Correlación de códigos ortogonales ópticos en una y dos dimensiones

Hamilton Mauricio Ruiz

Universidad del Cauca
Facultad de Ciencias Naturales, Exactas y de la Educación
Departamento de Matemáticas
Doctorado en Ciencias Matemáticas
Popayán
Marzo de 2023

Correlación de códigos ortogonales ópticos en una y dos dimensiones

Hamilton Mauricio Ruiz

Tesis presentada como requisito parcial para optar al título de:
Doctor en Ciencias Matemáticas

Director
Carlos Alberto Trujillo Solarte
Profesor de la Universidad del Cauca

Universidad del Cauca
Facultad de Ciencias Naturales, Exactas y de la Educación
Departamento de Matemáticas
Doctorado en Ciencias Matemáticas
Popayán
Marzo de 2023

NOTA DE ACEPTACIÓN

ACEPTADO

JUAN JOSE RUE PERNA - DNI 47679540B (TCAT)

Firmado digitalmente por JUAN JOSE RUE PERNA - DNI 47679540B (TCAT)
Fecha: 2023.02.28 14:31:22 +01'00'

Firma jurado, Dr. Juanjo Rué Perna

Javier A de la Cruz

Firma jurado, Dr. Javier Alfonso de la Cruz Cantillo

DIANA HAIDIVE BUENO C

Firma jurado, Dra. Diana Haidive Bueno

Popayán, 21 de febrero de 2023

Universidad del Cauca	Gestión Administrativa y Financiera Gestión de Admisiones, Registro y Control Académico Acta para Sustentación Pública de Trabajo de Grado	
Código: PA-GA-4.2-FOR-13	Versión: 2	Fecha de Actualización: 22-01-2019

Trabajo de Investigación (☒)	Pasantía (☐)	Seminario (☐)
Práctica Social (☐)	Monografía (☐)	Preparatorios (☐)

Fecha: 21 de febrero de 2023 Facultad: Facultad de Ciencias Naturales, Exactas y de la Educación

Lugar: Aula Máxima Edificio de Matemáticas Hora: 10 a.m.

Programa:	Doctorado en Ciencias Matemáticas	
1. Alumno: Hamilton Mauricio Ruiz	C.C: 1.085.247.118	Código: 220_1085247118
2. Alumno:	C.C:	Código:
3. Alumno:	C.C:	Código:
4. Alumno:	C.C:	Código:
5. Alumno:	C.C:	Código:
6. Alumno:	C.C:	Código:
7. Alumno:	C.C:	Código:
8. Alumno:	C.C:	Código:

Nombre del Director: Dr. Carlos Alberto Trujillo Solarte

Nombre del Trabajo: "Correlación de códigos ortogonales ópticos en una y dos dimensiones"

INFORME SOBRE LA SUSTENTACIÓN

Cumplimiento de Objetivos:
Los objetivos de su propuesta de investigación se cumplieron a cabalidad.

Desarrollo Metodológico: El trabajo de la tesis de Mauricio se ubica en la intersección de la teoría de códigos, la teoría aditiva y combinatoria de números. Interactúan conceptos y resultados de los códigos ortogonales ópticos y los conjuntos de Sidon.
El estudiante realizó una muy buena presentación y respondió con suficiencia a todas las preguntas realizadas por los jurados.

Logros del Trabajo o Aportes: Destacamos el detalle y la organización en la que se presentan los resultados, junto con la claridad en los argumentos. Los resultados derivados de la tesis son de buena calidad, algunos ya publicados y sometidos a revistas de la rama IEEE. Los objetivos de la formación doctoral de un candidato (sistematización, investigación y modificación del estado del arte) se han superado.
La disertación incluye contribuciones interesantes, de buena calidad y suficientemente novedosos, respaldados por publicaciones y presentaciones en ambientes académicos especializados.

Se considera el Trabajo de Grado de alto valor académico para que se le confiera:

MENCION HONORÍFICA SI (☐) NO (☐)

CALIFICACIÓN DE LAUREADO SI (☐) NO (☐)

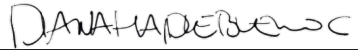
La tesis presenta aportes de gran calidad matemática que dieron origen a dos artículos, uno publicado y otro sometido en revistas de alto impacto e importancia científica, lo que evidencia la validación de expertos internacionales. Adicionalmente, el estudiante ha presentado sus resultados en diferentes eventos de carácter nacional e internacional, además hizo una muy buena presentación y respondió con suficiencia las preguntas de los jurados. El trabajo de tesis es un documento bien escrito y sus resultados de investigación tienen potencial para continuar desarrollándose.
Por lo anterior, aunque no se cumple algún requisito administrativo de la Facultad de Ciencias Naturales, Exacta y de la educación, el Jurado considera que el trabajo debe ser objeto de una distinción académica.

Otorgadas respectivamente por los Consejos de Facultad y Académico.
Sustentar brevemente: (Si es del caso ampliar el concepto por escrito, con Vº Bº del Depto. Anexo que debe hacer llegar al Consejo de Facultad):

CALIFICACIÓN FINAL		OSERVACIONES ADICIONALES
APROBADO	☒	
APROBADO CON CONDICIONES	☐	
APLAZADO	☐	
NO APROBADO	☐	

JURADOS

NOMBRE: Dr. Juanjo Rué Perna	NOMBRE: Dr. Javier Alfonso de la Cruz Cantillo
FIRMA: JUAN JOSE RUE PERNA - DNI 47679540B (TCAT) Firmado digitalmente por JUAN JOSE RUE PERNA - DNI 47679540B (TCAT) Fecha: 2023.02.21 18:25:24 +01'00'	FIRMA: Javier A de la Cruz
C.C. Nº: DNI (España) 47679540B	C.C. Nº: 7598640

NOMBRE: Dra. Diana Haidive Bueno	NOMBRE:
FIRMA: 	FIRMA:
C.C. Nº: 37520684	C.C. Nº:

Agradecimientos

Para empezar, quiero agradecer a Dios, por bendecir todos los proyectos que tiene para mi.

A mi madre, Luz Marina Ruiz, por el gran amor y apoyo que me brindi en vida y por el que me sigues brindando desde el cielo.

A mis hermanos, sobrinos, mi novia y demás familiares por todo el apoyo sentimental y moral que brindan en el desarrollo de mis proyectos.

A la Universidad del Cauca, especialmente al programa de Doctorado en Ciencias Matenáticas, por su excelente planta docente y directiva, que tanto aporto en mi formación personal y académica.

A Ministerio de Ciencia, Tecnología e Innovación por la oportunidad otorgada por medio de su sistemas de becas para adelantar mis estudios de posgrado.

A la PhD Diana Bueno, el PhD Juango Rué y el PhD Javier de la Cruz por la diligencia, comentarios y sugerencias en la revisión de este trabajo.

A mi compañero de estudio, Luis Miguel Delgado, por cada día compartido y dedicado al estudio de las matemáticas.

Al PhD John Castillo de la Universidad de Nariño por su motivación y apoyo para adelantar mis estudios de posgrado.

Y finalmente y no menos importante, mis más sinceros agradecimientos a mi director de trabajo grado, PhD Carlos Alberto Trujillo Solarte por brindarme la oportunidad de continuar mis estudios de posgrado, por confiarme sus conocimientos y haber aceptado la orientación de este trabajo de investigación.

Hamilton Mauricio Ruiz

Universidad del Cauca
Febrero 21 de 2023.

A mi madre, Luz Marina Ruiz, por el gran amor, por el apoyo ilimitado e incondicional que siempre tuvo en toda su vida, por tener siempre la fortaleza para salir adelante sin importar los obstáculos, por haberme formado como un hombre de bien, y por ser la mujer que me dio la vida y me enseñó a vivirla... no hay palabras en este mundo para agradecerte, Te amo mamá.

Resumen

El siguiente trabajo de investigación contiene el estudio de una familia de códigos denominada códigos ortogonales ópticos, los cuales son de vital importancia en sistemas de acceso múltiple por división de código. La investigación se centra principalmente en el estudio de la correlación de varias familias de códigos y también de conjuntos de Sidon, primordial para construir familias de códigos óptimos para infinitos valores de la longitud y peso. En el trabajo se combinan diferentes herramientas teóricas de Teoría de Números, Cuerpos Finitos, Combinatoria, entre otras. Los resultados de este estudio muestran que bajo ciertas condiciones es posible obtener códigos óptimos que mejoran los resultados presentados hasta el momento. También presentamos algunos problemas abiertos para futuras investigaciones. Algunos resultados importantes obtenidos durante el desarrollo de este trabajo se presentan publicados y otros en proceso de publicación.

Palabras clave: correlación, código ortogonal óptico, conjunto de Sidon, acceso múltiple por división de código, cuadrados latinos mutuamente ortogonales, conjuntos diferencia, teoría de números.

Abstract

The following research work contains the study of a family of codes called optical orthogonal codes, which are of vital importance in code division multiple access systems. The research focuses mainly on the study of the connections of several families of codes and also of Sidon sets, essential to build families of optimal codes for infinite values of length and weight. In the work, different theoretical tools of Number Theory, Finite Fields, Combinatorics, among others, are combined. The results of this study show that under certain conditions it is possible to obtain optimal codes that improve the results presented so far. We also present some open problems for future research. Some important results obtained during the development of this work are published and others are in the process of being published.

Keywords: correlation, optical orthogonal code, Sidon set, code division multiple access, mutually orthogonal Latin squares, difference sets, number theory.

Productos de la investigación

Artículos

[27] *A new construction of optimal optical orthogonal codes from Sidon sets*, IEEE Review, **8** (2020), 100749–100753. Con C. Trujillo y L. Delgado.

[26] *Two-dimensional optical orthogonal codes from Sidon sets*. Sometido a evaluación en IEEE Access. Con John López y Carlos Trujillo.

Ponencias

- *Códigos ortogonales ópticos y conjuntos* $B_2[g]$. VIII Encuentro Nacional de Matemáticas y Estadística, Universidad del Tolima, Ibagué-Colombia, Mayo 2-4, 2018.
- *A new construction of optimal optical orthogonal codes from Sidon sets*. XXII Congreso Nacional de Matemáticas, Universidad del Cauca, Popayán-Colombia, Junio 10-14, 2019.
- *Construcciones combinatorias de códigos ortogonales ópticos*. Marco de interacción de la combinatoria aditiva y la teoría de códigos, Universidad Politécnica de Catalunya, Barcelona-España, Abril 22, 2022.
- *Some two-dimensional optical orthogonal codes from Sidon sets*. II conferencia de matemáticas aplicadas e industriales (MAPI 2), Universidad Pontificia Bolivariana de Medellín, Medellín-Colombia, Junio 8-10, 2022.

– *Algunas construcciones combinatorias de códigos ortogonales ópticos*. Seminario Aritmética y Geometría en Valparaíso, Universidad de Valparaíso, Valparaíso-Chile, Julio 4-11, 2022.

Índice general

Capítulo 1

Introducción

Un problema importante que se presenta en los sistemas de comunicación consiste en diseñar técnicas de acceso múltiple. En este contexto, *múltiple* hace referencia al hecho de que varios usuarios tengan la posibilidad de establecer una comunicación simultánea por medio del uso del mismo canal de comunicación, evitando las interferencias que puedan ocurrir (interferencia de acceso múltiple (en inglés, multiple access interference (MAI)). En la actualidad, existen varias técnicas de acceso múltiple, una de éstas se denomina *acceso múltiple por división de código* (en inglés, code division multiple access (CDMA)). En un CDMA, varios usuarios asincrónicos hacen uso del mismo canal de comunicación de manera simultánea. El objetivo del CDMA consiste en extraer los datos con la información deseada incluso bajo la presencia de los datos de otros usuarios. Para lograr este objetivo se construye un conjunto de secuencias llamadas *palabras código* que cumplan las siguientes condiciones de correlación:

- cada secuencia es fácilmente distinguible de cada una de sus versiones cíclicas;
- cada secuencia es fácilmente distinguible de las otras secuencias (incluyendo sus versiones cíclicas).

La clase de secuencias llamada *códigos ortogonales ópticos* satisfacen las condiciones anteriores. Matemáticamente, algunas herramientas utilizadas en la construcción de éstos códigos son la teoría de diseños, geometría proyectiva, teoría de códigos, teoría de números, cuerpos finitos, entre otros, [6, 3, 22, 8, 9].
Por otro lado, un *conjunto de Sidon* es un subconjunto de un grupo con la propiedad de

que todas las diferencias no nulas entre sus elementos son distintas. Alternativamente, un conjunto de Sidon puede ser considerado como un código ortogonal óptico con una sola palabra código. Sin embargo, un código con una sola palabra código no es muy útil en la práctica, razón por la cual las construcciones de conjuntos de Sidon en grupos finitos han sido modificadas para obtener códigos ortogonales ópticos con más de una palabra código [22, 30, 27].

El propósito de este trabajo de investigación consiste en describir y analizar en detalle la propiedad de correlación de algunas familias de códigos ortogonales ópticos, así como de los conjuntos de Sidon sobre grupos finitos con el objetivo de optimizar el cardinal de los códigos estudiados tanto en una como en dos dimensiones.

En general, se realiza un enfoque algebraico para el estudio de la correlación. Sin embargo, también se realiza un tratamiento computacional que describa algunos de los procedimientos matemáticos usados en las construcciones. En este sentido, se hace uso del sistema de algebra computacional SAGE para programar los algoritmos correspondientes a cada una de las construcciones discutidas aquí.

El siguiente trabajo esta dividido en 6 capítulos. El presente capítulo presenta una introducción del trabajo. En el Capítulo 2 describimos los conceptos de código ortogonal óptico y conjuntos de Sidon en una y dos dimensiones. También presentamos algunas construcciones importantes de ambos conceptos. En el Capítulo 3 presentamos un análisis de la propiedad de la correlación cruzada para las construcciones asintóticamente óptimas de códigos ortogonales ópticos y cómo los resultados obtenidos pueden ser usados para obtener nuevas familias de códigos óptimos teniendo en cuenta ciertas condiciones sobre sus parámetros. El Capítulo 4 contiene nuevas construcciones de códigos ortogonales ópticos en dos dimensiones obtenidos a partir del estudio de la correlación de los conjuntos de Sidon en una y dos dimensiones. En el Capítulo 4 presentamos una construcción recursiva para códigos ortogonales ópticos en dos dimensiones. Los resultados obtenidos en este trabajo de investigación son presentados en el Capítulo 5. Finalmente, en el Capítulo 6 presentamos algunas conclusiones y problemas abiertos obtenidos del trabajo de investigación. Incluimos el Apéndice A con los principales algoritmos en SAGE empleados en el presente trabajo.

El contenido descrito anteriormente se realizó con el fin de alcanzar los siguientes objetivos.

1. Estudiar la estructura de las construcciones de códigos ortogonales ópticos asintóticamente óptimos.
2. Analizar la estructura y propiedades de las construcciones de conjuntos de Sidon

en dos dimensiones con el propósito de encontrar nuevas construcciones de códigos ortogonales ópticos en dos dimensiones.

3. Realizar una búsqueda computacional y estudiar nuevos conjuntos de Sidon en una dimensión para generar códigos ortogonales ópticos en una dimensión usando la construcción recursiva dada por Chu y Golomb [8].

4. Diseñar algoritmos para ejemplificar los conceptos y construcciones de códigos ortogonales ópticos obtenidos en esta investigación.

Los resultados más reelevantes obtenidos durante el desarrollo de este trabajo de investigación pueden consultarse en los siguientes artículos:

- H. M. Ruiz, L. M. Delgado and C. A. Trujillo, "A New Construction of Optimal Optical Orthogonal Codes From Sidon Sets," in *IEEE Access,* vol. 8, pp. 100749-100753, 2020.

- H. M. Ruiz, J. J López and C. A. Trujillo, "Some two-dimensional optical orthogonal codes from Sidon sets". Sometido a evaluación en IEEE. Octubre 2022.

Algunas charlas y minicursos que fueron importantes para el desarrollo y la divulgación de los resultados obtenidos en esta investigación se resumen a continuación:

- *Códigos ortogonales ópticos y conjuntos* $B_2[g]$. VIII Encuentro Nacional de Matemáticas y Estadística, Universidad del Tolima, Ibagué-Colombia, Mayo 2-4, 2018.

- Second Colombian Workshop on Coding Theory (CWC 19), Universidad del Norte, Barranquilla-Colombia, Enero 15-18, 2019.

- *A new construction of optimal orthogonal codes from Sidon sets.* Congreso Nacional de Matemáticas, Universidad del Cauca, Popayán-Colombia, Junio 10-14, 2019.

- *Introducción a la teoría de códigos.* Seminario Altenua Online, Universidad de Nariño, San Juan de Pasto-Colombia, Abril 22, 2021.

- *Cuadrados latinos y algunas de sus aplicaciones.* Seminario de estudiantes de posgrado en matemáticas SESPOMAT, Universidad del Cauca, Cauca, Popayán-Colombia, Marzo 14, 2022.

- *Construcciones combinatorias de códigos ortogonales ópticos*. Marco de interacción de la combinatoria aditiva y la teoría de códigos, Universidad Politécnica de Catalunya, Barcelona-España, Abril 22, 2022.
- *Some two-dimensional optical orthogonal codes from Sidon sets*. II conferencia de matemáticas aplicadas e industriales (MAPI 2), Universidad Pontificia Bolivariana de Medellín, Medellín-Colombia, Junio 8-10, 2022.
- *Algunas construcciones combinatorias de códigos ortogonales ópticos*. Seminario Aritmética y Geometría en Valparaíso, Universidad de Valparaíso, Valparaíso-Chile, Julio 4-11, 2022.

Participamos también en importantes reuniones, seminarios y pasantías con investigadores e investigadoras internacionales que proporcionaron algunas ideas usadas en el desarrollo de este trabajo.

- Elliptic Curves: Arithmetic and Computation, CIMPA research school, Universidad de la República, Montevideo-Uruguay, Febrero 11-22, 2019.
- Pasantía, Universidad Autónoma de México, campus Juriquilla, Querétaro-México, Julio-Octubre 2019. Investigadora encargada: Amanda Montejano.
- Pasantía, Universidad Autónoma de Zacatecas, Zacatecas-México, Julio 2021. Investigador encargado: Mario Huicoechea.
- Pasantía, Universidad Autónoma de México, campus Juriquilla, Querétaro-México, Noviembre-Diciembre 2021. Investigadora encargada: Amanda Montejano.
- Pasantía, Universidad Politécnica de Cataluña, Barcelona-España, Febrero-Marzo 2022. Investigadores encargados: Juanjo Rué y Oriol Serra.
- Pasantía, Universidad de Valparaíso, Valparaíso-Chile. Julio 2022. Investigadora encargada: Amalia Pizarro.

Capítulo 2

Preliminares

Iniciamos el siguiente trabajo de investigación presentando los conceptos básicos sobre códigos ortogonales ópticos y conjuntos de Sidon tanto en dimensión uno como en dimensión dos. La noción de código ortogonal óptico, dada por Chung, Salehi y Wei en [9], fue motivada por un problema que se presenta en algunos sistemas de comunicación. Este problema consiste básicamente en buscar técnicas y códigos adecuados que permitan que varios usuarios puedan utilizar un único canal de comunicación, evitando la interferencia de acceso múltiple que dichas comunicaciones ocasionan. Para reducir la interferencia en mención se diseñan códigos con buenas propiedades de autocorrelación y correlación cruzada.

2.1. Códigos ortogonales ópticos en una dimensión

Definición 2.1. Sean n, w, λ enteros positivos. Un código ortogonal óptico $\mathcal{C}$ con parámetros (n, w, λ) es una familia de secuencias binarias (palabras código) de longitud n, peso de Hamming w y correlación igual a λ que satisfacen las siguientes propiedades:

1. Autocorrelación: para todo $x \in \mathcal{C}$ y todo entero positivo $t \not\equiv 0 \mod n$ se tiene

$$\sum_{i=0}^{n-1} x_i x_{i+t} \leq \lambda. \tag{2.1}$$

2. Correlación cruzada: para todo $x, y \in \mathcal{C}$ con $x \neq y$ y todo entero positivo t se tiene

$$\sum_{i=0}^{n-1} x_i y_{i+t} \leq \lambda, \tag{2.2}$$

donde la suma que aparece en los subíndices de las Ecuaciones 2.1 y 2.2 es módulo n.

El número de palabras código de $\mathcal{C}$ es el tamaño del código ortogonal óptico y se denota por $|\mathcal{C}|$. Desde el punto de vista de las aplicaciones, los códigos ortogonales ópticos de gran tamaño son más importantes. Para un conjunto de valores dados de n, w y λ, se denota al mayor tamaño posible de un código ortogonal óptico con parámetros (n, w, λ) por $\Phi(n, w, \lambda)$. Un código que alcanza este valor se llama *óptimo*. La cota superior de Johnson para códigos correctores de errores de peso constante se puede adaptar para derivar una cota superior para el tamaño de un código ortogonal óptico con parámetros (n, w, λ). La cota de Johnson para $\Phi(n, w, \lambda)$ esta dada por

$$\Phi(n, w, \lambda) \leq \left\lfloor \frac{1}{w} \left\lfloor \frac{n-1}{w-1} \left\lfloor \frac{n-2}{w-2} \left\lfloor \cdots \left\lfloor \frac{n-\lambda}{w-\lambda} \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor \right\rfloor, \tag{2.3}$$

donde $\lfloor x \rfloor$ denota la función piso. En particular, para un código ortogonal óptico con parámetros $(n, w, 1)$, se tiene

$$\Phi(n, w, 1) \leq \left\lfloor \frac{n-1}{w(w-1)} \right\rfloor. \tag{2.4}$$

Un problema de interés en este campo consiste en determinar los valores exactos de la función $\Phi(n, w, \lambda)$, así como de las construcciones explícitas de los códigos que alcanzan dichos valores [9]. Cuando no es posible encontrar dichas construcciones óptimas se buscan construcciones asintóticas.

Definición 2.2. Sea $\mathcal{F}$ una familia de códigos ortogonales ópticos con parámetros $(n, w, 1)$ y tamaño L. Decimos que $\mathcal{F}$ es asintóticamente óptima si

$$\lim_{n\to\infty} \frac{L}{\Phi(n, w, 1)} = 1.$$

En esta investigación trabajamos con familias de códigos ortogonales ópticos con $\lambda = 1$. Para este caso, es conveniente representar los elementos de un código ortogonal óptico desde un punto de vista conjuntista, con el propósito de enunciar y analizar sus propiedades de correlación. Un código ortogonal óptico $\mathcal{C}$ con parámetros $(n, w, 1)$ puede

ser considerado como una familia de conjuntos cuyos elementos pertenecen al conjunto de enteros módulo n, denotado por $\mathbb{Z}_n$, donde cada conjunto tiene tamaño igual al peso w. Si $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in \mathcal{C}$, entonces $\mathbf{x}$ en notación conjuntista puede ser escrito como

$$\{k \in \mathbb{Z}_n : x_k = 1\}.$$

Sean $A, B \subset \mathbb{Z}_n$ y $x \in \mathbb{Z}_n$. La función de representación de x, denotada por $R_{A-B}(x)$ se define por

$$R_{A-B}(x) := |A \cap (x + B)|, \tag{2.5}$$

donde $x + B = \{x + b : b \in B\}$. Esta función cuenta el número de veces en las que x puede ser escrito como diferencia de un elemento de A y un elemento de B. Utlizando la notación conjuntista de un código y la función de representación, podemos enunciar las Propiedades (2.1) y (2.2) para un código ortogonal óptico con pámetros $(n, w, 1)$ de la siguiente manera:

1. Autocorrelación: para toda $A \in \mathcal{C}$ y todo $x \not\equiv 0 \mod n$ se tiene

$$R_{A-A}(x) \leq 1. \tag{2.6}$$

2. Correlación cruzada: para todo $A, B \in \mathcal{C}$ con $A \neq B$ y todo $x \in \mathbb{Z}_n$ se tiene

$$R_{A-B}(x) \leq 1. \tag{2.7}$$

Por otra parte, para un subconjunto X de un grupo aditivo G, denotamos por $\Delta(X)$ el conjunto de diferencias no nulas de X, es decir

$$\Delta(X) = \{a - b : a, b \in X, a \neq b\}. \tag{2.8}$$

Usando la notación anterior y la representación conjuntista para un código ortogonal óptico podemos enunciar el siguiente resultado.

Proposición 2.1. *[9] Sea $\mathcal{C}$ un código ortogonal óptico con parámetros $(n, w, 1)$. Entonces*

1. *Para todo $X \in \mathcal{C}$*

$$|\Delta(X)| = w(w - 1).$$

2. *Para todo $X, Y \in \mathcal{C}$ con $X \neq Y$*

$$\Delta(X) \cap \Delta(Y) = \emptyset.$$

Los métodos para construir códigos ortogonales ópticos pueden ser clasificados en dos casos: construcciones directas e indirectas [9]. Las construcciones directas usan estructuras matemáticas como geometría proyectiva, campos finitos, teoría de diseños, combinatoria, entre otras, mientras que las construcciones indirectas usan algoritmos computacionales tales como el algoritmo Greddy y algoritmo Greddy acelerado. Describimos a continuación algunas construcciones directas.
Los códigos ortogonales ópticos están relacionados con los diseños de empaquetamiento cíclicos óptimos [36]. Sea $\mathcal{F}$ una familia de subconjuntos de tamaño w del anillo de enteros módulo n denotado por $\mathbb{Z}_n$. Los elementos de $\mathcal{F}$ se llaman *bloques base*. Si $\Delta(\mathcal{F}) = \bigcup_{A\in\mathcal{F}} \Delta(A)$, cada elemento de $\mathbb{Z}_n$ aparece exactamente una vez en $\Delta(\mathcal{F})$ y para cada $A \in \mathcal{F}$ los conjuntos de la forma $A + i \subset \mathbb{Z}_n$ con $0 \leq i \leq n-1$, son disjuntos dos a dos, entonces la familia $\mathcal{F}$ se denomina un diseño de empaquetamiento cíclico con parámetros $2-(n, w, 1)$.

Si $\mathcal{F}$ es un diseño de empaquetamiento cíclico con parámetros $2-(n, w, 1)$, entonces la *deficiencia* L de $\mathcal{F}$ se define como aquel conjunto de enteros no cero en $\mathbb{Z}_n$ los cuales no pertenecen a $\Delta(\mathcal{F})$. Si además, L puede ser particionado en subconjuntos $L_1, L_2, \ldots, L_m$ tales que para cada $1 \leq i \leq m$ el conjunto $L_i \cup \{0\}$ forman un subgrupo de $\mathbb{Z}_n$ de orden g_i, entonces el diseño de empaquetamiento con parámetros $2-(n, w, 1)$ se llama $(g_1, g_2, \ldots, g_m)-$regular. Cuando $m = 1$, se dice simplemente que el diseño de empaquetamiento es $g-$regular.

Los resultados siguientes son consecuencia inmediata de las definiciones anteriores.

Proposición 2.2. *[36] Una condición necesaria para la existencia de un diseño de empaquetamiento cíclico con parámetros* $2-(n, w, 1)$ *y deficiencia* L *es*

$$n - |L| - 1 \equiv 0 \mod w(w-1).$$

Proposición 2.3. *[36] Un diseño de empaquetamiento cíclico con parámetros* $2-(n, w, 1)$ *y deficiencia* L *es óptimo, si el tamaño de* L *verifica* $0 \leq |L| \leq w(w-1)$.

Otra construcción de códigos ortogonales ópticos óptima fue presentada por Salehi y otros en [9] y se fundamenta en el uso de líneas y puntos sobre una geometría proyectiva finita. La construcción menciona que existe un código ortogonal óptico con parámetros $(n, w, 1)$ generado a partir de una geometría proyectiva $PG(d, q)$, donde d es un entero positivo y q es una potencia de un número primo tal que $n = \dfrac{q^{d+1}-1}{q-1}$ y $w = q+1$. El número de palabras código es igual a $\dfrac{q^d-1}{q^2-1}$ cuando d es par y $\dfrac{q^d-q}{q^2-1}$ cuando d is impar. En ambos casos se alcanza la cota de Johnson.

Por medio de métodos combinatorios, Chung, Salehi y Wei en [9] construyen códigos ortogonales ópticos óptimos con parámetros $(n, 3, 1)$ para todo $n \not\equiv 2 \mod 6$.

El trabajo de Wilson en [33] sobre diseño de bloques incompletos balanceados también ha sido una fuente para construir códigos ortogonales ópticos óptimos con parámetros $(n, w, 1)$. Las construcciones se describen a continuación.

Teorema 2.1. *Construcción 1 (Wilson): Sean $w = 2m + 1$ y $p = w(w-1)r + 1$, donde m y r son enteros positivos tales que p es un número primo. Sean α una raíz primitiva módulo p y $c = (w-1)r$. Denotemos por S_i para $0 \leq i \leq c-1$, al conjunto*

$$S_i = \{\alpha^{i+jc} : 0 \leq j \leq w-1\}.$$

Sea i_k el índice del conjunto S_i que contenga al elemento $\alpha^{kc} - 1$, para cada $1 \leq k \leq m$. Si $i_1, \ldots, i_m$ son todos distintos módulo m, entonces los conjuntos $S_0, S_m, \ldots, S_{(r-1)m}$ pueden ser tomados como palabras código de un código ortogonal óptico óptimo con parámetros $(p, w, 1)$.

Teorema 2.2. *Construcción 2 (Wilson): Sean $w = 2m$ y $p = w(w-1)r + 1$, donde m y r son enteros positivos tales que p es un número primo. Sean α una raíz primitiva módulo p y $c = wr$. Denotemos por S_i for $0 \leq i \leq c-1$, al conjunto*

$$S_i = \{\alpha^{i+jc} : 0 \leq j \leq w-2\} \cup \{0\}.$$

Sean $i_0, i_1, \ldots, i_{m-1}$ los índices de los conjunto S_i que contengan a los elementos $1, \alpha^c - 1, \ldots, \alpha^{(m-1)c} - 1$ respectivamente. Si $i_0, \ldots, i_{m-1}$ son todos distintos módulo m, entonces los conjuntos $S_0, S_m, \ldots, S_{(r-1)m}$ pueden ser tomados como palabras código de un código ortogonal óptico óptimo con parámetros $(p, w, 1)$.

Moreno y otros autores en [23] construyen tres familias de códigos ortogonales ópticos, dos de ellas para $\lambda = 1$. Resumimos a continuación dichas construccciones.

Familia $\mathcal{A}$. Sean p un número primo y m un divisor de $p-1$. Considere el conjunto

$$\mathcal{F} = \{f(x) = ax + b : f(x) \in \mathbb{F}_p[x], a \neq 0\}.$$

Sea α un elemento primitivo de $\mathbb{F}_p$ y $G = \{\alpha^{si} : i = 0, \ldots, m-1\}$ el subgrupo de $\mathbb{F}_p^*$ de orden m, donde $m = (p-1)/s$. Sobre $\mathcal{F}$ se define la siguiente relación de equivalencia: $f_1(x) \sim f_2(x)$ si y solo si existen $v \in G$ y $u \in \mathbb{F}_p$ tales que $f_1(x) = f_2(vx) + u$. Es fácil probar que cada clase de equivalencia contiene mp elementos. Sea $\mathcal{F}_A$ el conjunto de representantes de las clases de equivalencia, entonces $|\mathcal{F}_A| = \frac{p(p-1)}{pm} = s$. Para cada

$f(x) \in \mathcal{F}_A$ se construye una matriz A_f de tamaño $p \times m$ cuyas componentes son

$$A_f(i,j) = \begin{cases} 1 & \text{si } f(\alpha^{sj}) = p-1-i, \\ \\ 0 & \text{otro caso} \end{cases}$$

para $0 \leq i \leq p-1$ y $0 \leq j \leq m-1$. Para cada componente igual a 1 en la matriz A_f consideramos el sistema de congruencias

$$\begin{aligned} x &\equiv j \text{ mód } m \\ x &\equiv i \text{ mód } p \end{aligned} \tag{2.9}$$

donde $A_f(i,j) = 1$. Si S_f es la solución de cada sistema de congruencias, entonces

$$\mathcal{C} = \{S_f : f(x) \in \mathcal{F}_A\}$$

es un código ortogonal óptico asintóticamente óptimo con parámetros $(pm, m, 1)$ y s palabras código.

Familia $\mathcal{B}$: Sean m un entero positivo, p un número primo y $q = p^m$. Entonces existe un código ortogonal óptico asintóticamente óptimo respecto a la cota de Johnson cuando $p \to \infty$ con parámetros $(p(q-1), p-1, 1)$.

Chung y Yang en [11], presentan nuevas construcciones para códigos ortogonales ópticos asintóticamente óptimos.

Construcción $\mathcal{A}$ *(Chung and Yang)* Sean p un número primo, M y T enteros positivos tales que $p-1 = MT$, y n un entero positivo. Existe un código ortogonal óptico asintóticamente óptimo con parámetros $(Mp^n, M, 1)$ y T palabras código.

Construcción $\mathcal{B}$ *(Chung and Yang)* Sean $p_1, p_2, \ldots p_k$ números primos impares, M y T_i enteros positivos tales que $p_i - 1 = MT_i$ para $1 \leq i \leq k$. Existe un código ortogonal óptico asintóticamente óptimo con parámetros $(Mp_1p_2 \cdots p_k, M, 1)$ y $\dfrac{p_1p_2 \cdots p_k - 1}{M}$ palabras código. En particular, existe un código ortogonal óptico con parámetros $(Mp, M, 1)$ y $\dfrac{p-1}{M}$ palabras código, el cual es óptimo cuando $(M-1)^2 > p-1$.

Estudiamos más en detalle las construcciones asintóticas de códigos ortogonales ópticos en el Capítulo 3. Algunas de ellas se presentan de manera alternativa con el propósito de analizar su correlación y estudiar bajo qué condiciones se pueden optimizar sus cardinales.

Moreno y otros autores en [22], construyen un código ortogonal óptico óptimo con parámetros $(q^h - 1, q, 1)$, para toda potencia prima q y todo entero $h \geq 2$.

Teorema 2.3. *Generalización de Bose-Chowla (Moreno y otros autores). Sea q una potencia prima, $h \geq 2$ un entero, θ un elemento primitivo de $\mathbb{F}_{q^h}$ y*

$$\mathcal{P} = \{p(x) \in \mathbb{F}_p[x] : 1 \leq \deg(p(x)) \leq h-1, p(0) = 0 \text{ y } p(x) \text{ es mónico}\}.$$

Entonces

$$\mathcal{C} = \{\{\log_\theta(p(\theta) + a) : a \in \mathbb{F}_q\} : p(x) \in \mathcal{P}\}$$

es un código ortogonal óptico óptimo con parámetros $(q^h - 1, q, 1)$. En particular, si $h = 2$ el código obtenido coincide con la construcción de conjunto de Sidon dada por Bose-Chowla.

Chu and Golomb en [8] presentan una de las más interesantes construcciones recursivas para códigos ortogonales ópticos. En su trabajo los autores hacen uso del concepto de matrices $r-$*simples*. Los principales conceptos y resultados se resumen a continuación.

Definición 2.3. Sean G un grupo abeliano de orden n y r un entero positivo. Una matriz A de orden $s \times t$ sobre G se llama $r-$*simple*, si el vector diferencia de cualquier par de columnas de A contiene a cualquier elemento de G a lo sumo $r-1$ veces.

Lema 2.1. *Para cualquier número primo p y cualquier entero r, con $0 \leq r \leq p$, existe una matriz de orden $p \times p^{r-1}$ sobre $\mathbb{Z}_p$ $r-$simple.*

Teorema 2.4. *Suponga que existe un código ortogonal óptico con parámetros $(n, w, 1)$ y T palabras código. Sea p un número primo no menor que w. Entonces existe un código ortogonal óptico con parámetros $(np, w, 1)$ y Tp palabras código.*

Corolario 2.1. *Suponga que existe un código ortogonal óptico con parámetros$(n, w, 1)$ y T palabras código. Sea $m = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ un entero positivo, donde $p_1, p_2, \ldots p_t$ son números primos menores que w. Entonces existe un código ortogonal óptico con parámetros $(mn, w, 1)$ y Tm palabras código.*

Teorema 2.5. *Para cualquier potencia prima q, existe un un código ortogonal óptico con parámetros $(m(q^2+q+1), q+1, 1)$, donde m es un entero positivo cuyos divisores primos son más grandes que q. También, si $m < q^2+q+1$ el código obtenido es óptimo y tiene m palabras código.*

Corolario 2.2. *Sea q una potencia prima. Si todos los divisores de q^2+q+1 son más grandes que q, entonces para cada entero positivo t, existe un código ortogonal óptico óptimo con parámetros $((q^2+q+1)^t, q+1, 1)$.*

Un resumen de las construcciones de códigos ortogonales ópticos descritas anteriormente se muestran en la Tabla 2.1.

TABLA 2.1: Parámetros de códigos ortogonales ópticos con $\lambda = 1$, aquí p denota un número primo y q una potencia de p.

Nombre	Parámetros	Tamaño	Condiciones
Geometría proyectiva* [9]	$\left(\frac{q^{d+1}-1}{q-1}, q+1, 1\right)$	$\begin{cases} \frac{q^d-1}{q^2-1}, & d \text{ par}, \\ \frac{q^d-q}{q^2-1}, & d \text{ impar}. \end{cases}$	
Método combinatorio* [9]	$(n, 3, 1)$	$\lfloor \frac{n-1}{6} \rfloor$	$n \not\equiv 2$ mód 6
Generalización de Bose-Chowla* [22]	$(q^m - 1, q, 1)$	$\frac{q^{m-1}-1}{q-1}$	$m \geq 2$
Chu-Golomb* [8]	$(m(q^2+q+1), q+1, 1)$	m	Cada divisor primo de m es más grande que q y $m < q^2+q+1$
Chu-Golomb [8]	$((q^2+q+1)^t, q+1, 1)$	$(q^2+q+1)^{t-1}$	Los divisores primos de q^2+q+1 son más grandes que q
Construcción $\mathcal{A}$ de JK [11]	$(Mp^n, M, 1)$	$\frac{p^n-1}{M}$	$p-1 = MT$
Construcción $\mathcal{B}$ de JK* [11]	$(Mp, M, 1)$	T	$p-1 = MT$, $(M-1)^2 > p-1$
Generalización construcción $\mathcal{B}$ de JK [11]	$(Mp_1 \cdots p_k, M, 1)$	$\frac{p_1 \cdots p_k - 1}{M}$	$M \mid (p_i - 1)$ para $i = 1, \ldots, k$
Chung-Kumar* [33, 10]	$(p, w, 1)$	r	$p = w(w-1)r+1$ $w = 2t+1$, o $w = 2t$
Familia $\mathcal{A}$ de MZKZ [23]	(pm, m, t)	m divisor de $p-1$	$m \mid (p-1)$, $1 \leq t \leq m$
Familia $\mathcal{B}$ de MZKZ [23]	$((q-1)p, p-1, 1)$	$\frac{q}{p}$	$1 \leq t \leq (p-t)$

$*$ en la tabla indica que la construcción es óptima respecto a la cota de Johnson.

En el Capítulo 3, aplicamos la construcción recursiva para códigos ortogonales ópticos, a los conjuntos de Sidon y analizamos bajo qué condiciones el código obtenido es óptimo.

En la literatura, podemos encontrar una gran lista de publicaciones concernientes al problema de la existencia de códigos ortogonales ópticos óptimos. Algunos autores han clasificado las construcciones de códigos ortogonales ópticos óptimos para valores pequeños de w. Por ejemplo, en [9] se prueba que existen códigos ortogonales ópticos óptimos con parámetros $(n, 3, 1)$ para todo n excepto para $n = 6t + 2$ y $t \equiv 2, 3 \mod 4$. Cuando $w \geq 4$, el problema de la existencia de un código ortogonal óptico óptimo con parámetros $(n, w, 1)$ permanece aún sin resolver, aunque hay bastantes resultados para pesos pequeños. Resumimos algunos de ellos para $w = 4, 5, 6$.

Teorema 2.6. *[32] Existe un código ortogonal óptico óptimo con parámetros* $(v, 4, 1)$ *para todo* $v \leq 1212$*, excepto para* $v = 25$*.*

Las familias de diferencias perfectas también son útiles para construir códigos ortogonales ópticos. Sea $v = k(k-1)t+1$, entonces t bloques $B_i = \{b_{i1}, b_{i2}, \ldots, b_{ik}\}$, $1 \leq i \leq t$, forman una familia de diferencias perfecta con parámetros $(v, k, 1)$ sobre el anillo de enteros $\mathbb{Z}_v$, si las $tk(k-1)/2$ diferencias de la forma $b_{ic} - b_{ic'}$ $(1 \leq i \leq t, 1 \leq c' < c \leq k)$ cubren al conjunto $\{1, 2, \ldots, (v-1)/2\}$.

Teorema 2.7. *[32] Si existe una familia de diferencias perfecta con parámetros* $(g, 4, 1)$*, entonces*

1. *existe un código ortogonal óptico óptimo con parámetros* $((g+2)v, 4, 1)$ *para cada entero* v *cuyos factores primos son congruentes a 1 módulo 4;*

2. *existe un código ortogonal óptico óptimo con parámetros* $((g+1)v, 4, 1)$ *para cada entero* v *cuyos factores primos son congruentes a 1 módulo 6;*

3. *si* $g \equiv 1 \mod 48$*, entonces existe un código ortogonal óptico óptimo con parámetros* $((g+7)v, 4, 1)$ *para cada entero* v *cuyos factores primos son congruentes a 1 módulo 6.*

Mostramos a continuación algunos resultados conocidos sobre la existencia de códigos ortogonales ópticos con parámetros de $(n, w, 1)$ para $k = 5$ y $k = 6$.

Teorema 2.8. *[17, Hanani] Para cada número primo* $p \equiv 1 \mod 4$ *con* $p \neq 5$ *existe un código ortogonal óptico óptimo con parámetros* $(5p, 5, 1)$*.*

Teorema 2.9. *[37, Tang and Ying] Sea v un entero positivo, cuyos factores primos son congruentes a 1 módulo 4 y más grandes que 5, entonces existe un código ortogonal óptico óptimo con parámetros $(15v, 5, 1)$.*

Teorema 2.10. *[20, Chang and Ji] Para cualquier primo $p \equiv 1 \mod 10$, existe un código ortogonal óptico óptimo con parámetros $(4p, 5, 1)$ y para $u = 2, 3$ y cualquier primo $p \equiv 11 \mod 20$ existe un código ortogonal óptico óptimo con parámetros $(4up, 5, 1)$.*

Teorema 2.11. *[20] Existe un un código ortogonal óptico óptimo con parámetros $(gv, 5, 1)$ donde $g \in \{60, 80, 100, 120, 140, 160, 180\}$ y v es producto de primos más grandes que 5.*

Teorema 2.12. *[31] Existe un un código ortogonal óptico óptimo con parámetros $(gv, 6, 1)$ donde v es producto de primos congruentes a 7 módulo 12 más grandes que 7 y $g = 15, 20, 105, 140$.*

Algunos resultados sobre la existencia de códigos ortogonales ópticos óptimos con parámetros $(n, w, 1)$ para $w = 5, 6, 7$ se siguen de los resultados sobre empaquetamientos cíclicos g-regulares los cuales fueron estudiados por Chang y Ji en [20], por Fuji-Hara y Miao en [15] y también de resultados sobre familias de diferencias cíclicas en [3, 33].

2.2. Códigos ortogonales ópticos en dos dimensiones

Desde el punto de vista de las aplicaciones a las comunicaciones de fibra óptica, la principal desventaja que presentan los códigos ortogonales ópticos descritos en la sección anterior consiste en que la longitud de las secuencias se incrementan rápidamente cuando el número de usuarios o el peso del código se incrementan, lo cual requiere del uso de una banda ancha más larga. De ahí que el rendimiento de la banda ancha se reduce considerablemente y un código con longitudes largas ocasiona que la tasa de chips del sistema CDMA exceda la máxima tasa de chips disponible.
La razón de esta desventaja es porque los códigos ortogonales ópticos en una dimensión realizan la propagación de los datos de entrada solo en el dominio del tiempo, mientras que los códigos ortogonales ópticos en dos dimensiones realizan dicho proceso en los dominios del tiempo y la longitud de onda, lo cual hace posible que la tasa de chips sea reducida considerablemente. La llegada de la tecnología de multiplexores de división de longitud de onda (en inglés, WDM length-division-multiplexing) y multiplexores de division de longitud de onda denso (en inglés, D-WDM) ha hecho posible la propagación de los datos en ambos dominios, la longitud de onda y tiempo [34] . Estos códigos se les conoce como *códigos de salto de longitud de onda (en inglés, wavelength time hopping codes)*, *códigos multilongitud de onda*, (en inglés, multiple-wavelength codes) o *códigos*

ortogonales ópticos en dos dimensiones, los cuales por sus características tienden a requerir pequeñas longitudes y por lo tanto una baja tasa de chips. En adelante nos referimos a estos códigos como códigos ortogonales ópticos en dos dimensiones. La definición formal se presenta a continuación.

Definición 2.4. Sean m, n, w y λ enteros positivos. Un código ortogonal óptico $\mathcal{C}$ en dos dimensiones con parámetros $(m \times n, w, \lambda)$, es una familia de matrices binarias (palabras código) de tamaño $m \times n$, con peso de Hamming igual a w que satisfacen las siguientes propiedades:

1. Autocorrelación: para cada matriz $A = (a_{i,j}) \in \mathcal{C}$ y cada entero positivo $t \not\equiv 0$ mód n se cumple
$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j} a_{i,j+t} \leq \lambda.$$

2. Correlación cruzada: para cada par de matrices $A = (a_{i,j}), B = (b_{i,j}) \in \mathcal{C}$ distintas y cada entero positivo t se cumple
$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j} b_{i,j+t} \leq \lambda,$$
donde $j + t$ en ambos subíndices es módulo n.

El número de palabras código de un código ortogonal óptico se llama el tamaño del código. En la práctica son de mayor uso aquellos códigos con grandes tamaños. Para valores fijos de m, n, w y λ, el mayor tamaño posible de un código ortogonal óptico con parámetros $(m \times n, w, \lambda)$ se denota por $\Phi(m \times n, w, \lambda)$. Un código ortogonal óptico en dos dimensiones con parámetros $(m \times n, w, \lambda)$ con $\Phi(m \times n, w, \lambda)$ palabras código se llama *óptimo*. La cota superior de Johnson correspondiente para el valor de la función $\Phi(m \times n, w, \lambda)$ se enuncia a continuación.

Teorema 2.13.
$$\Phi(m \times n, w, \lambda) \leq \left\lfloor \frac{m}{w} \left\lfloor \frac{mn-1}{w-1} \left\lfloor \frac{mn-2}{w-2} \left\lfloor \cdots \left\lfloor \frac{mn-\lambda}{w-\lambda} \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor \right\rfloor. \tag{2.10}$$

En particular, para un código ortogonal óptico en dos dimensiones con parámetros $(m \times n, w, 1)$*, se cumple*
$$\Phi(m \times n, w, 1) \leq \left\lfloor \frac{m}{w} \left\lfloor \frac{mn-1}{w-1} \right\rfloor \right\rfloor. \tag{2.11}$$

Actualmente, se pueden encontrar muchos trabajos relacionados con el diseño y construcción de códigos ortogonales en dos dimensiones [35, 1, 6]. Muchas de estas construcciones son para valores de $\lambda = 1, 2$.
Matemáticamente, la teoría combinatoria de diseños, la geometría proyectiva y la teoría de campos finitos son tres de las principales herramientas teóricas utilizadas en la investigación sobre el diseño de códigos ortogonales ópticos en dos dimensiones. En este trabajo de investigación nos encargamos de estudiar algunos códigos ortogonales ópticos en dos dimensiones para $\lambda = 1$ que se puedan obtener principalmente a partir de conjuntos de Sidon. Describimos a continuación algunas de las construcciones más importantes.
Yang y Kwong en [34] utilizan un código ortogonal óptico en una dimensión para realizar la propagación de los datos en los dominios de la longitud de onda y el tiempo para construir códigos ortogonales ópticos en dos dimensiones.

Teorema 2.14. *[34, Yang and Kwong] Sean $\mathcal{C}$ un código ortogonal óptico óptimo con parámetros $(p, w, 1)$ y $\boldsymbol{c}_i = \{x_{i,0}, x_{i,1}, \ldots, x_{i,w-1}\} \in \mathcal{C}$ para $i = 0, \ldots, |\mathcal{C}| - 1$. Sea $\mathcal{F}_1$ la familia de matrices binarias $\boldsymbol{A}_i = (a_{i,j})$ de peso w, orden $p \times p$ y cuyas componentes igual a uno para $i = 0, \ldots, |\mathcal{C}| - 1$ se encuentran ubicadas en las posiciones descritas en el siguiente conjunto*

$$\{(x_{i,l} + k, jx_{i,l}) : l = 0, \ldots, w - 1, j \in [0, p - 1], k \in [0, p - 1]\}.$$

Si además, se adiciona la familia $\mathcal{F}_2$ de matrices binarias de orden $p \times p$ y peso w, $\boldsymbol{B}_i = (b_{i,j})$ cuyas componentes igual a uno para $i = 0, \ldots, |\mathcal{C}| - 1$ se encuentran ubicadas en las posiciones descritas en el siguiente conjunto

$$\{(j, x_{i,0}), (j, x_{i,1}), \ldots, (j, x_{i,w-1}) : j \in [0, p - 1]\},$$

entonces $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2$ es un código ortogonal óptico óptimo en dos dimensiones con parámetros $(p \times p, w, 1)$ y $p(p + 1)\,|\mathcal{C}|$ palabras código.

Por otra parte, Lee y Seo en [19] realizan la propagación de los datos en los dominios de la longitud de onda y el tiempo utilizando dos códigos ortogonales ópticos en una dimensión. El siguiente teorema describe el caso para $\lambda = 1$.

Teorema 2.15. *[19, Lee y Seo] Sean s y t los tamaños de dos códigos ortogonales ópticos en una dimensión con parámetros $(m, 3, 1)$ y $(n, 3, 1)$ respectivamente, donde $m, n \equiv 1$ mód 6. Entonces existe un código ortogonal óptico en dos dimensiones con parámetros $(m \times n, 3, 1)$ y $6mst + ms + mt$ palabras código.*

Shurong y otros autores en [29] utilizando un código de salto de frecuencia (en inglés, frecuency hopping code) y un código ortogonal óptico en una dimensión logran construir un código en dos dimensiones.

Teorema 2.16. *[29, Shurong y otros autores] Sean p un número primo, k un entero positivo y $\mathcal{C}$ un código ortogonal óptico óptimo con parámetros $(n, w, 1)$. Entonces existe un código ortogonal óptico óptimo en dos dimensiones con parámetros $(p^k \times n, w, 1)$ y $\Phi(p^k \times n, w, 1)$ palabras código.*

Alderson y Mellinger en [1] haciendo uso de ciertos conjuntos de puntos en espacios proyectivos finitos de dimensión k sobre $\mathbb{F}_q$ construyen una familia de códigos ortogonales ópticos en dos dimensiones.

Teorema 2.17. *[1, Alderson y Mellinger] Sea q una potencia prima.*

1. *Para cada entero positivo par k y cualquier factorización $mn = \frac{q^{k+1}-1}{q-1}$ existe un código ortogonal óptico óptimo con parámetros $(m \times n, q, 1)$.*
2. *Para cada entero positivo impar k y cualquier factorización $mn = \frac{q^{k+1}-1}{q-1}$ con $(q+1, n) = 1$, existe un código ortogonal óptico óptimo en dos dimensiones con parámetros $(m \times n, q, 1)$.*

Omrani y otros autores en [24] utilizando polinomios sobre campos finitos y funciones racionales, logran construir nueve familias de códigos ortogonales ópticos en dos dimensiones. Por otra parte, Cao y Wei en [6], proporcionan una descripción combinatoria de los códigos ortogonales ópticos en dos dimensiones. La siguiente descripción es para el caso $\lambda = 1$.

Definición 2.5. Un empaquetamiento con parámetros $(m \times n, w, 1)$ es un par $(\mathcal{X}, \mathcal{B})$, donde $\mathcal{X}$ es un conjunto con m elementos y $\mathcal{B}$ es una colección de subconjuntos de $\mathcal{X}$ (*bloques*) cada uno con w elementos, tal que cualquier par de elementos diferentes de $\mathcal{X}$ aparece a lo sumo en un bloque. El empaquetamiento es estrictamente cíclico si cada bloque bajo la acción de su grupo de automorfismos tiene longitud igual a m.

Teorema 2.18. *[6, Cao and Wei] Existe un código ortogonal óptico en dos dimensiones con parámetros $(m \times n, w, 1)$ si y solo si existe un empaquetamiento estrictamente cíclico con parámetros $(m \times n, w, 1)$.*

Con esta equivalencia logran construir infinitas familias de códigos. Uno de los resultados más importantes es el siguiente.

Teorema 2.19. *[6, Cao and Wei] Existe un código ortogonal óptico óptimo en dos dimensiones con parámetros $(m \times n, 3, 1)$ si y solo si $m \equiv n \equiv 1 \bmod 2$ y $m(mn-1) \equiv 0 \bmod 6$.*

TABLA 2.2: Parámetros de algunos códigos ortogonales ópticos en dos dimensiones. Aquí p denota un número primo y q es una potencia de p.

Parámetros	Condiciones	Tamaño del código	Referencia
$(m \times n, 3, 1)$	$n \equiv 1$ mód 2	$\Phi(m \times n, 3, 1) - 1$ si $m \equiv 5$ mód 6 y $n = 1$, $\Phi(m \times n, 3, 1)$ en otro caso	[6]
$(m \times n, 3, 1)$	s, t son los tamaños de códigos ortogonales ópticos óptimos con parámetros $(m, 3, 1)$ y $(n, 3, 1)$ respectivamente, tales que $m, n \equiv 1$ mód 6	$6mst + ms + mt$	[19]
$(p \times p, w, 1)$	$p \equiv 1$ mód $w(w-1)$	$\Phi(p \times p, w, 1)$	[6]
$(p^n \times p, p, 1)$	$n \geq 1$	$\Phi(p^n \times p, p, 1)$	[6]
$(p^k \times n, w, 1)$	n es la longitud de un código ortogonal óptico con parámetros $(n, w, 1)$	$\frac{m(mn-1)}{w(w-1)}$	[29]
$(m \times n, q, 1)$	$mn = q^t - 1$ y $t \geq 1$	$\Phi(m \times n, q, 1)$	[1]
$(m \times n, q+1, 1)$	$mn = (q^{t+1} - 1)/(q-1)$, $t \geq 1$, o $t \equiv 0$ mód 2 o $t \equiv 1$ mód 2 y $(q+1, t) = 1$.	$\Phi(m \times n, q+1, 1)$	[1]

Los casos en los que $w = 4$ o $w = 5$ también son investigados en [6], sin embargo la caracterización completa sobre la existencia de dichos códigos para todo valor de m y n sigue siendo un problema de investigación.
Un breve resumen de algunas de las construcciones más importantes de códigos ortogonales ópticos en dos dimensiones se pueden consultar en la Tabla 2.2.

2.3. Conjuntos de Sidon

En teoría de números, un problema de importante interés teórico es el de conjunto de Sidon, llamados así en honor al matemático húngaro Simon Sidon quien fue el primero en presentar el concepto cuando se encontraba investigando temas relacionados con series de Fourier. Sidon investigó sobre la existencia de aquellos conjuntos de enteros positivos con la propiedad de que todas las sumas entre dos elementos del conjunto sean diferentes. Esta propiedad es equivalente a la propiedad de que todas las diferencias no nulas entre cualquier par de elementos del conjunto sean diferentes. Sin embargo, este concepto aunque inicialmente fue definido sobre el conjunto de los enteros positivos, puede ser considerado también en situaciones más generales, como por ejemplo en los grupos abelianos finitos. Estos conjuntos, además tienen importantes aplicaciones principalmente en teoría de códigos [14].

Definición 2.6. Sean $(G,+)$ un grupo abeliano con elemento neutro igual a e y $A \subset G$. Se dice que A es un conjunto de Sidon en G, si para cualquier $x \in G$ diferente de e, se cumple

$$R_{A-A}(x) \leq 1. \tag{2.12}$$

Si $G = \mathbb{Z}_n$ y A verifica la propiedad anterior, entonces se dice que A es un conjunto de Sidon módulo n.

Un problema importante en esta área consiste en determinar construcciones explícitas de conjuntos de Sidon modulares para todo n con el mayor cardinal posible. Este problema se encuentra actualmente abierto. Hasta la fecha solo se conocen tres construcciones algebraicas de conjuntos de Sidon modulares. Las construcciones modulares han sido ampliamente estudiadas por Caicedo, Martos, Gómez, Trujillo, entre otros en [25, 16, 5, 21]. Resumimos estas construcciones a continuación.

Teorema 2.20. *[30, Singer] Sean q una potencia prima, θ un elemento primitivo del cuerpo finito $\mathbb{F}_{q^3}$ y $n = q^2 + q + 1$. Entonces*

$$\mathcal{S} = \{a \text{ mód } n : a \in \log_\theta(\theta + \mathbb{F}_q)\} \cup \{0\} \tag{2.13}$$

es un conjunto de Sidon módulo n con $q+1$ elementos, donde $\log_\theta(\theta + \mathbb{F}_q) = \{\log_\theta(\theta + a) : a \in \mathbb{F}_q\}$.

En la construcción de Singer todo elemento de $\mathbb{Z}_n$ diferente de cero, puede ser representado de manera única como diferencia de dos elementos de $\mathcal{S}$.

Teorema 2.21. *[2, Bose-Chowla] Sean q una potencia prima y θ un elemento primitivo del cuerpo finito $\mathbb{F}_{q^2}$. Entonces*

$$\mathcal{B} = \{\log_\theta(\theta + a) : a \in \mathbb{F}_q\} \tag{2.14}$$

es un conjunto de Sidon módulo $q^2 - 1$ con q elementos.

En la construcción de Bose-Chowla, todo elemento diferente de un múltiplo de $q+1$ en el grupo $\mathbb{Z}_{q^2-1}$ puede ser representado de manera única como diferencia de dos elementos de $\mathcal{B}$.

Teorema 2.22. *[28, Ruzsa] Sean p un número primo y θ una raíz primitiva módulo p. Entonces*

$$\mathcal{R} = \{x \in \mathbb{Z}_{p(p-1)} : x \equiv ip - \theta^i(p-1) \mod (p^2 - p) \text{ donde } 1 \leq i \leq p-1\} \tag{2.15}$$

es un conjunto de Sidon módulo $p(p-1)$ con $p-1$ elementos.

En la construcción de Ruzsa, todo elemento diferente de un múltiplo de p o de un múltiplo de $p-1$ en el grupo $\mathbb{Z}_{p(p-1)}$ puede ser representado de manera única como diferencia de dos elementos de $\mathcal{R}$.

Las construcciones anteriores son óptimas en el sentido de que no es posible agregar un elemento que conserve la propiedad de conjunto de Sidon. Estas conjuntos pueden ser considerados también como códigos ortogonales ópticos óptimos con un solo elemento. Vistos de esta manera y por los comentarios hechos anteriormente podemos caracterizar su conjunto deficiencia L.

- Si $\mathcal{S}$ es un conjunto de Sidon obtenido por la construcción de Singer, entonces $L = \{0\}$.
- Si $\mathcal{B}$ es un conjunto de Sidon obtenido por la construcción de Bose-Chowla, entonces $L = \{m(q+1) : 0 \leq m \leq q-2\}$.
- Si $\mathcal{R}$ es un conjunto de Sidon obtenido por la construcción de Ruzsa, entonces

$$L = \{mp : 0 \leq m \leq p-1\} \cup \{m(p-1) : 0 \leq m \leq p-1\}.$$

Como mencionamos anteriormente, uno de los principales problemas en conjuntos de Sidon consiste en determinar el mayor cardinal posible del conjunto de Sidon. Si G es

un grupo abeliano finito se pretende realizar un estudio del comportamiento asintótico de la función

$$f_2(G) := \text{máx}\{|A| : A \subset G, A \text{ es un conjunto de Sidon }\}.$$

El valor de esta función para grupos en general no es conocido aún, sin embargo existen cotas inferiores y superiores. Usando técnicas sencillas de conteo se puede probar que

$$f_2(G) \leq \left\lfloor \frac{1+\sqrt{4\,|G|-3}}{2} \right\rfloor.$$

Más detalles sobre el valor de esta función pueden ser consultados en [12].

Otros escenarios en los cuales se puede estudiar los conjuntos de Sidon son los grupos abelianos de la forma $\mathbb{Z}_m \times \mathbb{Z}_n$, los cuales se denominan conjuntos de Sidon en dos dimensiones. Presentamos en los siguientes resultados las únicas construcciones conocidas hasta el momento en dichos grupos.

Teorema 2.23. *[12] Sean p un número primo impar, $r(x)$ y $s(x)$ polinomios sobre $\mathbb{Z}_p$ de grados menor o igual a 2 tales que $r(x) - \alpha s(x)$ no es constante para cada $\alpha \in \mathbb{Z}_p$. Entonces*

$$A = \{(r(x), s(x)) : x \in \mathbb{Z}_p\}$$

es un conjunto de Sidon en $\mathbb{Z}_p \times \mathbb{Z}_p$ con p elementos. En particular,

$$A = \{(x, x^2) : x \in \mathbb{Z}_p\}$$

es un conjunto de Sidon en $\mathbb{Z}_p \times \mathbb{Z}_p$.

Teorema 2.24. *[12] Sean p un número primo y α una raíz primitiva módulo p. Entonces*

$$B = \{(x, \alpha^x) : x \in \mathbb{Z}_{p-1}\}$$

es un conjunto de Sidon en $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$ con $p-1$ elementos. Este conjunto puede ser descrito también como $B = \{(\log x, x) : x \in \mathbb{Z}_p^*\}$, donde $\log x = \log_\alpha x$ es el logaritmo discreto.

Teorema 2.25. *[12] Sean q una potencia prima, θ un elemento primitivo de $\mathbb{F}_q$ y $a \in \mathbb{F}_q$ con $a \neq 0$. Entonces*

$$C = \{(\log_\theta(\theta^k - a), k) : k \in \mathbb{Z}_{q-1}, k \neq \log_\theta a\}$$

es un conjunto de Sidon en $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$ con $q-2$ elementos.

Al igual que en el caso de conjuntos de Sidon en una dimensión, las construcciones de conjuntos de Sidon en dos dimensiones son óptimas respecto a su cardinal. Dichos conjuntos pueden ser usados para construir códigos ortogonales ópticos en dos dimensiones con m elementos, si se considera las palabras código obtenidas por las traslaciones sobre la primera componente de cada elemento del conjunto de Sidon en dos dimensiones. La deficiencia L del código obtenido también esta caracterizada.

- Si A es un conjunto de Sidon obtenido por el Teorema 2.23, entonces $L = \{0\} \times \mathbb{Z}_p$.
- Si B es un conjunto de Sidon obtenido por el Teorema 2.24, entonces $L = (\{0\} \times \mathbb{Z}_p) \cup (\mathbb{Z}_{p-1} \times \{0\})$.
- Si C es un conjunto de Sidon obtenido por el Teorema 2.25, entonces

$$L = (\{1\} \times \mathbb{Z}_p^*) \cup (\mathbb{Z}_p^* \times \{1\}) \cup \{(z, z) : z \in \mathbb{Z}_p^*\}.$$

Más propiedades de estos conjuntos pueden consultarse en [12, 25, 16, 5, 21].

Nota 2.1. Los códigos ortogonales ópticos puedes verse como una familia de conjuntos de Sidon cuyos conjuntos de diferencia son disjuntos dos a dos. También los conjuntos de Sidon en una dimensión pueden considerarse como un código ortogonal óptico con una sola palabra. Sin embargo, los conjuntos de Sidon se pueden generalizar para construir códigos ortogonales ópticos con más de una palabra código. Por ejemplo, Singer en [30] generalizó su construcción para códigos ortogonales ópticos óptimos usando geometría proyectiva sobre campos finitos. Moreno y otros en [22] generalizaron la construcción de Bose-Chowla para construir códigos ortogonales ópticos óptimos. En el Capítulo 3 de este trabajo de investigación, construimos un código ortogonal óptico óptimo en una dimensión que puede ser visto como una generalización de la construcción dada por Ruzsa para conjunto de Sidon. Este resultado puede consultarse en [27].

Nota 2.2. Los conjuntos de Sidon en dos dimensiones también tienen relación con los códigos ortogonales. Dependiendo de los grupos sobre los cuales se definen, podemos obtener códigos ortogonales ópticos en dos dimensiones con más de una palabra código. Estudiamos en detalle esta relación en el Capítulo 4.

2.4. Algunas aplicaciones

La tecnología de acceso múltiple por división de código (siglas en inglés, CDMA) tiene potentes aplicaciones. Por ejemplo, se pueden aplicar en comunicaciones inalámbricas,

transmisión de información multimedia, redes de radio sobre fibra (siglas en inglés, RoF), construcción de redes de área local (siglas en inglés, LANs) e interconexiones en entornos hostiles, redes de sensores ópticas, entre otras.

Describimos algunas de estas aplicaciones de manera breve a continuación. Más detalles pueden ser consultados en [35].

Óptica del espacio libre

La óptica del espacio libre es una tecnología de comunicación óptica que puede soportar altas velocidades en los servicios de acceso en zonas residenciales y comerciales. Mediante el despliegue de torres de radiofrecuencia, los enlaces de comunicación punto a punto se pueden apoyar en un área metropolitana para soportar servicios de altas y veloces tasas de datos de Gb/s. La tecnología CDMA óptica se aplica a la óptica del espacio libre mediante el empleo de su capacidad de direccionamiento para la creación de redes en formas que toman ventaja de la comunicación óptica inalámbrica.
Al mismo tiempo, el sistema óptico de la tecnología CDMA también se puede utilizar para comunicaciones infrarrojas inalámbricas para establecer redes de área local (LAN). Las comunicaciones de enlace ascendente entre las estaciones portátiles y los puntos de acceso de llamadas se pueden implementar mediante transmisores LED económicos en cada computadora portátil de la estación. El punto de acceso transmite datos en el enlace descendente y las estaciones portátiles detectan la dirección de la transmisión para seleccionar los datos destinados al nodo local, por lo que no se necesita la complicada sincronización del sistema y, por lo tanto, el costo de implementación es bajo.

Transmisión multimedia

El diseño flexible de la red y la variedad de opciones que presentan los sistemas CDMA ópticos pueden admitir muchos tipos de medios en una red de comunicación, como voz, datos, imágenes y video. Esta técnica se puede utilizar para codificar y multiplexar imágenes creadas por fibra óptica multinúcleo sobre una ruta de fibra común. Un plano de bits bidimensional $N \times N$ que comprende píxeles individuales de una imagen se codifica mediante un código ortogonal bidimensional de tamaño $M \times M$, donde el factor de dispersión CDMA es M^2. La imagen codificada tiene $MN \times MN$ píxeles, por lo que se requiere que la fibra de imagen central sea $MN \times MN$ para transmitir las imágenes codificadas. La multiplexación de imágenes en dos dimensiones tiene muchas aplicaciones, como la transmisión de imágenes médicas, interconexiones ópticas paralelas entre procesadores y memoria en alto rendimiento informático.

LAN e interconexiones de LAN para entornos hostiles

Debido a que la tecnología CDMA óptica es de tipo de espectro ensanchado, tiene capa-

cidad anti-interferencia. Por lo tanto, se puede aplicar en entornos móviles para aplicaciones civiles y militares (por ejemplo, aviones, barcos y campos de batalla). El diseño flexible del LAN CDMA óptica permite la capacidad en entornos hostiles y no es tan costosa como las LAN que utilizan otras tecnologías. También el sistema CDMA óptico en LAN soporta la confidencialidad de la información en tiempo real, lo cual es una ventaja en aplicaciones militares.

Capítulo 3

Códigos ortogonales ópticos en una dimensión

En este capítulo estudiamos la correlación de códigos ortogonales ópticos de algunas familias asintóticamente óptimas, los conjuntos de Sidon y la construcción recursiva presentada por Wensong Chu y S. W. Golomb en [8]. Lo anterior con el propósito de obtener nuevas familias de códigos ortogonales ópticos, algunos de ellos óptimos respecto a la cota de Johnson.

3.1. Correlación en códigos ortogonales ópticos asintóticamente óptimos

En el capítulo anterior vimos que existen varias construcciones explícitas de códigos ortogonales ópticos óptimos. Sin embargo, para algunos casos dados de la longitud y el peso solo se conocen construcciones caracterizadas por contener un número de palabras código cercano a la cota de Johnson. En esta sección estudiamos dichos códigos los cuales reciben el nombre de códigos ortogonales ópticos asintóticamente óptimos.
Nuestro objetivo es analizar las construcciones asintóticas que aparecen en [23, 11] con el fin de caracterizar sus respectivos conjuntos deficiencia para posteriormente establecer bajo qué condiciones el cardinal de dichos códigos se puede optimizar por medio de la adición adecuada de palabras código.
Las construcciones de códigos ortogonales ópticos trabajadas en esta sección se presentan

de manera alternativa para identificar sus propiedades de manera eficiente.
Las familias de códigos ortogonales ópticos asintóticamente óptimas a estudiar son:

1. Familia $\mathcal{A}$ y $\mathcal{B}$ de [23].
2. Construcción A y B de [11].

Definición 3.1. Sea $\mathcal{F}$ una familia de códigos ortogonales ópticos con parámetros $(n, w, 1)$ y tamaño L. Decimos que $\mathcal{F}$ es asintóticamente óptima si

$$\lim_{n\to\infty} \frac{L}{\Phi(n, w, 1)} = 1.$$

El siguiente resultado nos permite caracterizar el conjunto deficiencia de los códigos ortogonales ópticos estudiados en esta sección.

Lema 3.1. *Sean* $x \equiv a$ mód m, $x \equiv b$ mód n, $y \equiv c$ mód m, $y \equiv d$ mód n *con* $(m, n) = 1$, $a \neq c$ *y* $b \neq d$. *Entonces*

$$x - y \not\equiv 0 \text{ mód } m,$$
$$x - y \not\equiv 0 \text{ mód } n.$$

La primera construcción que estudiamos es la familia $\mathcal{A}$ que aparece en [23].

Familia $\mathcal{A}$. Sea p un número primo tal que $p = ms + 1$ para algunos enteros positivos m y s. Si α es una raíz primitiva módulo p, para $k = 0, \ldots, s-1$ consideremos las clases ciclotómicas sobre $\mathbb{F}_p$ de índice s

$$H_k^s = \{\alpha^{sj+k} : j = 0, \ldots, m-1\},$$

así como el conjunto

$$A_k = \{(j, -\alpha^{sj+k}) : j = 0, \ldots, m-1\},$$

del grupo $\mathbb{Z}_m \times \mathbb{Z}_p$. Si S_k denota el conjunto solución en $\mathbb{Z}_{pm}$ de los elementos de A_k ($|S_k| = s$ por el Teorema Chino de los Restos), entonces $\mathcal{C}' = \{S_k : k = 0 \ldots, s-1\}$ es un código ortogonal óptico con parámetros $(pm, m, 1)$ equivalente al código ortogonal óptico de la familia $\mathcal{A}$, el cual describimos en 2.1.
En efecto, en la descripción de la familia $\mathcal{A}$ en 2.1, los elementos de $\mathcal{F}_A$ pueden ser

caracterizados por los polinomios de la forma $f(x) = \alpha^k x - 1$, dado que si $f_1(x) = a_1 x + b_1$ y $f(x) = ax + b$ con $f_1(x) \sim f_2(x)$, entonces

$$a_1 v^{-1} = a,$$
$$b_1 - u = b,$$

para algunos $v \in G$ y $u \in \mathbb{Z}_p$, donde G es el subgrupo de $\mathbb{F}_p^*$ generado por α^s . Entonces podemos elegir $a = \alpha^k$ y $b = -1$ para algún $k = 0, \ldots, s-1$ para obtener

$$\mathcal{F}_A = \{f(x) = \alpha^k x - 1 : k = 0, \ldots, s-1\}.$$

Por lo tanto, para cada $f(x) \in \mathcal{F}_A$ tal que $A_f(i,j) = 1$, entonces $f(\alpha^{sj}) = p - 1 - i$, es decir

$$\alpha^{sj+k} - 1 = p - 1 - i$$

en $\mathbb{Z}_p$. Entonces $i = -\alpha^{sj+k}$ mód p y por lo tanto al reemplazar en el sistema de congruencias establecido en 2.1 tenemos

$$\begin{aligned} x &\equiv j \text{ mód } m, \\ x &\equiv -\alpha^{sj+k} \text{ mód } p. \end{aligned} \tag{3.1}$$

Esto prueba la equivalencia de los códigos.
Caracterizamos ahora el conjunto deficiencia para esta familia de códigos. Para cada $k = 0, \ldots, s-1$ sea

$$\Delta(A_k) = \{(i-j, \alpha^k(\alpha^{sj} - \alpha^{si}) : 0 \leq i, j \leq m-1, i \neq j\}.$$

Por la equivalencia probada entre los códigos sabemos que $|\Delta(A_k)| = m(m-1)$. Por la Proposición 2.1 tenemos

$$\left| \bigcup_{k=0}^{s-1} \Delta(A_k) \right| = sm(m-1).$$

Por el Lema 3.1 tenemos que la deficiencia del conjunto cuyos elementos son A_k esta dada por

$$L = \mathbb{Z}_m \times \mathbb{Z}_p \setminus \bigcup_{k=0}^{s-1} \Delta(A_k) = \{(0,x) : x \in \mathbb{Z}_p\} \cup \{(x,0) : x \in \mathbb{Z}_m\}.$$

Ahora, para cada $k = 0, \ldots, s-1$, definimos

$$S_k = \{x \in \mathbb{Z}_{mp} : x \equiv i \mod m \text{ y } x \equiv -\alpha^{is+k} \mod p, i = 0, \ldots, m-1\}.$$

Entonces, si $\mathcal{C}' = \{S_k : k = 0, \ldots, s-1\}$ tenemos que $\mathcal{C}'$ es un código ortogonal óptico con parámetros $(pm, m, 1)$ y s palabras código. También

$$\Phi(pm, m, 1) = \left\lfloor \frac{pm-1}{m(m-1)} \right\rfloor = \left\lfloor s + \frac{s}{m-1} + \frac{1}{m} \right\rfloor.$$

Note que si $s \leq m-2$, entonces $\mathcal{C}'$ es óptimo.
Si $s = m-1$, entonces por los Teoremas 2.1 y 2.2 es posible optimizar el número de palabras código de $\mathcal{C}'$. Hemos probado el siguiente resultado.

Teorema 3.1. *Sea p un número primo tal que $p = ms + 1$ para algunos enteros positivos m y s. Entonces existe un código ortogonal óptico con parámetros $(pm, m, 1)$ y s elementos. Además, si $s \leq m-2$ el código obtenido es óptimo y si $s = m-1$ es posible agregar adecuadamente palabras código que optimizan el código inicial.*

El caso $s > m-1$ es posible también optimizarlo combinando algunas contrucciones de códigos ortogonales óptimos. Por ejemplo, para $m = 4$ por el Teorema 2.6, se sabe que existe un código ortogonal óptico óptimo con parámetros $(v, 4, 1)$ para todo $v \leq 1212$ excepto para $v = 25$. Por tanto, tenemos el siguiente resultado.

Teorema 3.2. *Sea p un número primo tal que $p \equiv 1 \mod 4$ con $p < 1212$, entonces existe un código ortogonal óptico óptimo con parámetros $(4p, 4, 1)$.*

Más generalmente podemos usar la técnica empleada por Marco Buratti en [3] que se resume en el siguiente resultado.

Teorema 3.3. *Sean $m = ef$ o $m = ef + 1$ con e y f enteros positivos y e impar en ambos casos. Sea p un número primo tal que al aplicarle el algoritmo de la división a $p-1$ entre $m(m-1)$ este toma la forma*

$$p - 1 = m(m-1)t + r, 0 \leq r < m(m-1), r \text{ divisible por } 2et.$$

Sea α una raíz primitiva módulo p y $\epsilon = \alpha^{(p-1)/e}$ y asignemos a cualquier subconjunto $B = \{b_1 = 1, \ldots, b_f\}$ de $H =< \alpha >$, la lista definida como

$$L_B = (b_i - b_j\epsilon^h : [1 \leq i = j \leq f, 1 \leq h \leq \frac{1}{2}(e-1)] \text{ o } [1 \leq i < j \leq f, 1 \leq h \leq e]) + L_B^*$$

donde L_B^* es la lista nula si $m = ef$, y es la lista $(b_1, \ldots, b_f)$ si $m = ef + 1$.
Sea $H^{d_{2s}} \subset \cdots \subset H^{d_1}$ una cadena de subgrupos entre $H^{(p-1)/(2e)}$ y H, y hagamos $d_0 = 1$, $d_{2s+1} = (p-1)/(2e)$.
Supongamos que B satisface:

1. *L_B es un subconjunto de H.*
2. $\prod_{i=0}^{s} d_{2i+1}/d_{2i}$.
3. *Para todo $x, y \in L_B$ se tiene*

$$xy^{-1} \in \bigcup_{i=0}^{s} (H^{d_{2i-1}} \setminus H^{d_{2i}}) \cup \{1\}.$$

.

Si

$$I := \left\{ \sum_{i=0}^{s} d_{2i} a_i : 0 \leq a_i < d_{2i+1}/d_{2i} : i = 0, 1, \ldots, s \right\},$$

entonces la familia $\mathcal{F} = \{\alpha^i B \cdot H^{(p-1)/e} \cup B^* : i \in I\}$, donde $B^* = \emptyset$ o $B^* = \{0\}$ si $m = ef$ o $m = ef + 1$ respectivamente, es un código ortogonal óptico óptimo con parámetros $(p, m, 1)$.

Observación 3.1. Sea $n = (p-1)/(2e)$, la manera más eficiente de aplicar el teorema anterior es buscando un subconjunto B de tamaño f de H tal que: cualquier par de elementos de L_B aparecen en distintas clases laterales de H^n. Las condiciones enumeradas para el conjunto B se verifican en este caso tomando la cadena de subgrupos $H^n \subset H$.

Ejemplo 3.1. Sea $p = 97 = 6(16) + 1$, entonces $m = 6$ y $s = 16$. Por el Teorema 3.1, existe un código ortogonal óptico $\mathcal{C}_1$ con parámetros $(582, 6, 1)$ y 16 elementos. De acuerdo a la cota de Johnson para estos parámetros tenemos que faltan 3 elementos para garantizar la optimalidad del código. Con el fin de optimizar el cardinal del código, usamos el Teorema 3.3 con $e = 1$, $f = 65$, $\alpha = 5$, $\epsilon = \alpha^{96} = 1$ y $B = \{1, 2, 4, 8, 25, 67\}$. Si $n = 48$ es fácil mostrar que cada par de elementos de $L_B = (95, 93, 89, 72, 30, 94, 90, 73, 31, 92, 75, 33, 79, 37, 54)$ aparece en diferentes clases laterales de $H_0^{48} = \{5^{48}, 5^{96}\}$

$H_0^{48} = \{96, 1\}$	$H_8^{48} = \{91, 6\}$	$H_{16}^{48} = \{61, 36\}$	$H_{24}^{48} = \{75, 22\}$
$H_1^{48} = \{92, 5\}$	$H_9^{48} = \{67, 30\}$	$H_{17}^{48} = \{14, 83\}$	$H_{25}^{48} = \{84, 13\}$
$H_2^{48} = \{72, 25\}$	$H_{10}^{48} = \{44, 53\}$	$H_{18}^{48} = \{70, 27\}$	$H_{26}^{48} = \{32, 65\}$
$H_3^{48} = \{69, 28\}$	$H_{11}^{48} = \{26, 71\}$	$H_{19}^{48} = \{59, 38\}$	$H_{27}^{48} = \{63, 34\}$
$H_4^{48} = \{54, 43\}$	$H_{12}^{48} = \{33, 64\}$	$H_{20}^{48} = \{4, 93\}$	$H_{28}^{48} = \{24, 73\}$
$H_5^{48} = \{76, 21\}$	$H_{13}^{48} = \{68, 29\}$	$H_{21}^{48} = \{20, 77\}$	$H_{29}^{48} = \{23, 74\}$
$H_6^{48} = \{89, 8\}$	$H_{14}^{48} = \{49, 48\}$	$H_{22}^{48} = \{3, 94\}$	$H_{30}^{48} = \{18, 79\}$
$H_7^{48} = \{57, 40\}$	$H_{15}^{48} = \{51, 46\}$	$H_{23}^{48} = \{15, 82\}$	$H_{31}^{48} = \{90, 7\}$

$H_{32}^{48} = \{62, 35\}$ $H_{36}^{48} = \{47, 50\}$ $H_{40}^{48} = \{81, 16\}$ $H_{44}^{48} = \{88, 9\}$
$H_{33}^{48} = \{19, 78\}$ $H_{37}^{48} = \{41, 56\}$ $H_{41}^{48} = \{17, 80\}$ $H_{45}^{48} = \{52, 45\}$
$H_{34}^{48} = \{95, 2\}$ $H_{38}^{48} = \{11, 86\}$ $H_{42}^{48} = \{85, 12\}$ $H_{46}^{48} = \{66, 31\}$
$H_{35}^{48} = \{87, 10\}$ $H_{39}^{48} = \{55, 42\}$ $H_{43}^{48} = \{37, 60\}$ $H_{47}^{48} = \{39, 58\}$

Por tanto, existe un código ortogonal $\mathcal{C}_2'$ óptimo con parámetros $(97, 6, 1)$ con 3 elementos. Si $\mathcal{C}_2 = \{6\mathbf{c} : \mathbf{c} \in \mathcal{C}_2'\}$, donde $6\mathbf{c} = \{6c \mod pm : c \in \mathbf{c}\}$ tenemos que $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ es un código ortogonal óptico óptimo con parámetros $(582, 6, 1)$ y 19 elementos.

La segunda construcción que estudiamos es la familia $\mathcal{B}$ publicada en [23]. Mostramos una construcción alternativa que nos permite optimizar el tamaño del código. Los resultados de esta construcción se encuentran publicados en [27] por Trujillo, Delgado y el autor de este trabajo de investigación.

Familia $\mathcal{B}$. Sean p un número primo, h un entero positivo mayor a 1 y α un elemento primitivo de $\mathbb{F}_{p^h}$. Consideremos el siguiente conjunto de polinomios sobre $\mathbb{F}_{p^h}$

$$\mathcal{P} = \{p(x) \in \mathbb{F}_p[x] : 1 \leq \text{grad}(p(x)) \leq h - 1 \text{ y } p(0) = 0\}. \tag{3.2}$$

Probemos que

$$\mathcal{C}_1 = \{\{p^h \log_\alpha(p(\alpha) + a) - (p^h - 1)a : a \in \mathbb{F}_p\} : p(x) \in \mathcal{P}\}$$

es un código ortogonal óptico con parámetros $(p(p^h - 1), p, 1)$ y $p^{h-1} - 1$ elementos.

Demostración. La cardinalidad del conjunto es clara. Consideremos la familia de subconjuntos

$$\mathcal{R} = \{\{(a, \log_\alpha(p(\alpha) + a)) : a \in \mathbb{F}_p\} : p(x) \in \mathcal{P}\} \tag{3.3}$$

del grupo $(\mathbb{Z}_p, +) \times (\mathbb{Z}_{p^h-1}, +)$. Veamos la correlación cruzada, para ello necesitamos probar que cada elemento $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_{p^h-1}$ puede representarse como la diferencia $(x, y) - (x' - y')$ con $(x, y) \in X$ y $(x', y') \in Y$ de manera única para todo $X, Y \in \mathcal{R}$ con $X \neq Y$. Supongamos por contradicción que existen $a_1, a_2, a_3, a_4 \in \mathbb{Z}_p$ con $a_1 \neq a_2$, $a_3 \neq a_4$ y $p(x), q(x) \in \mathcal{P}$, $p(x) \neq q(x)$ con $\text{grad}(p) = i$ y $\text{grad}(q) = j$ tales que

$$(a_1, \log_\alpha(p(\alpha) + a_1) - (a_2, \log_\alpha(p(\alpha) + a_2) = (a_3, \log_\alpha(q(\alpha) + a_3) - (a_4, \log_\alpha(q(\alpha) + a_4).$$

Entonces

$$\begin{aligned} a_1 - a_2 &= a_3 - a_4 \mod p, \\ (p(\alpha) + a_1)(q(\alpha) + a_4) &= (q(\alpha) + a_3)(p(\alpha) + a_2). \end{aligned}$$

Por lo tanto

$$(a_1 - a_2)q(\alpha) + a_1a_4 = (a_3 - a_4)p(\alpha) + a_3a_2 \tag{3.4}$$

en $\mathbb{F}_{p^h}$. La Ecuación (3.4) puede ser utilizada para construir el siguiente polinomio

$$f(x) = (a_1 - a_2)q(x) + a_1a_4 - (a_3 - a_4)p(x) - a_3a_2,$$

con coeficientes en $\mathbb{F}_p$, de grado menor que h y que tiene a α como una raíz, por lo tanto este polinomio tiene que ser igual a cero.
Si $j > i$, entonces $a_1 = a_2$ lo cual es una contradicción, por tanto $i = j$ y dado que $\text{grad}(p(x)) > 0$ y $\text{grad}(q(x)) > 0$, entonces

$$\begin{aligned}(a_1 - a_2)q(\alpha) &= (a_3 - a_4)p(\alpha),\\ a_1a_4 &= a_3a_2.\end{aligned} \tag{3.5}$$

Por la Ecuación (3.5) tenemos

$$a_1 - a_2 = (a_3 - a_4)u, \tag{3.6}$$

para alguna unidad u de $\mathbb{Z}_p$. Por (3.1) y (3.6) tenemos $(a_3 - a_4)(u - 1) = 0 \mod p$. Si $u \not\equiv 1 \mod p$, entonces $a_3 - a_4 \equiv 0 \mod p$, lo cual es una contradicción. Por lo tanto $u = 1$ y así $q(\alpha) = p(\alpha)$ lo cual contradice el hecho de que $\text{grad}(\alpha, \mathbb{F}_p) = h$.
Veamos ahora la propiedad de la autocorrelación. En este caso podemos tomar $p(x) = q(x)$ en la anterior prueba. Por (3.5) tenemos que a_1, a_2, a_3 y a_4 son raíces de la ecuación $x^2 - (a_1 + a_4)x + a_1a_4 = 0$ sobre $\mathbb{F}_p$, entonces $\{a_1, a_4\} = \{a_2, a_3\}$. Como $a_1 \neq a_2$ y $a_3 \neq a_4$, entonces $a_1 = a_3$ y $a_2 = a_4$ lo cual corresponde a la autocorrelación para el desplazamiento cero.
Finalmente, por el Teorema Chino de los Restos aplicado a cada uno de los elementos del conjunto $\mathcal{R}$, tenemos que

$$\mathcal{C}_1 = \{\{p^h \log_\alpha(p(\alpha) + a) - (p^h - 1)a : a \in \mathbb{F}_p\} : p(x) \in \mathcal{P}\}$$

es un código ortogonal óptico con parámetros $(p(p^h - 1), p, 1)$ y $p^{h-1} - 1$ elementos.

Teorema 3.4. *Para cualquier número primo p y entero $h \geq 2$, existe un código ortogonal óptico con parámetros $(p(p^h - 1), p, 1)$ y $p^{h-1} - 1$ palabras código.*

El código descrito anteriormente permite construir la familia $\mathcal{B}$ de [23] para el caso $t = 1$ omitiendo un elemento de cada palabra. Sin embargo, el código obtenido no es óptimo respecto a la cota de Johnson. Para optimizar, determinemos la deficiencia L de $\mathcal{C}_1$. Por el Lema 3.1, aplicado al conjunto $\mathcal{R}$ junto con el Teorema Chino de los Restos, tenemos que $L = M_p \cup M_q$, donde M_p denota al conjunto de los múltiplos no cero de p

módulo $p(p^h-1)$ y M_q denota al conjunto de los múltiplos no cero de q módulo $p(p^h-1)$ donde $q=\frac{p^h-1}{p-1}$.

Ahora consideremos el conjunto

$$\mathcal{Q}=\{p(x)\in\mathcal{P}: p(x) \text{ es mónico }\}.$$

Entonces, por el Teorema 2.3 la familia de conjuntos

$$\mathcal{C}_1'=\{\{\log_\alpha(p(\alpha)+a): a\in\mathbb{F}_p\}: p(x)\in\mathcal{Q}\}$$

es un código ortogonal óptico óptimo con parámetros $(p^h-1,p,1)$ y $\frac{p^{h-1}-1}{p-1}$ elementos. Sea $\varphi:\mathbb{Z}_{p^h-1}\to\mathbb{Z}_{p(p^h-1)}$ dada por $\varphi(x)=px$, entonces tenemos que φ es un homomorfismo inyectivo. Aplicando φ a cada elemento de $\mathcal{C}'$ tenemos que

$$\mathcal{C}_2=\{\{p\log_\alpha(p(\alpha)+a): a\in\mathbb{F}_p\}: p(x)\in\mathcal{Q}\}$$

es un código ortogonal óptico óptimo con parámetros$(p(p^h-1),p,1)$ y $\frac{p^{h-1}-1}{p-1}$ elementos. Veamos ahora que $\mathcal{C}=\mathcal{C}_1\cup\mathcal{C}_2$ es un código ortogonal óptico óptimo con parámetros $(p(p^h-1),p,1)$. Es suficiente probar que el código es óptimo y que la propiedad de la correlación cruzada se cumple para toda $X\in\mathcal{C}_1$ y toda $Y\in\mathcal{C}_2$. Probemos primero que

$$|(X+a)\cap Y|\leq 1$$

para todo entero a. Supongamos por contradicción que

$$a=x-y=x'-y'$$

para algunos $x,x'\in X$, $y,y'\in Y$ con $x\neq x'$ y $y\neq y'$. Entonces $x-x'=y-y'$, lo cual es una contradicción ya que $x-x'\notin M_p$, mientras que $y-y'\in M_p$. También, dado que $\mathcal{C}_1\cap\mathcal{C}_2=\emptyset$, entonces $|\mathcal{C}|=p^{h-1}+p^{h-2}+\cdots+p^2+p$.
Veamos ahora que $\mathcal{C}$ es óptimo.

$$\Phi(p^{h+1}-p,p,1)=\left\lfloor\frac{p^{h+1}-p^2}{p^2-p}+\frac{p^2-p-1}{p^2-p}\right\rfloor=|\mathcal{C}|$$

Hemos probado el siguiente resultado.

Teorema 3.5. *Para cualquier número primo p y cualquier entero $h\geq 2$ existe un código ortogonal óptico óptimo con parámetros $(p(p^h-1),p,1)$.*

Ejemplo 3.2. Para $p = 3$ y $h = 3$ tenemos que $p(x) = x^3 + 2x + 1$ es un polinomio generador para $\mathbb{F}_{27}$. Sea α una raíz primitiva de $p(x)$, entonces tenemos las siguientes palabras código para un código ortogonal óptico $\mathcal{C}_1$ con parámetros $(78, 3, 1)$.

$$\begin{aligned}
c_1 &= \{27\log_\alpha(p_1(\alpha)+a) - 26a : a \in \mathbb{Z}_3\} = \{27, 29, 61\}\\
c_2 &= \{27\log_\alpha(p_2(\alpha)+a) - 26a : a \in \mathbb{Z}_3\} = \{16, 66, 74\}\\
c_3 &= \{27\log_\alpha(p_3(\alpha)+a) - 26a : a \in \mathbb{Z}_3\} = \{38, 54, 73\}\\
c_4 &= \{27\log_\alpha(p_4(\alpha)+a) - 26a : a \in \mathbb{Z}_3\} = \{71, 75, 76\}\\
c_5 &= \{27\log_\alpha(p_5(\alpha)+a) - 26a : a \in \mathbb{Z}_3\} = \{11, 36, 38\}\\
c_6 &= \{27\log_\alpha(p_6(\alpha)+a) - 26a : a \in \mathbb{Z}_3\} = \{8, 15, 25\}\\
c_7 &= \{27\log_\alpha(p_7(\alpha)+a) - 26a : a \in \mathbb{Z}_3\} = \{30, 59, 70\}\\
c_8 &= \{27\log_\alpha(p_8(\alpha)+a) - 26a : a \in \mathbb{Z}_3\} = \{5, 46, 69\}
\end{aligned}$$

donde $p_1(x) = x$, $p_2(x) = 2x$, $p_3(x) = x^2$, $p_4(x) = 2x^2$, $p_5(x) = x^2 + x$, $p_6(x) = 2x^2 + x$, $p_7(x) = x^2 + x$ y $p_8(x) = 2x^2 + 2x$. También tenemos las siguientes palabras código para un código ortogonal óptico $\mathcal{C}_2$ con parámetros $(78, 3, 1)$.

$$\begin{aligned}
c_9 &= \{3\log_\alpha(p_1(\alpha)+a) - 26a : a \in \mathbb{Z}_3\} = \{3, 9, 27\}\\
c_{10} &= \{3\log_\alpha(p_3(\alpha)+a) - 26a : a \in \mathbb{Z}_3\} = \{6, 36, 63\}\\
c_{11} &= \{3\log_\alpha(p_5(\alpha)+a) - 26a : a \in \mathbb{Z}_3\} = \{18, 30, 33\}\\
c_{12} &= \{3\log_\alpha(p_7(\alpha)+a) - 26a : a \in \mathbb{Z}_3\} = \{12, 21, 54\}
\end{aligned}$$

Por tanto, $\mathcal{C} = C_1 \cup \mathcal{C}_2$ es un código ortogonal óptico óptimo con parámetros $(78, 3, 1)$.

Continuamos ahora con la construcción A de [11]. Esta construcción es bastante interesante ya que explota la estructura del anillo $\mathbb{Z}_{p^n}$. Sea p un número primo tal que $p = mt+1$ para algunos enteros positivos m y t. Sea α una raíz primitiva módulo p^m para $1 \le m \le n$. Para $0 \le s \le mp^n - 1$ sea $s := (t_0, t_1)$ donde $t_0 \equiv s \pmod m$ y $t_1 \equiv s \pmod{p^n}$. Para cada $0 \le i \le p^k - 1$, $0 \le j \le t - 1$ y $0 \le k \le n - 1$ sea $x^k_{i,j} = x^k_{i,j}(s)$ la secuencia dada por

$$x^k_{i,j}(s) = \begin{cases} 1 & \text{si } t_1 = p^{n-1-k}\alpha^{i(p-1)+j+t_0 t} \pmod{p^n} \\ 0 & \text{en otro caso .} \end{cases},$$

donde $0 \le s \le mp^n - 1$.

Si

$$\mathcal{X}_A = \bigcup_{k=0}^{n-1} \mathcal{X}^k,$$

donde $\mathcal{X}^k = \{x_{i,j}^k : 0 \leq i \leq p^k - 1, 0 \leq j \leq t-1\}$, entonces $\mathcal{X}_A$ es un código ortogonal óptico asintóticamente óptimo con parámetros $(mp^n, m, 1)$ y $\frac{p^n-1}{m}$ palabras código. La demostración de que $\mathcal{X}_A$ satisface las propiedades de correlación se puede consultar en [11].
Por el Teorema Chino de los Restos, los elementos de $\mathcal{X}_A$ pueden ser expresados en la forma conjuntista así

$$A(i,j,k) = \{s \in \mathbb{Z}_{mp^n} : s \equiv ap^n - p^{n-1-k}\alpha^{i(p-1)+j+at}(p^n-1) \text{ mód } mp^n \text{ con } a \in \mathbb{Z}_m\},$$

donde s es la solución del sistema de congruencias

$$\begin{aligned} s &\equiv a \text{ mód } m, \\ s &\equiv p^{n-1-k}\alpha^{i(p-1)+j+at} \text{ mód } p^n. \end{aligned}$$

para cada $a \in \mathbb{Z}_m$. Por el Lema 3.1 tenemos que la deficiencia L de $\mathcal{X}_A$ expresado en la forma conjuntista es $L = M_m \cup M_{p^n}$, donde M_m y M_{p^n} denotan los múltiplos no nulos de m y p^n en $\mathbb{Z}_{mp^n}$, respectivamente. Por lo tanto, para garantizar la optimalidad del código hacen falta $\Phi(mp^n, m, 1) - |\mathcal{X}_A| = \dfrac{p^n-1}{m(m-1)}$ palabras código.
En general no es fácil determinar un código auxiliar con los mismos parámetros y que permita optimizar el tamaño del código anterior. Sin embargo, es posible encontrar dicho código cuando p es de la forma $p = m(m-1)q+1$ para algunos enteros positivos m y q. Para este caso, la cota de Johnson es

$$\begin{aligned} \Phi(mp^n, m, 1) &= \left\lfloor \frac{mp^n - 1}{m(m-1)} \right\rfloor \\ &= \frac{mp^n-1}{m(m-1)} - \frac{1}{m} \\ &= \frac{p^n-1}{m-1}. \end{aligned}$$

Para alcanzar este objetivo, probamos el siguiente teorema.

Teorema 3.6. *Sea p un número primo de la forma $p = m(m-1)q+1$ para algunos enteros positivos m y q. Supongamos que existe un código ortogonal óptico $\mathcal{C}$ con parámetros $(p, m, 1)$ y q palabras código. Para cada $x = \{x_1, x_2, \ldots, x_m\} \in \mathcal{C}$ sea*

$$C_x = \{\{x_j p^k + ip^{k+1} \text{ mód } p^n : j = 1, \ldots, m\} : k = 0, \ldots, n-1, i = 0, \ldots, p^{n-1-k} - 1\}.$$

Si $\mathcal{F} = \bigcup_{x \in \mathcal{C}} C_x$, entonces $\mathcal{F}$ es un código ortogonal óptico óptimo con parámetros $(p^n, m, 1)$.

Demostración. Sea $x \in \mathcal{C}$ y $u \in C_x$, entonces $u = \{x_j p^k + ip^{k+1}x_j \text{ mód } p^n : j = 1, \dots m\}$ para algunos k e i. Si $|\Delta(u)| < m(m-1)$ entonces existen j_1, j_2, j_3 y j_4 tales que $j_1 \neq j_2$, $j_3 \neq j_4$ y

$$x_{j1}p^k + ip^{k+1}x_{j1} - x_{j2}p^k - ip^{k+1}x_{j2} = x_{j3}p^k + ip^{k+1}x_{j3} - x_{j4}p^k - ip^{k+1}x_{j4} \text{ mód } p^n.$$

Entonces

$$(x_{j_1} - x_{j_2})p^k + ip^{k+1}(x_{j_1} - x_{j_2}) = (x_{j_3} - x_{j_4})p^k + ip^{k+1}(x_{j_3} - x_{j_4}) \text{ mód } p^n.$$

Luego

$$(x_{j_1} - x_{j_2}) + ip(x_{j_1} - x_{j_2}) = (x_{j_3} - x_{j_4}) + ip(x_{j_3} - x_{j_4}) \text{ mód } p^{n-k}.$$

Luego

$$x_{j_1} - x_{j_2} = x_{j_3} - x_{j_4} \text{ mód } p$$

lo cual contradice el hecho de que $\mathcal{C}$ es un código ortogonal óptico. Por tanto, $|\Delta(u)| = m(m-1)$.
Veamos ahora que $\Delta(u) \cap \Delta(w) = \emptyset$ para $u, w \in \mathcal{F}$ con $u \neq w$. Si $u, w \in C_x$ para alguna $x \in \mathcal{C}$, entonces

$$u = \{x_j p^{k_1} + i_1 p^{k_1+1}x_j \text{ mód } p^n : j = 1, \dots m\},$$
$$w = \{x_j p^{k_2} + i_2 p^{k_2+1}x_j \text{ mód } p^n : j = 1, \dots m\},$$

para algunos k_1, k_2, i_1 e i_2. Supongamos que $\Delta(u) \cap \Delta(w) \neq \emptyset$, luego existe al menos un elemento no nulo en común. Por tanto, existen j_1, j_2, j_3, j_4 con $j_1 \neq j_2$ y $j_3 \neq j_4$ tales que

$$x_{j_1}p^{k_1} + i_1p^{k_1+1}x_{j_1} - x_{j_2}p^{k_1} - i_1p^{k_1+1}x_{j_2} = x_{j_3}p^{k_2} + i_2p^{k_2+1}x_{j_3} - x_{j_4}p^{k_2} - i_2p^{k_2+1}x_{j_4} \text{ mód } p^n.$$

Reordenando términos tenemos

$$(x_{j_1} - x_{j_2})p^{k_1} + i_1p^{k_1+1}(x_{j_1} - x_{j_2}) = (x_{j_3} - x_{j_4})p^{k_2} + i_2p^{k_2+1}(x_{j_3} - x_{j_4}) \text{ mód } p^n.$$

Sin pérdida de generalidad, supongamos que $k_1 \leq k_2$, entonces

$$x_{j_1} - x_{j_2} + i_1p(x_{j_1} - x_{j_2}) = (x_{j_3} - x_{j_4})p^{k_2-k_1} + i_2p^{k_2-k_1+1}(x_{j_3} - x_{j_4}) \text{ mód } p^{n-k_1}.$$

Si $k_1 = k_2$, entonces $x_{j_1} - x_{j_2} = x_{j_3} - x_{j_4}$ mód p, lo cual contradice el hecho de que $\mathcal{C}$ es un código ortogonal óptico.
Si $k_1 < k_2$, entonces $x_{j_1} - x_{j_2} = 0$ mód p, lo cual contradice el hecho de que $j_1 \neq j_2$.
Si $u \in C_x$ y $w \in C_y$, para algunas $x, y \in \mathcal{C}$ con $x \neq y$, entonces

$$u = \{x_j p^{k_1} + i_1 p^{k_1+1}x_j \text{ mód } p^n : j = 1, \dots m\},$$

$$w = \{y_j p^{k_2} + i_2 p^{k_2+1}y_j \text{ mód } p^n : j = 1, \dots m\},$$

para algunos k_1, k_2, i_1 e i_2. Como antes, supongamos por contradicción $\Delta(u) \cap \Delta(w) \neq \emptyset$, por tanto, existen j_1, j_2, j_3, j_4 con $j_1 \neq j_2$ y $j_3 \neq j_4$ tales que

$$x_{j_1}p^{k_1} + i_1p^{k_1+1}x_{j_1} - x_{j_2}p^{k_1} - i_1p^{k_1+1}x_{j_2} = y_{j_3}p^{k_2} + i_2p^{k_2+1}y_{j_3} - y_{j_4}p^{k_2} - i_2p^{k_2+1}y_{j_4} \text{ mód } p^n.$$

Razonando como antes tenemos las mismas contradiciones del caso anterior. Por lo tanto $\Delta(u) \cap \Delta(w) = \emptyset$ para toda $u, w \in \mathcal{F}$ con $u \neq w$.
Finalmente, probemos que el código es óptimo. Tenemos

$$|C_x| = p^{n-1} + p^{n-2} + \ldots + p + 1 = \frac{p^n - 1}{p - 1},$$

para toda $x \in \mathcal{C}$. Por tanto,

$$|\mathcal{F}| = t\frac{p^n - 1}{p - 1} = \frac{p^n - 1}{m(m-1)} = \Phi(p^n, m, 1).$$

Usando la construcción A, la familia $m\mathcal{F}$, donde $\mathcal{F}$ es la familia del Teorema 3.6 y $m\mathcal{F} = \{m\mathbf{c} : \mathbf{c} \in \mathcal{F}\}$, donde $m\mathbf{c} = \{mc \text{ mód } mp^n : c \in \mathbf{c}\}$ obtenemos el siguiente resultado.

Corolario 3.1. *Sea p un número primo tal que $p = m(m-1)q+1$ para algunos enteros m y q. Si existe un código ortogonal óptico óptimo con parámetros $(p, m, 1)$, entonces, existe un código ortogonal óptico óptimo con parámetros $(mp^n, m, 1)$ para todo entero positivo n.*

Ejemplo 3.3. Sea $p = 41 = 5 \cdot 8 + 1$, entonces $m = 5$ y $t = 8$. Se puede verificar que $\alpha = 6$ es una raíz primitiva módulo 41. Resolviendo las congruencias planteadas en la construcción A con $n = 1$ podemos afirmar que el código $\mathcal{X}_A$ tiene parámetros $(205, 5, 1)$ y esta conformado por las siguientes palabras código

$\mathbf{c}_1 = \{51, 98, 119, 165, 182\}$
$\mathbf{c}_2 = \{67, 99, 101, 170, 178\}$
$\mathbf{c}_3 = \{43, 184, 196, 197, 200\}$
$\mathbf{c}_4 = \{53, 79, 151, 157, 175\}$
$\mathbf{c}_5 = \{25, 64, 86, 113, 122\}$
$\mathbf{c}_6 = \{63, 106, 117, 150, 179\}$
$\mathbf{c}_7 = \{21, 49, 80, 87, 173\}$
$\mathbf{c}_8 = \{13, 70, 89, 112, 126\}$

Por otra parte, $\mathcal{C} = \{\{0, 1, 13, 38, 31\}, \{0, 32, 6, 27, 8\}\}$ es un código ortogonal óptico con parámetros $(41, 5, 1)$. Si hacemos

$$\mathbf{c}_9 = 5\{0, 1, 13, 38, 31\} = \{0, 5, 65, 155, 190\} \text{ y}$$

$$\mathbf{c}_{10} = 5\{0, 32, 6, 27, 8\} = \{0, 30, 40, 135, 160\},$$

entonces $D = \{\mathbf{c}_i : i = 1, \ldots, 10\}$ es un código ortogonal óptico óptimo con parámetros $(205, 5, 1)$.

Continuamos ahora con la construcción B de [11]. Sea q una potencia prima, $\mathbb{F}_q$ el campo finito con q elementos, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ y α un elemento primitivo de $\mathbb{F}_q$. Para esta construcción se utilizan las siguientes suposiciones:

- $p_1, p_2, \ldots, p_k$ denotan números primos impares con $p_1 < p_2 < \cdots < p_k$.
- Existen enteros positivos m y T_i tales que $p_i = mT_i + 1$ para $1 \leq i \leq k$.
- α_i es un elemento primitivo de $\mathbb{F}_{p_i}$ para $1 \leq i \leq k$.

Sean $u = (u_1, \ldots, u_k) \in \mathbb{F}_{p_1} \times \cdots \times \mathbb{F}_{p_k}$, $r = (r_1, \ldots, r_k) \in \mathbb{Z}_{T_1} \times \cdots \times \mathbb{Z}_{T_k}$ y $d = (d_1, \ldots, d_k) \in \mathbb{Z}_m^k$ tales que

- $u_i = 0$ o $u_i = 1$.
- Si $u_i = 0$, entonces $r_i = 0$ y $d_i = 0$.
- Existe i^* con $1 \leq i^* \leq k$ tal que $u_1 = \cdots = u_{i^*-1} = 0$, $u_{i^*} = 1$ y $d_{i^*} = 0$.

Si $\mathcal{J}$ es el conjunto de todas las $3k$-uplas $\mathbf{u} : \mathbf{r} : \mathbf{d}$ que satisfacen las condiciones anteriores, entonces $|\mathcal{J}| = \dfrac{p_1 \ldots p_k - 1}{m}$.
Por el Teorema Chino de los Restos, existe $0 \leq t \leq mp_1 \cdots p_k - 1$ tal que

$$t := (t_0, t_1, \ldots, t_k),$$

donde $t = t_0$ mód m y $t = t_i$ mód p_i para $1 \leq i \leq k$. Para cada $\mathbf{u} : \mathbf{r} : \mathbf{d} \in \mathcal{J}$, sea $S_{\mathbf{u:r:d}} = \{S_{\mathbf{u:r:d}}(t) : 0 \leq t \leq mp_1 \cdots p_k - 1\}$ la secuencia de ceros y unos dada por

$$S_{\mathbf{u:r:d}}(t) = \begin{cases} 1 & \text{si } (t_1, \ldots, t_k) = (u_1\alpha_1^{(t_0+d_1)T_1+r_1}, \ldots, u_k\alpha_k^{(t_0+d_k)T_k+r_k}), \\ 0 & \text{en otro caso.} \end{cases}$$

Entonces $\mathcal{X}_B = \{S_{\mathbf{u:r:d}} : \mathbf{u} : \mathbf{r} : \mathbf{d} \in \mathcal{J}\}$ es un código ortogonal óptico con parámetros $(mp_1 \cdots p_k, m, 1)$ y $\dfrac{p_1 \cdots p_k - 1}{m}$ elementos. Podemos notar que los elementos del código construido anteriormente en la forma conjuntista pueden ser vistos como el conjunto

solución del siguiente sistema de congruencias.

$$\begin{aligned} t &= t_0 \text{ mód } m, \\ t &= u_1\alpha_1^{(t_0+d_1)t_1+r_1} \text{ mód } p_1, \\ t &= u_2\alpha_2^{(t_0+d_2)t_2+r_2} \text{ mód } p_2, \\ &\vdots \\ t &= u_k\alpha_k^{(t_0+d_k)t_k+r_k} \text{ mód } p_k. \end{aligned}$$

Por tanto, por el Lema 3.1, la deficiencia de $\mathcal{X}_B$ expresado en la forma conjuntista es $L = M_m \cup M_{p_1} \cup \cdots \cup M_{p_k}$.

Ejemplo 3.4. Con $p_1 = 7$ y $p_2 = 13$ tomamos $m = 3$, por tanto $T_1 = 2$ y $T_2 = 4$. Tenemos que $\alpha_1 = 3$ y $\alpha_2 = 2$ son elementos primitivos de $\mathbb{F}_7$ y $\mathbb{F}_{13}$, respectivamente. Un cálculo sencillo muestra que

$$\begin{aligned} \mathcal{J} = \{&(0,1,0,0,0,0),(0,1,0,1,0,0),(0,1,0,2,0,0),(0,1,0,3,0,0),(1,0,0,0,0,0),\\ &(1,0,1,0,0,0),(1,1,0,0,0,0),(1,1,0,0,0,1),(1,1,0,0,0,2),(1,1,0,1,0,0),\\ &(1,1,0,1,0,1),(1,1,0,1,0,2),(1,1,0,2,0,0),(1,1,0,2,0,1),(1,1,0,2,0,2),\\ &(1,1,0,3,0,0),(1,1,0,3,0,1),(1,1,0,3,0,2),(1,1,1,0,0,0),(1,1,1,0,0,1),\\ &(1,1,1,0,0,2),(1,1,1,1,0,0),(1,1,1,1,0,1),(1,1,1,1,0,2),(1,1,1,2,0,0),\\ &(1,1,1,2,0,1),(1,1,1,2,0,2),(1,1,1,3,0,0),(1,1,1,3,0,1),(1,1,1,3,0,2)\}\\ &\subset \mathbb{F}_7 \times \mathbb{F}_{13} \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3^2. \end{aligned}$$

Para cada $(u_1, u_2, r_1, r_2, d_1, d_2) \in \mathcal{D}$ resolviendo cada sistema de congruencias

$$\begin{aligned} t &= t_0 \text{ mód } 3, \\ t &= u_1 3^{2(t_0+d_1)+r_1} \text{ mód } 7, \\ t &= u_2 2^{4(t_0+d_2)+r_2} \text{ mód } 13, \end{aligned}$$

para $t_0 \in \mathbb{Z}_3$ tenemos que

$$\begin{aligned} \mathcal{X}_B = \{&\{105,133,35\},\{210,175,161\},\{147,259,140\},\{21,154,98\},\{78,247,221\},\\ &\{234,13,26\},\{183,16,74\},\{120,100,53\},\{204,79,263\},\{15,58,200\},\\ &\{162,226,158\},\{57,184,32\},\{225,142,179\},\{246,205,95\},\{36,121,116\},\\ &\{99,37,137\},\{141,163,242\},\{267,268,11\},\{66,55,152\},\{3,139,131\},\\ &\{87,118,68\},\{171,97,5\},\{45,265,236\},\{213,223,110\},\{108,181,257\},\\ &\{129,244,173\},\{192,160,194\},\{255,76,215\},\{24,202,47\},\{150,34,89\}\}, \end{aligned}$$

es un código ortogonal óptico con parámetros $(273, 3, 1)$.

En lo que sigue mostramos una serie de definiciones y resultados que permiten optimizar el código anterior y además proporcionamos una forma alternativa de construir familias de diferencias para primos p de la forma $p \equiv 1 \bmod m(m-1)$ donde m es un número primo.

Definición 3.2. Sea B un conjunto con n elementos llamados símbolos. Un cuadrado latino de orden n es una matriz de tamaño $n \times n$ para la cual los n símbolos de B aparecen exactamente una vez en cada fila y en cada columna del arreglo. El conjunto B se llama conjunto base del cuadrado latino.

Definición 3.3. Dos cuadrados latinos de orden n son ortogonales si al sobreponer uno de ellos en el otro cada uno de los posibles n^2 pares ordenados aparece exactamente una vez. Un conjunto de cuadrados latinos de orden n es mutuamente ortogonal si cualquier dos cuadrados latinos diferentes del conjunto son ortogonales.

Un resultado conocido afirma que el máximo cardinal de un conjunto de cuadrados latinos de orden n mutuamente ortogonales es a lo sumo $n-1$ [13], mientras que para todo n, excepto $n = 2$ y $n = 6$ existe un par de cuadrados latinos ortogonales de orden n. Aunque la existencia de conjuntos de cuadrados latinos de orden n, para n un número primo o potencia prima está probada explícitamente, mostramos una construcción alternativa para estos órdenes en la Observación 3.2, cuya demostración es similar a la encontrada en [13].

Teorema 3.7. *[13] Para toda potencia prima q existe un conjunto de cuadrados latinos mutuamente ortogonales de orden q con $q-1$ elementos.*

Observación 3.2. Sea $\mathbb{F} = \{0, a_1, \ldots, a_{q-1}\}$ un campo finito con q elementos. Para cada $a \in \mathbb{F}^*$ considere los arreglos de tamaño $q \times q$ de la forma $M_a = (M_{i,j})$, donde $M_{i,j} = ja + i$ para $1 \leq i, j \leq q-1$. Entonces el conjunto $M = \{M_a : a \in \mathbb{F}^*\}$ es un conjunto de cuadrados latinos mutuamente ortogonales con $q-1$ elementos. Los cuadrados latinos construidos de esta manera tienen la propiedad de que cualquier par de filas bien sea del mismo arreglo o de diferentes arreglos, tienen a lo más un elemento en común al ser superpuestas y que los pares ordenados con componentes iguales obtenidos al sobreponer dos cuadrados latinos, aparecen en la primera columna.

Usando el hecho anterior podemos demostrar alternativamente un resultado probado por Jungnickel en [18], el cual generalizamos en el siguiente capítulo en el Teorema 4.6 y del cual deducimos el siguiente resultado importante para el presente capítulo.

Corolario 3.2. *Sean p_1, p_2, m números primos tales que $p_i \equiv 1 \bmod m(m-1)$ para $i = 1, 2$. Supongamos que existen códigos ortogonales ópticos óptimos $\mathcal{C}_1$ y $\mathcal{C}_2$ con parámetros $(p_1, m, 1)$ y $(p_2, m, 1)$, respectivamente. Entonces*

1. *si $p_1 \neq p_2$ existe un código ortogonal óptico óptimo con parámetros $(p_1p_2, m, 1)$,*

2. *si $p_1 = p_2$ existe una familia de diferencias en el grupo $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Demostración. Como $p_i \equiv 1$ mód $m(m-1)$ para $i = 1, 2$, entonces existen enteros positivos t_1 y t_2 tales que $p_1 = m(m-1)t_1 + 1$ y $p_2 = m(m-1)t_2 + 1$. Sean

$$\mathcal{C}_1 = \{\{x_{i,1}, \ldots, x_{i,m}\} : i = 1, \ldots, t_1\},$$

$$\mathcal{C}_2 = \{\{y_{i,1}, \ldots, y_{i,m}\} : i = 1, \ldots, t_2\}.$$

Como m es un número primo, existe un conjunto M de cuadrados latinos mutuamente ortogonales de orden m con $m-1$ elementos. Usemos los números desde 0 hasta $m-1$ para denotar las componentes de cada elemento de M.
Consideremos $\mathcal{D} \subset \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2}$ como la unión de los siguientes conjuntos

$$\mathcal{D}_1 = \{\{(x_{i,1}, 0), \ldots, (x_{i,m}, 0)\} : i = 1, \ldots, t_1\},$$

$$\mathcal{D}_2 = \{\{(0, y_{i,1}), \ldots, (0, y_{i,m})\} : i = 1, \ldots, t_2\},$$

$$\mathcal{D}_3 = \{\{(x_{i,1}, y_{j,k_1}), \ldots, (x_{i,m}, y_{j,k_m})\} : i = 1, \ldots, t_1, j = 1, \ldots, t_2\},$$

donde $(k_1, \ldots k_m)$ es cualquier fila de un elemento de M.
Dado que $\mathcal{C}_1$ y $\mathcal{C}_2$ son códigos ortogonales ópticos, entonces cada elemento en $\mathcal{D}$ satisface la propiedad de la autocorrelación. Para probar la propiedad de la correlación cruzada, supongamos por contradicción que existen $X, Y \in \mathcal{D}$ con $X \neq Y$ tales que $\Delta(X) \cap \Delta(Y) \neq \emptyset$. Por hipótesis no es posible que esta afirmación se cumpla si $X \in \mathcal{D}_1 \cup \mathcal{D}_2$ o $Y \in \mathcal{D}_1 \cup \mathcal{D}_2$. Por tanto, supongamos que $X, Y \in \mathcal{D}_3$, es decir

$$X = \{(x_{i,1}, y_{j,k_1}), \ldots, (x_{i,m}, y_{j,k_m})\},$$

$$Y = \{(x_{i',1}, y_{j',k'_1}), \ldots, (x_{i',m}, y_{j',k'_m})\}.$$

Si $\Delta(X) \cap \Delta(Y) \neq \emptyset$, entonces existen i_1, i_2, i_2 e i_4 tales que

$$(x_{i,i_1}, y_{j,k_{i_1}}) - (x_{i,i_2}, y_{j,k_{i_2}}) = (x_{i',i_3}, y_{j',k'_{i_3}}) - (x_{i',i_4}, y_{j',k'_{i_4}}).$$

La igualdad sobre la diferencia de las primeras componentes implican que $i = i'$ ya que $\mathcal{C}_1$ es un código ortogonal óptico, por lo tanto, $i_1 = i_3$ e $i_2 = i_4$. Similarmente, la igualdad sobre la diferencia de las segundas componentes implican que $j = j'$ y por tanto $k_{i_1} = k'_{i_3}$ y $k_{i_2} = k'_{i_4}$, sin embargo esto implica que $k = k'$ lo cual contradice el hecho de que $X \neq Y$ o $k \neq k'$ y que M es un conjunto de cuadrados latinos mutuamente ortogonales.
Si $p_1 \neq p_2$, entonces por el Teorema Chino de los Restos aplicado a cada elemento de $X \in \mathcal{D}$ se obtiene un código ortogonal óptico óptimo con parámetros $(p_1p_2, m, 1)$ y

$$|\mathcal{D}| = |D_1| + |D_2| + |D_3| = t_1 + t_2 + t_1t_2(m-1)m = \Phi(p_1p_2, m, 1)$$

elementos.
Si $p_1 = p_2 = p$, entonces $\mathcal{D}$ es una familia de diferencias en $\mathbb{Z}_p \times \mathbb{Z}_p$ con

$$|\mathcal{D}| = |D_1| + |D_2| + |D_3| = 2t + t^2(m-1)m$$

elementos, donde $t_1 = t_2 = t$.

El resultado anterior podemos generalizarlo usando inducción sobre el número de primos que satisfacen la condición.

Corolario 3.3. *Sean p_i para $i = 1, \ldots, t$ números primos y m un número primo tales que $p_i \equiv 0$ mód $m(m-1)$ para todo i. Supongamos que para cada i existe un código ortogonal óptico óptimo $\mathcal{C}_i$ con parámetros $(p_i, m, 1)$. Entonces existe una familia de diferencias en $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_t}$. En particular, si todos los primos p_i son diferentes, entonces existe un código ortogonal óptico óptimo con parámetros $(p_1 p_2 \cdots p_t, m, 1)$.*

Combinando el resultado anterior con la construcción $\mathcal{X}_B$ tenemos el siguiente resultado.

Corolario 3.4. *Sean p_i para $i = 1, \ldots, k$ números primos diferentes y m un número primo tal que $p_i \equiv 0$ mód $m(m-1)$ para todo i. Supongamos que para cada i existen un código ortogonal óptico óptimo $\mathcal{C}_i$ con parámetros $(p_i, m, 1)$. Entonces existe un código ortogonal óptico óptimo $\mathcal{C}$ con parámetros $(mp_1 \cdots p_k, m, 1)$.*

Demostración. Sea $\mathcal{C} = \mathcal{X}_B \cup m\mathcal{D}'$, donde $\mathcal{X}_B$ es la construcción B dada por [11], $\mathcal{D}'$ es el conjunto del Corolario 3.2 visto en $\mathbb{Z}_{p_1 \cdots p_k}$ y $m\mathcal{D}' = \{mX : X \in \mathcal{D}'\}$ donde $mX = \{mx \in \mathbb{Z}_{mp_1 \cdots p_k} : x \in X\}$. Entonces $\mathcal{C}$ es un código ortogonal óptico óptimo con parámetros $(mp_1 \cdots p_k, m, 1)$. Además

$$|\mathcal{C}| = |\mathcal{X}_B| + |m\mathcal{D}'| = \frac{p_1 \cdots p_k - 1}{m} + \frac{p_1 \cdots p_k - 1}{m(m-1)} = \Phi(mp_1 \cdots p_k, m, 1).$$

Ejemplo 3.5. Sean $p_1 = 7$ y $p_2 = 13$ como en el Ejemplo 3.4. Es fácil verificar que $\mathcal{C}_1 = \{0, 1, 3\}$ y $\mathcal{C}_2 = \{\{0, 1, 4\}, \{0, 2, 7\}\}$ son códigos ortogonales ópticos óptimos con parámetros $(7, 3, 1)$ y $(13, 3, 1)$, respectivamente. Por el Teorema 3.7, podemos construir el conjunto de cuadrados latinos mutuamente ortogonal de orden 3 con dos elementos

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Por tanto, por el Teorema 3.2 el conjunto

$$\begin{aligned}\mathcal{D} = \{&\{(0,0),(1,0),(3,0)\},\{(0,0),(0,1),(0,4)\},\{(0,0),(0,2),(0,7)\},\\ &\{(0,0),(1,1),(3,4)\},\{(0,1),(1,4),(3,0)\},\{(0,4),(1,0),(3,1)\},\\ &\{(0,0),(1,4),(3,1)\},\{(0,1),(1,0),(3,4)\},\{(0,4),(1,1),(3,0)\},\\ &\{(0,0),(1,2),(3,7)\},\{(0,2),(1,7),(3,0)\},\{(0,7),(1,0),(3,2)\},\\ &\{(0,0),(1,7),(3,2)\},\{(0,2),(1,0),(3,7)\},\{(0,7),(1,2),(3,0)\}\end{aligned}$$

es una familia de diferencias en $\mathbb{Z}_7 \times \mathbb{Z}_{13}$. Por el Teorema Chino de los Restos

$$\begin{aligned}\mathcal{D}' = \{&\{0,78,52\},\{0,14,56\},\{0,28,7\},\{0,1,17\},\{14,43,52\},\\ &\{56,78,66\},\{0,43,66\},\{14,78,17\},\{56,1,52\},\{0,15,59\},\\ &\{28,85,52\},\{7,78,80\},\{0,85,80\},\{28,78,59\},\{7,15,52\}\}\end{aligned}$$

es un código ortogonal óptico con parámetros $(91,3,1)$. Luego $\mathcal{C} = \mathcal{X}_B \cup 3\mathcal{D}'$ es un código ortogonal óptico óptimo con parámetros $(273,3,1)$.

Observación 3.3. Los corolarios anteriores pueden generalizarse aún más eligiendo códigos que no necesariamente tengan la longitud dada en éstos, sin embargo no se puede garantizar la optimalidad del código obtenido.

Ejemplo 3.6. $\mathcal{C}_1 = \{\{0,2,6\}$ y $\mathcal{C}_2 = \{\{0,1,3\}\}$ son códigos ortogonales ópticos óptimos con parámetros $(7,3,1)$ y $(8,3,1)$, respectivamente. Considerando los cuadrados latinos

$$M_{B,1} = \begin{pmatrix} 0 & 1 & 3 \\ 1 & 3 & 0 \\ 3 & 0 & 1 \end{pmatrix} M_{B,2} = \begin{pmatrix} 0 & 3 & 1 \\ 1 & 0 & 3 \\ 3 & 1 & 0 \end{pmatrix}$$

los subconjuntos $\mathcal{D}_1 = \{\{(0,0),(2,0),(6,0)\}\}$, $\mathcal{D}_2 = \{\{(0,0),(0,1),(0,3)\}\}$ y $\mathcal{D}_3 = \{\{(0,m_{j,1}^{B,k}),(2,m_{j,2}^{B,k}),(6,m_{j,3}^{B,k})\} : j = 1,\ldots,3, k = 1,2\}$ de $\mathbb{Z}_7 \times \mathbb{Z}_8$. Tenemos por el Teorema Chino de los Restos el siguiente código ortogonal óptico

$$\begin{aligned}\mathcal{C} = \{&\{0,16,48\},\{0,49,35\},\{0,9,27\},\{49,51,48\},\\ &\{35,16,41\},\{0,51,41\},\{49,16,27\},\{35,9,48\}\}\end{aligned}$$

con parámetros $(56,3,1)$. Sin embargo, la cota de Johson para estos parámetros es igual a 9, por tanto el código obtenido no es óptimo.

3.2. Códigos ortogonales ópticos a partir de conjuntos de Sidon

En esta sección presentamos la construcción recursiva para códigos ortogonales ópticos obtenida por Chu y Golomb en [8]. Esta contrucción es bastante interesante porque permite obtener códigos con nuevos parámetros, sin embargo la conclusión dada por los autores respecto a su uso consiste en analizar qué tan lejos están los códigos ortogonales obtenidos por la construcción de ser óptimos, si el código ortogonal óptico de base es óptimo. Nuestro propósito en esta sección es usar la construcción recursiva con los conjuntos de Sidon modulares y analizar dicha conclusión.
En [8] se usa el concepto de matriz $r-$simple. Recordamos su definición, la cual fue vista en 2.3.

Definición 3.4. Sean G un grupo abeliano de tamaño n y r un entero positivo. Una matriz $A = (a_{ij})$ de tamaño $s \times t$ sobre G es $r-$simple, si el vector diferencia entre cualquier par de vectores columnas de A contiene a los elementos de G a los sumo $r-1$ veces.

Presentamos algunos resultados de [8] para el caso $\lambda = 1$ y $r = 2$.

Teorema 3.8. *Sea $\mathcal{C}$ un código ortogonal óptico con parámetros $(n, w, 1)$. Si existe una matriz de tamaño $w \times N$ $2-$simple sobre $\mathbb{Z}_g$, entonces existe un código ortogonal óptico $\mathcal{C}'$ con parámetros $(ng, w, 1)$ y $N\,|\mathcal{C}|$ palabras código.*

Observación 3.4. El código $\mathcal{C}'$ del teorema anterior puede describirse usando la siguiente notación. Si $\mathcal{C} = \{C_i : 1 \leq i \leq |\mathcal{C}|\}$ es un código ortogonal óptico con parámetros $(n, w, 1)$ donde $C_i = \{b_{i,1}, b_{i,2}, \ldots, b_{i,w}\}$ con $b_{i.j} \in \mathbb{Z}_n$, $1 \leq i \leq |\mathcal{C}|$, $1 \leq j \leq w$ y $D = (d_{ij})$ es una matriz de tamaño $w \times N$ $2-$simple sobre $\mathbb{Z}_g$, entonces se construyen por cada elemento C_i de $\mathcal{C}$ las N palabras código siguientes

$$F_{il} = \{(b_{i,j} + nd_{jl}) \text{ mód } ng : 1 \leq j \leq w\},$$

donde $1 \leq l \leq N$.
Luego $\mathcal{C}'$ puede expresarse en la forma

$$\mathcal{C}' = \{F_{il} : 1 \leq i \leq |\mathcal{C}|\,, 1 \leq l \leq N\}.$$

El siguiente resultado muestra cómo construir matrices $2-$simples.

Lema 3.2. *Sean p un número primo y $f(x)$ un polinomio en $\mathbb{F}_p[x]$. La matriz $D = (d_{ij})$ de tamaño $p \times p$, donde $d_{ij} = ij + f(i)$ para $0 \leq i, j \leq p-1$ es una matriz $2-$simple sobre $\mathbb{Z}_p$.*

Combinando los resultados del Teorema 3.8 y el Lema 3.2 se obtiene el siguiente corolario que nos permite construir familias infinitas de códigos ortogonales ópticos.

Corolario 3.5. *Suponga que existe un código ortogonal óptico $\mathcal{C}$ con parámetros $(n, w, 1)$. Sea p el menor número primo mayor o igual a w, entonces existe un código ortogonal óptico con parámetros $(np, w, 1)$ y $p|\mathcal{C}|$ elementos.*

Usando el resultado anterior de manera recursiva se obtiene.

Corolario 3.6. *Suponga que existe un código ortogonal óptico $\mathcal{C}$ con parámetros $(n, w, 1)$. Sea $m = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ un entero positivo, donde p_i es un número primo mayor o igual a w para todo $1 \leq i \leq t$. Entonces, existe un código ortogonal óptico con parámetros $(mn, w, 1)$ y $m|\mathcal{C}|$ elementos.*

Analicemos ahora la aplicación del resultado del Corolario 3.5 a los conjuntos de Sidon modulares para obtener códigos ortogonales ópticos óptimos. Primero aplicamos el resultado al conjunto de Sidon tipo Bose.

Teorema 3.9. *Sean q potencia prima y θ una raíz primitiva sobre $\mathbb{F}_{q^2}$. Entonces el conjunto $B = \{\log_\theta(\theta + a) : a \in \mathbb{F}_q\}$ es un conjunto de Sidon módulo $q^2 - 1$ con q elementos y deficiencia L igual a $L = M_{q+1}$.*

Aplicando el Corolario 3.5 al conjunto del Teorema 3.9 obtenemos el siguiente resultado.

Teorema 3.10. *Para cualquier potencia prima q, existe un código ortogonal óptico $\mathcal{C}$ con parámetros $(p(q^2-1), q, 1)$ y p elementos, donde p es el menor número primo mayor o igual a q. En particular, si q es un número primo, el código obtenido es óptimo.*

Demostración. La existencia del código es un resultado inmediato por el Corolario 3.5. Si q es un número primo, entonces $q = p$ y por tanto

$$\begin{aligned}\Phi(p(p^2-1), p, 1) &= \left\lfloor \frac{p(p^2-1)-1}{p(p-1)} \right\rfloor \\ &= \left\lfloor p + 1 - \frac{1}{p(p-1)} \right\rfloor \\ &= p = |\mathcal{C}|\,.\end{aligned}$$

El siguiente resultado nos permite caracterizar la deficiencia del código del Teorema 3.10.

Teorema 3.11. *Sea $\mathcal{C}$ el código ortogonal óptico del Teorema 3.10, entonces la deficiencia L de $\mathcal{C}$ es $L = M_{q+1}$, donde M_{q+1} es el conjunto de los múltiplos no nulos de $q+1$ en $\mathbb{Z}_{p(q^2-1)}$.*

Demostración. Sean $B = \{\log_\theta(\theta + a) : a \in \mathbb{F}_q\} = \{a_0, a_1, \ldots, a_{q-1}\}$ el conjunto de Sidon del Teorema 3.9 y $D = (d_{i,j})$ una matriz de tamaño $q \times p$ sobre $\mathbb{Z}_p$ 2−simple, donde $d_{i,j} = ij$ para $0 \leq i, j \leq p-1$ y p es el menor número primo mayor o igual a q. Por la Observación 3.4 tenemos

$$\mathcal{C} = \{C_j : 0 \leq j \leq p-1\},$$

donde

$$C_j = \{(a_i + (q^2-1)d_{ij}) \text{ mód } p(q^2-1) : 0 \leq i \leq q-1\}.$$

Supongamos por contradicción que existen $C_j \in \mathcal{C}$ y un múltiplo no nulo de $q+1$ en $\mathbb{Z}_{p(q^2-1)}$, digamos $m(q+1)$ con $m \not\equiv 0$ mód $p(q^2-1)$ tal que $m(q+1) \in \Delta(C_j)$. Entonces existen índices $0 \leq i \neq j \leq q-1$ tales que

$$(a_i + (q^2-1)d_{ij}) - (a_{il} + (q^2-1)d_{lj}) \equiv m(q+1) \text{ mód } p(q^2-1).$$

Entonces

$$a_i - a_l \equiv 0 \text{ mód } q+1.$$

Lo cual contradice el Teorema 3.9.

El código ortogonal óptico obtenido en el Teorema 3.10 no es óptimo si q no es igual a un número primo, sin embargo en algunos casos es posible optimizarlo agregando un número de palabras código adecuadas. El número de palabras código a agregar se calcula de la siguiente manera

$$\begin{aligned}\Phi(p(q^2-1), q, 1) - |\mathcal{C}| &= \left\lfloor \frac{p(q^2-1)-1}{q(q-1)} \right\rfloor - p \\ &= \left\lfloor p + \frac{p}{q} - \frac{1}{q(q-1)} \right\rfloor - p \\ &= \left\lfloor \frac{p}{q} - \frac{1}{q(q-1)} \right\rfloor.\end{aligned}$$

Teorema 3.12. *Sean q una potencia prima no igual a un número primo y $\mathcal{C}$ el código ortogonal óptico con parámetros $(p(q^2-1), q, 1)$ del Teorema 3.10. Si existe un código ortogonal óptico óptimo $\mathcal{C}'$ con parámetros $(p(q-1), q, 1)$, entonces existe un código ortogonal óptico óptimo con parámetros $(p(q^2-1), q, 1)$.*

Demostración. Basta agregar al código $\mathcal{C}$ todas las palabras código de la forma $(q+1)\mathbf{c} = \{(q+1)c \text{ mód } p(q^2-1) : c \in \mathbf{c}\}$, donde $\mathbf{c} \in \mathcal{C}'$.

Ejemplo 3.7. Tomemos $q = 9$. Por el Teorema 3.9 se puede construir el siguiente conjunto de Sidon

$$B = \{1, 6, 13, 14, 28, 49, 52, 75, 77\}$$

módulo 80. Como el menor número primo mayor a igual a 9 es 11 tomamos $p = 11$ y construimos la matriz $D = (d_{i,j})$ de tamaño 9×11 sobre $\mathbb{Z}_{11}$ 2−simple, donde $d_{i,j} = ij$ para $0 \leq i, j \leq 10$ es

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

Luego

$$\begin{aligned} \mathcal{C} = \{&\{1, 6, 13, 14, 28, 49, 52, 75, 77\}, \{1, 86, 173, 254, 348, 449, 532, 635, 717\}, \\ &\{1, 132, 166, 315, 333, 477, 494, 668, 849\}, \{1, 108, 237, 246, 369, 493, 612, 734, 875\}, \\ &\{1, 94, 212, 326, 428, 555, 653, 769, 877\}, \{1, 235, 289, 334, 406, 637, 692, 748, 813\}, \\ &\{1, 93, 188, 292, 397, 486, 574, 689, 795\}, \{1, 157, 209, 253, 475, 508, 566, 772, 814\}, \\ &\{1, 155, 174, 372, 413, 609, 646, 797, 828\}, \{1, 129, 268, 414, 557, 573, 715, 726, 852\}, \\ &\{1, 317, 395, 452, 529, 588, 654, 733, 806\}\} \end{aligned}$$

es un código ortogonal óptico con parámetros $(880, 9, 1)$. La correspondiente cota de Johnson es $\Phi(880, 9, 1) = 12$. Si se agrega la palabra código

$$\mathbf{c} = 10\{0, 2, 5, 13, 17, 31, 37, 38, 47\} = \{0, 20, 50, 130, 170, 310, 370, 380, 470\}$$

a $\mathcal{C}$ se obtiene un código ortogonal óptico óptimo.

El caso en el que se aplica el Corolario 3.5 al conjunto de Sidon tipo Singer fue investigado en [8]. Recordamos la construcción de Singer de conjunto de Sidon [30] y los principales resultados obtenidos para esta construcción en [8].

Teorema 3.13. *Para toda potencia prima q, existe un conjunto de Sidon módulo q^2+q+1 con $q+1$ elementos.*

Teorema 3.14. *Para toda potencia prima q, existe un código ortogonal óptico asintóticamente óptimo con parámetros $(m(q^2+q+1), q+1, 1)$ donde m es un entero positivo cuyos divisores primos son mayores a q.*

Los siguientes resultados muestran bajo qué condiciones es óptimo el código obtenido por el teorema anterior.

Corolario 3.7. *Sean q potencia prima, m un entero positivo tal que sus divisores primos son mayores a q y $q < m < q^2+q+1$. Entonces*

$$\Phi(m(q^2+q+1), q+1, 1) = m.$$

Corolario 3.8. *Sean q potencia prima. Si todos los divisores primos de q^2+q+1 son mayores a q, entonces para todo entero positivo t existe un código ortogonal óptico óptimo con parámetros $((q^2+q+1)^t, q+1, 1)$.*

Por último, aplicamos el Corolario 3.5 a la construcción de conjunto de Sidon tipo Ruzsa. Recordemos la construcción.

Teorema 3.15. *Sean p un número primo impar y α una raíz primitiva módulo p. El conjunto*

$$R = \{(ip - \alpha^i(p-1)) \text{ mód } p(p-1) : i = 0, \ldots, p-2\}$$

es un conjunto de Sidon módulo $p(p-1)$ con $p-1$ elementos y deficiencia $L = M_p \cup M_{p-1}$, donde M_p y M_{p-1} son los múltiplos no nulos de p y $p-1$ en $\mathbb{Z}_{p(p-1)}$, respectivamente.

Aplicando el Corolario 3.5 a la construcción de Ruzsa tenemos el siguiente resultado.

Corolario 3.9. *Sea p un número primo impar. Existe un código ortogonal óptico $\mathcal{C}$ con parámetros $(p^2(p-1), p-1, 1)$ y p elementos.*

Veamos qué tan óptimo es el código obtenido en el Corolario 3.9. Para tal propósito

comparemos su tamaño con la correspondiente cota de Johnson.

$$\begin{aligned}\Phi(p^2(p-1),p-1,1)-|\mathcal{C}| &= \left\lfloor \frac{p^2(p-1)-1}{(p-1)(p-2)} \right\rfloor - p \\ &= \left\lfloor \frac{p^2}{p-2} - \frac{1}{(p-1)(p-2)} \right\rfloor - p \\ &= \left\lfloor p+2+\frac{4p-5}{(p-1)(p-2)} \right\rfloor - p \\ &= \begin{cases} 5 & \text{si} \quad p=3, \\ 3 & \text{si} \quad p=5, \\ 2 & \text{si} \quad p\geq 7. \end{cases}\end{aligned}$$

Si $p=3$ el peso del código es igual a 2 y este caso siempre se puede optimizar [35]. Si $p=5$ obtenemos el siguiente código

$$\mathcal{C}=\{\{3,14,16,17\},\{3,34,56,77\},\{3,37,54,96\},\{3,36,74,97\},\{3,57,76,94\}\}$$

con parámetros $(100,4,1)$. Un cálculo muestra que la deficiencia de $\mathcal{C}$ es $L=M_4\cup M_5$, donde M_4 y M_5 denotan los múltiplos no nulos de 4 y 5 en $\mathbb{Z}_{100}$, respectivamente. Si se agrega las palabras código $\mathbf{c}_1=\{0,4,12,28\}$ y $\mathbf{c}_2=\{0,5,15,35\}$ a $\mathcal{C}$ obtenemos un código ortogonal óptico con 7 elementos. En este caso no es posible agregar una elemento más, ya que por el Teorema 2.6 no existe un código ortogonal óptico óptimo con parámetros $(25,4,1)$.
Si $p\geq 7$ hacen falta agregar dos palabras código para optimizar el código. Para describir la forma de dichas palabras código caracterizamos la deficiencia de $\mathcal{C}$.

Teorema 3.16. *Sean p un número primo impar y $\mathcal{C}$ el código ortogonal óptico con parámetros $(p^2(p-1),p-1,1)$ obtenido por el Corolario 3.9. La deficiencia de $\mathcal{C}$ es $L=M_p\cup M_{p-1}$, donde M_p y M_{p-1} denotan los múltiplos no nulos de p y $p-1$ en $\mathbb{Z}_{p^2(p-1)}$.*

Demostración. Sean $R=\{(ip-\alpha^i(p-1) \text{ mód } p(p-1) : i=0,\ldots,p-2\}$ el conjunto de Sidon obtenido por el Teorema 3.15 y $D=(d_{i,j})$ la matriz de tamaño $(p-1)\times p$ sobre $\mathbb{Z}_p$ 2−simple usada para construir el código ortogonal óptico $\mathcal{C}$ del Corolario 3.9. Entonces

$$\mathcal{C}=\{\{ip-\alpha^i(p-1)+p(p-1)d_{i,j} : i=0,\ldots,p-2\} : j=0,\ldots,p-1\}.$$

Supongamos por contradicción que existen $\mathbf{c}_i\in\mathcal{C}$ y un múltiplo de p, digamos mp tal que $mp\in\Delta(\mathbf{c}_i)$. Entonces, existen índices $0\leq i\neq l\leq p-2$ tales que

$$(ip-\alpha^i(p-1)+p(p-1)d_{i,j})-(lp-\alpha^l(p-1)+p(p-1)d_{l,j})\equiv p \text{ mód } p^2(p-1).$$

Por tanto,

$$(ip - \alpha^i(p-1)) - (lp - \alpha^l(p-1)) \equiv p \text{ mód } p(p-1),$$

lo cual contradice el Teorema 3.15. El caso $p-1$ se demuestra similarmente.

Tenemos el siguiente resultado.

Corolario 3.10. *Sea $p \geq 7$ un número primo. Suponga que existe un conjunto de Sidon módulo p^2 con $p-1$ elementos, entonces existe un código ortogonal óptico óptimo con parámetros $(p^2(p-1), p-1, 1)$.*

Demostración. Sea $\mathcal{C}$ el código ortogonal óptico con parámetros $(p^2(p-1), p-1, 1)$ obtenido por el Corolario 3.9. Como $p \geq 7$, entonces basta agregar dos palabras código adecuadas a $\mathcal{C}$ para garantizar su optimización. Por hipótesis, existe un conjunto de Sidon $S = \{a_1, \ldots, a_{q-1}\}$ módulo p^2. Si agregamos a $\mathcal{C}$ las siguientes palabras código

$$\mathbf{c}_1 = (p-1)S = \{(p-1)a_i \text{ mód } p^2(p-1) : i = 1, \ldots, p-1\}$$

y $\mathbf{c}_2 = pR = \{pa_i \text{ mód } p^2(p-1) : a_i \in R\}$, donde R es el conjunto de Sidon tipo Ruzsa del Teorema 3.15, obtenemos el resultado deseado.

La aplicación del resultado anterior requiere la existencia de un conjunto de Sidon módulo p^2 con $p-1$ elementos para $p \geq 7$. Desafortunamente, para este módulo no existe una construcción explícita de dicho conjunto y la búsqueda computacional se complica conforme p aumenta. Buratti y Stinson en [4] encontraron computacionalmente el siguiente conjunto de Sidon módulo 49 con 6 elementos

$$S = \{0, 2, 3, 10, 16, 21, 25\}$$

el cual nos sirve para optimizar el código para $p = 7$. Para $p = 11$ encontramos computacionalmente el conjunto de Sidon

$$S = \{0, 1, 3, 7, 12, 20, 30, 46, 86, 100\}$$

módulo 121 con 10 elementos, para $p = 13$ encontramos el siguiente conjunto de Sidon

$$S = \{0, 1, 3, 7, 12, 59, 76, 89, 109, 130, 144, 154\}$$

módulo 169 con 12 elementos, pero para los siguientes números primos $p \geq 17$ ya no fue posible encontrar dichos conjuntos, razón por la cual consideramos un problema para futuras investigaciones.

Capítulo 4

Códigos ortogonales ópticos en dos dimensiones

En el presente capítulo mostramos algunas nuevas construcciones de códigos ortogonales ópticos en dos dimensiones que se pueden obtener por medio de conjuntos de Sidon y por medio de construcciones recursivas. Gran parte de los resultados obtenidos son propios y hemos incluido algunos que no lo son pero que están relacionados con el objetivo del capítulo.

4.1. Códigos ortogonales ópticos en dos dimensiones a partir de conjuntos de Sidon

Un código ortogonal en dos dimensiones es una familia de matrices binarias de tamaño $m \times n$ con buenas propiedades (en el sentido de las condiciones de correlación dadas en la Introducción 1) de autocorrelación y correlación cruzada. Su estudio ha sido motivado en las últimas décadas debido a sus variadas aplicaciones en sistemas de acceso múltiple por división de código (OCDMA) [9]. Como en el caso de una dimensión, en un OCDMA a diferentes usuarios se les asigna diferentes códigos durante la transmisión para ser identificados. Cuando $m = 1$ tenemos los códigos ortogonales ópticos en una dimensión estudiados en los capítulos anteriores. Éstos últimos han sido ampliamente estudiados en [9, 3, 8, 22, 35, 36]. La principal desventaja que presentan los códigos ortogonales ópticos en una dimensión es el número limitado de usuarios que pueden albergar debido a que el

tamaño del código es directamente proporcional a la longitud de las secuencias, mientras que la tasa de datos de información de un solo usuario es inversamente proporcional a la longitud de las secuencias. Esta dificultad se puede superar de manera eficiente por medio de los códigos ortogonales ópticos en dos dimensiones, debido a que estos últimos trabajan en los dominios del tiempo y la longitud de onda, lo que hace que la tasa de datos requerida pueda ser reducida considerablemente. En la Figura 4.1 se ilustra cómo se realiza la transmisión de una palabra código en el dominio del tiempo t para un código en una dimensión y en los dominios del tiempo t y la longitud de onda λ para un código en dos dimensiones. El primer código es óptimo, mientras que el segundo código permite agregar 4 palabras código adicionales obtenidas por las traslaciones verticales de la palabra código mostrada en b) de la Figura 4.1.

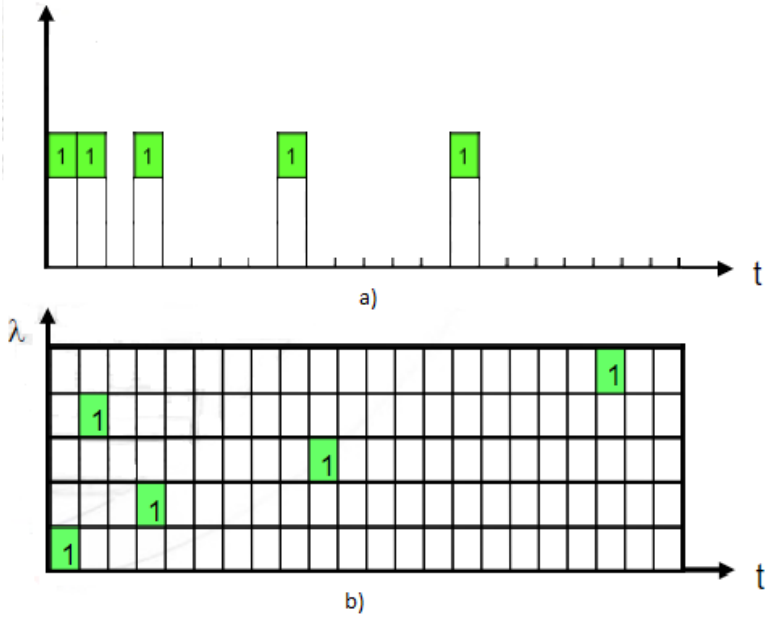


Figura 4.1: a) Código ortogonal óptico en una dimensión con parámetros $(22, 5, 1)$. b) Código ortogonal óptico en dos dimensiones con parámetros $(5 \times 22, 5, 1)$.

En este capítulo construimos códigos ortogonales ópticos a partir de conjuntos de Sidon. Algunas construcciones alcanzan el valor de la cota de Johnson correspondiente. Empezamos definiendo lo siguiente.

Definición 4.1. [34] Un código ortogonal óptico $\mathcal{C}$ en dos dimensiones con parámetros $(m \times n, k, \lambda)$ es un conjunto de matrices binarias de tamaño $m \times n$, cada una de ellas con peso de Hamming igual a k y que satisfacen las siguientes propiedades:

1. (Autocorrelación). Para cada matriz

$$X = \begin{pmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,n-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,n-1} \\ \vdots & & & \\ x_{m-1,0} & x_{m-1,1} & \cdots & x_{m-1,n-1} \end{pmatrix}$$

en $\mathcal{C}$, tenemos

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j} x_{i.j+t} \leq \lambda, \tag{4.1}$$

para cualquier $t \not\equiv 0 \mod n$.

2. (Correlación cruzada). Para cualquier par de matrices distintas

$$X = \begin{pmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,n-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,n-1} \\ \vdots & & & \\ x_{m-1,0} & x_{m-1,1} & \cdots & x_{m-1,n-1} \end{pmatrix} \text{ y}$$

$$Y = \begin{pmatrix} y_{0,0} & y_{0,1} & \cdots & y_{0,n-1} \\ y_{1,0} & y_{1,1} & \cdots & y_{1,n-1} \\ \vdots & & & \\ y_{m-1,0} & y_{m-1,1} & \cdots & y_{m-1,n-1} \end{pmatrix}$$

en $\mathcal{C}$, tenemos

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j} y_{i,j+t} \leq \lambda, \tag{4.2}$$

para cualquier entero t.

En ambos casos, la suma $j + t$ es reducida módulo n.

Cuando $m = 1$, la definición anterior coincide con la definición de código ortogonal óptico en una dimensión.

Tenemos en cuenta ahora algunos hechos importantes sobre la función de representación y conjuntos, con el propósito de presentar de manera alternativa la definición de código ortogonal óptico en dos dimensiones.

Sean $(G,+)$ un grupo conmutativo finito y $A, B \in G$. La función de representación de A y B en $x \in G$ se define como

$$R_{A-B}(x) := \mid (A+x) \cap B \mid, \tag{4.3}$$

donde $A + x := \{a + x : a \in A\}$.
La función de representación cuenta el número de veces en las que x puede ser representado como diferencia de un elemento de A y un elemento de B.

De manera análoga al caso de códigos ortogonales en una dimensión, asociamos un conjunto de pares ordenados a las matrices que forman un código ortogonal óptico como se muestra a continuación.

Sea $\mathcal{C}$ un código ortogonal óptico en dos dimensiones con parámetros $(m \times n, k, 1)$. Para cada $X = (x_{i,j}) \in \mathcal{C}$ asociamos el siguiente conjunto

$$A = \{(i,j) \in \mathbb{Z}_m \times \mathbb{Z}_n : x_{i,j} = 1\}.$$

Usando la función de representación y la notación conjuntista para los elementos de un código ortogonal óptico en dos dimensiones, podemos enunciar las propiedades de correlación de la siguiente manera.

1. Autocorrelación: para cada $A \in \mathcal{C}$ y todo entero t tal que $t \not\equiv 0 \mod n$ se cumple

$$R_{A-A}(0,t) \leq 1. \tag{4.4}$$

2. Correlación cruzada: para cada $A, B \in \mathcal{C}$ con $A \neq B$ y cualquier entero t se cumple

$$R_{A-B}(0,t) \leq 1. \tag{4.5}$$

En la práctica, se requieren códigos ortogonales ópticos con un gran número de palabras. Para un conjunto de valores dados de m, n, k y λ, el mayor tamaño posible de un código ortogonal en dos dimensiones con parámetros $(m \times n, k, \lambda)$ se denota por $\Phi(m \times n, k, \lambda)$. Un código que alcanza este valor se denomina *óptimo*. La correspondiente cota superior de Johnson para este caso toma la forma

$$\Phi(m \times n, k, \lambda) \leq \left\lfloor \frac{m}{k} \left\lfloor \frac{mn-1}{k-1} \left\lfloor \ldots \left\lfloor \frac{mn-\lambda}{k-\lambda} \right\rfloor \right\rfloor \right\rfloor \right\rfloor.$$

En lo que sigue, trabajamos con $\lambda = 1$. En este caso la cota de Johnson toma la forma enunciada a continuación.

Teorema 4.1. *(Cota de Johnson) [34]*

$$\Phi(m \times n, k, 1) = \left\lfloor m \left\lfloor \frac{mn-1}{k(k-1)} \right\rfloor \right\rfloor. \tag{4.6}$$

Recordamos ahora la definición de conjuntos de Sidon sobre grupos finitos.

Definición 4.2. [12] Sea $(G, +)$ un grupo conmutativo finito con identidad e y A un subconjunto no vacío de G. Se dice que A es un conjunto de Sidon en G, si para cualquier $x \not\equiv e \mod G$, tenemos

$$R_{A-A}(x) \leq 1. \tag{4.7}$$

Observación 4.1. Sea $(G, +, \cdot)$ un anillo conmutativo con unidad. Si A es un conjunto de Sidon en G, entonces

$$uA + b := \{u \cdot a + b : a \in A\}$$

es un conjunto de Sidon para toda unidad $u \in G$ y todo elemento $b \in G$.

Además de las construcciones de conjuntos de Sidon en una dimensión dadas en los Teoremas 3.9, 2.20 y 3.15, recordamos también las construcciones en dos dimensiones en los grupos $\mathbb{Z}_p \times \mathbb{Z}_p$, $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$ y $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$, donde p es un número primo y q es una potencia prima, las cuales fueron estudiadas en los Teoremas 2.23, 2.24 y 2.25. Uno de los conceptos más importantes a tener en cuenta en las construcciones del presente capítulo es el de cuadrados latinos mutuamente ortogonales. Recordemos las definiciones 3.2 y 3.3, así como algunos resultados sobre cuadrados latinos, los cuales pueden ser consultados en más detalle en [13].

Definición 4.3. [13] Sean n un entero positivo y A un conjunto finito con n elementos. Un cuadrado latino de orden n es una matriz de tamaño $n \times n$ con la propiedad de que cada elemento de A aparece exactamente una vez en cada fila y en cada columna. Al valor de n se le llama el orden del cuadrado latino y A su conjunto base.

Definición 4.4. [13] Sean $A = (a_{i,j})$ y $B = (b_{i,j})$ matrices de tamaño $n \times n$. La unión de A y B denotada por (A, B) es la matriz de tamaño $n \times n$ cuya componente ij es igual a $(a_{i,j}, b_{i,j})$. Dos cuadrados latinos A y B de orden n son ortogonales si en (A, B) aparecen cada uno de los posibles n^2 pares ordenados exactamente una vez.

Definición 4.5. [13] Un conjunto de cuadrados latinos $M_1, \ldots, M_r$ del mismo orden se llama conjunto de cuadrados latinos mutuamente ortogonales (siglas en inglés, MOLS), si cada par de matrices diferentes del conjunto son ortogonales.

Teorema 4.2. *[13] Para cualquier potencia prima q, existe un conjunto de cuadrados latinos mutuamente ortogonales de orden q con $q - 1$ elementos.*

Presentamos a continuación, la primera construcción de código ortogonal óptico a partir de un conjunto de Sidon, obtenida por nuestra parte.

Teorema 4.3. *Sean p un número primo impar y $C_i = \{(x, x^2) + (i, 0) : x \in \mathbb{Z}_p\}$ para $i = 1, \dots p$. Entonces*

$$\mathcal{C} = \{C_j : j = 0, \dots, p-1\} \tag{4.8}$$

es un código ortogonal óptico óptimo en dos dimensiones con parámetros $(p \times p, p, 1)$.

Demostración. Por el Teorema 2.23 tenemos que C_0 satisface la autocorrelación. Por la Observación 4.1, tenemos también que $C_1, C_2, \dots, C_{p-1}$ satisfacen la propiedad de autocorrelación.
Para probar la correlación cruzada, sean $C_i, C_j \in \mathcal{C}$ con $i < j$. Entonces

$$\begin{aligned} R_{C_i - C_j}(0,t) =& \left|(C_i + (0,t)) \cap C_j\right|, \\ =& \left|(C_0 + (i,t)) \cap (C_0 + (j,0)\right|, \\ =& \left|(C_0 + (j-i, -t)) \cap C_0\right|, \\ =& R_{C_0 - C_0}(j-i, t), \\ \leq& 1, \end{aligned} \tag{4.9}$$

para todo entero $t \not\equiv 0$ mód p.

Además,

$$\Phi(p \times p, p, 1) = \left\lfloor p \left\lfloor \frac{pp-1}{p(p-1)} \right\rfloor \right\rfloor = p = |\mathcal{C}|.$$

Por tanto, $\mathcal{C}$ es óptimo.

De manera similar, usando el Teorema 2.25 y la Observación 4.1 tenemos el siguiente resultado.

Teorema 4.4. *Sean q una potencia prima, θ un elemento primitivo de $\mathbb{F}_q$, $a \in \mathbb{F}_q^*$ y*

$$C_i = \{(\log_\theta(\theta^k - a), a) + (i, 0) : k \in \mathbb{Z}_{q-1}, k \neq \log_\theta a\}.$$

Entonces $\mathcal{C} = \{C_i : i = 0, \dots, q-3\}$ es un código ortogonal óptico en dos dimensiones, con parámetros $((q-1) \times (q-1), q-2, 1)$ y $q-2$ palabras código.

La siguiente construcción se basa en el Teorema 2.24 con una ligera generalización que consiste en tomar a q como el cuadrado de un número primo impar.

Sean p un número primo impar, $q = p^2$ y $h \geq 2$ un entero positivo. Sea α un elemento primitivo de $\mathbb{F}_{q^h}$ y

$$\begin{aligned} \mathcal{P} =& \{g(x) \in \mathbb{F}_q[x] : 1 \leq \text{grad}(g(x)) \leq h-1 \text{ y } g(0) = 0\}, \\ \mathcal{Q} =& \{g(x) \in \mathcal{P} : g \text{ es mónico}\}. \end{aligned} \tag{4.10}$$

Sean

$$\begin{aligned} C_1 =& \{\{(a, \log_\alpha(g(\alpha) + a)) : a \in \mathbb{F}_q\} : g(x) \in \mathcal{P}\}, \\ C_2 =& \{\{(0, \log_\alpha(g(\alpha) + a)) : a \in \mathbb{F}_q\} : g(x) \in \mathcal{Q}\}. \end{aligned} \tag{4.11}$$

subconjuntos de $\mathbb{F}_q \times \mathbb{Z}_{q^h-1}$.

Si $C = C_1 \cup C_2$, afirmamos que

$$\begin{aligned} R_{A-A}(x, y) \leq& 1 \text{ para todo } A \in C \text{ y } (x, y) \neq (0, 0) \text{ y} \\ R_{A-B}(x, y) \leq& 1 \text{ para todo } A, B \in C, A \neq B \text{ y para todo} \\ & (x, y) \in \mathbb{F}_q \times \mathbb{Z}_{q^h-1} \end{aligned} \tag{4.12}$$

Para la primera desigualdad, sea $A \in C$.

- Si $A \in C_1$, supongamos que existe $(x, y) \neq (0, 0)$ tal que

$$\begin{aligned} (x, y) =& (a_1, \log_\alpha(g(\alpha) + a_1)) - (a_2, \log_\alpha(g(\alpha) + a_2)), \\ =& (a_3, \log_\alpha(g(\alpha) + a_3)) - (a_3, \log_\alpha(g(\alpha) + a_3)), \end{aligned} \tag{4.13}$$

  para algún $g(x) \in \mathcal{P}$ y algunos $a_1, a_2, a_3, a_4 \in \mathbb{F}_q$ con $(a_1, a_2) \neq (a_3, a_4)$. Entonces

$$\begin{aligned} a_1 - a_2 =& a_3 - a_4 \text{ y} \\ (g(\alpha) + a_1)(g(\alpha) + a_4) =& (g(\alpha) + a_2)(g(\alpha) + a_3)). \end{aligned} \tag{4.14}$$

  Por tanto

$$\begin{aligned} a_1 - a_2 =& a_3 - a_4 \text{ y} \\ a_1 a_4 =& a_2 a_3. \end{aligned} \tag{4.15}$$

  Entonces a_1, a_2, a_3, a_4 son raíces de $x^2 - (a_1 + a_4)x + a_1 a_4 = 0$ sobre $\mathbb{F}_q$ y por tanto $\{a_1, a_4\} = \{a_2, a_3\}$ lo cual es una contradicción en cualquier caso.

- Si $A \in C_2$, supongamos que existe $y \neq 0$ tal que

$$\begin{aligned} (0, y) =& (0, \log_\alpha(g(\alpha) + a_1)) - (0, \log_\alpha(g(\alpha) + a_2)) \\ =& (0, \log_\alpha(g(\alpha) + a_3)) - (0, \log_\alpha(g(\alpha) + a_3)), \end{aligned} \tag{4.16}$$

para algún $g(x) \in \mathcal{Q}$ y algunos $a_1, a_2, a_3, a_4 \in \mathbb{F}_q$ con $(a_1, a_2) \neq (a_3, a_4)$. Entonces

$$(g(\alpha) + a_1)(g(\alpha) + a_4) = (g(\alpha) + a_2)(g(\alpha) + a_3)).$$

Por tanto,

$$g(\alpha)(a_1 + a_4 - a_2 - a_3) + a_1a_4 - a_2a_3 = 0.$$

Como $\text{grad}(\alpha, \mathbb{F}_q) = h$ y $\text{grad}(g(x)) \leq h - 1$, entonces $a_1 + a_4 = a_2 + a_3$ y así, como antes, tenemos que $\{a_1, a_4\} = \{a_2, a_3\}$ lo cual es una contradicción.

Probemos ahora la segunda desigualdad. Sean $A, B \in C$ con $A \neq B$ y supongamos que existe (x, y) tal que

$$\begin{aligned}(x, y) =&(a_1, \log_\alpha(g(\alpha) + b_1)) - (c_1, \log_\alpha(f(\alpha) + d_1)) \\ =&(a_2, \log_\alpha(g(\alpha) + b_2)) - (c_2, \log_\alpha(f(\alpha) + d_2)),\end{aligned} \tag{4.17}$$

para algunos $g(x), f(x) \in \mathcal{P}$ con $g(x) \neq f(x)$ y algunos $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2 \in \mathbb{F}_q$ con $(a_1, b_1, c_1, d_1) \neq (a_2, b_2, c_2, d_2)$. Entonces

$$\begin{aligned}a_1 - c_1 =&a_2 - c_2, \\ (g(\alpha) + b_1)(f(\alpha) + d_2) =&(g(\alpha) + b_2)(f(\alpha) + d_1).\end{aligned} \tag{4.18}$$

Sea $r(x) = (g(x) + b_1)(f(x) + d_2) - (g(x) + b_2)(f(x) + d_1)$, entonces $r(x) \in \mathbb{F}_q[x]$, $\text{grad}(r(x)) \leq h - 1$ y $r(\alpha) = 0$, por tanto $r(x) = 0$. Tenemos los siguientes casos.

- Si $\text{grad}(g(x)) > \text{grad}(f(x))$, entonces $d_1 = d_2$ y así $b_1 = b_2$. Si $A, B \in C_1$, entonces por lo anterior $a_1 = a_2$ y $c_1 = c_2$, lo cual es una contradicción. Si $A, B \in C_2$, entonces $a_1 = a_2 = c_1 = c_2 = 0$ y así $(a_1, b_1, c_1, d_1) = (a_1, b_1, c_1, d_1)$, lo cual es una contradicción. Si $A \in C_1$ y $B \in C_2$, entonces $a_1 = b_1 = b_2 = a_2$ and $c_1 = c_2 = 0$, nuevamente una contradicción.
- El caso $\text{grad}(g(x)) < \text{grad}(f(x))$ se obtiene de manera similar.
- Si $\text{grad}(g(x)) = \text{grad}(f(x))$, entonces

$$\begin{aligned}d_2 - d_1 =&u(b_2 - b_1), \\ b_1d_2 =&b_2d_1,\end{aligned} \tag{4.19}$$

para alguna unidad $u \in \mathbb{F}_q$.
Si $A, B \in C_1$, entonces $a_1 = b_1$, $c_1 = d_1$, $a_2 = b_2$ y $c_2 = d_2$, entonces por (4.18) y por (4.19) tenemos $u = 1$, así $g(\alpha) = f(\alpha)$. Como $\text{grad}(g(x)) = \text{grad}(f(x))$, entonces $1 \leq \text{grad}(g(x) - f(x)) \leq h - 1$. Como $\text{grad}(\alpha, \mathbb{F}_q) = h$ y $g(\alpha) - f(\alpha) = 0$, entonces

$g(x) = f(x)$, lo cual es una contradicción.
Si $A, B \in C_2$, entonces $a_1 = c_1 = a_2 = c_2 = 0$ y así $g(x), f(x) \in \mathcal{Q}$. Luego $u = 1$ y como antes llegamos a una contradicción.
Si $A \in C_1$ y $B \in C_2$, entonces $a_1 = b_1$, $a_2 = b_2$ y $c_1 = c_2 = 0$, por tanto $a_1 = a_2 = b_1 = b_2$. Por (4.19) tenemos $d_1 = d_2$ lo cual es una contradicción.

Por el teorema de los grupos abelianos finitamente generados, tenemos que existe un isomorfismo de grupos φ tal que $\mathbb{F}_q \times \mathbb{Z}_{q^h-1} \simeq \mathbb{Z}_p \times \mathbb{Z}_{p(q^h-1)}$. Usando este hecho, podemos obtener un código ortogonal óptico $\varphi(C)$ en dos dimensiones con parámetros $(p \times p(q^h - 1), p^2, 1)$. Para cada $A \in \varphi(C)$ sea

$$A_i = A + (i, 0) \text{ para } i = 0, 1, \ldots, p-1,$$

entonces es fácil probar que $A_i \neq A_j$ para todo $i \neq j$ y $A_i \neq B_j$ para todo $A, B \in \varphi(C)$ con $A \neq B$ y para todo i, j. Sea

$$\mathcal{C}' = \bigcup_{A \in \varphi(C)} \bigcup_{i=0}^{p-1} \{A_i\}.$$

Entonces

$$\begin{aligned} |\mathcal{C}'| =& |\mathcal{P}|\, p + |\mathcal{Q}|\, p \\ =& p(|\mathcal{P}| + |\mathcal{Q}|) \\ =& p\left(q^{h-1} - 1 + \frac{q^{h-1} - 1}{q - 1}\right) \\ =& pq\left(\frac{q^{h-1} - 1}{q - 1}\right). \end{aligned}$$

Hemos probado el siguiente teorema.

Teorema 4.5. *Para cualquier número primo p y cualquier entero h mayor que 1, existe un código ortogonal óptico óptimo en dos dimensiones con parámetros $(p \times p(p^{2h} - 1), p^2, 1)$.*

Demostración. Basta probar que el código descrito anteriormente es óptimo.

$$\begin{aligned}\Phi(p \times p(q^h-1), p^2, 1) &= \left\lfloor p \left\lfloor \frac{p^2(p^{2h}-1)-1}{p^2(p^2-1)} \right\rfloor \right\rfloor \\ &= \left\lfloor p \left\lfloor \frac{q(q^h-1)-1}{q(q-1)} \right\rfloor \right\rfloor \\ &= \left\lfloor p \left\lfloor \frac{q^h-1}{q-1} - \frac{1}{q(q-1)} \right\rfloor \right\rfloor \\ &= \left\lfloor p \left(\frac{q^h-1}{q-1} - 1 \right) \right\rfloor \\ &= |\mathcal{C}'| \,.\end{aligned}$$

Veamos ahora la manera de construir códigos ortogonales ópticos en dos dimensiones a partir de códigos ortogonales ópticos en una dimensión.

Sean n_1, n_2 enteros positivos y w un número primo. Suponga que existen dos códigos ortogonales ópticos $\mathcal{C}_1$ y $\mathcal{C}_2$ con parámetros $(n_1, w, 1)$ y $(n_2, w, 1)$, respectivamente. Podemos escribir

$$\begin{aligned}\mathcal{C}_1 =& \{\{x_{i,1}, x_{i,2}, \ldots, x_{i,w}\} : i = 1, \ldots, |\mathcal{C}_1|\}, \\ \mathcal{C}_2 =& \{\{y_{j,1}, y_{j,2}, \ldots, y_{j,w}\} : j = 1, \ldots, |\mathcal{C}_2|\}.\end{aligned} \tag{4.20}$$

Para cada $B \in \mathcal{C}_2$, construyamos un conjunto de cuadrados mutuamente ortogonales $M_B = \{M_{B,k} = (m_{i,j}^{B,k}) : k = 1, \ldots, w-1\}$ de orden w y conjunto base igual a B.

Consideremos ahora los siguientes subconjuntos de $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ descritos a continuación.

$$\begin{aligned}\mathcal{D}_1 =& \{\{(x_{i,1}, 0), \ldots, (x_{i,w}, 0)\} : i = 1, \ldots, |\mathcal{C}_1|\}, \\ \mathcal{D}_2 =& \{\{(0, y_{i,1}), \ldots, (0, y_{i,w})\} : i = 1, \ldots, |\mathcal{C}_2|\}, \\ \mathcal{D}_3 =& \{\{(x_{i,1}, m_{l,1}^{B,k}), \ldots, (x_{i,w}, m_{l,w}^{B,k})\} : i = 1, \ldots, |\mathcal{C}_1|\,, \\ & \quad l = 1, \ldots, w, k = 1, \ldots, w-1, B \in \mathcal{C}_2\}.\end{aligned} \tag{4.21}$$

Sean $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3 \subset \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, entonces $|\mathcal{D}| = |\mathcal{C}_1| + |\mathcal{C}_2| + w(w-1)|\mathcal{C}_1||\mathcal{C}_2|$. Probamos a continuación que $\mathcal{D}$ es un código ortogonal óptico en dos dimensiones con parámetros $(n_1 \times n_2, w, 1)$.

Teorema 4.6. *$\mathcal{D}$ es un código ortogonal óptico en dos dimensiones con parámetros $(n_1 \times n_2, w, 1)$ y $|\mathcal{C}_1| + |\mathcal{C}_2| + w(w-1)|\mathcal{C}_1||\mathcal{C}_2|$ elementos.*

Demostración. Primero probemos la propiedad de la autocorrelación. Sea $X \in \mathcal{D}$, si $X \in \mathcal{D}_1 \cup \mathcal{D}_2$, entonces la afirmación se cumple de manera trivial. Supongamos por tanto que $X \in \mathcal{D}_3$, entonces $A = \{(x_{i,1}, m_{l,i}^{B,k}), \ldots, (x_{i,w}, m_{l,w}^{B,k})\}$, para algunos i, l, k y B. Supongamos por contradicción que existe $(x, y) \neq (0, 0)$ tal que $R_{X-X}(x, y) \geq 2$, entonces

$$(x_{i_1,j_1}, m_{l_1,j_1}^{B,k}) - (x_{i_2,j_2}, m_{l_2,j_2}^{B,k}) = (x_{i_3,j_3}, m_{l_3,j_3}^{B,k}) - (x_{i_4,j_4}, m_{l_4,j_4}^{B,k}),$$

para algún $(i_1, i_3) \neq (i_2, i_4)$. Entonces

$$\begin{aligned} x_{i_1,j_1} - x_{i_2,j_2} &= x_{i_3,j_3} - x_{i_4,j_4} \text{ mód } n_1, \\ m_{l_1,j_1}^{B,k} - m_{l_2,j_2}^{B,k} &= m_{l_3,j_3}^{B,k} - m_{l_4,j_4}^{B,k} \text{ mód } n_2. \end{aligned} \tag{4.22}$$

Como $\{x_{i,1}, \ldots, x_{i,w}\} \in \mathcal{C}_1$ y $\{m_{l_1,j_1}^{B,k} \ldots, m_{l_w,j_w}^{B,k}\} \in \mathcal{C}_2$ y ambos son códigos ortogonales ópticos, entonces las anteriores ecuaciones implican que $(i_1, i_3) = (i_2, i_4)$ lo cual es una contradicción.
Ahora, probamos la propiedad de la correlación cruzada. Sean $X, Y \in \mathcal{D}$ con $X \neq Y$. Tenemos los siguientes casos

1. $X, Y \in \mathcal{D}_1$ o $X, Y \in \mathcal{D}_2$ o $X \in \mathcal{D}_2$ y $Y \in \mathcal{D}_3$.
2. $X \in \mathcal{D}_1$ y $Y \in \mathcal{D}_2$.
3. $X \in \mathcal{D}_1$ y $Y \in \mathcal{D}_3$.
4. $X, Y \in \mathcal{D}_3$.

El primer caso es trivial, puesto que el resultado deseado se obtiene por hipótesis de que $\mathcal{C}_1$ y $\mathcal{C}_2$ son códigos ortogonales ópticos.
Para el segundo caso, sean

$$X = \{(x_{i,1}, 0), \ldots, (x_{i,w}, 0)\} \text{ y } Y = \{(0, y_{j,1}), \ldots, (0, y_{j,w})\},$$

para algún $i = 1, \ldots, |\mathcal{C}_1|$ y algún $j = 1, \ldots, |\mathcal{C}_2|$. Note que si $R_{X-Y}(t_1, t_2) \geq 2$ para algún $(t_1, t_2) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, entonces

$$\begin{aligned} x_{i,l_1} - 0 &= x_{i,l_2} - 0 \text{ mód } n_1, \\ 0 - y_{j,k_1} &= 0 - y_{j,k_2} \text{ mód } n_2, \end{aligned} \tag{4.23}$$

lo cual implica que $l_1 = l_2$ y $k_1 = k_2$ ya que $\mathcal{C}_1$ y $\mathcal{C}_2$ son códigos ortogonales ópticos, respectivamente. Sin embargo, esto contradice la suposición de que $R_{X-Y}(t_1, t_2) \geq 2$.
Para el tercer caso, sean

$$X = \{(x_{i,1}, 0), \ldots, (x_{i,w}, 0)\} \text{ y } Y = \{(x_{j,1}, m_{l,1}^{B,k}), \ldots, (x_{j,w}, m_{l,w}^{B,k})\},$$

para algunos $i, j = 1, \ldots, |\mathcal{C}_1|$, algún $l = 1, \ldots, w$, algún $k = 1, \ldots, w-1$ y algún $B \in \mathcal{C}_2$. Note que si $R_{X-Y}(t_1, t_2) \geq 2$ para algún $(t_1, t_2) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, entonces

$$\begin{aligned} x_{i,k_1} - x_{j,s_1} &= x_{i,k_2} - x_{j,s_2} \text{ mód } n_1, \\ 0 - m_{l,s_1}^{B,k} &= 0 - m_{l,s_2}^{B,k} \text{ mód } n_2. \end{aligned} \tag{4.24}$$

La segunda ecuación implica que $s_1 = s_2$ ya que $\mathcal{C}_2$ es un código ortogonal óptico. Reescribiendo la primera ecuación y usando el hecho anterior se tiene

$$x_{i_1,k_1} - x_{i_3,k_2} = 0 \text{ mód } n_1. \tag{4.25}$$

La ecuación anterior implica que $k_1 = k_2$ dado que $\mathcal{C}_1$ es un código ortogonal óptico, lo cual contradice la suposición de que $R_{X-Y}(t_1, t_2) \geq 2$.
Para el cuarto caso, sean

$$X = \{(x_{i,1}, m_{l,1}^{A,k}), \ldots, (x_{i,w}, m_{l,w}^{A,k})\} \text{ y } Y = \{(x_{j,1}, m_{f,1}^{B,h}), \ldots, (x_{j,w}, m_{f,w}^{B,h})\}$$

para algunos $i, j = 1, \ldots, |\mathcal{C}_1|$, $l, f = 1, \ldots, w$, $k, h = 1, \ldots, w-1$ y algunos $A, B \in \mathcal{C}_2$.

Note que si $R_{X-Y}(t_1, t_2) \geq 2$, para algún $(t_1, t_2) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, entonces

$$\begin{aligned} x_{i,k_1} - x_{j,s_1} &= x_{i,k_2} - x_{j,s_2} \text{ mód } n_1, \\ m_{l,k_1}^{A,k} - m_{f,s_1}^{B,h} &= m_{l,k_2}^{A,k} - m_{f,s_2}^{B,h} \text{ mód } n_2. \end{aligned} \tag{4.26}$$

Reordenando tenemos

$$\begin{aligned} x_{i,k_1} - x_{i,k_2} &= x_{j,s_1} - x_{j,s_2} \text{ mód } n_1, \\ m_{l,k_1}^{A,k} - m_{l,k_2}^{A,k} &= m_{f,s_1}^{B,h} - m_{f,s_2}^{B,h} \text{ mód } n_2. \end{aligned} \tag{4.27}$$

Como $\mathcal{C}_1$ es un código ortogonal óptico, entonces de la primera ecuación tenemos

$$i = j, k_1 = s_1 \text{ y } k_2 = s_2.$$

Usando lo anterior, la segunda ecuación y el hecho de que $\mathcal{C}_2$ es un código ortogonal óptico tenemos que $A = B$. Ahora, por construcción del conjunto de cuadrados latinos mutuamente ortogonales tenemos que $l = f$ y $k = h$, lo cual contradice el hecho de que $R_{X-Y}(t_1, t_2) \geq 2$ para algún $(t_1, t_2) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$.

Usando los elementos del código obtenido en el Teorema 4.6 junto con sus traslaciones sobre la primera componente en cada elemento es fácil probar el siguiente resultado.

Corolario 4.1. *Sea $\mathcal{D}$ el código ortogonal óptico en dos dimensiones con parámetros $(n_1 \times n_2, w, 1)$, obtenido por el Teorema 4.6. Entonces existe un código ortogonal óptico óptimo en dos dimensiones con parámetros $(n_1 \times n_2, w, 1)$ y $n_1|\mathcal{D}|$ elementos.*

4.2. Construcción recursiva para códigos ortogonales ópticos en dos dimensiones

En la presente sección mostramos una construcción recursiva para códigos ortogonales ópticos en dos dimensiones generalizando la idea que presentaron Chu y Golomb en [8] para el caso de una dimensión.
Los aspectos más importantes en toda construcción recursiva son los siguientes.

- Los códigos obtenidos por la aplicación de la construcción recursiva deben conservar o disminuir el valor de la constante de correlación λ.
- El código obtenido por la construcción recursiva es óptimo o asintóticamente óptimo si el código de partida es óptimo.

Con respecto a lo anterior, en muchas ocasiones uno o los dos aspectos no se satisfacen, debido a que dependen mucho de los parámetros y propiedades de los códigos utilizados para construirlos [8].

Las definiciones y resultados mostrados en esta sección fueron presentados por Cao y Wei en [6] usando herramientas combinatorias como matrices diferencia y empaquetamientos estrictamente cíclicos [13]. Nosotros generalizamos la construcción presentada por estos autores. Para mostrar la construcción recursiva requerimos de el concepto de matriz diferencia que es el análogo en algún sentido al de la Definición de matriz $r-$simple 3.4 usada en la construcción de Chu y Golomb en [8].

Definición 4.6. [6] Sea G un grupo finito de orden v. Una matriz diferencia sobre G con parámetros (v, k, λ) es una matriz $D = (d_{ij})$ de tamaño $k \times \lambda v$ con componentes en G, tal que el vector diferencia entre dos filas diferentes de D contiene cada elemento de G exactamente λ veces.

El siguiente resultado en [13] nos proporciona una manera de construir matrices diferencia.

Teorema 4.7. *[13] Sean v y k enteros positivos tales que el $m.c.d(v, (k-1)!) = 1$ y $d_{ij} = ij$ mód v para $0 \leq i \leq k-1$ y $0 \leq j \leq v-1$. Entonces $D = (d_{ij})$ es una matriz diferencia sobre $\mathbb{Z}_v$ con parámetros $(v, k, 1)$. En particular, si v es un número primo impar, entonces existe una matriz diferencia sobre $\mathbb{Z}_v$ con parámetros $(v, k, 1)$ para todo $2 \leq k \leq v$.*

Presentamos el principal resultado obtenido en este capítulo, así como su demostración, el cual es omitido en [6], un caso particular de nuestro resultado.

Teorema 4.8. *Sea $\mathcal{C}$ un código ortogonal óptico en dos dimensiones con parámetros $(m \times n, k, 1)$. Si existe una matriz diferencia sobre $\mathbb{Z}_v$ con parámetros $(v, k, 1)$, entonces existe un código ortogonal óptico en dos dimensiones $\mathcal{C}'$ con parámetros $(m \times nv, k, 1)$ y $|\mathcal{C}'| = v\,|\mathcal{C}|$ palabras código.*

Demostración. Sea $\mathcal{C} = \{X_l : 1 \leq l \leq |\mathcal{C}|\}$ un código ortogonal óptico con parámetros $(m \times n, k, 1)$ donde $X_l = \{(x_{l,i} + s, y_{l,i}) : 0 \leq i \leq k-1\}$ para algún $0 \leq s \leq m-1$ con $(x_{l,i}, y_{l,i}) \in \mathbb{Z}_m \times \mathbb{Z}_n$ para todo $0 \leq l \leq |\mathcal{C}|$ e $0 \leq i \leq k-1$.
Sea $D = (d_{ij})$ para $0 \leq i \leq w-1$ y $\leq j \leq v-1$ una matriz diferencia sobre $\mathbb{Z}_v$ con parámetros $(v, k, 1)$. Para cada $X_l \in \mathcal{C}$ podemos asumir $s = 0$ por la Observación 4.1 y construir v palabras código como sigue

$$B_{l,j} = \{(x_{l,i}, y_{l,i}) + (0, nd_{ij}) \in \mathbb{Z}_m \times \mathbb{Z}_{nv} : 0 \leq i \leq k-1\},$$

para $0 \leq j \leq v-1$.

Sea $\mathcal{C}' = \{B_{l,j} + (s, 0) : 1 \leq l \leq |\mathcal{C}|\,, 0 \leq j \leq v-1, 0 \leq s \leq m-1\}$, entonces $\mathcal{C}'$ es un código ortogonal óptico en dos dimensiones con parámetros $(m \times nv, k, 1)$ y $v\,|\mathcal{C}|$ palabras código. Para probar la autocorrelación y la correlación cruzada supongamos por contradicción que existen l_1, l_2, j_i y j_2, tales que

$$R_{B_{l_1,j_1,0} - B_{l_2,j_2,0}}(0, t) \geq 2,$$

para algún $t \in \mathbb{Z}_{nv}$. Luego, existen i_1, i_1', i_2 e i_2' tales que

$$\begin{aligned} (x_{l_1,i_1}, y_{l_1,i_1} + nd_{i_1,j_1}) =& (x_{l_2,i_1'}, y_{l_2,i_1'} + nd_{i_1',j_2} + t), \\ (x_{l_1,i_2}, y_{l_1,i_2} + nd_{i_2,j_2}) =& (x_{l_2,i_2'}, y_{l_2,i_2'} + nd_{i_2',j_2} + t). \end{aligned} \tag{4.28}$$

Entonces

$$\begin{aligned} x_{l_1,i_1} =& x_{l_2,i_1'} \text{ mód } m, \\ y_{l_1,i_1} + nd_{i_1,j_1} =& y_{l_2,i_1'} + nd_{i_1',j_2} + t \text{ mód } nv, \\ x_{l_1,i_2} =& x_{l_2,i_2'} \text{ mód } m, \\ y_{l_1,i_2} + nd_{i_2,j_2} =& y_{l_2,i_2'} + nd_{i_2',j_2} + t \text{ mód } nv. \end{aligned} \tag{4.29}$$

Para la autocorrelación tenemos que $l_1 = l_2 = l$, $j_1 = j_2$ y $t \not\equiv 0$ mód nv, entonces las anteriores ecuaciones toman la forma

$$\begin{aligned} x_{l_1,i_1} =& x_{l_2,i_1'} \text{ mód } m, \\ y_{l_1,i_1} =& y_{l_2,i_1'} + t \text{ mód } n, \\ x_{l_1,i_2} =& x_{l_2,i_2'} \text{ mód } m, \\ y_{l_1,i_2} =& y_{l_2,i_2'} + t \text{ mód } n. \end{aligned} \tag{4.30}$$

Las anteriores ecuaciones implica que $R_{X_l - X_l}(0,t) \geq 2$, lo cual contradice la hipótesis de que $\mathcal{C}$ es un código ortogonal óptico.
Para la correlación cruzada tenemos $t \in \mathbb{Z}_{nv}$ y los siguientes casos

1. $l_1 \neq l_2$ y $j_1 = j_2$.
2. $l_1 \neq l_2$ y $j_1 \neq j_2$.
3. $l_1 = l_2 = l$ y $j_1 \neq j_2$.

Obtenemos contradicciones similares a la prueba de la autocorrelación en los casos 1 y 2. Para el caso 3, usando las Ecuaciones 4.29 tenemos

$$\begin{aligned} x_{l,i_1} &= x_{l,i'_1} \text{ mód } m, \\ y_{l,i_1} - y_{l,i'_1} &= n(d_{i'_1,j_2} - d_{i_1,j_1}) + t \text{ mód } v, \\ x_{l,i_2} &= x_{l,i'_2} \text{ mód } m, \\ y_{l,i_2} - y_{l,i'_2} &= n(d_{i'_2,j_2} - d_{i_2,j_2}) + t \text{ mód } v, \end{aligned} \tag{4.31}$$

lo cual no es posible ya que D es una matriz diferencia sobre $\mathbb{Z}_v$.

Ejemplo 4.1. Las siguientes palabras código

$$\{(0,0),(1,1),(1,4)\},\{(0,0),(2,0),(1,2)\},\{(0,0),(2,2),(2,3)\},\{(0,0),(2,1),(4,0)\}$$

junto con las palabras código obtenidas por traslaciones de la forma $(i,0)$ para $i = 0,\ldots,4$ forman un código ortogonal óptico óptimo $\mathcal{C}$ con parámetros $(5\times 5, 3, 1)$ como aparece en [6]. Tomando $v = 3$, $k = 3$ y el Teorema 4.7 tenemos que

$$D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix},$$

es una matriz diferencia sobre $\mathbb{Z}_3$ con parámetros $(3,3,1)$. Por el Teorema 4.8 tenemos que el conjunto $\mathcal{C}'$ que consta de los siguientes elementos

$$\begin{gathered} \{(0,0),(1,1),(1,4)\},\{(0,0),(1,6),(1,14)\},\{(0,0),(1,11),(1,9)\}, \\ \{(0,0),(2,0),(1,2)\},\{(0,0),(2,5),(1,12)\},\{(0,0),(2,10),(1,7)\}, \\ \{(0,0),(2,2),(2,3)\},\{(0,0),(2,7),(2,13)\},\{(0,0),(2,12),(2,8)\}, \\ \{(0,0),(2,1),(4,0)\},\{(0,0),(2,6),(4,10)\},\{(0,0),(2,11),(4,5)\}, \end{gathered}$$

junto con las palabras código obtenidas por traslaciones de la forma $(i,0)$ para $i = 0,\ldots,4$ forman un código ortogonal óptico óptimo con parámetros $(5\times 15, 3, 1)$ y 60 palabras código.

Observación 4.2. La construcción anterior no siempre produce códigos óptimos si el código de partida lo es. Por ejemplo, por el Teorema 4.3 existe un código ortogonal óptico óptimo con parámetros $(p \times p, p, 1)$ con p elementos para todo número primo p. Aplicando la construcción recursiva obtenemos un código ortogonal óptico en dos dimensiones con parámetros $(p \times p^2, p, 1)$ con p^2 elementos. Sin embargo, la cota de Johnson para estos parámetros es $p^2 + p$.

Capítulo 5

Resultados

Los resultados obtenidos en el presente trabajo de investigación son:

- Optimizamos algunas construcciones de códigos ortogonales ópticos asintóticamente óptimos a partir del análisis de la correlación de estos códigos y de las formas alternativas de presentar dichos códigos. Específicamente, logramos optimizar los códigos enunciados en los Teoremas 3.2, 3.5, 3.1 y 3.4. Además, encontramos una forma alternativa para construir familias de diferencia como se enuncia en el Teorema 3.6. Cabe destacar que este análisis permite obtener una construcción de código ortogonal óptico óptimo con parámetros $(p(p^h-1), p, 1)$, para todo número primo p y $h \geq 2$ un entero, cuyo resultado se puede consultar en el Teorema 3.5.
- Construimos nuevos códigos ortogonales ópticos a partir del uso de la construcción recursiva de Chu y Golomb en [8] aplicada a los conjuntos de Sidon en una dimensión. Dichos resultados se pueden consultar en los Teoremas 3.10 y 3.12, y en los Corolarios 3.9 y 3.10.
- Obtuvimos nuevas construcciones de códigos ortogonales ópticos en dos dimensiones a partir de conjuntos de Sidon en dos dimensiones como se muestra en los Teoremas 4.3, 4.4, 4.5 y también logramos construir códigos en dos dimensiones a partir de códigos en una dimensión como se muestra en el Teorema 4.6 y el Corolario 4.1.
- Generalizando las ideas de la construcción recursiva de códigos ortogonales en una dimensión presentada por Chu y Golomb en [7], presentamos una construcción recursiva para el caso de dos dimensiones como se muestra en los conceptos

y resultados mostrados en la Sección 4.2. El resultado principal obtenido puede consultarse en el Teorema 4.8.

- En general, logramos construir nuevas familias de códigos ortogonales ópticos (algunos de ellos óptimos) en una dimensión y dos dimensiones a partir de la combinación de diferentes técnicas como fue el análisis de la correlación de códigos y conjuntos de Sidon, uso de herramientas combinatorias como los cuadrados latinos mutuamente ortogonales y construcciones recursivas principalmente.

Capítulo 6

Conclusiones

Las conclusiones del presente trabajo de investigación se resumen a continuación.

- Las construcciones asintóticas de códigos ortogonales ópticos asintóticamente óptimas estudiadas en este trabajo, en algunos casos particulares de los parámetros involucrados, pueden ser optimizadas a partir de la adición de nuevas palabras código obtenidas de construcciones auxiliares de códigos. A excepción de la familia $\mathcal{B}$ que aparece en [23], las construcciones no se pueden optimizar completamente debido a los parámetros, a las propiedades de las estructuras algebraicas sobre las cuales se definen y a la ausencia de códigos ortogonales ópticos con parámetros parecidos a los dados en las construcciones. Sin embargo, para algunos casos particulares de los parámetros se pueden obtener infinitas familias de códigos ortogonales ópticos óptimos.

- Las construcciones de códigos ortogonales ópticos en una dimensión a partir de la aplicación de la construcción recursiva de Chu y Golomb a los conjuntos de Sidon modulares conocidos proporcionó nuevas familias de códigos, algunas de ellas óptimas como en el caso de Bose y Singer. En la aplicación de la construcción recursiva al conjunto de Sidon tipo Ruzsa queda como problema de investigación buscar una forma explícita de construir conjuntos de Sidon módulo p^2 con $p-1$ elementos para todo primo $p \geq 7$. La búsqueda computacional no produce buenos resultados.

- Los conjuntos de Sidon tanto en una dimensión como en dos dimensiones permiten encontrar nuevas familias de códigos ortogonales ópticos en dos dimensiones e in-

cluso en una dimensión para algunos parámetros particulares de los grupos sobre los cuales se definen los conjuntos de Sidon.

- La construcción recursiva para códigos ortogonales ópticos en dos dimensiones proporciona infinitas familias de éstos. Algunas de las construcciones obtenidas son óptimas. Dejamos para un trabajo futuro el análisis de determinar cuáles son las construcciones adecuadas para obtener códigos óptimos por construcción recursiva, debido a la gran variedad de artículos en la literatura dedicada a este tema.

Apéndice A

Apéndice

Algoritmos en SAGE

En este apéndice se presentan algunos algoritmos utilizados en el presente trabajo y su implementación en el Sistema de Álgebra Computacional SAGE.
Para el lector interesado, Los algoritmos estan disponibles en el siguiente repositorio

https://github.com/mao138/codigos-ortogonales-opticos

Algoritmo 1 (Código ortogonal óptico)**.** Este algoritmo determina si un conjunto dado es un código ortogonal óptico en una dimensión con parámetros (n, w, λ), por medio de la verificación de las propiedades de correlación. Para su implementación en SAGE el algoritmo recibe una lista, la longitud n y los valores de la autocorrelación a y correlación cruzada c. Si la lista es un código ortogonal óptico retorna 1 y 0 en caso contrario.

```
def COO(T,n,a,c):
       for X in T:
           for Y in T:
               if X==Y:
                   for t in Set(Integers(n)).difference({0}):
                       C=Set([y+t for y in Y ])
                       if len(C.intersection(X))>a:
                           return 0
               else:
```

```
                    for t in Integers(n):
                        C=Set([y+t for y in Y ])
                        if len(C.intersection(X))>c:
                            return 0
        return 1
```

Algoritmo 2 (Cota de Johnson)**.** Este algoritmo calcula la Cota de Johnson para un código ortogonal óptico. El algoritmo recibe la longitud del código n, su peso w y la constante de correlación λ.

```
def Johnson(n,w,l):
    if n>=w>l>=1:
        c=((n-l)/(w-l)).floor()
        for i in range(1,l):
            c=c*(n-(l-i))/(w-(l-i)).floor()
        d=(c/w).floor()
        print d
    else:
        print 'Los valores de n, w y l deben cumplir n>=w>l>=1'
```

Algoritmo 3 (Construcción de Moreno, Omrani y Lu [22])**.** Este algoritmo construye las palabras del código ortogonal óptico del Teorema 2.3. Recibe los valores del primo q, el entero positivo m y construye las palabras del código ortogonal óptico óptimo con parámetros $(q^m - 1, q, 1)$.

```
 def moreno(q,m):
    P.<x>=PolynomialRing(GF(q))
    K.<a>=GF(q^m, name='a')
    f=K.modulus()
    L=[]
    for g in [1..m-1]:
        T=[]
        for p in P.monics( of_degree = g):
            T.append(p)
        L.append(T)
    R=[]
    for k in [0..m-2]:
        n=len(L[k])
        e=Integer(n/q)
```

```
        for j in [0..e-1]:
            X=[]
            for i in [0..q-1]:
                X.append(log(L[k][q*j+i](a),a))
                X.sort()
            R.append(X)
    return R
```

Algoritmo 4 (Construcción de Wilson [33])**.** Este algoritmo construye las palabras del código ortogonal óptico de los Teoremas 2.1 y 2.2. Recibe el valor del número primo p, el entero positivos c y construye un código ortogonal óptico de longitud p, peso $(p-1)/c$ y $\lambda = 1$.

```
def Wilson(p,c):
    w=(p-1)/c
    b=(p-1) % c
    if b==0:
        P=Primes()
        if p in P:
            F.<a>=GF(p)
            t=F.multiplicative_generator()
            g=t^c
            Q=[]
            for i in [1..w]:
                Q.append(g^i)
            T=Set(Q)
            V=[]
            for i in [0..c-1]:
                U=[]
                for j in T:
                    U.append(j*t^i)
                V.append(U)
            print(V)
        else:
            print "p no es primo"
    else:
        print "c no divide a p-1"
```

Algoritmo 5 (Tabla de diferencias)**.** Este algoritmo construye la tabla de diferencias

de dos palabras de un código ortogonal óptico. Recibe las dos palabras X, Y del código (no necesariamente distintas), el módulo n y construye la tabla.

```
def trianglesetm(X,Y,n):
    k=len(X);
    m = matrix(QQ, k, k, lambda i, j:mod(Y[j]-X[i],n));
    return(m)
```

Algoritmo 6 (Construcción de Bose)**.** Este algoritmo construye un conjunto de Sidon tipo Bose. El algoritmo recibe la potencia prima q y calcula el conjunto de Sidon módulo $q^2 - 1$ con q elementos.

```
def Bose(q):
    F.<a>=FiniteField(q^2)
    B=[]
    for i in [1..q]:
        B.append(discrete_log(a+i,a))
    print B
```

Algoritmo 7 (Construcción de Ruzsa)**.** Este algoritmo construye un conjunto de Sidon tipo Ruzsa. El algoritmo recibe el número primo p, una raíz primitiva r módulo p y calcula un conjunto de Sidon módulo $p(p-1)$ con $p-1$ elementos.

```
def Ruzsa(p,r):
    A=[]
    for i in [1..p-1]:
        A.append(mod(p*i-(p-1)*r^i,p*(p-1)))
    print A
```

Algoritmo 8 (Construcción A de [11])**.** Los siguientes algoritmos permiten construir el código ortogonal asintóticamente óptimo que se encuentra en [11] denominado en dicho artículo como construcción A.

```
def dif(A,n):
    D=[]
    for i in [0..len(A)-1]:
        for j in [0..len(A)-1]:
            if i!=j:
```

```
                D.append(mod(A[i]-A[j],n))
    R=[a for a in D]
    R.sort()
    return(R)

def code(i,j,k,p,m,t,a):
    D=[]
    for  l in [0..m-1]:
        D.append(crt(l-l,p^(1-k)*a^(40*i+j+t*l),m,p^2))
        D.sort()
    return(D)

def todos(p,m,t,a):
    H=[]
    for i in [0..p-1]:
        for j in [0..t-1]:
            H.append(dif(code(i,j,1,p,m,t,a),m*p^2))
    print(H)
```

Bibliografía

[1] TL Alderson and Keith E Mellinger, *Optical orthogonal codes from singer groups*, Advances In Coding Theory And Cryptography, World Scientific, 2007, pp. 51–69.

[2] RC Bose, *An affine analogue of singer's theorem*, The Journal of the Indian Mathematical Society **6** (1942), 1–15.

[3] Marco Buratti, *A powerful method for constructing difference families and optimal optical orthogonal codes*, Designs, Codes and cryptography **5** (1995), no. 1, 13–25.

[4] Marco Buratti and Douglas R Stinson, *New results on modular golomb rulers, optical orthogonal codes and related structures*, arXiv preprint arXiv:2007.01908 (2020).

[5] Nidia Yadira Caicedo Bravo, *Conjuntos de sidón en dimensión dos*, (2016).

[6] Haitao Cao and Ruizhong Wei, *Combinatorial constructions for optimal two-dimensional optical orthogonal codes*, IEEE transactions on information theory **55** (2009), no. 3, 1387–1394.

[7] Yanxun Chang, Ryoh Fuji-Hara, and Ying Miao, *Combinatorial constructions of optimal optical orthogonal codes with weight 4*, IEEE Transactions on Information theory **49** (2003), no. 5, 1283–1292.

[8] Wensong Chu and Solomon W Golomb, *A new recursive construction for optical orthogonal codes*, IEEE Transactions on Information Theory **49** (2003), no. 11, 3072–3076.

[9] Fan RK Chung, Jawad A Salehi, and Victor K Wei, *Optical orthogonal codes: design, analysis and applications*, IEEE Transactions on Information theory **35** (1989), no. 3, 595–604.

[10] Habong Chung and P Vijay Kumar, *Optical orthogonal codes-new bounds and an optimal construction*, IEEE Transactions on Information theory **36** (1990), no. 4, 866–873.

[11] Jin-Ho Chung and Kyeongcheol Yang, *Asymptotically optimal optical orthogonal codes with new parameters*, IEEE transactions on information theory **59** (2013), no. 6, 3999–4005.

[12] Javier Cilleruelo, *Conjuntos de sidon*, Instituto Venezolano de Investigaciones Científicas, 2014.

[13] Charles J Colbourn, *Crc handbook of combinatorial designs*, CRC press, 2010.

[14] Konstantinos Drakakis, *A review of costas arrays*, Journal of Applied Mathematics **2006** (2006).

[15] Ryoh Fuji-Hara and Ying Miao, *Optical orthogonal codes: Their bounds and new optimal constructions*, IEEE Transactions on Information theory **46** (2000), no. 7, 2396–2406.

[16] Carlos Alexis Gómez Ruiz and Carlos Alberto Trujillo Solarte, *Una nueva construcción de conjuntos [b. sub. h] modulares*, (2011).

[17] Haim Hanani, *Balanced incomplete block designs and related designs*, Discrete Mathematics **11** (1975), no. 3, 255–369.

[18] Dieter Jungnickel, *Composition theorems for difference families and regular planes*, Discrete Mathematics **23** (1978), no. 2, 151–158.

[19] Ssang-Soo Lee and Seung-Woo Seo, *New construction of multiwavelength optical orthogonal codes*, IEEE transactions on communications **50** (2002), no. 12, 2003–2008.

[20] Shikui Ma and Yanxun Chang, *Constructions of optimal optical orthogonal codes with weight five*, Journal of Combinatorial Designs **13** (2005), no. 1, 54–69.

[21] Carlos Martos and Yadira Caicedo, *Reglas g-golomb*, (2014).

[22] Oscar Moreno, Reza Omrani, P Vijay Kumar, and Hsiao-feng Lu, *A generalized bose-chowla family of optical orthogonal codes and distinct difference sets*, IEEE transactions on information theory **53** (2007), no. 5, 1907–1910.

[23] Oscar Moreno, Zhen Zhang, P Vijay Kumar, and Victor A Zinoviev, *New constructions of optimal cyclically permutable constant weight codes*, IEEE Transactions on Information Theory **41** (1995), no. 2, 448–455.

[24] Reza Omrani, Gagan Garg, P Vijay Kumar, Petros Elia, and Pankaj Bhambhani, *Large families of asymptotically optimal two-dimensional optical orthogonal codes*, IEEE transactions on information theory **58** (2012), no. 2, 1163–1185.

[25] Rigo Julián Osorio, Diego Fernando Ruiz, Carlos Alberto Trujillo, and Cristhian Leonardo Urbano, *Secuencias sonar y conjuntos de sidon*, Revista de Ciencias **18** (2014), no. 1, 33–42.

[26] H. Ruiz, J. López, and C. Trujillo, *Two-dimensional optical orthogonal codes from sidon sets*, IEEE Access Review, Sometido a evaluación.

[27] Hamilton M Ruiz, Luis M Delgado, and Carlos A Trujillo, *A new construction of optimal optical orthogonal codes from sidon sets*, IEEE Access **8** (2020), 100749–100753.

[28] Imre Z Ruzsa, *Solving a linear equation in a set of integers i*, Acta arithmetica **65** (1993), no. 3, 259–282.

[29] Sun Shurong, Hongxi Yin, Ziyu Wang, and Anshi Xu, *A new family of 2-d optical orthogonal codes and analysis of its performance in optical cdma access networks*, Journal of lightwave technology **24** (2006), no. 4, 1646.

[30] James Singer, *A theorem in finite projective geometry and some applications to number theory*, Transactions of the American Mathematical Society **43** (1938), no. 3, 377–385.

[31] Su Wang, Lingye Wang, and Jinhua Wang, *A new class of optimal optical orthogonal codes with weight six*, 2015 Seventh International Workshop on Signal Design and its Applications in Communications (IWSDA), IEEE, 2015, pp. 66–69.

[32] Xiaomiao Wang and Yanxun Chang, *Further results on (v, 4, 1)-perfect difference families*, Discrete mathematics **310** (2010), no. 13-14, 1995–2006.

[33] Richard M Wilson, *Cyclotomy and difference families in elementary abelian groups*, Journal of Number Theory **4** (1972), no. 1, 17–47.

[34] Guu-Chang Yang and Wing C Kwong, *Performance comparison of multiwavelength cdma and wdma+ cdma for fiber-optic networks*, IEEE Transactions on Communications **45** (1997), no. 11, 1426–1434.

[35] Hongxi Yin and David J Richardson, *Optical code division multiple access communication networks*, chap **2** (2008), 34.

[36] Jianxing Yin, *Some combinatorial constructions for optical orthogonal codes*, Discrete Mathematics **185** (1998), no. 1-3, 201–219.

[37] Tang Yu and Yin Jianxing, *The combinatorial construction for a class of optimal optical orthogonal codes*, Science in China Series A: Mathematics **45** (2002), no. 10, 1268–1275.