código $\varphi(\mathscr{C}_{\delta_1})$. Como consecuencia de este hecho, el código $\Phi(\mathscr{C}_{\delta_1})$ es cíclico. Esto muestra que, desde el punto de vista de las propiedades de casi-negaciclicidad y casi-ciclicidad, las imágenes bajo φ y Φ de los códigos $(1+2^{k-1})$-cíclicos y $(1+2^{k-1}+2^k)$-cíclicos pueden ser objetos interesantes de estudio.

Generadores	Cardinalidad	$\Phi(\mathscr{C})$ cíclico	Generadores	Cardinalidad	$\Phi(\mathscr{C})$ cíclico
$\langle 2\rangle$	2^6	✓	$\langle 2^2 b_2\rangle$	2	✓
$\langle 2^2\rangle$	2^3	✓	$\langle b_1, 2b_2\rangle$	2^8	✓
$\langle b_1\rangle$	2^6	–	$\langle b_1, 2^2 b_2\rangle$	2^7	✓
$\langle 2b_1\rangle$	2^4	✓	$\langle b_2, 2b_1\rangle$	2^7	✓
$\langle 2^2 b_1\rangle$	2^2	✓	$\langle b_2, 2^2 b_1\rangle$	2^5	✓
$\langle b_2\rangle$	2^3	–	$\langle 2b_1, 2^2 b_2\rangle$	2^5	✓
$\langle 2b_2\rangle$	2^2	✓	$\langle 2b_2, 2^2 b_1\rangle$	2^4	✓

$x^3-3=b_1b_2, \quad b_1=x+5, \quad b_2=x^2+3x+1$

✓: $\Phi(\mathscr{C})$ es un código binario cíclico

–: $\Phi(\mathscr{C})$ no es código binario cíclico

Cuadro 6.1: Códigos 3-cíclicos lineales de longitud 3 sobre $\mathbb{Z}_8$ cuya imagen de Gray es cíclica.

Después de haber presentado a los códigos $\mathscr{C}$ y $\mathscr{C}_{\delta_1}$, es natural preguntarse qué sucede con los otros códigos 3-cíclicos lineales de longitud 3 sobre $\mathbb{Z}_8$. Con la ayuda del programa computacional MAGMA® V2.15-13 (Student Version), construimos el Cuadro 6.1, el cual contiene una lista de de todos los códigos 3-cíclicos lineales (no triviales) de longitud 3 sobre $\mathbb{Z}_8$. Hemos señalado con ✓ aquellos códigos 3-cíclicos cuya imagen de Gray es un código cíclico binario (compare esto con el Cuadro 4.1). Observe que 2 de los 14 códigos 3-cíclicos lineales de longitud 3 sobre $\mathbb{Z}_8$ no satisfacen lo que observamos en este ejemplo. De este modo, si $\mathscr{C}$ es un código 3-cíclico, entonces no necesariamente $\varphi(\mathscr{C})$ es un código cíclico. Así, la propiedad de negaciclicidad no puede caracterizar a esta familia de códigos. Entonces cabe la pregunta, ¿qué propiedades debe satisfacer un código 3-cíclico $\mathscr{C}$ sobre $\mathbb{Z}_8$ para que $\varphi(\mathscr{C})$ sea un código negacíclico y como consecuencia, su imagen de Gray sea un código cíclico?

En las siguientes secciones analizaremos algunas propiedades de casi-negacíclicidad y casi-ciclícidad de las imágenes bajo φ y Φ de códigos 3-cíclicos y 7-cíclicos. En particular, daremos respuesta a la pregunta antes planteada.

6.3. Imágenes de códigos 3-cíclicos sobre $\mathbb{Z}_8$

En esta sección analizaremos algunas propiedades de casi-negaciclicidad y casi-ciclicidad de la imagen bajo φ de los códigos 3-cíclicos sobre $\mathbb{Z}_8$. Esto corresponde a los casos $k=2$ y $\delta_1=3$ que no fueron considerados en los principales resultados del capítulo 5, lo cual se debió principalmente a que parte del Lema 5.2.7 es válido únicamente para $k\geq 3$.

Introduciremos dos caracterizaciones de la imagen bajo φ de un código 3-cíclico. La primera es similar a la de los códigos δ_2-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, con $k \geq 3$, enunciada en el Teorema 5.3.3. La segunda establece que la imagen bajo φ de un código 3-cíclico es un código negacíclico sobre $\mathbb{Z}_4$, módulo una traslación de un vector $\widehat{d}$ definido de manera similar al vector $\widehat{c}$ que apareció en los resultados del Capítulo 5. Esta segunda caracterización nos permitirá dar propiedades de ciclícidad de la imagen de Gray de un código 3-cíclico sobre $\mathbb{Z}_8$.

6.3.1. Imágenes sobre $\mathbb{Z}_4$: primera caracterización

En lo sucesivo introduciremos una primera caracterización de la imagen bajo φ de los códigos 3-cílicos sobre $\mathbb{Z}_8$. Siendo $k = 2$ una hipótesis general, varios definiciones y resultados expuestos en capítulos previos, adquieren una forma particular. A continuación, mencionaremos algunos de particular interés.

La representación 2-ádica de $Z \in \mathbb{Z}_8^n$ queda expresada como $Z = r_0(Z) + 2r_1(Z) + 2^2 r_2(Z)$, $r_i(Z) \in \{0,1\}^n$, y los vectores $c_0^{k-1} = c_0^1$ y $c_{k-1}^{k-1} = c_1^1$ son, respectivamente, $u = (0,1)$ y $v = (1,1)$ (Subsección 2.1.1). Consecuentemente, la isometría φ queda definida de la siguiente manera:

$$\varphi(Z) = v \otimes r_0(Z) + 2\left[u \otimes r_1(Z) \oplus v \otimes r_2(Z)\right],$$

(Subsección 2.2.2 y Ejemplo 2.2.8). Asimismo, la permutación π introducida en la relación (5.3) como

$$\pi = (0,l)(n,n+l)(2n,2n+l)\cdots((2^{k-2-1})n,(2^{k-2-1})n+l), \qquad n \geq 1,\ l = 2^{k-2}n,$$

queda dada por $\pi = (0,n)$. A razón de este hecho, el Lema 5.2.7 no es válido para $k = 2$. Si $k = 2$, entonces tenemos el siguiente resultado.

Lema 6.3.1. *Sea $n \geq 1$ un entero, $\mathbf{b} = (0,\ldots,0,z) \in \mathbb{Z}_4^n$ y $\widetilde{\pi}$ la permutación sobre $\mathbb{Z}_4^{2n}$ inducida por la permutación $\pi = (0,n)$. Entonces*

$$\nu^{\otimes 2}\left(3v \otimes \mathbf{b} + 2u \otimes \mathbf{b}\right) = \widetilde{\pi}(\nu \otimes \sigma))(v \otimes \mathbf{b}).$$

Demostración. En virtud del Lema 5.2.7,

$$\nu^{\otimes 2}\left(3v \otimes \mathbf{b} + 2u \otimes \mathbf{b}\right) = (\sigma \otimes \nu)(v \otimes \mathbf{b}) = (z,0,\ldots,0,-z,0,\ldots,0).$$

Por otra parte, $(\nu \otimes \sigma)(v \otimes \mathbf{b}) = (z,0,\ldots,0,-z,0,\ldots,0)$. Así, basta intercambiar las coordenadas z y $-z$ en el vector anterior para obtener $\nu^{\otimes 2}\left(3v \otimes \mathbf{b} + 2u \otimes \mathbf{b}\right)$. Dado que esta es precisamente la acción de la permutación $\widetilde{\pi}$, el resultado se sigue. □

El Lema 6.3.1, aunado a los Lemas 5.2.5, 5.2.6, 5.2.8 y 5.2.9, dan lugar al siguiente resultado, cuya demostración es similar a la del Teorema 5.2.10; razón por la cual la omitimos.

Teorema 6.3.2. *Continuando con la notación anterior, para todo* $Z = (z_0, \ldots, z_{n-1}) \in \mathbb{Z}_8^n$,

$$\begin{aligned}(\varphi \circ \nu_3)(Z) &= \widetilde{\pi}(\nu \otimes \sigma)\left(\varphi(Z) + \varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)\right)\\ &= \widetilde{\pi}(\nu \otimes \sigma)\left(\varphi(Z)\right) + \widetilde{\pi}(\nu \otimes \sigma)\left(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)\right)\\ &= \widetilde{\pi}(\nu \otimes \sigma)\left(\varphi(Z)\right) + (\nu \otimes \sigma)\left(\varphi(2^k\mathbf{b}_Z \odot 2\mathbf{b}_Z)\right),\end{aligned}$$

donde $\mathbf{b}_Z = (0, \ldots, 0, z_{n-1}) \in \mathbb{Z}_8^n$.

Una aplicación del Teorema anterior permite obtener una primera caracterización de los códigos 3-cíclicos sobre $\mathbb{Z}_8$.

Teorema 6.3.3. *Sean* $n \geq 1$ *un entero y* $\widetilde{\pi}$ *la permutación sobre* $\mathbb{Z}_4^{2n}$ *inducida por la permutación* $\pi = (0, n)$. *Las siguientes afirmaciones son equivalentes:*

(1) $\mathscr{C} \subseteq \mathbb{Z}_8^n$ *es un código 3-cíclico (no necesariamente lineal);*

(2) $\varphi(\mathscr{C}) \subseteq \mathbb{Z}_4^{2n}$ *es un código (no necesariamente lineal) tal que*

$$\widetilde{\pi}(\nu \otimes \sigma)(c) + \widehat{c} \in \varphi(\mathscr{C}), \qquad \forall\, c \in \varphi(\mathscr{C})$$

donde $\widehat{c} = (1,1) \otimes (2,0,\ldots,0)$ *si y sólo si* $t \in \{(1,3),(3,1)\}$, *y* t *es el vector obtenido al concatenar en orden las coordenadas de* c *con subíndice en el conjunto* $\{n-1, 2n-1\}$. *En caso contrario,* $\widehat{c} = (0)_{2n} \in \mathbb{Z}_4^{2n}$.

Demostración. Sea $Z = (z_0, \ldots, z_{n-1}) \in \mathbb{Z}_8^n$ y $c = \varphi(Z)$. Entonces $t = \varphi(z_{n-1})$ y, por lo tanto, el resultado se sigue del Teorema 6.3.2. □

Ejemplo 6.3.4. Considere el código $\mathscr{C} \subseteq \mathbb{Z}_8^3$ cuyos elementos son:

1726	2172	2635	3562
5621	6217	6356	7263

Este código consiste de todos los corrimientos 3-cíclicos del vector 7263 y, por lo tanto, $\mathscr{C}$ es un código 3-cíclico. Consecuentemente, $\varphi(\mathscr{C})$ satisface la propiedad enunciada en el punto (2) del Teorema 6.3.3. Veamos que efectivamente así es. Preservando el orden en el que aparecen listados los elementos de $\mathscr{C}$, calculamos que $\varphi(\mathscr{C})$ consta de los siguientes vectores en $\mathbb{Z}_4^8$:

1302 1120	0130 2112	0213 2033	1320 3302
3201 3021	2013 0211	2132 0330	3021 1203

A cada elemento de $\varphi(\mathscr{C})$ le aplicamos el $\mathbb{Z}_4$-automorfismo $\nu \otimes \sigma$, obteniendo lo siguiente:

2130 0112	0013 2211	1021 3203	0132 2330
3320 1302	1201 1021	2213 0033	3302 3120

Ahora, aplicamos la permutacón $\widetilde{\pi}$ sobre $\mathbb{Z}_4^8$ inducida por la permutación $\pi = (0,4)$:

$$\begin{array}{cccc} 0130\,2112 & 2013\,0211 & 3021\,1203 & 2132\,0330 \\ 1320\,3302 & 1201\,1021 & 0213\,2033 & 3302\,3120 \end{array}$$

Por otra parte, para cada $c \in \varphi(\mathscr{C})$, los correspondientes vectores t son:

$$\begin{array}{cccc} 2\,0 & 0\,2 & 3\,3 & 0\,2 \\ 1\,1 & 3\,1 & 2\,0 & 1\,3 \end{array}$$

En consecuencia, los vectores $\widehat{c}$ son:

$$\begin{array}{cccc} 0000\,0000 & 0000\,0000 & 0000\,0000 & 0000\,0000 \\ 0000\,0000 & 2000\,2000 & 0000\,0000 & 2000\,2000 \end{array}$$

De este modo, al sumar los vectores $\widetilde{\pi}(\nu \otimes \sigma)(c)$ y $\widehat{c}$, obtenemos

$$\begin{array}{cccc} 0130\,2112 & 2013\,0211 & 3021\,1203 & 2132\,0330 \\ 1320\,3302 & 3201\,3021 & 0213\,2033 & 1302\,1120 \end{array}$$

Es claro que esta nueva colección de vectores coincide con los elementos del código $\varphi(\mathscr{C})$ y, por lo tanto, hemos comprobado que efectivamente $\varphi(\mathscr{C})$ satisface la propiedad (2) del Teorema 6.3.3. Con esto finalizamos el ejemplo.

Observe que en el Teorema 6.3.3 usamos el automorfismo $\nu \otimes \sigma$ seguido de la permutación $\widetilde{\pi}$ para dar una caracterización de los códigos δ_1-cíclicos (3-cíclicos) sobre $\mathbb{Z}_8$; mientras que para establecer una caracterización de los códigos δ_1-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, con $k \geq 3$, se usó el automorfismo $(\sigma \otimes \nu)^{2^{k-2}}$ seguido de la permutación $\widetilde{\pi}$. Note que las aplicaciones σ y ν están en un orden invertido. Sin embargo, el automorfismo $\nu \otimes \sigma$ apareció en el Teorema 5.3.3, en el cual se estableció una caracterización de los códigos δ_2-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$ con $k \geq 3$. Estos hechos nos han inducido a considerar por separado los resultados para $k \geq 3$ y $k = 2$.

Algunos casos particulares del Teorema 6.3.3 son de particular interés.

Primero, si $\mathscr{C}$ es un código tal que $\mathscr{C} \subseteq (2\mathbb{Z}_8)^n$, entonces los elementos de $\varphi(\mathscr{C})$ tienen todas sus coordenadas en el ideal maximal de $\mathbb{Z}_4$ y, por lo tanto, para todo $c \in \varphi(\mathscr{C})$, se tiene que $\widehat{c} = (0)_{2n} \in \mathbb{Z}_4$. Como consecuencia de este hecho, tenemos el siguiente resultado.

Proposición 6.3.5. *Sea $\mathscr{C} \subseteq (2\mathbb{Z}_8)^n$ un código. Entonces $\mathscr{C}$ es un código* 3*-cíclico si y sólo si*

$$\widetilde{\pi}(\nu^{\otimes 2})(\varphi(\mathscr{C})) = \widetilde{\pi}(\sigma^{\otimes 2})(\varphi(\mathscr{C})) = \varphi(\mathscr{C}).$$

Por otro lado, similarmente a la Proposición 5.2.20 tenemos el siguiente resultado.

Proposición 6.3.6. *Sea $\mathscr{C} \subseteq \mathbb{Z}_8$ es un código tal que $2^2\mathbf{b}_Z \in \mathscr{C}$ y $\varphi(\mathscr{C})$ es lineal. Entonces $\mathscr{C}$ es 3-cíclico si y sólo si $\widetilde{\pi}(\nu \otimes \sigma)(c) \in \varphi(\mathscr{C})$ para todo $c \in \varphi(\mathscr{C})$.*

Si la condición de linealidad es añadida al código $\mathscr{C}$, entonces es posible suprimir en la proposición anterior la condición de linealidad en el código $\varphi(\mathscr{C})$.

Proposición 6.3.7. *Sea $\mathscr{C} \subseteq \mathbb{Z}_8$ es un código lineal tal que $2^2\mathbf{b}_Z \in \mathscr{C}$. Entonces $\mathscr{C}$ es 3-cíclico si y sólo si $\widetilde{\pi}(\nu \otimes \sigma)(c) \in \varphi(\mathscr{C})$ para todo $c \in \varphi(\mathscr{C})$.*

El Teorema 6.3.3 establece una caracterización de los códigos 3-cíclicos en términos de sus imágenes con respecto a la isometría φ. Sin embargo, la propiedad que satisfacen esas imágenes no es la más adecuada para introducir una caracterización de los códigos 3-cíclicos sobre $\mathbb{Z}_8$ en términos de sus imágenes de Gray. El propósito de la siguiente subsección es analizar una nueva caracterización de los códigos 3-cíclicos con respecto a sus imágenes bajo φ, y a raíz de este hecho, naturalmente derivaremos propiedades de ciclícidad de la imagen de Gray de los códigos 3-cíclicos sobre $\mathbb{Z}_8$. Más aún, veremos que tales propiedades serán suficientes para caracterizar a tales códigos.

6.3.2. Segunda caracterización e imágenes de Gray

En esta subsección analizaremos una segunda caracterización de los códigos 3-cíclicos sobre $\mathbb{Z}_8$ con respecto a su imagen bajo φ. Como consecuencia de este resultado, estableceremos propiedades de ciclícidad de la imagen de Gray de esta familia de códigos.

Como motivación e introducción, retomemos el código $\mathscr{C}$ del ejemplo 6.3.4. Recordemos que la imagen bajo φ de este código es:

1302 1120	0130 2112	0213 2033	1320 3302
3201 3021	2013 0211	2132 0330	3021 1203

Ahora, en lugar de calcular el vector $\widetilde{\pi}(\nu \otimes \sigma)(c) + \widehat{c}$ para cada elemento $c \in \varphi(\mathscr{C})$, calculemos el corrimiento negacíclico $\nu(c)$ de cada elemento $c \in \varphi(\mathscr{C})$:

0130 2112	2013 0211	1021 3203	2132 0330
3320 1302	3201 3021	0213 2033	1302 1120

También, en lugar de considerar los vectores $\widehat{c}$ del Teorema 6.3.3, consideremos ahora los siguientes vectores $\widehat{d}$:

0000 0000	0000 0000	2000 2000	0000 0000
2000 2000	0000 0000	0000 0000	0000 0000

Sumando éstos a los vectores $\nu(c)$ obtenemos:

$$\begin{array}{cccc} 0130\,2112 & 2013\,0211 & 3021\,1203 & 2132\,0330 \\ 1320\,3302 & 3201\,3021 & 0213\,2033 & 1302\,1120 \end{array}$$

Note que en conjunto, estos últimos forman el código $\varphi(\mathscr{C})$. En consecuencia, tenemos que

$$\nu(c)+\widehat{d}\in\varphi(\mathscr{C}) \qquad \forall\, c\in\varphi(\mathscr{C}).$$

La propiedad anterior no es particular del código $\mathscr{C}$ dado en el ejemplo 6.3.4. Con el fin de dar una prueba general a esta observación, recordemos los siguientes hechos. En virtud del Teorema 2.3.5, para todo $X,Y,Z\in\mathbb{Z}_8^n$,

$$\begin{aligned}\varphi(Z+2Y+2^2X) &= \varphi(Z)+\varphi(2Y)+\varphi(2^2X)+\varphi(2^2Y\odot 2Z)\\ &= \varphi(Z)+\varphi(2Y)+2\varphi(X)+\varphi(2^2Y\odot 2Z),\end{aligned} \tag{6.1}$$

donde "$\odot$" ha sido definida en el capítulo 2 como

$$X\odot Y = r_0(X)*r_1(X)+2r_1(X)*r_1(Y)+2^2r_2(X)*r_1(Y), \qquad \forall X,Y\in\mathbb{Z}_8^n,$$

y "$*$" denota la multiplicación coordenada por coordenada. Si tomamos $X=Y=Z$ en la relación (6.1), entonces

$$\varphi(7Z)=\varphi(Z+2Z+2^2Z)=\varphi(Z)+\varphi(2Z)+2\varphi(Z)+\varphi(2^2Z\odot 2Z).$$

Similarmente, si $X=(0)_n$ y $Y=Z$, entonces

$$\varphi(3Z)=\varphi(Z+2Z)=\varphi(Z)+\varphi(2Z)+\varphi(2^2Z\odot 2Z).$$

Observe que $2^2Z\odot 2Z = 2^2r_0(Z)*r_1(Z)$. De este modo, en general el término $\varphi(2^2Z\odot 2Z)$ no se anula a menos que $r_0(Z)*r_1(Z)=(0)_n$. En particular, si $\mathbf{b}=(0,\ldots,0,z_{n-1})\in\mathbb{Z}_8^n$, entonces $r_0(\mathbf{b}_Z)*r_1(\mathbf{b}_Z)=(0)_n$ si y sólo si $2^2z_{n-1}\odot 2z_{n-1}=0$, o equivalentemente, si y sólo si $r_0(z_{n-1})r_1(z_{n-1})=0$, lo cual ocurre si y sólo si $r_0(z_{n-1})=0$ o $r_1(z_{n-1})=0$. Es fácil verificar que los elementos en $\mathbb{Z}_8$ que satisfacen estas propiedades son $0,2,4,6,1,5$. Consecuentemente, $\varphi(2^2\mathbf{b}_Z\odot 2\mathbf{b}_Z)=v\otimes(0,\ldots,0,2)\in\mathbb{Z}_4^{2n}$ si y sólo si $z_{n-1}=3,7$.

Teorema 6.3.8. *Sea $n\geq 1$ un entero y $Z=(z_0,\ldots,z_{n-2},z_{n-1})\in\mathbb{Z}_8^n$. Entonces*

$$(\varphi\circ\nu_3)(Z)=\nu(\varphi(Z))+\nu(\varphi(2^2\mathbf{b}_Z+2^2\mathbf{b}_Z\odot 2\mathbf{b}_Z)),$$

donde $\mathbf{b}_Z=(0,\ldots,0,z_{n-1})\in\mathbb{Z}_8^n$.

Demostración. Sea $Z = \mathbf{a} + \mathbf{b}_Z$, con $\mathbf{a} = (z_0, \ldots, z_{n-2}, 0)$ y $\mathbf{b}_Z = Z - \mathbf{a} = (0, \ldots, 0, z_{n-1})$, teniendo en cuenta que si $n = 1$, entonces $\mathbf{a} = 0$. En virtud del Teorema 3.3.3,

$$(\varphi \circ \nu_3)(Z) = (\nu^{\otimes 2} \circ \varphi \circ \eta_7)(\mathbf{a} + \mathbf{b}_Z) = (\nu^{\otimes 2} \circ \varphi)(\mathbf{a} + 7\mathbf{b}_Z),$$

donde $\eta_7(Z) = (z_0, \ldots, z_{n-2}, 7z_{n-1})$. Además, por el Lema 3.3.1,

$$(\nu^{\otimes 2} \circ \varphi)(\mathbf{a} + 7\mathbf{b}_Z) = \nu^{\otimes 2}(\varphi(\mathbf{a}) + \varphi(7\mathbf{b}_Z)) = \nu^{\otimes 2}(\varphi(\mathbf{a})) + \nu^{\otimes 2}(\varphi(7\mathbf{b}_Z)).$$

Del Lema 5.2.5 deducimos que $\nu^{\otimes 2}(\varphi(\mathbf{a})) = \nu(\varphi(\mathbf{a}))$. Por otro lado,

$$\nu^{\otimes 2}(\varphi(7\mathbf{b}_Z)) = \nu^{\otimes 2}(-\varphi(\mathbf{b}_Z) + \varphi(2\mathbf{b}_Z)) + \nu^{\otimes 2}(\varphi(2^2\mathbf{b}_Z \otimes 2\varphi(\mathbf{b}_Z))).$$

Como $\varphi(2^2\mathbf{b}_Z \otimes 2\mathbf{b}_Z) = (1,1) \otimes (0, \ldots, 0, 2^2 r_0(z_{n-1}) r_1(z_{n-1}))$, se tiene que

$$\nu^{\otimes 2}(\varphi(2^2\mathbf{b}_Z \otimes 2\mathbf{b}_Z)) = \nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)).$$

De este modo, la parte interesante de la prueba reside en el término

$$\nu^{\otimes 2}(-\varphi(\mathbf{b}_Z) + \varphi(2\mathbf{b}_Z)).$$

Aplicando la definición de φ a la representación 2-ádica de $\mathbf{b}_Z$ es fácil demostrar que

$$\begin{aligned}\varphi(2\mathbf{b}_Z) - \varphi(\mathbf{b}_Z) = (3v \otimes r_0(\mathbf{b}_Z) + 2u \otimes r_0(\mathbf{b}_Z)) \\ + (2u \otimes r_1(\mathbf{b}_Z) + 2v \otimes r_1(\mathbf{b}_Z)) + 2v \otimes r_2(\mathbf{b}_Z).\end{aligned}$$

Por lo tanto,

$$\begin{aligned}\nu^{\otimes 2}(\varphi(2\mathbf{b}_Z) - \varphi(\mathbf{b}_Z)) = \nu^{\otimes 2}(3v \otimes r_0(\mathbf{b}_Z) + 2u \otimes r_0(\mathbf{b}_Z)) \\ + \nu^{\otimes 2}(2u \otimes r_1(\mathbf{b}_Z) + 2v \otimes r_1(\mathbf{b}_Z)) + \nu^{\otimes 2}(2v \otimes r_2(\mathbf{b}_Z)).\end{aligned}$$

Debido a la naturaleza de los vectores $u = (0,1)$, $v = (1,1)$ y $\mathbf{b}_Z = (0, \ldots, 0, z_{n-1})$,

$$\begin{aligned}\nu^{\otimes 2}(3v \otimes r_0(\mathbf{b}_Z) + 2u \otimes r_0(\mathbf{b}_Z)) &= \nu(3v \otimes r_0(\mathbf{b}_Z)), \\ \nu^{\otimes 2}(2u \otimes r_1(\mathbf{b}_Z) + 2v \otimes r_1(\mathbf{b}_Z)) &= \nu(2u \otimes r_1(\mathbf{b}_Z)), \\ \nu^{\otimes 2}(2v \otimes r_2(\mathbf{b}_Z)) &= \nu(2v \otimes r_2(\mathbf{b}_Z)).\end{aligned}$$

Note que $2v \otimes r_0(\mathbf{b}_Z) = \varphi(2^2\mathbf{b}_Z)$. Así,

$$\nu^{\otimes 2}(\varphi(2\mathbf{b}_Z) - \varphi(\mathbf{b}_Z)) = \nu(\varphi(\mathbf{b}_Z)) + \nu(\varphi(2^2\mathbf{b}_Z)).$$

Consecuentemente,

$$\begin{aligned}\nu^{\otimes 2}(\varphi(7\mathbf{b}_Z)) &= \nu(\varphi(\mathbf{b}_Z)) + \nu(\varphi(2^2\mathbf{b}_Z)) + \nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) \\ &= \nu(\varphi(\mathbf{b}_Z)) + \nu(\varphi(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)).\end{aligned}$$

Por lo tanto, al sustituir las expresiones anteriores, obtenemos

$$\begin{aligned}(\varphi \circ \nu_3)(Z) &= \nu(\varphi(\mathbf{a})) + \nu(\varphi(\mathbf{b}_Z)) + \nu(\varphi(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) \\ &= \nu(\varphi(Z)) + \nu(\varphi(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)),\end{aligned}$$

tal como queríamos demostrar. □

Una aplicación inmediata del Teorema 6.3.8 nos permite dar una segunda caracterización de los códigos 3-cíclicos sobre $\mathbb{Z}_8$ a través de su imagen con respecto a la isometría φ.

Teorema 6.3.9. *Sea $n \geq 1$ un entero. Las siguientes afirmaciones son equivalentes*

(1) $\mathscr{C} \subseteq \mathbb{Z}_8^n$ es un código 3-cíclico (no necesariamente lineal);

(2) $\varphi(\mathscr{C}) \subseteq \mathbb{Z}_4^{2n}$ es un código (no necesariamente lineal) tal que

$$\nu(c) + \widehat{d} \in \varphi(\mathscr{C}), \qquad \forall\, c \in \varphi(\mathscr{C})$$

donde $\widehat{d} = (1,1) \otimes (2,0,\ldots,0)$ si y sólo si $t \in \{(3,3),(1,1)\}$, y t es el vector obtenido al concatenar en orden las coordenadas de c con subíndice en el conjunto $\{n-1, 2n-1\}$. En caso contrario, $\widehat{d} = (0)_{2n} \in \mathbb{Z}_4^{2n}$.

Demostración. Sea $\mathbf{b}_Z = (0,\ldots,0,z_{n-1}) \in \mathbb{Z}_8^n$. Entonces $2^2\mathbf{b}_Z = 2^2 r_0(\mathbf{b}_Z)$ y $2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z = 2^2 r_0(\mathbf{b}_Z) * r_1(\mathbf{b}_Z)$. Así,

$$2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z = 2^2(r_0(\mathbf{b}_Z) + r_0(\mathbf{b}_Z) * r_1(\mathbf{b}_Z)).$$

A partir de aquí, es fácil verficar que $2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z = (0)_{n-1}$ si y sólo si $z_{n-1} \in \{1,5\}$. Si $z_{n-1} \in \{1,5\}$, entonces

$$\varphi(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z) = (1,1) \otimes (0,\ldots,0,2) \in \mathbb{Z}_4^{2n}$$

y, por lo tanto,

$$\nu(\varphi(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) = (1,1) \otimes (2,0,\ldots,0).$$

Por otra parte, si $Z = (z_0,\ldots,z_{n-2},z_{n-1}) \in \mathbb{Z}_8^n$, note que la imagen bajo φ de la coordenada z_{n-1} del vector Z puede recuperarse al concatenar en orden las coordenada de $\varphi(Z)$ con subíndice en el conjunto $\{n-1, 2n-1\}$. Ya que $\varphi(1) = (1,1)$ y $\varphi(5) = (3,3)$, entonces

$$\widehat{d} = \nu(\varphi(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) = (1,1) \otimes (2,0,\ldots,0)$$

si y sólo si $t \in \{(1,1),(3,3)\}$, donde t es el vector obtenido al concatenar en orden las coordenadas de $\varphi(Z)$ con subíndice en $\{n-1, 2n-1\}$. De este modo, el resultado se sigue de aplicar el Teorema 6.3.8 y de las observaciones realizadas en esta demostración. □

En los Capítulos 2 y 3 analizamos varias relaciones que satisfacen las isometrías φ, Φ de Gray y la isometría $\phi : \mathbb{Z}_4^m \to \mathbb{F}_2^{2m}$ clásica de Gray. En particular, en el Lema 2.3.4 se demostró que

$$\phi(Y+2Z) = \phi(Y) \oplus \phi(2Z), \qquad Y,Z \in \mathbb{Z}_4^m$$

Otra propiedad importante de la isometría clásica de Gray fue establecida en la Proposición 3.4.3:

$$\phi \circ \nu = \sigma \circ \phi,$$

donde σ y ν son, respectivamente, el corrimiento cíclico y negacíclico sobre $\mathbb{F}_2^{2m}$ y $\mathbb{Z}_4^m$. Finalmente, debemos recordar que las isometrías φ, ϕ y Φ están relacionadas por medio de la identidad $\Phi = \phi \circ \varphi$.

El siguiente resultado caracteriza a los códigos 3-cíclicos sobre $\mathbb{Z}_8$ en términos de sus imágenes de Gray, por lo que es una aportación más de este trabajo.

Teorema 6.3.10. *Sea $n \geq 1$ un entero y $\mathscr{C} \subseteq \mathbb{Z}_8^n$ un código. Las siguientes afirmaciones son equivalentes:*

(1) $\mathscr{C} \subseteq \mathbb{Z}_8^n$ es un código 3-cíclico (no necesariamente lineal);

(2) $\Phi(\mathscr{C}) \subseteq \mathbb{F}_2^{4n}$ es un código (no necesariamente lineal) tal que

$$\sigma(c) + \widehat{d_1} \in \Phi(\mathscr{C}), \qquad \forall\, c \in \Phi(\mathscr{C})$$

donde $\widehat{d_1} = (1,1,1,1) \otimes (1,0,\ldots,0)$ si y sólo si $t \in \{(0,0,1,1),(1,1,0,0)\}$, y t es el vector obtenido al concatenar en orden las coordenadas de c con subíndice en $\{n-1, 2n-1, 3n-1, 4n-1\}$. En caso contrario, $\widehat{d_1} = (0)_{4n} \in \mathbb{F}_2^{4n}$.

Demostración. Supongamos que $\mathscr{C}$ es un código 3-cíclico y sea $e \in \Phi(\mathscr{C})$. Como $\Phi(\mathscr{C}) = \phi(\varphi(\mathscr{C}))$, existe $c \in \varphi(\mathscr{C})$ tal que $e = \phi(c)$. Aplicando el corrimiento cíclico a e, obtenemos

$$\sigma(e) = \sigma(\phi(c)) = \phi(\nu(c)).$$

Sea $\widehat{d}$ como en el Teorema 6.3.9, entonces $\widehat{d} \in (2\mathbb{Z}_4)^{2n}$ y, por lo tanto, $\widehat{d} + \widehat{d} = (0)_{2n}$. Así,

$$\sigma(e) = \phi(\nu(c) + \widehat{d} + \widehat{d}) = \phi(\nu(c) + \widehat{d}) \oplus \phi(\widehat{d}),$$

o equivalentemente,

$$\sigma(e) \oplus \phi(\widehat{d}) = \phi(\nu(c) + \widehat{d} + \widehat{d}) = \phi(\nu(c) + \widehat{d}).$$

Por el Teorema 6.3.9, $\nu(c) + \widehat{d} \in \varphi(\mathscr{C})$ y, por lo tanto, $\phi(\nu(c) + \widehat{d}) \in \Phi(\mathscr{C}) = \phi(\varphi(\mathscr{C}))$. Por otra parte, si $\widehat{d} = (0)_{2n} \in \mathbb{Z}_4^{2n}$, entonces $\phi(\widehat{d}) = (0)_{4n} \in \mathbb{F}_2^{4n}$. En caso contrario,

$$\begin{aligned} \phi(\widehat{d}) &= \phi((1,1) \otimes (2,0,\ldots,0)) = (1,1) \otimes (1,1) \otimes (1,0,\ldots,0) \\ &= (1,1,1,1) \otimes (1,0,\ldots,0) \in \mathbb{F}_2^{4n}. \end{aligned}$$

Ésto sucede si y sólo si el vector $t' = \varphi(z_{n-1}) \in \{(1,1),(3,3)\}$, donde $c = \varphi(z_0,\ldots,z_{n-1})$. De este modo, por la inyectividad de ϕ, $\phi(\widehat{d}) = (1,1,1,1) \otimes (1,0,\ldots,0)$ si y sólo si

$$t = \phi(t') = \Phi(z_{n-1}) \in \{\phi(1,1),\phi(3,3)\} = \{(0,0,1,1),(1,1,0,0)\}.$$

Para finalizar esta parte de la demostración, basta observar que $\Phi(z_{n-1})$ puede recuperarse al concatenar en orden las coordenadas de $e = \phi(c) = \Phi(z_0,\ldots,z_{n-1})$ con subíndice en $\{0, n-1, 2n-1, 3n-1\}$.
Recíprocamente, supongamos que la afirmación (2) del Teorema 6.3.10 es cierta, y demostremos que $\mathscr{C}$ es un código 3-cíclico. Sea $Z \in \mathscr{C}$. Entonces $c = \varphi(Z) \in \varphi(\mathscr{C})$ y $\phi(c) \in \Phi(\mathscr{C})$. Consecuentemente,

$$\sigma(\phi(c)) + \widehat{d_1} \in \Phi(\mathscr{C}).$$

Observe que $\sigma(\phi(c)) = \phi(\nu(c))$. También, $\widehat{d_1} = \phi(\widehat{d})$, donde $\widehat{d}$ es definido como en el Teorema 6.3.9. Consecuentemente,

$$\sigma(\phi(c)) + \widehat{d_1} = \phi(\nu(c)) + \phi(\widehat{d}) = \phi(\nu(c) + \widehat{d}) \in \Phi(\mathscr{C}),$$

donde la última igualdad se debe a que $\widehat{d} \in (2\mathbb{Z}_4)^{2n}$. A raíz de la inyectividad de la isometría clásica de Gray, lo anterior implica que $\nu(c) + \widehat{d} \in \varphi(\mathscr{C})$, lo que por el Teorema 6.3.9 significa que $\mathscr{C}$ es 3-cíclico. □

Ejemplo 6.3.11. Consideremos nuevamente el código $\mathscr{C} \subseteq \mathbb{Z}_8^3$ cuyos elementos son:

1726	2172	2635	3562
5621	6217	6356	7263

Como se ha señalado en el ejemplo 6.3.4, este código es 3-cíclico. Verifiquemos entonces que $\Phi(\mathscr{C})$ satisface la afirmación (2) del Teorema 6.3.10. Preservando el orden en que se han listado los elementos de $\mathscr{C}$, $\Phi(\mathscr{C})$ es el siguiente código:

0101 0010 1001 1110	0010 1001 0100 1111	0101 1011 0110 1000	0110 1101 1010 0001
1100 1010 0101 0011	1001 0100 1010 0111	1011 0110 1101 0000	1010 0101 0011 1100

Ahora aplicamos el corrimiento cíclico a cada uno de estos vectores, obteniendo:

0010 1001 0100 1111	1001 0100 1010 0111	0010 1101 1011 0100	1011 0110 1101 0000
1110 0101 0010 1001	1100 1010 0101 0011	0101 1011 0110 1000	0101 0010 1001 1110

Los correspondientes vectores t de los elementos $e \in \Phi(\mathscr{C})$ son:

1010	0101	1100	0101
0011	1001	1010	0110

En consecuencia, los vectores $\widehat{d_1}$ son:

0000 0000 0000 0000 0000 0000 0000 0000 1000 1000 1000 1000 0000 0000 0000 0000
1000 1000 1000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

Sumando éstos con los corrimientos cíclicos de los elementos de $\Phi(\mathscr{C})$, obtenemos:

0010 1001 0100 1111 1001 0100 1010 0111 1010 0101 0011 1100 1011 0110 1101 0000
0110 1101 1010 0001 1100 1010 0101 0011 0101 1011 0110 1000 0101 0010 1001 1110

Observemos que hemos obtenido de nuevo la imagen de Gray de $\mathscr{C}$ con sus vectores dispuestos en otro orden. De este modo, hemos probado que $\Phi(\mathscr{C})$ satisface la propiedad (2) establecida en el Teorema 6.3.10.

Algunos casos particulares de los resultados enunciados en esta sección son mencionados a continuación.

Primero supongamos que $\mathscr{C} \subseteq (2\mathbb{Z}_8)^n$. Entonces $\varphi(\mathscr{C}) \subseteq (2\mathbb{Z}_4)^n$ y, por lo tanto, el vector $\widehat{d}$ del Teorema 6.3.9 es igual al vector cero para todo $c \in \varphi(\mathscr{C})$. Como consecuencia de esta observación, obtenemos el siguiente resultado.

Proposición 6.3.12. *Sea $\mathscr{C} \subseteq \mathbb{Z}_8^n$ un código. Entonces las siguientes afirmaciones son equivalentes.*

(1) $\mathscr{C}$ es un código 3-cíclico (no necesariamente lineal),

(2) $\varphi(\mathscr{C}) \subseteq (2\mathbb{Z}_4^{2n})$ es un código cíclico y negacíclico a la vez,

(3) $\Phi(\mathscr{C})$ es un código binario cíclico de longitud $4n$. Asimismo, $\Phi(\mathscr{C})$ es un código casi-cíclico de índice 2 y longitud $4n$ sobre $\mathbb{F}_2$.

Similarmente a la Proposición 6.3.7 tenemos lo siguiente.

Proposición 6.3.13. *Supongamos que $\mathscr{C}$ es un código tal que $2^2\mathbf{b}_Z \in \mathscr{C}$ y $\varphi(\mathscr{C})$ es lineal. Entonces las siguientes afirmaciones son equivalentes*

(1) $\mathscr{C}$ es un código 3-cíclico (no necesariamente lineal),

(2) $\varphi(\mathscr{C})$ es un código negacíclico de longitud $2n$ sobre $\mathbb{Z}_4$,

(3) $\Phi(\mathscr{C})$ es un código cíclico de longitud $4n$ sobre $\mathbb{F}_2$.

Finalmente, supongamos que $\mathscr{C}$ es un código lineal sobre $\mathbb{Z}_8$ tal que $2^2\mathbf{b}_Z \in \mathscr{C}$ para todo $Z \in \mathscr{C}$. Entonces $2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z \in \mathscr{C}$ y, por lo tanto, $Z + 2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z \in \mathscr{C}$ para todo $Z \in \mathscr{C}$. En consecuencia,

$$\varphi(Z + 2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z) = \varphi(Z) + \varphi(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z) \in \varphi(\mathscr{C}), \qquad \forall Z \in \mathscr{C}.$$

Si, suponemos además que $\mathscr{C}$ es 3-cíclico, por el Teorema 6.3.9 tenemos que

$$\nu(\varphi(Z)) + \nu(\varphi(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) + \widehat{c} \in \varphi(\mathscr{C}),$$

donde $c = \varphi(Z)$. Como $\widehat{c} = \nu(\varphi(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z))$,

$$\nu(\varphi(Z)) \in \varphi(\mathscr{C}).$$

Por lo tanto, lo anterior demuestra que si $\mathscr{C}$ es un código lineal tal que es 3-cíclico y $2^2\mathbf{b}_Z \in \mathscr{C}$ para todo $Z \in \mathbb{Z}$, entonces $\varphi(\mathscr{C})$ es un código negacíclico.
Recíprocamente, supongamos que $\mathscr{C}$ es un código lineal tal que $2^2\mathbf{b}_Z \in \mathscr{C}$ para todo $Z \in \mathbb{Z}$ y $\varphi(\mathscr{C})$ es un código negacíclico. Entonces deseamos establecer que $\mathscr{C}$ es un código 3-cíclico. Sea $Z \in \mathscr{C}$ y probemos que $\nu_3(Z) \in \mathscr{C}$. Por el Teorema 6.3.8,

$$\varphi(\nu_3(Z)) = \nu(\varphi(Z)) + \nu(\varphi(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) \in \varphi(\mathscr{C}),$$

o equivalentemente,

$$\varphi(\nu_3(Z)) + \nu(\varphi(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) = \varphi(Z) \in \varphi(\mathscr{C}).$$

Ya que $2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z \in (4\mathbb{Z}_8)^n$ y este vector pertence a $\mathscr{C}$, entonces

$$\nu(\varphi(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) = \varphi(\nu_3(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) \in \varphi(\mathscr{C}).$$

Así,

$$\varphi(\nu_3(Z) + \nu_3(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) \in \varphi(\mathscr{C}).$$

Debido a la inyectividad de φ, $\nu_3(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z) \in \mathscr{C}$ y $\nu_3(Z) + \nu_3(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z) \in \mathscr{C}$. Finalmente, como $\mathscr{C}$ es lineal, $\nu_3(Z) \in \mathscr{C}$, tal como queríamos demostrar.

Mediante argumentos similares podemos demostrar que un código $\mathscr{C}$ lineal sobre $\mathbb{Z}_8$ tal que $2^2\mathbf{b}_Z$ es 3-cíclico si y sólo si $\Phi(\mathscr{C})$ es un código cíclico binario de longitud $4n$. De este modo, los argumentos previos constituyen una demostración del siguiente resultado.

Proposición 6.3.14. *Sea $\mathscr{C}$ un código lineal de longitud n sobre $\mathbb{Z}_8$ tal que $2^2\mathbf{b}_Z \in \mathscr{C}$ para todo $Z \in \mathscr{C}$. Las siguientes son equivalentes.*

(1) $\mathscr{C}$ es un código 3-cíclico,

(2) $\varphi(\mathscr{C})$ *es un código negacíclico de longitud* $2n$ *sobre* $\mathbb{Z}_4$,

(3) $\Phi(\mathscr{C})$ *es un código cíclico de longitud* $4n$ *sobre* $\mathbb{F}_2$.

La Proposición anterior da una explicación satisfactoria a lo que se observó en el ejemplo particular de la Sección 6.2. Asimismo, retomando la información del Cuadro 6.1, recordemos que hemos marcado con el símbolo ✓aquellos códigos 3-cíclicos de longitud 3 sobre $\mathbb{Z}_8$ cuya imagen de Gray es un código cíclico binario. No es difícil verificar que en todos esos códigos $2^2\mathbf{b}_Z \in \mathscr{C}$ y, por lo tanto, estos códigos 3-cíclicos satisfacen son tales que $\varphi(\mathscr{C})$ es un código negacíclico.

Con el fin de ilustrar los resultados anteriores con códigos de otras longitudes, en el Apéndice *A* se han construido tablas de códigos cíclicos lineales de longitudes $3, 5$ y 7 sobre $\mathbb{Z}_8$. Se han senãlado con el símbolo ✓aquellos códigos cíclicos que son a su vez códigos 5-cíclicos sobre $\mathbb{Z}_8$. Estos códigos contienen al vector $2^2\mathbf{b}_Z$ para todo vector Z en el código (ver la demostración de la Proposición 4.5.6).

6.4. Imágenes de códigos negacíclicos

A continuación examinaremos algunas propiedades de los códigos δ_2-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, donde $k = 2$. Con esta consideración en mente, los códigos δ_2-cíclicos son precisamente los códigos 7-cíclicos sobre $\mathbb{Z}_8$. Ya que en $\mathbb{Z}_8$, $7 = -1$, llamaremos a los códigos 7-cíclicos sobre $\mathbb{Z}_8$ *códigos negacíclicos*, lo que es consistente con la terminología introducida en [7,54,55] para describir aquellos códigos sobre un campo ([7]) o el anillo $\mathbb{Z}_4$ ([54,55]) que son invariantes bajo el corrimiento negacíclico, mismo que se definió como

$$\nu(z_0, \ldots, z_{n-2}, z_{n-1}) \mapsto (-z_{n-1}, z_0, \ldots, z_{n-2}).$$

De hecho, para continuar siendo congruentes con la notación, denotaremos al corrimiento 7-cíclico ν_7 sobre $\mathbb{Z}_8^n$ como ν, puesto que $\nu_7(Z) = \nu(Z)$ para todo $Z \in \mathbb{Z}_8^n$. De este modo, a lo largo de esta sección y de las siguientes, ν denota al corrimiento negacíclico sobre $\mathbb{Z}_8^n$, o bien al corrimiento negacíclico $\mathbb{Z}_4^n$. Será claro a partir del contexto el dominio de la función ν.

Por otro parte, vale la pena señalar que de forma natural introduciremos tres caracterizaciones de dichos códigos. La primera es análoga a la descripción de los códigos 3-cíclicos dada en el Teorema 6.3.3. La segunda, es similar a la de los códigos δ_1-cíclicos sobre $\mathbb{Z}_{2^{k+1}}$, con $k \geq 3$; y la tercera se ve relacionada con códigos negacíclicos sobre $\mathbb{Z}_4$; siendo esta última una aportación más de este trabajo. Como consecuencia de la tercera caracterizacón, obtendremos propiedades de ciclícidad de la imagen de Gray de los códigos negacíclicos sobre $\mathbb{Z}_8$.

6.4.1. Imágenes sobre $\mathbb{Z}_4$

En este apartado introduciremos tres caracterizaciones de la imagen de códigos negacíclicos sobre $\mathbb{Z}_8$, con respecto a sus imágenes bajo la isometría φ. Esencialmente estas caracterizaciones se derivan del análisis de la siguiente relación (Teorema 3.3.3)

$$(\varphi \circ \nu)(Z) = (\nu^{\otimes 2} \circ \varphi \circ \eta_3)(Z),$$

donde η_3 es el automorfismo sobre $\mathbb{Z}_8^n$ que multiplica por 3 la última coordenada de Z. Sea $Z = \mathbf{a} + \mathbf{b}_Z$, con $\mathbf{a} = (z_0, \ldots, z_{n-2}, 0)$ y $\mathbf{b}_Z = Z - \mathbf{a} = (0, \ldots, 0, z_{n-1})$. Entonces

$$(\varphi \circ \nu)(Z) = (\nu^{\otimes 2} \circ \varphi \circ \eta_3)(\mathbf{a} + \mathbf{b}_Z) = (\nu^{\otimes 2} \circ \varphi)(\mathbf{a} + 3\mathbf{b}_Z) = \nu^{\otimes 2}(\varphi(\mathbf{a})) + \nu^{\otimes 2}(\varphi(3\mathbf{b}_Z)).$$

Del Lema 5.2.5 deducimos que

$$\nu^{\otimes 2}(\varphi(\mathbf{a})) = \nu(\varphi(\mathbf{a})) = (\nu \otimes \sigma)(\varphi(Z)) = \widetilde{\pi}(\sigma \otimes \nu)(\varphi(Z)),$$

donde $\widetilde{\pi}$ es la permutación sobre $\mathbb{Z}_4^{2n}$ inducida por la permutación $\pi = (0, n)$. Por otro lado,

$$\nu^{\otimes 2}(\varphi(3\mathbf{b}_Z)) = \nu^{\otimes 2}(\varphi(\mathbf{b}_Z) + \varphi(2\mathbf{b}_Z)) + \nu^{\otimes 2}(\varphi(2^2\mathbf{b}_Z \otimes 2\varphi(\mathbf{b}_Z))).$$

Como $\varphi(2^2\mathbf{b}_Z \otimes 2\mathbf{b}_Z) = (1,1) \otimes (0, \ldots, 0, 2^2 r_0(z_{n-1}) r_1(z_{n-1}))$, se tiene que

$$\begin{aligned} \nu^{\otimes 2}(\varphi(2^2\mathbf{b}_Z \otimes 2\mathbf{b}_Z)) &= \nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) \\ &= (\nu \otimes \sigma)(\varphi(2^2\mathbf{b}_Z \otimes 2\mathbf{b}_Z)) \\ &= \widetilde{\pi}(\sigma \otimes \nu)(\varphi(\mathscr{C})). \end{aligned}$$

De este modo, tal como ocurrió en la sección 6.3, la parte interesante del análisis reside en el término

$$\nu^{\otimes 2}(\varphi(\mathbf{b}_Z) + \varphi(2\mathbf{b}_Z)).$$

A partir de la definición de φ se sigue que

$$\begin{aligned} \varphi(\mathbf{b}_Z) + \varphi(2\mathbf{b}_Z)) = (v \otimes r_0(\mathbf{b}_Z) + 2u \otimes r_0(\mathbf{b}_Z)) \\ + (2u \otimes r_1(\mathbf{b}_Z) + 2v \otimes r_1(\mathbf{b}_Z)) + 2v \otimes r_2(\mathbf{b}_Z). \end{aligned}$$

Por lo tanto,

$$\begin{aligned} \nu^{\otimes 2}(\varphi(\mathbf{b}_Z) + \varphi(2\mathbf{b}_Z)) = \nu^{\otimes 2}(v \otimes r_0(\mathbf{b}_Z) + 2u \otimes r_0(\mathbf{b}_Z)) \\ + \nu^{\otimes 2}(2u \otimes r_1(\mathbf{b}_Z) + 2v \otimes r_1(\mathbf{b}_Z)) + \nu^{\otimes 2}(2v \otimes r_2(\mathbf{b}_Z)). \quad (6.2) \end{aligned}$$

Debido a la naturaleza de los vectores involucrados en las expresiones anteriores, tenemos lo siguiente

$$\nu^{\otimes 2}(3v\otimes r_0(\mathbf{b}_Z)+2u\otimes r_0(\mathbf{b}_Z))=\begin{cases}\nu(v\otimes r_0(\mathbf{b}_Z)),\\(\nu\otimes\sigma)(v\otimes r_0(\mathbf{b}_Z)),\\\widetilde{\pi}(\sigma\otimes\nu)(v\otimes r_0(\mathbf{b}_Z)),\end{cases}$$

$$\nu^{\otimes 2}(2u\otimes r_1(\mathbf{b}_Z)+2v\otimes r_1(\mathbf{b}_Z))=\begin{cases}\nu(2u\otimes r_1(\mathbf{b}_Z)),\\(\nu\otimes\sigma)(2u\otimes r_1(\mathbf{b}_Z)),\\\widetilde{\pi}(\sigma\otimes\nu)(2u\otimes r_1(\mathbf{b}_Z)),\end{cases}$$

y

$$\nu^{\otimes 2}(2v\otimes r_2(\mathbf{b}_Z))=\begin{cases}\nu(2v\otimes r_2(\mathbf{b}_Z)),\\(\nu\otimes\sigma)(2v\otimes r_2(\mathbf{b}_Z)),\\\widetilde{\pi}(\sigma\otimes\nu)(2v\otimes r_2(\mathbf{b}_Z)).\end{cases}$$

Note que $2v\otimes r_0(\mathbf{b}_Z)=\varphi(2^2\mathbf{b}_Z)$. Así, la última terna puede ser expresada como

$$\nu^{\otimes 2}(2v\otimes r_2(\mathbf{b}_Z))=\begin{cases}\nu(\varphi(2^2\mathbf{b}_Z)),\\(\nu\otimes\sigma)(\varphi(2^2\mathbf{b}_Z)),\\\widetilde{\pi}(\sigma\otimes\nu)(\varphi(2^2\mathbf{b}_Z)).\end{cases}$$

Consecuentemente, al sustituir en la relación (6.2) obtenemos las siguientes expresiones:

$$\nu^{\otimes 2}(\varphi(\mathbf{b}_Z)+\varphi(2\mathbf{b}_Z))=\begin{cases}\nu(\varphi(\mathbf{b}_Z)),\\(\nu\otimes\sigma)(\varphi(\mathbf{b}_Z)),\\\widetilde{\pi}(\sigma\otimes\nu)(\varphi(\mathbf{b}_Z)).\end{cases}$$

Por lo tanto,

$$\nu^{\otimes 2}(\varphi(3\mathbf{b}_Z))=\begin{cases}\nu(\varphi(\mathbf{b}_Z))+\nu(\varphi(2^2\mathbf{b}_Z\odot 2\mathbf{b}_Z)),\\(\nu\otimes\sigma)(\varphi(\mathbf{b}_Z))+(\nu\otimes\sigma)(\varphi(2^2\mathbf{b}_Z\odot 2\mathbf{b}_Z)),\\\widetilde{\pi}(\sigma\otimes\nu)(\varphi(\mathbf{b}_Z))+\widetilde{\pi}(\nu\otimes\sigma)(\varphi(2^2\mathbf{b}_Z\odot 2\mathbf{b}_Z)).\end{cases}$$

De este modo,

$$(\varphi\circ\nu)(Z)=\begin{cases}\nu(\varphi(\mathbf{a}))+\nu(\varphi(\mathbf{b}_Z))+\nu(\varphi(2^2\mathbf{b}_Z\odot 2\mathbf{b}_Z)),\\(\nu\otimes\sigma)(\varphi(\mathbf{a}))+(\nu\otimes\sigma)(\varphi(\mathbf{b}_Z))+(\nu\otimes\sigma)(\varphi(2^2\mathbf{b}_Z\odot 2\mathbf{b}_Z)),\\\widetilde{\pi}(\nu\otimes\sigma)(\varphi(\mathbf{a}))+\widetilde{\pi}(\sigma\otimes\nu)(\varphi(\mathbf{b}_Z))+\widetilde{\pi}(\nu\otimes\sigma)(\varphi(2^2\mathbf{b}_Z\odot 2\mathbf{b}_Z)).\end{cases}$$

Finalmente, por el Lema 3.3.1,

$$(\varphi\circ\nu)(Z)=\begin{cases}\nu(\varphi(Z))+\nu(\varphi(2^2\mathbf{b}_Z\odot 2\mathbf{b}_Z)),\\(\nu\otimes\sigma)(\varphi(Z)+(\nu\otimes\sigma)(\varphi(2^2\mathbf{b}_Z\odot 2\mathbf{b}_Z)),\\\widetilde{\pi}(\nu\otimes\sigma)(\varphi(Z))+\widetilde{\pi}(\nu\otimes\sigma)(\varphi(2^2\mathbf{b}_Z\odot 2\mathbf{b}_Z)).\end{cases}$$

Es a partir de estas relaciones que derivamos las tres caracterizaciones de los códigos negacíclicos sobre $\mathbb{Z}_8$.

Teorema 6.4.1. *Sea $n \geq 1$ un entero, $\widetilde{\pi}$ la permutación sobre $\mathbb{Z}_4^{2n}$ inducida por la permutación $\pi = (0,4)$, y $\mathscr{C}$ un código de longitud n sobre $\mathbb{Z}_8$. Las siguientes afirmaciones son equivalentes.*

(1) $\mathscr{C}$ es un código negacíclico sobre $\mathbb{Z}_8$,

(2) $\nu(c) + \widehat{c} \in \varphi(\mathscr{C})$, para todo $c \in \varphi(\mathscr{C})$,

(3) $(\nu \otimes \sigma)(c) + \widehat{c} \in \varphi(\mathscr{C})$, para todo $c \in \varphi(\mathscr{C})$,

(4) $\widetilde{\pi}(\nu \otimes \sigma)(c) + \widehat{c} \in \varphi(\mathscr{C})$, para todo $c \in \varphi(\mathscr{C})$,

donde $\widehat{c} = (1,1) \otimes (2,0,\ldots,0)$ si y sólo si $t \in \{(1,3),(3,1)\}$, y t es el vector obtenido al concatenar en orden las coordenadas de c con subíndice en el conjunto $\{n-1, 2n-1\}$. De otro modo, $\widehat{c} = (0)_{2n} \in \mathbb{Z}_4^{2n}$.

Demostración. Veamos que (1) implica (2). Dado que $\mathscr{C}$ es un código negacíclico,

$$\begin{aligned}\varphi(\mathscr{C}) &= \varphi(\nu(\mathscr{C})) = \{\varphi(\nu(Z)) \,|\, Z \in \mathscr{C}\} \\ &= \{\nu(\varphi(Z)) + \nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) \,|\, \varphi(Z) \in \varphi(\mathscr{C})\}.\end{aligned}$$

Sea $c = \varphi(Z)$. Entonces al concatenar en orden las coordenadas de c con subíndice en el conjunto $\{n-1, 2n-1\}$ obtenemos el vector $\varphi(z_{n-1})$, donde $Z = (z_0, \ldots, z_{n-1})$. Ahora, en la Sección 6.3.2, demostramos que $\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z) = v \otimes (0,\ldots,0,2) \in \mathbf{Z}_4^{2n}$ si y sólo si $z_{n-1} = 3,7$. Dado que φ es una función inyectiva, $\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z) = v \otimes (0,\ldots,0,2)$ si y sólo si $\varphi(z_{n-1}) \in \{\varphi(3), \varphi(7)\} = \{(1,3),(3,1)\}$. De otro modo, $\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z) = (0)_{2n}$. Por lo tanto,

$$\varphi(\mathscr{C}) = \{\nu(c) + \widehat{c} \,|\, c \in \varphi(\mathscr{C})\},$$

donde $\widehat{c} = (1,1) \otimes (2,0,\ldots,0)$ si y sólo si $t \in \{(1,3),(3,1)\}$, y t es el vector obtenido al concatenar en orden las coordenadas de c con subíndice en el conjunto $\{n-1, 2n-1\}$. De otro modo, $\widehat{c} = (0)_{2n} \in \mathbb{Z}_4^{2n}$.
Veamos ahora que (2) implica (1). Sea $Z \in \mathscr{C}$ y probemos que $\nu(Z) \in \mathscr{C}$. Como $Z \in \mathscr{C}$, entonces $c = \varphi(Z) \in \varphi(\mathscr{C})$ y, por lo tanto,

$$\nu(c) + \widehat{c} = \nu(\varphi(Z)) + \widehat{c} \in \varphi(\mathscr{C}).$$

En virtud del análisis del vector $\widehat{c}$, podemos sustituir $\widehat{c}$ por $\nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z))$. Así,

$$\varphi(\nu(Z)) = \nu(\varphi(Z)) + \nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) \in \varphi(\mathscr{C}).$$

Debido a la inyectividad de φ, la relación anterior implica que $\nu(Z) \in \mathscr{C}$, tal como queríamos demostrar.
Similarmente, se prueba que (1) es equivalente a (3) y (4). □

Algunos casos particulares del teorema anterior, similares a los que se presentaron en la Sección 6.3, pueden ser establecidos fácilmente para la familia de códigos negacíclicos sobre $\mathbb{Z}_8$. Para obtenerlos, basta reemplazar la condición de ser 3-cíclico por la de negacíclico; razón por la cual no los incluimos en este apartado.

Después de haber caracterizado a los códigos negacíclicos sobre $\mathbb{Z}_8$ en términos de sus imágenes bajo φ, en la siguiente subsección presentaremos una caracterización más de estos códigos con respecto a la sus imágenes de Gray.

6.4.2. Imágenes de Gray

En esta subsección estableceremos que la imagen de Gray de un código negacíclico sobre $\mathbb{Z}_8$ es un código cíclico binario, módulo una traslación de un vector que denotamos por $\widehat{d_2}$. Este resultado, enunciado en el Teorema 6.4.2, es similar al Teorema 6.3.10. Pero más aún, puede ser considerado como una generalización de [54, Teorema 3.5], en el que se establece que la imagen clásica de Gray de un código negacíclico sobre $\mathbb{Z}_4$ es un código cíclico binario. Vale la pena mencionar que el Teorema 3.5 de [54] es una de las aportaciones más importantes de ese trabajo.

Teorema 6.4.2. *Sea $n \geq 1$ un entero y $\mathscr{C} \subseteq \mathbb{Z}_8^n$ un código. Las siguientes afirmaciones son equivalentes.*

(1) $\mathscr{C} \subseteq \mathbb{Z}_8^n$ es un código negacíclico (no necesariamente lineal);

(2) $\Phi(\mathscr{C}) \subseteq \mathbb{F}_2^{4n}$ es un código (no necesariamente lineal) tal que

$$\sigma(c) + \widehat{d_2} \in \Phi(\mathscr{C}), \qquad \forall\, c \in \Phi(\mathscr{C})$$

donde $\widehat{d_2} = (1,1,1,1) \otimes (1,0,\ldots,0)$ si y sólo si $t \in \{(0,1,1,0),(1,0,0,1)\}$, y t es el vector obtenido al concatenar en orden las coordenadas de c con subíndice en $\{n-1, 2n-1, 3n-1, 4n-1\}$. En caso contrario, $\widehat{d_2} = (0)_{4n} \in \mathbb{F}_2^{4n}$.

Demostración. Es similar a la demostración del Teorema 6.3.10. □

6.5. Códigos consta-cíclicos lineales sobre $\mathbb{Z}_8$

El propósito de esta sección es analizar algunos resultados que conciernen a los códigos 3-cíclicos y negacíclicos lineales de longitud n impar sobre $\mathbb{Z}_8$, y sus relaciones entre ellos y los códigos cíclicos de longitud n sobre el mismo anillo.

Recuerde que si $\gamma \in U(\mathbb{Z}_8) = \{1,3,5,7\}$ y $n \geq 1$ es un entero, entonces η_γ denota al $\mathbb{Z}_8$-automorfismo definido sobre $\mathbb{Z}_8^n$ como,

$$\eta_\gamma : (z_0, \ldots, z_{n-2}, z_{n-1}) \mapsto (z_0, \ldots, z_{n-2}, \gamma z_{n-1}).$$

Asimismo, note que en $\mathbb{Z}_8$, $5 \cdot 3 = 7$ y $5 \cdot 7 = 3$, lo cual corresponde a las relaciones $\lambda\,\delta_1 = \delta_2$ y $\lambda \cdot \delta_2 = \delta_1$, respectivamente, donde $\lambda = 1 + 2^k$, $\delta_1 = 1 + 2^{k-1}$, $\delta_2 = 1 + 2^{k-1} + 2^k$ y $k = 2$. Con base en estas observaciones, obtenemos las relaciones

$$\nu_3 \circ \eta_5 = \nu, \qquad \nu \circ \eta_5 = \nu_3.$$

A partir de aquí se concluye que si $\mathscr{C}$ es un código γ-cíclico, con $\gamma \in \{3,7\}$, entonces $\mathscr{C}$ es un código 5γ-cíclico si y sólo si $\eta_5(\mathscr{C}) = \mathscr{C}$. Como consecuencia de este hecho y en virtud del Teorema 3.3.4, si $\mathscr{C} \subseteq \mathbb{Z}_8^n$ es un código 3-cíclico y negacíclico a la vez, entonces

$$(\varphi \circ \eta_5)(\mathscr{C}) = (\eta_{-1}^{\otimes 2} \circ \varphi)(\mathscr{C}),$$

es decir, $\varphi(\mathscr{C})$ permanece fijo bajo la acción del $\mathbb{Z}_4$-automorfismo $\eta_{-1}^{\otimes 2}$, el cual se ha definido como

$$\eta_{-1}^{\otimes 2} : (z_0, \ldots, z_{n-2}, z_{n-1}, z_n, \ldots, z_{2n-2}, z_{2n-1}) \mapsto (z_0, \ldots, z_{n-2}, -z_{n-1}, z_n, \ldots, z_{2n-2}, -z_{2n-1}).$$

Si a lo anterior le añadimos la condición de linealidad al código $\mathscr{C}$, entonces obtenemos el siguiente resultado que caracteriza a los códigos que son 3-cíclicos y negacíclicos a la vez.

Teorema 6.5.1. *Sea $\mathscr{C} \subseteq \mathbb{Z}_8^n$ un código lineal . Las siguientes afirmaciones son equivalentes*

(1) $\mathscr{C}$ es un código 3-cíclico y negacíclico,

(2) $\varphi(\mathscr{C})$ es un código negacíclico de longitud $2n$ sobre $\mathbb{Z}_4$,

(3) $\Phi(\mathscr{C})$ es un código cíclico de longitud $4n$ sobre $\mathbb{F}_2$.

Demostración. Veamos que (1) implica (2). De este modo, supongamos que $\mathscr{C}$ es un código 3-cíclico y negacíclico a la vez. Entonces $\eta_5(\mathscr{C}) = \mathscr{C}$, es decir,

$$\eta_5(Z) = (z_0, \ldots, z_{n-2}, 5 \cdot z_{n-1}) \in \mathscr{C}, \qquad \forall\, Z = (z_0, \ldots, z_{n-2}, z_{n-1}) \in \mathscr{C}$$

Como $\mathscr{C}$ es lineal, $\eta_5(Z) - Z = (0, \ldots, 0, 4z_{n-1}) = 2^2\mathbf{b}_Z \in \mathscr{C}$, donde $\mathbf{b}_Z = (0, \ldots, 0, z_{n-1})$. Así, para todo $Z \in \mathscr{C}$, se tiene que $2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z \in \mathscr{C}$ y, en consecuencia, $w = Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z \in \mathscr{C}$. Además, siendo $\mathscr{C}$ un código negacíclico sobre $\mathbb{Z}_8$, $\nu(w) \in \mathscr{C}$.
Por otra parte,

$$\begin{aligned}(\varphi \circ \nu)(w) &= \nu(\varphi(w)) + \nu(\varphi(2^2\mathbf{b}_w \odot 2\mathbf{b}_w)) \\ &= \nu(\varphi(z) + \varphi(2^2\mathbf{b}_Z \odot \mathbf{b}_Z)) + \nu(\varphi(2^2\mathbf{b}_w \odot 2\mathbf{b}_w)) \\ &= \nu(\varphi(z)) + \nu(\varphi(2^2\mathbf{b}_Z \odot \mathbf{b}_Z)) + \nu(\varphi(2^2\mathbf{b}_w \odot 2\mathbf{b}_w))\end{aligned}$$

Ya que $2^2\mathbf{b}_w \odot 2\mathbf{b}_w = 2^2\mathbf{b}_Z \odot \mathbf{b}_Z$ y el vector $\nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z))$ tiene todas sus coordenadas en el ideal maximal de $\mathbb{Z}_4$,

$$\nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) + \nu(\varphi(2^2\mathbf{b}_w \odot 2\mathbf{b}_w)) = (0)_{2n} \in \mathbb{Z}_4^{2n}.$$

Por lo tanto, $(\varphi \circ \nu)(w) = \nu(\varphi(Z)) \in \mathscr{C}$, lo cual prueba que $\mathscr{C}$ es un código negacíclico.
Para demostrar que (2) ocurre si y sólo si (3) se da, basta recordar que la imagen clásica de Gray de un código $\mathscr{D}$ sobre $\mathbb{Z}_4$ es un código cíclico si y sólo si $\mathscr{D}$ es un código negacíclico, y que $\Phi = \phi \circ \varphi$, donde ϕ es la isometría clásica de Gray.
Finalmente, veamos que (2) implica (1), esto es, probemos que $\nu_3(Z) \in \mathscr{C}$ y $\nu(Z) \in \mathscr{C}$ para cada $Z \in \mathscr{C}$. Primero observe que

$$\varphi(\nu(Z)) = \nu(\varphi(Z)) + \nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)),$$

o equivalentemente,

$$\varphi(\nu(Z)) + \nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) = \nu(\varphi(Z)).$$

Como $\varphi(Z) \in \varphi(\mathscr{C})$ y $\varphi(\mathscr{C})$ es un código negacíclico sobre $\mathbb{Z}_4$, entonces

$$\varphi(\nu(Z)) + \nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) \in \varphi(\mathscr{C}).$$

Analizando el término $\nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z))$, es fácil probar que $\nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) = \varphi(\nu(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z))$. De este modo,

$$\varphi(\nu(Z)) + \nu(\varphi(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)) = \varphi(\nu(Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z))) \in \varphi(\mathscr{C}),$$

donde la última relación se debe a que $2^2\mathbf{b}_Z \odot \mathbf{b}_Z$ tiene todas sus coordenadas en el ideal $\langle 4 \rangle$ de $\mathbb{Z}_8$ (Corolario 2.3.6). Debido a la propiedad de inyectividad de la isometría φ, de lo anterior concluimos que

$$\nu(Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z) \in \mathscr{C}. \tag{6.3}$$

De manera similar, usando la relación $\varphi(\nu_3(Z)) = \nu(\varphi(Z)) + \nu(\varphi(2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot \mathbf{b}_Z))$, obtenemos

$$\nu_3(Z + 2^2\mathbf{b}_Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z) \in \mathscr{C}. \tag{6.4}$$

De (6.3) y (6.4) es de donde derivaremos las propiedades de 3-ciclícidad y negacíclicidad del código $\mathscr{C}$. La idea será probar que $\nu(2^2\mathbf{b}_Z) = \nu_3(2^2\mathbf{b}_Z)$ pertence a $\mathscr{C}$ para todo $Z \in \mathscr{C}$.
Sea $Z \in \mathscr{C}$. Debido a que $\mathscr{C}$ es lineal, se tiene que $-Z \in \mathscr{C}$. Por lo tanto, en virtud de (6.3),

$$\nu(Z + 2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z) + \nu(Z + 2^2\mathbf{b}_{-Z} \odot 2\mathbf{b}_{-Z}) = \nu(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z + 2^2\mathbf{b}_{-Z} \odot 2\mathbf{b}_{-Z}) \in \mathscr{C}.$$

Como

$$2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z = (0, \ldots, 0, 2^2 r_0(z_{n-1}) r_1(z_{n-1}))$$

y

$$2^2\mathbf{b}_{-Z} \odot 2\mathbf{b}_{-Z} = (0, \ldots, 0, 2^2 r_0(z_{n-1})(r_1(z_{n-1}) \oplus r_0(z_{n-1})),$$

donde $\oplus$ denota la suma en $\mathbb{F}_2$, entonces

$$2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z + 2^2\mathbf{b}_{-Z} \odot 2\mathbf{b}_{-Z} = (0,\ldots,0,2^2 r_0(z_{n-1})r_0(z_{n-1})).$$

Además, ya que $r_0(z_{n-1}) \in \{0,1\}$, $r_0(z_{n-1})r_0(z_{n-1}) = r_0(z_{n-1})$ y, por lo tanto,

$$2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z + 2^2\mathbf{b}_{-Z} \odot 2\mathbf{b}_{-Z} = (0,\ldots,0,2^2 r_0(z_{n-1})) = 2^2\mathbf{b}_Z.$$

En consecuencia, $\nu(2^2\mathbf{b}_Z) \in \mathscr{C}$. Esto implica que $\nu(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z) \in \mathscr{C}$ para todo $Z \in \mathscr{C}$. Además, ya que las coordenas de los vectores $2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z$ y $2^2\mathbf{b}_Z$ están en el ideal $\langle 4\rangle$ de $\mathbb{Z}_8$, se tiene que $\nu(2^2\mathbf{b}_Z) = \nu_3(2^2\mathbf{b}_Z)$ y $\nu(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z) = \nu_3(2^2\mathbf{b}_Z \odot 2\mathbf{b}_Z)$. Así, la relación (6.3) implica que $\nu(Z) \in \mathscr{C}$, y la relación (6.4) implica que $\nu_3(Z) \in \mathscr{C}$, tal como queríamos demostrar. □

A modo de ejemplo podemos considerar el código lineal $\mathscr{C}$ presentado en la Sección 6.2, donde se demostró que $\varphi(\mathscr{C})$ es un código negacíclico y que $\Phi(\mathscr{C})$ es un código cíclico binario. En virtud del Teorema 6.5.1 el código $\mathscr{C}$ es un código 3-cíclico y negacíclico sobre $\mathbb{Z}_8$. Más ejemplos de este estilo han sido señalados en el Cuadro 6.1 y en el Apéndice A de este material.

Para finalizar este capítulo, es importante señalar que códigos cíclicos, en particular códigos cíclicos binarios, son de las familias de códigos más importantes en la Teoría de Códigos. Esto no sólo se debe a su rica estructura matemática sino también a sus interesantes aplicaciones prácticas. De este modo, el Teorema 6.5.1 proporciona una forma de construir códigos cíclicos binarios a partir de código 3-cíclico y negacíclicos sobre $\mathbb{Z}_8$. Debido a este hecho, dicho resultado puede ser considerado uno de los más importantes de todo esta tesis.

Capítulo 7

Conclusiones y perspectivas

En este trabajo hemos estudiado diversas propiedades de las imágenes bajo las isometrías $\varphi : (\mathbb{Z}_{2^{k+1}}^n, \delta_h) \to (\mathbb{Z}_4^{2^{k-1}n}, \delta_L)$ y de Gray $\Phi : (\mathbb{Z}_{2^{k+1}}^n, \delta_h) \to (\mathbb{F}_2^{2^k n}, \delta_H)$ de códigos consta-cíclicos (no necesariamente lineales) sobre $\mathbb{Z}_{2^{k+1}}$, $k \geq 2$, con el fin de responder los Problemas 1 y 2 planteados en la Introducción de este manuscrito, y que a continuación retomamos para esbozar los alcances y las limitaciones que se tuvieron.

Primero, debemos enfatizar que en todo el trabajo consideramos dos grandes grupos de códigos consta-cíclicos: aquellos que son invariantes con respecto a los corrimientos casi-cíclicos y $(1+2^k)$-casi-cíclicos, y aquellos que son invariantes bajo los corrimientos $(1+2^{k-1})$-cíclicos y $(1+2^{k-1}+2^k)$-cíclicos.

En el Problema 1 se propuso analizar las propiedades de ciclícidad de las imágenes de Gray del primer grupo de códigos; lo cual fue analizado en el Capítulo 4. En ese apartado demostramos que las imágenes bajo φ de tales códigos son códigos casi-cíclicos y casi-negacíclicos, y que las imágenes de Gray de los mismos son códigos casi-cíclicos. Pero que el índice de casi-ciclícidad era menor en el caso de los códigos que son invariantes con respecto al corrimiento $(1+2^k)$-casi-cíclico. También notamos que ciertos códigos sobresalientes, tales como algunos códigos de Reed-Muller, pueden ser obtenidos como imágenes de Gray de este primer grupo de códigos. Desde este punto de vista, las aportaciones del Capítulo 4 pueden contribuir al estudio de familias de códigos. Por tal razón, consideramos que futuros trabajos pueden investigar qué otras familias de códigos pueden ser construidas, o más aún, qué nuevas familias de códigos pueden ser obtenidas a través de los resultados presentados en ese capítulo.

Por su parte, en el Problema 2 se propuso el estudio de las propiedades de las imágenes de Gray del segundo grupo de códigos. Este problema fue considerado en dos partes: cuando $k \geq 3$ y cuando $k = 2$. En el Capítulo 5 se estudió el caso $k \geq 3$ y se probó que los códigos de este grupo están relacionados con códigos sobre $\mathbb{Z}_4$ que son invariantes (módulo una traslación) bajo las aplicaciones $\widetilde{\pi}(\nu \otimes \sigma)^{\otimes 2^{k-2}}$ y $\widetilde{\pi}(\sigma \otimes \nu)^{\otimes 2^{k-2}}$, dando lugar a nuevas familias de códigos sobre $\mathbb{Z}_4$, que hasta el momento no han sido reportadas en la literatura. Por otra parte, debido a la naturaleza de estas propiedades, en primera instancia, no fue posible describir propiedades generales de las imágenes de Gray de esos códigos. De este modo, un problema abierto consiste en estudiar las propiedades generales de las imágenes de Gray de dichos códigos.

La situación fue más afortunada para códigos 3-cíclicos y 7-cíclicos sobre $\mathbb{Z}_8$, lo cual corresponde al caso $k = 2$ estudiado en el Capítulo 6. En este contexto, demostramos que esos códigos están relacionados con códigos negacíclicos (módulo una traslación) sobre $\mathbb{Z}_4$, y con

códigos cíclicos binarios (módulo una traslación). En particular, demostramos que si un código es 3-cíclico y 7-cíclico, entonces su imagen bajo φ es un código negacíclico, y en consecuencia su imagen de Gray es un código cíclico. En consecuencia, hemos mostrado que una manera de obtener códigos cíclicos binarios es a través de códigos 3-cíclicos y negacíclicos sobre $\mathbb{Z}_8$, lo cual resulta similar a los trabajos de J. Wolfman [54, 55].

Vale la pena señalar que varios de los resultados encontrados a lo largo de esta tesis no han sido respotados en la literatura. Asimismo, cabe mencionar que el presente material ofrece una primera pauta para iniciar, y también continuar, con el estudio de propiedades de las imágenes de Gray de códigos consta-cíclicos, similares a las que se propusieron en los Problemas 1 y 2 planteados en la Introducción del presente escrito. Es en esta dirección que los siguientes problemas pueden ser abordados en futuros trabajos de investigación, y cuya solución, podrían ser de particular interés en la Teoría de Códigos Algebraicos.

1. Generalizar los resultados alcanzados en esta tesis a otras familias de anillos finitos de cadena. Por ejemplo, los anillos de enteros módulo p^{k+1}, los anillos de Galois $GR(p^{k+1}, s)$, donde p es un primo y $k \geq 1$, e incluso establecer resultados similares sobre anillos finitos de cadena en general.

2. Recientemente, el estudio de propiedades de ciclícidad de las imágenes de Gray de códigos cíclicos se ha extendido a otras clases de anillos finitos que no son de cadena (cf. [17]). En consecuencia, un segundo problema abierto consiste en investigar propiedades de las imágenes de Gray de códigos consta-cíclicos, tales como las que se plantearon en los Problemas 1 y 2, sobre esos tipos de anillos.

3. Estudiar las estructuras algebraicas de las familias de códigos consta-cíclicos mencionados en los Problemas 1 y 2, para determinar la estructura algebraica de los códigos obtenidos como imágenes de Gray de tales códigos.

Apéndice A

Tablas de códigos consta-cíclicos lineales

En este apartado presentamos tablas de códigos γ-cíclicos lineales de longitudes $n = 3,5,7$ sobre $\mathbb{Z}_8$, y de longitudes $n = 3,5$ sobre $\mathbb{Z}_{16}$, para las unidades $\gamma \in \{1, 1+2^{k-1}, 1+2^k, 1+2^{k-1}+2^k\}$, con $k = 2,3$. Como se ha hecho en el transcurso de todo este manuscrito, usaremos la notación $\delta_1 = 1+2^{k-1}$, $\delta_2 = 1+2^{k-1}+2^k$ y $\lambda = 1+2^k$. Todos los cálculos han sido realizados con el Programa Computacional MAGMA® V2.15-13 (Student Version), en el *Laboratorio de Códigos y Criptografía* del Departamento de Matemáticas de la Universidad Autónoma Metropoliana-Iztapalapa.

A.1. Notas sobre las tablas

Las tablas contienen información sobre los generadores de los códigos cíclicos lineales $\mathscr{C}$ (no triviales), identificados como ideales del anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n - 1\rangle$; la cardinalidad de los códigos $\#\mathscr{C}$ y las distancias mínimas homogéneas $\delta_h(\mathscr{C})$ de esos códigos, las cuales coinciden con sus pesos mínimos homogéneos $\omega_h(\mathscr{C})$, pues los códigos son lineales. También contienen tres columnas referentes a la γ-ciclícidad de los códigos $\mathscr{C}$, que determinan si el código cíclico $\mathscr{C}$ es a su vez δ_1-cíclico, λ-cíclico o δ_2-cíclico. Dicha información se incluyó con el fin de ilustrar varios de los resultados alcanzados en este trabajo. Dado que algunos de éstos requieren de la linealidad de la imagen del código $\mathscr{C}$ con respecto a las isometrías φ o Φ de Gray, también se han agregado cuatro columnas en las cuales se especifica la linealidad del código $\Phi(\mathscr{C})$, y la linealidad de la imagen de Gray de los códigos γ-cíclicos, donde $\gamma \in \{\delta_1, \lambda, \delta_2\}$. Escribiremos $[M,e]$ para denotar que $\Phi(\mathscr{C})$ es un código lineal de longitud M y dimensión e. En caso contrario, escribiremos (M,c) para denotar que $\Phi(\mathscr{C})$ tiene longitud M y cardinalidad c.

Con el fin de esclarecer cómo hemos construido esas tablas, en los siguientes párrafos daremos un breve repaso a la teoría presentada en la Sección 1.3 de este manuscrito.

Debido al Corolario 1.1.2, si n es impar, entonces $x^n - 1$ se factoriza como un producto de polinomios mónicos, básicos irreducibles y coprimos en $\mathbb{Z}_{2^{k+1}}[x]$. Esta factorización será escrita como

$$x^n - 1 = a_1(x)a_2(x)\cdots a_r(x).$$

Consecuentemente, por el Lema 1.3.8, una tal factorización de $x^n - \gamma$ es:

$$x^n - \gamma = b_1(x)b_2(x)\cdots b_r(x),$$

donde $b_i(x) = \beta^{-gr(a_i(x))}a_i(\beta x)$ y β es la raíz n-ésima de γ^{-1}, es decir, $\beta^n = \gamma^{-1}$.

Para construir un código cíclico, elegimos $k+2$ polinomios mónicos y coprimos, denotados como f_0, f_1, ..., f_{k+1}, con la posibilidad de que algunos de ellos sean iguales al polinomio constante 1, y tales que $f_0 f_1 \cdots f_{k+1} = x^n - 1$. En la práctica, esto se hace colocando los factores $a_1(x), \ldots, a_r(x)$ dentro de $k+2$ casillas (los polinomios f_i) sin colocar un mismo factor $a_i(x)$ en dos o más casillas distintas. Colocar varios factores $a_i(x)$ en una misma casilla es permitido.

Hecho lo anterior, construimos $\widehat{f_i}(x) = (x^n-1)/f_i$ y $\widehat{F_i}(x) = \widehat{f_i}(x) + \langle x^n - 1\rangle$. Entonces el ideal $\langle \widehat{F_1}, 2\widehat{F_2}, \ldots, 2^k \widehat{F}_{2^{k+1}}\rangle$, del anillo $\mathbb{Z}_{2^{k+1}}[x]/\langle x^n-1\rangle$, es la representación polinomial $P(\mathscr{C})$ de un código cíclico $\mathscr{C}$ de longitud n sobre $\mathbb{Z}_{2^{k+1}}$ y cardinalidad 2^S, donde

$$S = \sum_{i=0}^{k} (k+1-i) gr(f_{i+1}) = (k+1)gr(f_1) + kgr(f_2) + \cdots + 1gr(f_{k+1}).$$

Por medio del isomorfismo

$$\mu_\beta : \mathbb{Z}_{2^{k+1}}[x]/\langle x^n-1\rangle \to \mathbb{Z}_{2^{+1}}[x]/\langle x^n - \gamma\rangle,$$

definido como

$$a(x) + \langle x^n - 1\rangle \mapsto a(\beta x) + \langle x^n - \gamma\rangle,$$

donde β es la raíz n-ésima de γ^{-1}, calculamos el ideal $\mu_\beta(\langle \widehat{F_1}, 2\widehat{F_2}, \ldots, 2^k \widehat{F}_{2^{k+1}}\rangle)$, el cual corresponde a la representación polinomial $P(\mathscr{C}_\gamma)$ de un código γ-cíclico lineal $\mathscr{C}_\gamma$ de longitud n, misma cardinalidad y distancia mínima homogénea que el código cíclico $\mathscr{C}$. Los generadores del código $\mathscr{C}_\gamma$ se obtienen reemplazando los factores $a_i(x)$ que aparecen en los polinomios $\widehat{F_i}$ por los factores $b_i(x)$ que aparecen en la factorización del polinomio $x^n - \gamma$.

Ejemplo A.1.1. Sean $k = 2$ y $n = 7$. Entonces $\delta_1 = 3$, $\lambda = 5$ y $\delta_2 = 7$. Las raíces n-ésimas de estas unidades en $\mathbb{Z}_8$ son, respectivamente, $\beta_1 = 3$, $\beta_\lambda = 5$ y $\beta_2 = 7$ (Proposición 1.3.14). Por otro lado, la factorización $x^7 - 1$ como producto de polinomios mónicos, básicos irreducibles y coprimos en $\mathbb{Z}_8[x]$ es:

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

Sean $a_1(x) = x+7$, $a_2(x) = x^3 + 6x^2 + 5x + 7$ y $a_3(x) = x^3 + 3x^2 + 2x + 7$. Entonces las factorizaciones de $x^7 - \delta_1$, $x^7 - \lambda$ y $x^7 - \delta_2$ como producto de polinomios mónicos, básicos irreducibles y coprimos son:

$$x^7 - \delta_1 = b_1(x)b_2(x)b_3(x), \quad x^7 - \lambda = c_1(x)c_2(x)c_3(x), \quad x^7 - \delta_2 = d_1(x)d_2(x)d_3(x),$$

donde

$$
\begin{aligned}
b_1(x) &= \beta_1^{-gr(a_1(x))} a_1(\beta_1 x) = 3^{-1} a_1(3x) = x+5,\\
b_2(x) &= \beta_1^{-gr(a_2(x))} a_1(\beta_1 x) = 3^{-3} a_2(3x) = x^3+2x^2+5x+5,\\
b_3(x) &= \beta_1^{-gr(a_3(x))} a_3(\beta_1 x) = 3^{-3} a_3(3x) = x^3+x^2+2x+5,
\end{aligned}
$$

$$
\begin{aligned}
c_1(x) &= \beta_\lambda^{-gr(a_1(x))} a_1(\beta_\lambda x) = 5^{-1} a_1(5x) = x+3,\\
c_2(x) &= \beta_\lambda^{-gr(a_2(x))} a_1(\beta_\lambda x) = 5^{-3} a_2(5x) = x^3+6x^2+5x+3,\\
c_3(x) &= \beta_\lambda^{-gr(a_3(x))} a_3(\beta_\lambda x) = 5^{-3} a_3(5x) = x^3+7x^2+2x+3,
\end{aligned}
$$

$$
\begin{aligned}
d_1(x) &= \beta_2^{-gr(a_1(x))} a_1(\beta_2 x) = 7^{-1} a_1(7x) = x+1,\\
d_2(x) &= \beta_2^{-gr(a_2(x))} a_1(\beta_1 x) = 7^{-3} a_2(7x) = x^3+2x^2+5x+1,\\
d_3(x) &= \beta_2^{-gr(a_3(x))} a_3(\beta_2 x) = 7^{-3} a_3(7x) = x^3+5x^2+2x+1.
\end{aligned}
$$

Construyamos ahora un código cíclico lineal $\mathscr{C}$ de longitud 7 sobre $\mathbb{Z}_8$, y a partir de él obtengamos los correspondientes códigos γ-cíclicos lineales $\mathscr{C}_\gamma$, donde $\gamma \in \{3,5,7\}$. Como especificamos anteriormente, debemos colocar los 3 factores $a_1(x), a_2(x)$ y $a_3(x)$ en $k+2=4$ polinomios f_0, f_1, f_2, f_3 de tal modo que no haya ningún factor repetido entre los f_i. Coloquémoslos de la siguiente forma (otro arreglo daría lugar a otro código cíclico):

$$f_0 = 1, \quad f_1(x) = a_1(x), \quad f_2 = a_2(x), \quad f_3 = a_3(x).$$

Consecuentemente,

$$\widehat{f_0} = x^7 - 1, \quad \widehat{f_1} = a_2(x)a_3(x), \quad \widehat{f_2} = a_1 a_3(x), \quad \widehat{f_3} = a_1(x)a_2(x).$$

y, por lo tanto, al identificar las clases laterales de $\mathbb{Z}_8[x]/\langle x^7-1\rangle$ con los polinomios de grado a lo más 6, obtenemos

$$\widehat{F_0} = 0, \quad \widehat{F_1} = a_2(x)a_3(x), \quad \widehat{F_2} = a_1(x)a_3(x), \quad \widehat{F_3} = a_1(x)a_2(x).$$

Entonces el ideal

$$I = \langle \widehat{F_1}, 2\widehat{F_2}, 2^2\widehat{F_3}\rangle = \langle a_2(x)a_3(x), 2a_1(x)a_3(x), 2^2 a_1(x)a_2(x)\rangle$$

es la representación polinomial $P(\mathscr{C})$ de un código cíclico lineal $\mathscr{C}$ de longitud 7 y cardinalidad 2^S, donde

$$S = (2+1)gr(f_1) + (2)gr(f_2) + (1)gr(f_3) = (3)(1) + (2)(3) + (1)(3) = 12.$$

Las correspondientes representaciones polinomiales de los códigos γ-cíclicos se obtienen al reemplazar los polinomios a_i por los polinomios b_i (código $\mathscr{C}_{\delta_1}$ δ_1-cíclico lineal), c_i (código $\mathscr{C}_{\lambda}$ λ-cíclico lineal) y d_i (código $\mathscr{C}_{\delta_2}$ δ_2-cíclico lineal):

$$\begin{aligned} P(\mathscr{C}_{\delta_1}) &= \langle b_2(x)b_3(x), 2b_1(x)b_3(x), 2^2 b_1(x)b_2(x)\rangle, \\ P(\mathscr{C}_{\lambda}) &= \langle c_2(x)c_3(x), 2c_1(x)c_3(x), 2^2 c_1(x)c_2(x)\rangle, \\ P(\mathscr{C}_{\delta_2}) &= \langle d_2(x)d_3(x), 2d_1(x)d_3(x), 2^2 d_1(x)d_2(x)\rangle. \end{aligned}$$

Estos códigos tienen la misma cardinalidad y distancia mínima homogénea que $\mathscr{C}$. Por tal razón basta especificar en las tablas los datos de $\mathscr{C}$.

En el desarrollo de este trabajo hemos escrito $\mathscr{C} = \langle a_2(x)a_3(x), 2a_1(x)a_3(x), 2^2 a_1(x)a_2(x)\rangle$ denotando que $P(\mathscr{C}) = \langle a_2(x)a_3(x), 2a_1(x)a_3(x), 2^2 a_1(x)a_2(x)\rangle$. Seguiremos esta filosofía en las tablas.

Durante todo este apéndice usaremos la siguiente notacón. Las factorizaciones de $x^n - 1$, $x^n - \delta_1$, $x^n - \lambda$ y $x^n - \delta_2$ serán escritas respectivamente como:

$$\begin{aligned} x^n - 1 &= a_1(x)a_2(x)\cdots a_r(x), \\ x^n - \delta_1 &= b_1(x)b_2(x)\cdots b_r(x), \\ x^n - \lambda &= c_1(x)c_2(x)\cdots c_r(x), \\ x^n - \delta_2 &= d_1(x)d_2(x)\cdots d_r(x). \end{aligned}$$

Las raíces n-ésimas de δ_1, λ y δ_2 serán denotadas como β_1, β_λ y β_2.

A.2. Códigos consta-cíclicos lineales sobre $\mathbb{Z}_8$

Las unidades $\delta_1 = 1 + 2^{k-1}$, $\lambda = 1 + 2^k$ y $\delta_2 + 1 + 2^{k-1} + 2^k$ en $\mathbb{Z}_8$ ($k = 2$) son:

$$\delta_1 = 3, \qquad \lambda = 5, \qquad \delta_2 = 7$$

Cada una de estas raíces es de orden 2 en $\mathbb{Z}_8$ y, por lo tanto, sus raíces n-ésismas son ellas mismas para todo $n \geq 1$ impar. Esto es,

$$\beta_1 = 3, \qquad \beta_\lambda = 5, \qquad \beta_1 = 7, \qquad \forall\, n \geq 1 \text{ impar.}$$

A.2.1. Longitud $n = 3$

Factorización de los polinomios $x^3 - \gamma$

i	1	2
$a_i(x)$	$x+7$	x^2+x+1
$b_i(x)$	$x+5$	x^2+3x+1
$c_i(x)$	$x+3$	x^2+5x+1
$d_i(x)$	$x+1$	x^2+7x+1

Cuadro A.1: Códigos γ-cíclicos de longitud 3 sobre $\mathbb{Z}_8$.

$\mathscr{C}$	$\#\mathscr{C}$	$\delta_h(\mathscr{C})$	γ-ciclícidad			Linealidad de $\Phi(\mathscr{C})$			
			3	5	7	1	3	5	7
$\langle 2\rangle$	4^3	2	✓	✓	✓	$[12,6]$	$[12,6]$	$[12,6]$	$[12,6]$
$\langle 2^2\rangle$	2^3	4	✓	✓	✓	$[12,3]$	$[12,3]$	$[12,3]$	$[12,3]$
$\langle a_1\rangle$	8^2	4	–	–	–	$(12,2^6)$	$(12,2^6)$	$(12,2^6)$	$(12,2^6)$
$\langle 2a_1\rangle$	4^2	4	–	✓	–	$(12,2^4)$	$(12,2^4)$	$(12,2^4)$	$(12,2^4)$
$\langle 2^2a_1\rangle$	2^2	8	✓	✓	✓	$[12,2]$	$[12,2]$	$[12,2]$	$[12,2]$
$\langle a_2\rangle$	8	6	–	–	–	$[12,3]$	$(12,2^3)$	$[12,3]$	$(12,2^3)$
$\langle 2a_2\rangle$	4	6	–	✓	–	$[12,2]$	$[12,2]$	$[12,2]$	$[12,2]$
$\langle 2^2a_2\rangle$	2	12	✓	✓	✓	$[12,1]$	$[12,1]$	$[12,1]$	$[12,1]$
$\langle a_1,2a_2\rangle$	$8^2\cdot 4$	2	✓	✓	✓	$[12,8]$	$[12,8]$	$[12,8]$	$[12,8]$
$\langle a_1,2^2a_2\rangle$	$8^2\cdot 2$	4	–	✓	–	$(12,2^7)$	$(12,2^7)$	$(12,2^7)$	$(12,2^7)$
$\langle a_2,2a_1\rangle$	$8\cdot 4^2$	2	✓	✓	✓	$[12,7]$	$[12,7]$	$[12,7]$	$[12,7]$
$\langle a_2,2^2a_1\rangle$	$8\cdot 2^2$	4	–	✓	–	$[12,5]$	$[12,5]$	$[12,5]$	$[12,5]$
$\langle 2a_1,2^2a_2\rangle$	$4^2\cdot 2$	4	✓	✓	✓	$[12,5]$	$[12,5]$	$[12,5]$	$[12,5]$
$\langle 2a_2,2^2a_1\rangle$	$4\cdot 2^2$	4	✓	✓	✓	$[12,4]$	$[12,4]$	$[12,4]$	$[12,4]$

A.2.2. Longitud $n = 5$

Factorización de los polinomios $x^5 - \gamma$

i	1	2
$a_i(x)$	$x+7$	$x^4+x^3+x^2+x+1$
$b_i(x)$	$x+5$	$x^4+3x^3+x^2+3x+1$
$c_i(x)$	$x+3$	$x^4+5x^3+x^2+5x+1$
$d_i(x)$	$x+1$	$x^4+7x^3+x^2+7x+1$

Cuadro A.2: Códigos γ-cíclicos de longitud 5 sobre $\mathbb{Z}_8$.

$\mathscr{C}$	$\#\mathscr{C}$	$\delta_h(\mathscr{C})$	γ-ciclícidad			Linealidad de $\Phi(\mathscr{C})$			
			3	5	7	1	3	5	7
$\langle 2\rangle$	4^5	2	✓	✓	✓	$[20,10]$	$[20,10]$	$[20,10]$	$[20,10]$
$\langle 2^2\rangle$	2^5	4	✓	✓	✓	$[20,5]$	$[20,5]$	$[20,5]$	$[20,5]$
$\langle a_1\rangle$	8^4	4	–	–	–	$(20,2^{12})$	$(20,2^{12})$	$(20,2^{12})$	$(20,2^{12})$
$\langle 2a_1\rangle$	4^4	4	–	✓	–	$(20,2^8)$	$(20,2^8)$	$(20,2^8)$	$(20,2^8)$
$\langle 2^2a_1\rangle$	2^4	8	✓	✓	✓	$[20,4]$	$[20,4]$	$[20,4]$	$[20,4]$
$\langle a_2\rangle$	8	10	–	–	–	$[20,3]$	$(20,2^3)$	$[20,3]$	$(20,2^3)$
$\langle 2a_2\rangle$	4	10	–	✓	–	$[20,2]$	$[20,2]$	$[20,2]$	$[20,2]$
$\langle 2^2a_2\rangle$	2	20	✓	✓	✓	$[20,1]$	$[20,1]$	$[20,1]$	$[20,1]$
$\langle a_1,2a_2\rangle$	$8^4\cdot 4$	2	✓	✓	✓	$[20,14]$	$[20,14]$	$[20,14]$	$[20,14]$
$\langle a_1,2^2a_2\rangle$	$8^4\cdot 2$	4†	–	✓	–	$(20,2^{13})$	$(20,2^{13})$	$(20,2^{13})$	$(20,2^{13})$
$\langle a_2,2a_1\rangle$	$8\cdot 4^4$	2	✓	✓	✓	$[20,11]$	$[20,11]$	$[20,11]$	$[20,11]$
$\langle a_2,2^2a_1\rangle$	$8\cdot 2^4$	4	–	✓	–	$[20,7]$	$[20,7]$	$[20,7]$	$[20,7]$
$\langle 2a_1,2^2a_2\rangle$	$4^4\cdot 2$	4	✓	✓	✓	$[20,9]$	$[20,9]$	$[20,9]$	$[20,9]$
$\langle 2a_2,2^2a_1\rangle$	$4\cdot 2^4$	4	✓	✓	✓	$[20,6]$	$[20,6]$	$[20,6]$	$[20,6]$

A.2.3. Longitud $n = 7$

Factorización de los polinomios $x^7 - \gamma$

i	1	2	
$a_i(x)$	$x+7$	x^3+6x^2+5x+7	x^3+3x^2+2x+7
$b_i(x)$	$x+5$	x^3+2x^2+5x+1	x^3+5x^2+2x+1
$c_i(x)$	$x+3$	x^3+2x^2+5x+5	x^3+x^2+2x+5
$d_i(x)$	$x+1$	x^3+6x^2+5x+3	x^3+7x^2+2x+3

Cuadro A.3: Códigos γ-cíclicos de longitud 7 sobre $\mathbb{Z}_8$.

$\mathscr{C}$	$\#\mathscr{C}$	$\delta_h(\mathscr{C})$	γ-ciclícidad			Linealidad de $\Phi(\mathscr{C})$			
			3	5	7	1	3	5	7
$\langle 2\rangle$	4^7	2	✓	✓	✓	$[28,14]$	$[28,14]$	$[28,14]$	$[28,14]$
$\langle 2^2\rangle$	2^7	4	✓	✓	✓	$[28,7]$	$[28,7]$	$[28,7]$	$[28,7]$
$\langle a_1\rangle$	8^6	4	–	–	–	$(28,2^{18})$	$(28,2^{18})$	$(28,2^{18})$	$(28,2^{18})$
$\langle a_2\rangle$	8^4	8†	–	–	–	$(28,2^{12})$	$(28,2^{12})$	$(28,2^{12})$	$(28,2^{12})$
$\langle a_3\rangle$	8^4	8†	–	–	–	$(28,2^{12})$	$(28,2^{12})$	$(28,2^{12})$	$(28,2^{12})$
$\langle 2a_1\rangle$	4^6	4	–	✓	–	$(28,2^{12})$	$(28,2^{12})$	$(28,2^{12})$	$(28,2^{12})$
$\langle 2a_2\rangle$	4^4	10	–	✓	–	$(28,2^8)$	$(28,2^8)$	$(28,2^8)$	$(28,2^8)$
$\langle 2a_3\rangle$	4^4	8	–	✓	–	$(28,2^8)$	$(28,2^8)$	$(28,2^8)$	$(28,2^8)$
$\langle 2^2a_1\rangle$	2^6	8	✓	✓	✓	$[28,6]$	$[28,6]$	$[28,6]$	$[28,6]$
$\langle 2^2a_2\rangle$	2^4	12	✓	✓	✓	$[28,4]$	$[28,4]$	$[28,4]$	$[28,4]$
$\langle 2^2a_3\rangle$	2^4	12	–	✓	–	$[28,4]$	$[28,4]$	$[28,4]$	$[28,4]$
$\langle a_1a_2\rangle$	8^3	10†	–	–	–	$(28,2^9)$	$(28,2^9)$	$(28,2^9)$	$(28,2^9)$
$\langle a_1a_3\rangle$	8^3	10†	–	–	–	$(28,2^9)$	$(28,2^9)$	$(28,2^9)$	$(28,2^9)$
$\langle a_2a_3\rangle$	8	14	–	–	–	$[28,3]$	$(28,3)$	$[28,2^3]$	$(28,2^3)$
$\langle 2a_1a_2\rangle$	4^3	12†	–	✓	–	$(28,2^6)$	$(28,2^6)$	$(28,2^6)$	$(28,2^6)$
$\langle 2a_1a_3\rangle$	4^3	12†	–	✓	–	$(28,2^6)$	$(28,2^6)$	$(28,2^6)$	$(28,2^6)$

Continúa

Cuadro A.3 – Continuación

$\mathscr{C}$	$\#\mathscr{C}$	$\delta_h(\mathscr{C})$	γ-ciclícidad			Linealidad de $\Phi(\mathscr{C})$			
			3	5	7	1	3	5	7
$\langle 2a_2a_3\rangle$	4	14	–	✓	–	$[28,2]$	$[28,2]$	$[28,2]$	$[28,2]$
$\langle 2^2a_1a_2\rangle$	8	16†	✓	✓	✓	$[28,3]$	$[28,3]$	$[28,3]$	$[28,3]$
$\langle 2^2a_1a_3\rangle$	2^3	16†	✓	✓	✓	$[28,3]$	$[28,3]$	$[28,3]$	$[28,3]$
$\langle 2^2a_2a_3\rangle$	2	28†	✓	✓	✓	$[28,1]$	$[28,1]$	$[28,1]$	$[28,1]$
$\langle a_1,2a_2a_3\rangle$	$8^6\cdot 4$	2	✓	✓	✓	$[28,20]$	$[28,20]$	$[28,20]$	$[28,20]$
$\langle a_2,2a_1a_3\rangle$	$8^4\cdot 4^3$	2	✓	✓	✓	$[28,18]$	$[28,18]$	$[28,18]$	$[28,18]$
$\langle a_3,2a_1a_2\rangle$	$8^4\cdot 4^3$	2	✓	✓	✓	$[28,18]$	$[28,18]$	$[28,18]$	$[28,18]$
$\langle a_1a_2,2a_3\rangle$	$8^3\cdot 4^4$	2	✓	✓	✓	$[28,17]$	$[28,17]$	$[28,17]$	$[28,17]$
$\langle a_1a_3,2a_2\rangle$	$8^3\cdot 4^4$	2	✓	✓	✓	$[28,17]$	$[28,17]$	$[28,17]$	$[28,17]$
$\langle a_2a_3,2a_1\rangle$	$8\cdot 4^6$	2	✓	✓	✓	$[28,15]$	$[28,15]$	$[28,15]$	$[28,15]$
$\langle a_1,2^2a_2a_3\rangle$	$8^6\cdot 2$	4†	–	✓	–	$(28,2^{19})$	$(28,2^{19})$	$(28,2^{19})$	$(28,2^{19})$
$\langle a_2,2^2a_1a_3\rangle$	$8^4\cdot 2^3$	4	–	✓	–	$(28,2^{15})$	$(28,2^{15})$	$(28,2^{15})$	$(28,2^{15})$
$\langle a_3,2^2a_1a_2\rangle$	$8^4\cdot 2^3$	4	–	✓	–	$(28,2^{15})$	$(28,2^{15})$	$(28,2^{15})$	$(28,2^{15})$
$\langle a_1a_2,2^2a_3\rangle$	$8^3\cdot 2^4$	4	–	✓	–	$(28,2^{13})$	$(28,2^{13})$	$(28,2^{13})$	$(28,2^{13})$
$\langle a_2a_3,2^2a_1\rangle$	$8\cdot 2^6$	4	–	✓	–	$[28,9]$	$[28,9]$	$[28,9]$	$[28,9]$
$\langle a_1a_3,2^2a_2\rangle$	$8^3\cdot 2^4$	4	–	✓	–	$(28,2^{13})$	$(28,2^{13})$	$(28,2^{13})$	$(28,2^{13})$
$\langle 2a_1,2^2a_2a_3\rangle$	$4^6\cdot 2$	4	✓	✓	✓	$[28,13]$	$[28,13]$	$[28,13]$	$[28,13]$
$\langle 2a_2,2^2a_1a_3\rangle$	$4^4\cdot 2^3$	4	✓	✓	✓	$[28,11]$	$[28,11]$	$[28,11]$	$[28,11]$
$\langle 2a_3,2^2a_1a_2\rangle$	$4^4\cdot 2^3$	4	✓	✓	✓	$[28,11]$	$[28,11]$	$[28,11]$	$[28,11]$
$\langle 2a_1a_2,2^2a_3\rangle$	$4^3\cdot 2^4$	4	✓	✓	✓	$[28,10]$	$[28,10]$	$[28,10]$	$[28,10]$
$\langle 2a_2a_3,2^2a_1\rangle$	$4\cdot 2^6$	4	✓	✓	✓	$[28,8]$	$[28,8]$	$[28,8]$	$[28,8]$
$\langle 2a_1a_3,2^2a_2\rangle$	$4^3\cdot 2^4$	4	✓	✓	✓	$[28,10]$	$[28,10]$	$[28,10]$	$[28,10]$
$\langle a_2a_3,2a_1a_2\rangle$	$8\cdot 4^3$	8	–	–	–	$(28,2^9)$	$(28,2^9)$	$(28,2^9)$	$(28,2^9)$
$\langle a_2a_3,2a_1a_3\rangle$	$8\cdot 4^3$	8	–	–	–	$(28,2^9)$	$(28,2^9)$	$(28,2^9)$	$(28,2^9)$
$\langle a_1a_2,2a_1a_3\rangle$	$8^3\cdot 4^3$	4	–	–	–	$(28,2^{15})$	$(28,2^{15})$	$(28,2^{15})$	$(28,2^{15})$
$\langle a_1a_2,2a_2a_3\rangle$	$8^3\cdot 4$	8†	–	–	–	$(28,2^{11})$	$(28,2^{11})$	$(28,2^{11})$	$(28,2^{11})$
$\langle a_1a_3,2a_1a_2\rangle$	$8^3\cdot 4^3$	4	–	–	–	$(28,2^{15})$	$(28,2^{15})$	$(28,2^{15})$	$(28,2^{15})$

Continúa

Cuadro A.3 – Continuación

$\mathscr{C}$	$\#\mathscr{C}$	$\delta_h(\mathscr{C})$	γ-ciclícidad			Linealidad de $\Phi(\mathscr{C})$			
			3	5	7	1	3	5	7
$\langle a_1a_3, 2a_2a_3\rangle$	$8^3\cdot 4$	8†	–	–	–	$(28,2^{11})$	$(28,2^{11})$	$(28,2^{11})$	$(28,2^{11})$
$\langle a_2a_3, 2^2a_1a_2\rangle$	$8\cdot 2^3$	12†	–	–	–	$[28,6]$	$[28,6]$	$(28,2^6)$	$(28,2^6)$
$\langle a_2a_3, 2^2a_1a_3\rangle$	$8\cdot 2^3$	12†	–	–	–	$[28,6]$	$[28,6]$	$(28,2^6)$	$(28,2^6)$
$\langle a_1a_2, 2^2a_1a_3\rangle$	$8^3\cdot 2^3$	8†	–	–	–	$(28,2^{12})$	$(28,2^{12})$	$(28,2^{12})$	$(28,2^{12})$
$\langle a_1a_2, 2^2a_2a_3\rangle$	$8^3\cdot 2$	8	–	–	–	$(28,2^{10})$	$(28,2^{10})$	$(28,2^{10})$	$(28,2^{10})$
$\langle a_1a_3, 2^2a_1a_2\rangle$	$8^3\cdot 2^3$	8†	–	–	–	$(28,2^{12})$	$(28,2^{12})$	$(28,2^{12})$	$(28,2^{12})$
$\langle a_1a_3, 2^2a_2a_3\rangle$	$8^3\cdot 2$	8	–	–	–	$(28,2^{10})$	$(28,2^{10})$	$(28,2^{10})$	$(28,2^{10})$
$\langle 2a_1a_2, 2^2a_1a_3\rangle$	$4^3\cdot 2^3$	8	–	✓	–	$[28,9]$	$[28,9]$	$[28,9]$	$[28,9]$
$\langle 2a_1a_2, 2^2a_2a_3\rangle$	$4^3\cdot 2$	8	–	✓	–	$(28,2^7)$	$(28,2^7)$	$(28,2^7)$	$(28,2^7)$
$\langle 2a_2a_3, 2^2a_1a_2\rangle$	$4\cdot 2^3$	12	–	✓	–	$[28,5]$	$[28,5]$	$[28,5]$	$[28,5]$
$\langle 2a_2a_3, 2^2a_1a_3\rangle$	$4\cdot 2^3$	12	–	✓	–	$[28,5]$	$[28,5]$	$[28,5]$	$[28,5]$
$\langle 2a_1a_3, 2^2a_1a_2\rangle$	$4^3\cdot 2^3$	8	–	✓	–	$[28,9]$	$[28,9]$	$[28,5]$	$[28,9]$
$\langle 2a_1a_3, 2^2a_2a_3\rangle$	$4^3\cdot 2$	8	–	✓	–	$(28,2^7)$	$(28,2^7)$	$(28,2^7)$	$(28,2^7)$
$\langle a_2a_3, 2a_1a_3, 2^2a_1a_2\rangle$	$8\cdot 4^3\cdot 2^3$	4	–	✓	–	$[28,12]$	$[28,12]$	$[28,12]$	$[28,12]$
$\langle a_2a_3, 2a_1a_2, 2^2a_1a_3\rangle$	$8\cdot 4^3\cdot 2^3$	4	–	✓	–	$[28,12]$	$[28,12]$	$[28,12]$	$[28,12]$
$\langle a_1a_2, 2a_3a_2, 2^2a_1a_3\rangle$	$8^3\cdot 4\cdot 2^3$	4	–	✓	–	$(28,2^{14})$	$(28,2^{14})$	$(28,2^{14})$	$(28,2^{14})$
$\langle a_1a_2, 2a_1a_3, 2^2a_2a_3\rangle$	$8^3\cdot 4^3\cdot 2$	4	–	✓	–	$[28,16]$	$[28,16]$	$[28,16]$	$[28,16]$
$\langle a_1a_3, 2a_2a_3, 2^2a_1a_2\rangle$	$8^3\cdot 4\cdot 2^3$	4	–	✓	–	$(28,2^{14})$	$(28,2^{14})$	$(28,2^{14})$	$(28,2^{14})$
$\langle a_1a_3, 2a_1a_2, 2^2a_2a_3\rangle$	$8^3\cdot 4^3\cdot 2$	4	–	✓	–	$[28,16]$	$[28,16]$	$[28,16]$	$[28,16]$

A.3. Códigos consta-cíclicos lineales sobre $\mathbb{Z}_{16}$

A.3.1. Longitud $n = 3$

Unidades y sus raíces n-ésimas, $n = 3$

Unidad	1	δ_1	λ	δ_2
	1	5	9	13
Ráiz n-ésima	1	5	9	13

Factorización de los polinomios $x^3 - \gamma$

i	1	2
$a_i(x)$	$x+15$	x^2+x+1
$b_i(x)$	$x+3$	$x^2+13x+9$
$c_i(x)$	$x+7$	x^2+9x+1
$d_i(x)$	$x+11$	$x^2+13x+9$

Cuadro A.4: Códigos γ-cíclicos de longitud 3 sobre $\mathbb{Z}_{16}$.

$\mathscr{C}$	$\#\mathscr{C}$	$\delta_h(\mathscr{C})$	γ-ciclícidad			Linealidad de $\Phi(\mathscr{C})$			
			3	5	7	1	3	5	7
$\langle 2 \rangle$	8^3	4	✓	✓	✓	$[24,9]$	$[24,9]$	$[24,9]$	$[24,9]$
$\langle 2^2 \rangle$	4^3	4	✓	✓	✓	$[24,6]$	$[24,6]$	$[24,6]$	$[24,6]$
$\langle 2^3 \rangle$	2^3	8	✓	✓	✓	$[24,6]$	$[24,6]$	$[24,6]$	$[24,6]$
$\langle a_1 \rangle$	16^2	8†	–	–	–	$(24,2^8)$	$(24,2^8)$	$(24,2^8)$	$(24,2^8)$
$\langle 2a_1 \rangle$	8^2	8	–	✓	–	$(24,2^6)$	$(24,2^6)$	$(24,2^6)$	$(24,2^6)$
$\langle 2^2 a_1 \rangle$	4^2	8	✓	✓	✓	$(24,2^4)$	$(24,2^4)$	$(24,2^4)$	$(24,2^4)$
$\langle 2^3 a_1 \rangle$	2^2	16†	✓	✓	✓	$[24,2]$	$[24,2]$	$[24,2]$	$[24,2]$
$\langle a_2 \rangle$	16	12†	–	–	–	$[24,4]$	$[24,4]$	$(24,2^4)$	$(24,2^4)$
$\langle 2a_2 \rangle$	8	12	–	✓	–	$[24,3]$	$[24,3]$	$[24,3]$	$[24,3]$

Continúa

Cuadro A.4 – Continuación

$\mathscr{C}$	$\#\mathscr{C}$	$\delta_h(\mathscr{C})$	γ-ciclícidad			Linealidad de $\Phi(\mathscr{C})$			
			3	5	7	1	3	5	7
$\langle 2^2 a_2 \rangle$	4	12	✓	✓	✓	$[24,2]$	$[24,2]$	$[24,2]$	$[24,2]$
$\langle 2^3 a_2 \rangle$	2	24†	✓	✓	✓	$[24,1]$	$[24,1]$	$[24,1]$	$[24,1]$
$\langle a_1, 2a_2 \rangle$	$16^2 \cdot 8$	4	✓	✓	✓	$[24,11]$	$[24,11]$	$[24,11]$	$[24,11]$
$\langle a_1, 2^2 a_2 \rangle$	$16^2 \cdot 4$	4	✓	✓	✓	$(24,2^{10})$	$(24,2^{10})$	$(24,2^{10})$	$(24,2^{10})$
$\langle a_1, 2^3 a_2 \rangle$	$16^2 \cdot 2$	8	–	✓	–	$(24,2^{10})$	$(24,2^{10})$	$(24,2^{10})$	$(24,2^{10})$
$\langle a_2, 2a_1 \rangle$	$16 \cdot 8^2$	4	✓	✓	✓	$[24,10]$	$[24,10]$	$[24,10]$	$[24,10]$
$\langle a_2, 2^2 a_1 \rangle$	$16 \cdot 4^2$	4	✓	✓	✓	$[24,8]$	$[24,8]$	$[24,8]$	$[24,8]$
$\langle a_2, 2^3 a_1 \rangle$	$16 \cdot 2^2$	8	–	✓	–	$[24,6]$	$[24,6]$	$[24,6]$	$[24,6]$
$\langle 2a_1, 2^2 a_2 \rangle$	$8^2 \cdot 4$	4	✓	✓	✓	$[24,8]$	$[24,8]$	$[24,8]$	$[24,8]$
$\langle 2a_1, 2^3 a_2 \rangle$	$8^2 \cdot 2$	8	✓	✓	✓	$(24,2^7)$	$(24,2^7)$	$(24,2^7)$	$(24,2^7)$
$\langle 2a_2, 2^2 a_1 \rangle$	$8 \cdot 4^2$	4	✓	✓	✓	$[24,7]$	$[24,7]$	$[24,7]$	$[24,7]$
$\langle 2a_2, 2^3 a_1 \rangle$	$8 \cdot 2^2$	8	✓	✓	✓	$[24,5]$	$[24,5]$	$[24,5]$	$[24,5]$
$\langle 2^2 a_1, 2^3 a_2 \rangle$	$4^2 \cdot 2$	8	✓	✓	✓	$[24,7]$	$[24,7]$	$[24,7]$	$[24,7]$
$\langle 2^2 a_2, 2^3 a_1 \rangle$	$4 \cdot 2^2$	8	✓	✓	✓	$[24,4]$	$[24,4]$	$[24,4]$	$[24,4]$

A.3.2. Longitud $n = 5$

Unidades y sus raíces n-ésimas, $n = 3$

Unidad	1	δ_1	λ	δ_2
	1	5	9	13
Ráiz n-ésima	1	13	9	5

Factorización de los polinomios $x^3 - \gamma$

i	1	2
$a_i(x)$	$x+15$	$x^4+x^3+x^2+x+1$
$b_i(x)$	$x+3$	$x^4+13x^3+9x^2+5x+1$
$c_i(x)$	$x+7$	$x^4+9x^3+x^2+9x+1$
$d_i(x)$	$x+11$	$x^4+5x^3+9x^2+13x+1$

Cuadro A.5: Códigos γ-cíclicos de longitud 5 sobre $\mathbb{Z}_{16}$.

$\mathscr{C}$	$\#\mathscr{C}$	$\delta_h(\mathscr{C})$	γ-ciclícidad			Linealidad de $\Phi(\mathscr{C})$			
			3	5	7	1	3	5	7
$\langle 2\rangle$	8^5	4	✓	✓	✓	$[40,15]$	$[40,15]$	$[40,15]$	$[40,15]$
$\langle 2^2\rangle$	4^5	4	✓	✓	✓	$[40,10]$	$[40,10]$	$[40,10]$	$[40,10]$
$\langle 2^3\rangle$	2^5	8	✓	✓	✓	$[40,5]$	$[40,5]$	$[40,5]$	$[40,5]$
$\langle a_1\rangle$	16^4	8	–	–	–	$(40,2^{16})$	$(40,2^{16})$	$(40,2^{16})$	$(40,2^{16})$
$\langle 2a_1\rangle$	8^4	8	–	✓	–	$(40,2^{12})$	$(40,2^{12})$	$(40,2^{12})$	$(40,2^{12})$
$\langle 2^2a_1\rangle$	4^4	8	✓	✓	✓	$(40,2^8)$	$(40,2^8)$	$(40,2^8)$	$(40,2^8)$
$\langle 2^3a_1\rangle$	2^4	16	✓	✓	✓	$[40,4]$	$[40,4]$	$[40,4]$	$[40,4]$
$\langle a_2\rangle$	16	20†	–	–	–	$[40,4]$	$[40,4]$	$(40,2^4)$	$(40,2^4)$
$\langle 2a_2\rangle$	8	20	–	✓	–	$[40,3]$	$[40,3]$	$[40,3]$	$[40,3]$
$\langle 2^2a_2\rangle$	4	20	✓	✓	✓	$[40,2]$	$[40,2]$	$[40,2]$	$[40,2]$
$\langle 2^3a_2\rangle$	2	40†	✓	✓	✓	$[40,1]$	$[40,1]$	$[40,1]$	$[40,1]$

Continúa

Cuadro A.5 – Continuación

$\mathscr{C}$	$\#\mathscr{C}$	$\delta_h(\mathscr{C})$	γ-ciclícidad			Linealidad de $\Phi(\mathscr{C})$			
			3	5	7	1	3	5	7
$\langle a_1, 2a_2\rangle$	$16^4 \cdot 8$	4	✓	✓	✓	$[40,19]$	$[40,19]$	$[40,19]$	$[40,19]$
$\langle a_1, 2^2a_2\rangle$	$16^4 \cdot 4$	4	✓	✓	✓	$(40,2^{18})$	$(40,2^{18})$	$(40,2^{18})$	$(40,2^{18})$
$\langle a_1, 2^3a_2\rangle$	$16^4 \cdot 2$	8	–	✓	–	$(40,2^{17})$	$(40,2^{17})$	$(40,2^{17})$	$(40,2^{17})$
$\langle a_2, 2a_1\rangle$	$16 \cdot 8^4$	4	✓	✓	✓	$[40,16]$	$[40,16]$	$[40,16]$	$[40,16]$
$\langle a_2, 2^2a_1\rangle$	$16 \cdot 4^4$	4	✓	✓	✓	$[40,12]$	$[40,12]$	$[40,12]$	$[40,12]$
$\langle a_2, 2^3a_1\rangle$	$16 \cdot 2^4$	8	–	✓	–	$[40,8]$	$[40,8]$	$[40,8]$	$[40,8]$
$\langle 2a_1, 2^2a_2\rangle$	$8^4 \cdot 4$	4	✓	✓	✓	$[40,14]$	$[40,14]$	$[40,14]$	$[40,14]$
$\langle 2a_1, 2^3a_2\rangle$	$8^4 \cdot 2$	8	✓	✓	✓	$(40,2^{13})$	$(40,2^{13})$	$(40,2^{13})$	$(40,2^{13})$
$\langle 2a_2, 2^2a_1\rangle$	$8 \cdot 4^4$	4	✓	✓	✓	$[40,11]$	$[40,11]$	$[40,11]$	$[40,7]$
$\langle 2a_2, 2^3a_1\rangle$	$8 \cdot 2^4$	8	✓	✓	✓	$[40,7]$	$[40,7]$	$[40,7]$	$[40,7]$
$\langle 2^2a_1, 2^3a_2\rangle$	$4^4 \cdot 2$	8	✓	✓	✓	$[40,9]$	$[40,9]$	$[40,9]$	$[40,9]$
$\langle 2^2a_2, 2^3a_1\rangle$	$4 \cdot 2^4$	8	✓	✓	✓	$[40,6]$	$[40,6]$	$[40,6]$	$[40,6]$

Apéndice B

φ es una isometría: una prueba distinta

Nuestro interés en este apéndice es dar una prueba distinta a la que se presentó en la Sección 2.2.2 para establecer que la función φ es una isometría entre $(\mathbb{Z}_{2^{k+1}}^n, \delta_h)$ y $(\mathbb{Z}_4^{2^{k-1}n}, \delta_L)$, donde δ_h y δ_L son la distancia homogénea y de Lee, respectivamente. Recuerde que en tal sección usamos el hecho de que la función $\varphi^k : (\mathbb{Z}_{2^{k+1}}^n, \delta_h) \to (\mathbb{Z}_4^{2^{k-1}n}, \delta_L)$ (introducida [51,52]) es una isometría.

B.1. Preliminares

En esta breve sección recordaremos algunas definiciones básicas y resultados que son necesarios para el propósito de este apéndice. Aunque cada uno de ellos se encuentran dentro del texto principal de este manuscrito, los hemos incluido aquí para una rápida referencia.

Sean $u = (0,1)$, $v = (1,1)$ y $k \geq 1$ un entero. Por medio del producto de Kronecker definimos una familia de vectores $c_i^k \in \mathbb{F}_2^{2^k}$, $0 \leq i \leq k$, de la siguiente manera:

$$c_0^k = u \otimes c_{k-1}^{k-1},\ c_1^k = v \otimes c_0^{k-1}, \ldots, c_{k-1}^k = v \otimes c_{k-2}^{k-1},\ c_k^k = v \otimes c_{k-1}^{k-1},$$

donde acordamos que $c_0^0 = 1 \in \mathbb{F}_2$ y $\otimes$ es el producto de Kronecker. (Para más detalles, el lector puede consultar la Sección 2.1 de este manuscrito.) Por la Proposición 2.1.2, el conjunto $\{c_0^k, \ldots, c_k^k\}$ es linealmente independiente sobre $\mathbb{F}_2$ y forma una base para el código de Reed-Muller de primer orden, $\mathrm{RM}(1,k)$, (Lema 2.1.3). Es importante tener en cuenta que todos los vectores en $\mathrm{RM}(1,k)$, excepto los vectores $(1)_{2^k}$ y $(0)_{2^k}$ tienen peso de Hamming igual a 2^{k-1}.

Recordemos que dado un entero $k \geq 1$ fijo, cualquier $z \in \mathbb{Z}_{2^{k+1}}$ puede ser escrito de manera única en su representación 2-ádica. Esto es, z puede ser escrito como

$$z = r_0(z) + r_1(z)2 + \cdots + r_{k-1}(z)2^{k-1} + r_k(z)2^k,$$

donde $r_i(z) \in \{0,1\}$, $1 \leq i \leq k$. De esta expresión se ve que un elemento $z \in \mathbb{Z}_{2^{k+1}}$ es una unidad en $\mathbb{Z}_{2^{k+1}}$ si y sólo si $r_0(z) = 1$. En consecuencia, para todo $z \in \mathbb{Z}_{2^{k+1}}$ es una unidad o pertenece al ideal maximal $\langle 2 \rangle$.

Si $Z = (z_0, z_1, \ldots, z_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$, entonces cada coordenada z_i de Z puede ser escrito en su representación 2-ádica, digamos

$$z_i = r_0(z_i) + r_1(z_i)2 + \cdots + r_{k-1}(z_i)2^{k-1} + r_k(z_i)2^k.$$

Esto implica que, haciendo uso de la estructura de $\mathbb{Z}_{2^{k+1}}$-módulo de $\mathbb{Z}_{2^{k+1}}^n$, el elemento Z puede ser escrito de manera única en su representación 2-ádica:

$$Z = r_0(Z) + r_1(Z)2 + \cdots + r_{k-1}(Z)2^{k-1} + r_k(Z)2^k,$$

donde $r_j(Z) = (r_j(z_0), r_j(z_1), \ldots, r_j(z_{n-1})) \in \{0,1\}^n$. Recordemos que la suma sobre $\mathbb{Z}_4$ y la suma binaria (Corolario 2.3.3) están ligadas de la siguiente manera:

Lema B.1.1. *Para cualesquiera $A, B \in \{0,1\}^n \subseteq \mathbb{Z}_4^n$ y cualesquiera $y, z \in \mathbb{Z}_4$*

$$2(Ay + Bz) = 2(Ar_0(y) \oplus Br_0(z)),$$

donde la suma "$\oplus$" del lado derecho de la expresión anterior es la suma sobre $\mathbb{F}_2^n$.

Para todo $k \geq 1$ definimos el *peso homogéneo* $\omega_h : \mathbb{Z}_{2^{k+1}} \to \mathbb{Z}$ como

$$\omega_h(a) = \begin{cases} 0, & a = 0 \\ 2^k, & a = 2^k \\ 2^{k-1}, & \text{en otro caso} \end{cases}$$

Esta aplicación se extiende a una función $\omega_h : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}$ de manera natural. Esto es, para todo $Z = (z_0, \ldots, z_{n-1})$ se define $\omega_h(Z) = \omega_h(z_0) + \cdots + \omega_h(z_{n-1})$. La métrica $\delta_h : \mathbb{Z}_{2^{k+1}}^n \times \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}$ inducida por ω_h es llamada la *distancia homogénea* y definida como $\delta_h(A,B) = \omega_h(A - B)$.

Finalmente, recordemos que para todo $Z \in \mathbb{Z}_{2^{k+1}}^n$ definimos la función $\varphi : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}_4^{2^{k-1}n}$ como

$$\varphi(Z) = c_{k-1}^{k-1} \otimes r_0(Z) + 2\left[\left(c_0^{k-1} \otimes r_1(Z)\right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes r_k(Z)\right)\right].$$

Note que si $k = 1$, entonces φ es la función identidad sobre $\mathbb{Z}_4^n$. Asimismo, note que la definición de $\varphi(Z)$ está dada en términos de su representación 2-ádica. Las siguientes propiedades de la función φ son importantes (Corolario 2.3.6), para lo cual señalamos que $2^k Z \odot 2Z = 2^k r_0(Z) * r_{k-1}(Z)$, donde $r_0(Z), r_{k-1}(Z) \in \{0,1\}^n$ son las componentes que aparecen en la respresentación 2-ádica del vector $Z \in \mathbb{Z}_{2^{k+1}}^n$ y "$*$" es la multiplicación coordenada por coordenada.

Lema B.1.2. *Sean $n \geq 1$, $k \geq 2$ enteros y sean $Y, Z \in \mathbb{Z}_{2^{k+1}}^n$. Entonces*

1. $\varphi(2^k Y + Z) = \varphi(2^k Y) + \varphi(Z) = 2\varphi(Y) + \varphi(Z)$,
2. $\varphi(2^k Z + Z) = -\varphi(Z)$,
3. $\varphi(2^{k-1} Z + Z) = \varphi(2^{k-1} Z) + \varphi(Z) + \varphi(2^k Z \odot 2Z)$,
4. $\varphi(2^{k-1} Z + 2^k Z + Z) = \varphi(2^{k-1} Z) - \varphi(Z) + \varphi(2^k Z \odot 2Z)$.

Sean $n \geq 1$ un entero, $Z = (z_0, \ldots, z_{n-1}) \in \mathbb{Z}_{k+1}^n$ y escriba a Z como $Z = A + B$, donde $A = (z_0, \ldots, z_{n-2}, 0)$ y $B = (0, \ldots, 0, z_{n-1})$. Entonces, para todo entero i tal que $0 \leq i \leq k$, obtenemos que $r_i(A+B) = r_i(A) \oplus r_i(B)$ y, por lo tanto,

$$c_j^{k-1} \otimes r_j(Z) = c_j^{k-1} \otimes (r_i(A) \oplus r_j(B)) = \left(c_j^{k-1} \otimes r_j(A)\right) \oplus \left(c_j^{k-1} \otimes r_i(B)\right), \quad 0 \leq j \leq k-1.$$

Con el propósito de simplicar y darle claridad a las demostraciones que presentaremos a continuación, para cualesquiera dos enteros $m, n \geq 1$ definimos los siguientes conjuntos:

$$I(m,n) = \{n-1, 2n-1, 3n-1, \ldots, mn-1\}, \tag{B.1}$$
$$J(m,n) = \mathbb{Z}_{mn} \setminus I(m,n). \tag{B.2}$$

Lema B.1.3. *Sean $n \geq 2, k \geq 1$ enteros y $Z \in \mathbb{Z}_{2^{k+1}}^n$. Entonces*

$$\varphi(Z) = \varphi(A) + \varphi(B).$$

Para más detalles acerca de estos úlitmos puntos, refiérase a la Sección 3.3.

B.2. Resultado principal

El siguiente resultado es útil para establecer que la aplicación φ es una isometría entre $(\mathbb{Z}_{2^{k+1}}^n, \delta_h)$ y $(\mathbb{Z}_4^{2^{k-1}n}, \delta_L)$, donde δ_h y δ_L son la distancia homogénea y de Lee, respectivamente.

Lema B.2.1. *Sean $n \geq 1, k \geq 1$ enteros y considere a los vectores $Y = (y_0, \ldots, y_{n-1}) = A_1 + B_1$ y $Z = (z_0, \ldots, z_{n-1}) = A + B$ de $\mathbb{Z}_{2^{k+1}}^n$, donde $B_1 = (0, \ldots, 0, y_{n-1})$ y $B = (0, \ldots, 0, z_{n-1})$. Entonces*

1. $\delta_L(\varphi(A_1), \varphi(A)) = \delta_L(\varphi(y_0, \ldots, y_{n-2}), \varphi(z_0, \ldots, z_{n-2}))$.
2. $\delta_L(\varphi(B_1), \varphi(B)) = \delta_L(\varphi(y_{n-1}), \varphi(z_{n-1}))$.

Demostración. Por definición $\delta_L(\varphi(A_1), \varphi(A)) = \omega_L(\varphi(A_1) - \varphi(A))$, donde

$$\begin{aligned}\varphi(A_1) - \varphi(A) &= \varphi(A_1) + 3\varphi(A) \\ &= c_{k-1}^{k-1} \otimes r_0(A_1) + 2\left[\left(c_0^{k-1} \otimes r_1(A_1)\right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes r_k(A_1)\right)\right] + \\ &\qquad c_{k-1}^{k-1} \otimes 3r_0(A) + 2\left[\left(c_0^{k-1} \otimes r_1(A)\right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes r_k(A)\right)\right].\end{aligned}$$

Por el Corolario 2.3.3, la expresión anterior es igual a la siguiente:

$$c_{k-1}^{k-1} \otimes X_0 + 2\left[\left(c_0^{k-1} \otimes X_1\right) \oplus \cdots \oplus \left(c_{k-1}^{k-1} \otimes X_k\right)\right], \tag{B.3}$$

donde $X_0 = r_0(A_1) + 3r_0(A)$ y $X_i = r_i(A_1) + r_i(A)$, $1 \leq i \leq k$. Dado $i \in \{0,1,\ldots,k-1\}$, supongamos que

$$c_i^{k-1} = (\varepsilon_{i,0},\ldots,\varepsilon_{i,2^{k-1}-1}) \in \mathbb{F}_2^{2^{k-1}}.$$

Con la introducción de esta notación, cada producto de Kronecker $c_i^{k-1} \otimes A_j$ involucrado en la expresión (B.3) es igual a la concatenación de los renglones de la siguiente matriz

$$\begin{pmatrix} \varepsilon_{i,0}(r_j(z_0)+3r_j(z_0)) & \cdots & \varepsilon_{i,0}(r_j(z_{n-1})+3r_j(z_{n-1})) & 0 \\ \varepsilon_{i,1}(r_j(z_0)+3r_j(z_0)) & \cdots & \varepsilon_{i,1}(r_j(z_{n-1})+3r_j(z_{n-1})) & 0 \\ \vdots & \ddots & \vdots & \vdots \\ \varepsilon_{i,2^{k-1}-1}(r_j(z_0)+3r_i(z_0)) & \cdots & \varepsilon_{i,2^{k-1}-1}(r_j(z_{n-1})+3r_j(z_{n-1})) & 0 \end{pmatrix}.$$

Ya que cada coordenada de la última columna de la matriz anterior tiene peso de Lee igual a cero, podemos eliminarla para obtener

$$\begin{pmatrix} \varepsilon_{i,0}(r_j(z_0)+3r_j(z_0)) & \cdots & \varepsilon_{i,0}(r_j(z_{n-1})+3r_j(z_{n-1})) \\ \varepsilon_{i,1}(r_j(z_0)+3r_j(z_0)) & \cdots & \varepsilon_{i,1}(r_j(z_{n-1})+3r_j(z_{n-1})) \\ \vdots & \ddots & \vdots \\ \varepsilon_{i,2^{k-1}-1}(r_j(z_0)+3r_j(z_0)) & \cdots & \varepsilon_{i,2^{k-1}-1}(r_j(z_{n-1})+3r_j(z_{n-1})) \end{pmatrix}.$$

Concatenando los renglones de esta última matriz, obtenemos

$$c_i^{k-1} \otimes \big((r_j(y_0,\ldots,y_{n-1})) - (r_j(z_0,\ldots,z_{n-1}))\big),$$

de donde se sigue que $\omega_L(\varphi(A_1)-\varphi(A)) = \omega_L(\varphi(y_0,\ldots,y_{n-1}) - \varphi(z_0,\ldots,z_{n-1}))$. De manera análoga se ve que $\omega_L(\varphi(B_1)-\varphi(B)) = \omega_L(\varphi(y_n)-\varphi(z_n))$. □

De la definición de la distancia homogénea, es claro que para todo $y,z \in \mathbb{Z}_{2^{k+1}}$, $\delta_h(y,z)$ puede tomar los siguientes valores:

$$\delta_h(y,z) = \begin{cases} 0, & \text{si } y = z \\ 2^k, & \text{si } y = 2^k + z \\ 2^{k-1}, & \text{en otra situación} \end{cases}$$

Si $y = z$, entonces $0 = \delta_L(\varphi(y),\varphi(z)) = \delta_h(y,z)$. Si $y = 2^k + z$, se sigue del Lema B.1.2 que

$$\varphi(y) = \varphi(2^k + z) = \varphi(2^k) + \varphi(z) = (2)_{2^{k-1}} + \varphi(z),$$

y por lo tanto, $\delta_L(\varphi(y),\varphi(z)) = \omega_L(\varphi(y)-\varphi(z)) = \omega_L((2)_{2^{k-1}}) = 2^k = \delta_h(y,z)$.

En el último caso, si $y-z \notin \{0,2^k\}$, entonces existen dos posibilidades: $y-z \in \langle 2 \rangle$ o bien $y-z$ es una unidad. Si $y-z \in \langle 2 \rangle$, entonces

$$\varphi(y-z) = 2[c_0^{k-1} r_1(y-z) \oplus \cdots \oplus c_{k-1}^{k-1} r_k(y-z)],$$

y ya que

$$c_0^{k-1} r_1(y-z) \oplus \cdots \oplus c_{k-1}^{k-1} r_k(y-z) \in RM(1,k-1) \setminus \{(0)_{2^{k-1}}, (1)_{2^{k-1}}\},$$

obtenemos $\omega_L(\varphi(y-z)) = 2^{k-1}$. Además, como $y-z \in \langle 2 \rangle$, sucede una de las siguientes situaciones: y y z son divisores de cero o bien y y z son unidades. Note que en ambos casos $\varphi(y) - \varphi(z)$ es precisamente de la forma

$$2[c_0^{k-1}(r_1(y) \oplus r_1(z)) \oplus \cdots \oplus c_{k-1}^{k-1}(r_k(y) \oplus r_k(z))],$$

donde

$$c_0^{k-1}(r_1(y) \oplus r_1(z)) \oplus \cdots \oplus c_{k-1}^{k-1}(r_k(y) \oplus r_k(z)) \in RM(1,k-1) \setminus \{(0)_{2^{k-1}}, (1)_{2^{k-1}}\}.$$

Por lo tanto, $\delta_L((\varphi(y), \varphi(z))) = \omega_L(\varphi(y) - \varphi(z)) = 2^{k-1} = \delta_h(y,z)$.

La segunda posibilidad se da cuando $y-z$ es una unidad. Entonces $\varphi(y-z)$ tiene todas sus coordenadas iguales a 1 o 3 y así, $\omega_L(\varphi(y-z)) = 2^{k-1}$. Por otro lado, como $y-z$ es una unidad, sucede que $r_0(y) = 1$ o $r_0(z) = 1$ pero no ambos. Consecuentemente, $\varphi(y) - \varphi(z)$ tiene todas sus coordenadas iguales a 1 o 3. De este modo, $\omega_L(\varphi(y) - \varphi(z)) = 2^{k-1}$. Entonces

$$\delta_L(\varphi(y), \varphi(z)) = \omega_L(\varphi(y) - \varphi(z)) = \omega_L(\varphi(y-z)) = \omega_h(y-z) = \delta_h(y,z).$$

En resumen, el análisis anterior demuestra que $\varphi : (\mathbb{Z}_{2^{k+1}}, \delta_h) \to (\mathbb{Z}_4^{2^{k-1}}, \delta_L)$ es una isometría.

Teorema B.2.2. *Para todo $n,k \geq 1$, la función $\varphi : (\mathbb{Z}_{2^{k+1}}^n, \delta_h) \to (\mathbb{Z}_4^{2^{k-1}n}, \delta_L)$ es una isometría.*

Demostración. Por inducción sobre n. Supongamos que para algún $n \geq 1$ el enunciado se cumple y sean $Y = A_1 + B_1$, $Z = A + B \in \mathbb{Z}_{2^{k+1}}^{n+1}$. Entonces

$$\begin{aligned}
\delta_L(\varphi(Y), \varphi(Z)) &= \omega_L(\varphi(A_1) + \varphi(B_1) - \varphi(A) - \varphi(B)) \\
&= \omega_L(\varphi(A_1) - \varphi(A) + \varphi(B_1) - \varphi(B)) \\
&= \omega_L(\varphi(A_1) - \varphi(A)) + \omega_L(\varphi(B_1) - \varphi(B)) \\
&= \delta_L(\varphi(A_1), \varphi(A)) + \delta_L(\varphi(B_1), \varphi(B)),
\end{aligned}$$

donde la última igualdad se justifica pues el arreglo $\varphi(A_1) - \varphi(A)$ tiene ceros en $I(k,n)$ y el arreglo $\varphi(B_1) - \varphi(B)$ tiene ceros en $J(k,n)$. Ahora, aplicamos el Lema B.2.1 y la hipótesis de

inducción para obtener

$$\begin{aligned}\delta_L(\varphi(Y),\varphi(Z)) &= \delta_L(\varphi(A_1),\varphi(A)) + \delta_L(\varphi(B_1),\varphi(B)) \\ &= \delta_L(\varphi(y_0,\ldots,y_{n-1}),\varphi(z_0,\ldots,z_{n-1})) + \delta_L(\varphi(y_n),\varphi(z_n)) \\ &= \delta_h((y_0,\ldots,y_{n-1}),(z_0,\ldots,z_{n-1})) + \delta_h(y_n,z_n) \\ &= \delta_h(y_0,z_0) + \cdots + \delta_h(y_{n-1},z_{n-1}) + \delta_h(y_n,z_n) \\ &= \delta_h(Y,Z).\end{aligned}$$

Por lo tanto, $\delta_L(\varphi(Y),\varphi(Z)) = \delta_h(Y,Z)$, lo que finaliza la prueba. □

Referencias

[1] T. Abualrub and R. Oehmke, *Cyclic codes of lenght* 2^e *over* $\mathbb{Z}_4$, Discrete Applied Mathematics **128** (2003), no. 1, 3-9.

[2] E. F. Assmus and J. D. Key, *Designs and their Codes (Cambridge Tracts in Mathematics)*, Cambridge University Press, Cambridge, 1994.

[3] T. Asamov and A. Nuh, *The* Z_4 *database* (2011-09-26), www.asamov.com/Z4Codes/.

[4] A. Ashikhmin and A. R. Calderbank, *Space-time Reed-Muller codes for noncoherent MIMO transmission*, Proceedings. International Symposium on Information Theory. ISIT 2005. (2005), 1952 - 1956.

[5] I. F. Blake, *Codes over certain rings*, Information and Control **20** (1972), no. 4, 396-404.

[6] _____, *Codes over integer residue rings*, Information and Control **29** (1975), no. 4, 295-300.

[7] E. R. Berlekamp, *Algebraic Coding Theory*, Revised 1984 edition, Aegean Park Press, New York, 1984.

[8] T. Blackford, *Cyclic codes over* $\mathbb{Z}_4$ *of oddly even length*, Discrete Applied Mathematics **128** (2003), no. 1, 27-46.

[9] _____, *Negacyclic codes over* $\mathbb{Z}_4$ *of even length*, IEEE Transactions on Information Theory **49** (2003), no. 6, 1417-1424.

[10] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links (London Mathematical Society Student Texts)*, Cambridge University Press, Cambridge, 1991.

[11] C. Carlet, $\mathbb{Z}_{2^k}$*-Linear Codes*, IEEE Transactions on Information Theory **44** (1998), no. 4, 1543-1547.

[12] H. Q. Dinh, *Negacyclic codes of lenght* 2^s *over Galois Rings*, IEEE Transactions on Information Theory **51** (2005), no. 12, 4252-4262.

[13] _____, *Constacyclic codes of lenght* 2^s *over Galois extensions rings of* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Transactions on Information Theory **55** (2009), no. 4, 1730-1740.

[14] H. Q. Dinh and S. R. López-Permounth, *Cyclic and Negacyclic codes over Finite Chain Rings*, IEEE Transactions on Information Theory **50** (2004), no. 8, 1728-1744.

[15] S. T. Dougherty and S. Ling, *Cyclic Codes over* $\mathbb{Z}_4$ *of even length*, Designs, Codes and Cryptography **39** (2006), no. 2, 127-153.

[16] S. T. Dougherty and Y. H. Park, *On Modular Cyclic Codes*, Finite Fields and Their Applications **13** (2007), no. 1, 31-57.

[17] S. T. Dougherty, B. Yildiz, and S. Karadeniz, *Codes over R_k, Gray Maps and their binary images*, Finite Fields and Their Applications **17** (2011), no. 3, 205-219.

[18] M. Grassi, *Bounds on the minimum distance of linear codes and quantum codes* (2011-09-26), http://www.codetables.de.

[19] M. Esmaeili, T. A. Gulliver, and N. P. Secord, *Quasi-Cyclic Structure of Reed-Muller Codes and their Smallest Regullar Trellis Diagram*, IEEE Transactions on Information Theory **43** (1997), no. 3, 1040-1052.

[20] M. J. E. Golay, *Notes on Digital Coding*, Proc. IRE **37** (1949), 637.

[21] M. Greferath and S. E. Schmidt, *Gray Isometries for Finite Chain Rings and a Nonlinear Ternary* $(36, 3^{12}, 15)$ *Code*, IEEE Transactions on Information Theory **45** (1999), no. 7, 2522-2524.

[22] R. W. Hamming, *Error Detecting and Correcting Codes*, Bell System Tech. J. **29** (1950), 147-160.

[23] 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 Transactions on Information Theory **40** (1994), no. 2, 301-319.

[24] B. Honary and G. Markarian, *Trellis Decoding of Block Codes: A Practical Approach (The Kluwer International Series in Engineering and Computer Science, 391)*, 1st ed., Kluwer Academic, Boston, 1997.

[25] T. Honold and I. Landjev, *Linear Codes over Finite Chain Rings*, The Electronic Journal of Combinatorics **7** (2000), no. R11, 1-22.

[26] R. A. Horn and C. R. Johnson, *Topics in Matrix Analisis*, Cambridge University Press, Cambridge, 1994.

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

[28] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, 1990.

[29] S. Jitman and P. Udomkavanich, *The Gray Image of Codes over Finite Chain Rings*, International Journal of Contemporary Mathematical Sciences **5** (2010), no. 9-12, 449-458.

[30] 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.

[31] H. M. Kiah, K. H. Leung, and S. Ling, *Cyclic codes over $GR(p^2, m)$ of length p^k*, Finite Fields and Their Applications **14** (2008), no. 3, 834-846.

[32] S. Lin, T. Kassami, T. Fujiwara, and M. Fossorier, *Trellises and Trellis-Based Decoding Algorithms for Linear Block Codes (The Kluwer International Series in Engineering and Computer Science 443)*, 1st ed., Kluwer Academic, Boston, 1998.

[33] S. Ling and T. Blackford, $\mathbb{Z}_{p^{k+1}}$*-Linear Codes*, IEEE Transactions on Information Theory **48** (2002), no. 9, 2592-2605.

[34] Z. Liu, *Notes on linear codes over finite commutative chain rings*, Acta Mathematicae Applicatae Sinica (English Series) **27** (2011), no. 1, 141-148.

[35] 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*, Lecture Notes in Computer Science, ICMCTA **5228** (2008), 107-116.

[36] ———, *On the Linearity and Quasi-Cyclicity of the Gray Image of Codes over Galois Rings*, Contemporary Mathematics **537** (2011), 255-268.

[37] S. López-Permounth and S. Zsabo, *Repeated roots cyclic and negacyclic codes over Galois Rings*, Lecture Notes in Computer Science, AAECC 2009 **5227** (2009), 219-222.

[38] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, The Netherlands: Nort-Holland, Amsterdam, 1977.

[39] B. McDonald, *Finite Rings with Identity*, Vol. 28, Pure and Applied Mathematics, New York, 1974.

[40] A. A. Nechaev, *Kerdock code in a cyclic form*, Discrete Mathematics and Applications **1** (1991), no. 4, 365–384.

[41] K. Paterson and A. E. Jones, *Efficient Decoding Algorithms for Generalized Reed-Muller Codes*, IEEE Transactions on Communications **48** (2000), no. 8, 1272-1275.

[42] V. Pless and N. J. A. Sloane, *On the Classification and Enumeration of Self-Dual Codes*, Journal of Combinatorial Theory, Series A **18** (1975), no. 3, 313-335.

[43] E. Rains and N. J. A. Sloane, *Self-Dual Codes*, Handbook of Coding Theory (V. S Pless and W. C. Huffman, eds.), Elsevier, Amsterdam, 1998, pp. 177-294.

[44] R. M. Roth, *Introduction to Coding Theory*, Cambridge University Press, Cambridge, 2006.

[45] S. Roman, *Coding and Information Theory (GTM)*, Springer-Verlag, New York, 1992.

[46] A. Sălăgean, *Repeated-root Cyclic and Negacyclic Codes over Finite Chain Rings*, Discrete Applied Mathematics **154** (2006), no. 2, 413-419.

[47] C. E. Shannon, *A Mathematical Theory of Communications*, Bell System Tech. J. **27** (1948), 379-423, 623-656.

[48] E. Spiegel, *Codes over* $\mathbb{Z}_m$, Information and Control **35** (1977), no. 1, 48-51.

[49] _____, *Codes over $\mathbb{Z}_m$, Revisited*, Information and Control **37** (1978), no. 1, 100-104.

[50] H. Tapia-Recillas, *The Gray Map on* $\mathrm{GR}(p^2,n)$ *and Repeated-Root Cyclic Codes*, Lecture Notes in Computer Science **2948** (2004), 181-196.

[51] H. Tapia-Recillas and G. Vega, *On $\mathbb{Z}_{2^k}$-Linear Codes and Quaternary Codes*, SIAM J. Discrete Math. **17** (2003), no. 1, 103-113.

[52] _____, *Some Constacyclic codes over $\mathbb{Z}_{2^k}$ and Binary Quasi-Cyclic Codes*, Discrete Applied Mathematics **128** (2003), no. 1, 305-316.

[53] J. H. Van Lint, *Coding, Decoding and Combinatorics*, Applications of Combinatorics (R.J. Wilson, ed.), Shiva Publishing, 1982, pp. 67-74.

[54] J. Wolfman, *Negacyclic and Cyclic Codes over* $\mathbb{Z}_4$, IEEE Transactions on Information Theory **45** (1999), no. 7, 2527-2532.

[55] _____, *Binary Images of Cyclic Codes over* $\mathbb{Z}_4$, IEEE Transactions on Information Theory **47** (2001), no. 5, 1773-1779.

[56] H. Xiang-Dong, J. T. Lahtonen, and S. Koponen, *The Reed-Muller code* $\mathrm{R}(r,m)$ *is not* $\mathbb{Z}_4$*-linear for* $3 \leq r \leq m-2$, IEEE Transactions on Information Theory **44** (1998), no. 2, 798-799.

[57] B. Yildiz and S. Karadeniz, *Linear codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Designs, Codes and Criptography **54** (2010), 61-81.

[58] E. Zhi, *A Database on Binary Quasi-Cyclic Codes* (2011-09-26), http://www.tec.hkr.se/~chen/research/codes/searchqc2.htm.

[59] Z. Zhu and X. Kai, *A Class of Constacyclic codes over $\mathbb{Z}_{p^m}$*, Finite Fields and Their Applications **16** (2010), no. 4, 243-254.