Reglas Golomb generalizadas y la teoría de Ramsey

Luis Miguel Delgado Ordoñez

Universidad del Cauca
Facultad de Ciencias Naturales, Exactas y de la Educación
Departamento de Matemáticas
Doctorado en Ciencias Matemáticas
Popayán
Diciembre de 2022

Reglas Golomb generalizadas y la teoría de Ramsey

Luis Miguel Delgado Ordoñez

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

Director
Dr. 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
Diciembre de 2022

NOTA DE ACEPTACIÓN

ACEPTADO

Firma jurado, Dr. Mario Alejandro Huicochea Mason

Firma jurado, Dr. Carlos Alexis Gómez Ruiz

Firma jurado, Dr. Jhon Jairo Bravo Grijalba

Popayán, 23 de marzo de 2023

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

Fecha: 23 de marzo de 2023 Facultad: Facultad de Ciencias Naturales, Exactas y de la Educación

Lugar: Auditorio Jesús María Otero Hora: 5 p.m.

Programa:	Doctorado en Ciencias Matemáticas	
1. Alumno: Luis Miguel Delgado Ordoñez	C.C: 1.085.260.596	Código: 220_1085260596
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: “Reglas Golomb Generalizadas y la Teoría de Ramsey”

INFORME SOBRE LA SUSTENTACIÓN

Cumplimiento de Objetivos:

Los objetivos propuestos en su proyecto de investigación se cumplieron completamente.

Desarrollo Metodológico:
El trabajo de la tesis de Luis Miguel se ubica en el área de la teoría aditiva y combinatoria de números, junto con algunas de sus aplicaciones. Interactúan conceptos y resultados de las secuencias sonar, los casi conjuntos diferencia y los números Sidon-Ramsey. El estudiante realizó una muy buena presentación y respondió con suficiencia a todas las preguntas realizadas por los jurados.

Logros del Trabajo o Aportes:

Adicionalmente, el Jurado destaca la publicación realizada, la cual está disponible en Revista Indexada por MINCIENCIAS, categoría A1: IEEE Access. También considera que los resultados obtenidos aportan a la comunidad matemática y recomienda someter a publicación los otros resultados obtenidos durante el desarrollo de la tesis doctoral.

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

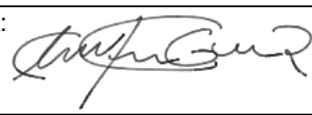
MENCION HONORÍFICA SI (☐) NO (X☐)

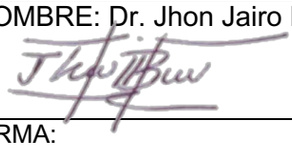
CALIFICACIÓN DE LAUREADO SI (☐) NO (X☐)

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	☐X	
APROBADO CON CONDICIONES	☐	
APLAZADO	☐	
NO APROBADO	☐	

JURADOS

NOMBRE: Dr. Mario Alejandro Huicochea Mason	NOMBRE: Dr. Carlos Alexis Gómez Ruiz
FIRMA: 	FIRMA: 
C.C. Nº: Pasaporte Número 639058033	C.C. Nº: 94420734

NOMBRE: Dr. Jhon Jairo Bravo Grijalba 	NOMBRE:
FIRMA:	FIRMA:
C.C. Nº: 76328867	C.C. Nº:

A mi familia. Porque cada uno de sus miembros aportó para alcanzar esta meta tan anhelada. Especialmente a mi madre Inesita por darme la vida y formarme como una persona de bien. A mi hijo Juan José que es mi orgullo y el motor de mi vida. Finalmente a mi esposa Maria Nelcy porque gracias a ella he alcanzado las metas más importantes de mi vida.

Agradecimientos

Para empezar, quiero agradecer a mis padres, José Felix Delgado e Ines Ordoñez por su gran amor, ejemplo y apoyo durante mi crianza. A mi hijo Juan José por ser mi mayor orgullo, mi motor y por apoyarme desde su inocencia durante el doctorado. A mi esposa Maria Nelcy Alomia López quien ha sido mi apoyo y compañia durante mis estudio de posgrado, gracias por creer en mi y por impulsarme a mejorar cada día, te amo infinitamente. A mis hermanos, sobrinos 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 Doctorado en Ciencias Matemáticas, por su excelente planta docente y directiva, que tanto aporto en mi formación personal y académica.

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

Al PhD Mario Huicochea por su apoyo tanto académico como personal, gracias por ser tan incondicional en todo momento. Al PhD Jhon Jairo Bravo Grigalba por sus enseñanzas como profesor, por su amistad y por la dedicación en la revisión de mi tesis doctoral. Al PhD Carlos Alexis Gomez por sus comentarios y sugerencias en la revisión de este trabajo.

A mi compañero de estudio Hamilton Mauricio Ruiz por toda su colaboración y por todos los momentos que vivimos a lo largo de la maestría y del doctorado.

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 compartirme sus conocimientos y haber aceptado la orientación de este trabajo de investigación.

Luis Miguel Delgado O.

Universidad del Cauca
Marzo 24 de 2023.

Resumen

Una regla Golomb es un conjunto de enteros positivos con la propiedad de que todas las diferencias no nulas que generan sus elementos son distintas. Aunque su relación con los conjuntos de Sidon es inmediata, pasaron varias décadas antes de que se estableciera su equivalencia.

En este trabajo estudiamos las reglas $g-$Golomb que son una generalización de las reglas Golomb que permite la repetición de las diferencias hasta g veces. En primer lugar, basados en el trabajo que iniciaron Erdös y Freud sobre la distribución de conjuntos de Sidon maximales, demostramos la buena distribución que tienen las reglas $g-$Golomb óptimamente densas cuando están contenidas en un intervalo entero o en progresiones aritméticas disjuntas de la misma diferencia. En segundo lugar, reunimos las diversas definiciones de reglas $g-$Golomb en diferentes contextos y las sintetizamos en el concepto de arreglos $g-$Golomb, dichos arreglos resultan ser una generalización de las reglas $g-$Golomb cuando son consideradas en un grupo cualquiera. Lo anterior nos permitió determinar el comportamiento asintótico de una función maximal de dichos arreglos, proporcionar resultados sobre los arreglos $g-$Golomb en $\mathbb{Z}^d$ y encontrar nuevas construcciones de secuencias sonar extendidas que son casos particulares de los arreglos $g-$Golomb en $\mathbb{Z}^2$.

Finalmente, estudiamos los números Sidon Ramsey en el caso modular y logramos establecer cotas superiores e inferiores junto con 6 valores exactos de este parámetro. Como consecuencia de nuestra investigación, aportamos nuevos resultados a la teoría de los conjuntos casi diferencia, mostramos familias infinitas de parámetros para los cuales no existen conjuntos casi diferencia y en consecuencia obtuvimos cotas superiores para una función maximal de los conjuntos de Sidon modulares.

Palabras clave: Reglas $g-$Golomb, arreglos $g-$Golomb, conjuntos de Sidon, números Sidon Ramsey y conjuntos casi diferencia.

Abstract

A Golomb ruler is a set of positive integers with the property that all nonzero differences generated by its elements are distinct. Although its relationship with Sidon sets is immediate, its equivalence was established several decades later.

In this work we study the $g-$Golomb rules, which are a generalization of the Golomb rules that allow the repetition of differences up to g times. First, based on the work started by Erdös and Freud on the distribution of maximal Sidon sets, we show the well-distribution of optimally dense $g-$Golomb rules when they are contained in an integer interval or in disjoint arithmetic progressions of the same difference. Second, we bring together the various definitions of $g-$Golomb rules in different contexts and synthesize them into the concept of $g-$Golomb arrays, such arrays turn out to be a generalization of $g-$Golomb rules when considered in any group. The above allowed us to determine the asymptotic behavior of a maximal function of such arrays, provide results on the $g-$Golomb arrays in $\mathbb{Z}^d$ and find new constructions of extended sonar sequences which are particular cases of $g-$Golomb arrays in $\mathbb{Z}^2$.

Finally, we study the Sidon Ramsey numbers in the modular case and manage to set upper and lower bounds together with 6 exact values of this parameter. As a consequence of our research, we provide new results to the theory of almost difference sets, we show infinite families of parameters for which there are no almost difference sets and therefore we obtain upper bounds for a maximal function of the modular Sidon sets.

Keywords: $g-$Golomb ruler, $g-$Golomb array, Sidon set, Sidon Ramsey numbers and almost difference sets.

Productos de la investigación

Artículos

[11] *New constructions of extended sonar sequences from Sidon sets*, IEEE Access, **10** (2021), 3343–3350. Con C. Martos y C. Trujillo.

Artículos en preparación

[12] *Sidon Ramsey Numbers and Almost Difference sets*. Preprint. Con A. Montejano y C. Trujillo.

[13] *Generalized Golomb rulers in* $\mathbb{Z}^d$. Preprint. Con C. Trujillo.

Ponencias

- *Secuencias sonar como conjuntos de Sidon y nuevas construcciones*. Octavo congreso de Algebra, Teoría de Números, Combinatoria y Aplicaciones, Popayán Colombia, Julio 23–27, 2018.
- *Sidon Ramsey Numbers*. Seminario Preguntón de Matemáticas Discretas, Juriquilla, Querétaro México, Octubre 15, 2019.
- *Número Sidon Ramsey*. VI Seminario Regional de Teoría de Números, Popayán Colombia, Marzo 11–14, 2020.

– *Número Sidon Ramsey en* $\mathbb{Z}_n$. LIMDA Seminar, Barcelona España, Abril 7, 2022.

– *New constructions of Extended Sonar Sequences from Sidon sets*. Segunda Conferencia de Matemáticas Aplicadas e Industriales MAPI2, Medellín Colombia, Junio 13, 2022.

– *Números Sidon Ramsey en* $\mathbb{Z}_n$. Seminario Aritmética y Geometría en Valparaíso, Valparaíso Chile, Julio 6, 2022.

Pasantías de investigación

– Universidad Nacional Autónoma de México, Juriquilla México, Noviembre, 2021. Con Amanda Montejano Cantoral.

– Universidad Politécnica de Cataluña, Barcelona España, Abril, 2022. Con Juan José Rué Perna.

– Universidad de Valparaíso, Valparaíso Chile, Julio, 2022. Con Amalia Pizarro Madariaga.

Índice general

Capítulo 1

Introducción

Una regla Golomb es un conjunto de enteros positivos con la propiedad de que las diferencias no nulas, generadas por sus elementos, son todas distintas. Este concepto apareció como solución al problema de evitar la distorsión de intermodulación entre bandas de radio [2]. Aunque fue Babcock quien lo introdujo en [2], el impulso determinante para su investigación se debe al profesor Solomon Golomb quien demostró una importante aplicación para etiquetar grafos [20]. Las reglas Golomb tiene otras aplicaciones en ingeniería, por ejemplo en la generación de códigos convolucionales auto-ortogonales y en la formación de arreglos telescópicos lineales óptimos en radio-astronomía [15]. Varios años antes, en teoría de números ya existían los conjuntos de Sidon, que son conjuntos de enteros positivos donde todas las sumas de dos de sus elementos son distintas salvo por conmutatividad. Aunque los conjuntos de Sidon aparecieron en 1932 y las reglas Golomb en 1950, fue hasta el año 2002 que se estableció su equivalencia por parte de Dimitromanolakis en [14].

El concepto de conjunto de Sidon fue generalizado a conjunto $B_h[g]$ al considerar sumas con h sumandos y permitir que los resultados se repitan hasta g veces (salvo permutación) [35]. Cuando $h > 2$ y $g > 1$ este nuevo concepto pierde su relación con las reglas Golomb. Por otra parte, la aplicación en la interferencia de señales de radio generó la necesidad de extender las reglas Golomb. En este sentido, Atkinson, Santoro y Urrutia en [1] introdujeron el concepto de reglas $g-$Golomb, que son básicamente conjuntos de enteros cuyos elementos generan diferencias no nulas que se repiten hasta g veces. Las reglas $1-$Golomb se denominan simplemente reglas Golomb.

Existen dos problemas clásicos en la teoría de las reglas $g-$Golomb. El primero consiste

en determinar el máximo cardinal que tiene una regla $g-$Golomb cuando está contenida en un intervalo entero.

El segundo problema consiste en encontrar la menor longitud que puede tener una regla $g-$Golomb con k marcas, donde la longitud de una regla $g-$Golomb es la mayor distancia entre dos elementos y la denotamos con $\ell(A)$, mientras que a los elementos de la regla los denominamos marcas. Para profundizar más sobre la teoría de las reglas $g-$Golomb, se puede consultar [1, 6, 15, 31].

La teoría de las reglas $g-$Golomb es relativamente nueva y en los últimos años ha adquirido interés por su relación con varios conceptos combinatorios entre los cuales están: los código ortogonales ópticos, los conjuntos diferencia, los conjuntos casi diferencia, diseños y otros más. Todas estas conexiones se pueden revisar en [4, 6, 34, 41].

El estudio de las reglas $g-$Golomb que realizamos en este trabajo lo dividimos en varios capítulos de la siguiente manera: El Capítulo 2 contiene las definiciones, la notación y los resultados más relevantes que serán utilizados a lo largo del documento. Iniciamos con los conjuntos de Sidon, reglas $g-$Golomb y energía aditiva, después revisamos las construcciones modulares de conjuntos de Sidon, conjuntos casi diferencia, una introducción a la teoría de Ramsey y finalmente las reglas Golomb disjuntas.

1.1. Reglas $g-$Golomb en $\mathbb{Z}$

En la literatura se encuentra una serie de artículos donde se estudia la distribución de los conjuntos de Sidon maximales cuando están contenidos en un intervalo entero o en clases residuales. En ellos se establecen cotas superiores para la máxima distancia que pueden tener dos elementos consecutivos en un conjunto de Sidon, la cual se denomina Gap. Podemos encontrar estos resultados en [8, 9, 16, 23, 25, 29].

Motivados por el resultado de Erdös y Freud en [16] sobre la buena distribución en $[1, n]$ de conjuntos de Sidon maximales, en el Capítulo 3 demostramos que las reglas $g-$Golomb óptimamente densas también están bien distribuidas cuando están contenidas en un intervalo entero, lo cual generaliza los resultados de [16] y [23]. De igual forma, extendemos los resultados de Lindström [29], Kolountzakis [25] y Cilleruelo [9] al demostrar que las reglas $g-$Golomb están bien distribuidas en clases residuales.

Finalmente, establecemos una cota superior para el cardinal de una regla $g-$Golomb contenida en progresiones aritméticas disjuntas que tengan la misma diferencia. Este

último resultado nos permitió dar una cota superior para el Gap de una regla $g-$Golomb, que generaliza la encontrada por Cilleruelo en [8]. Los anteriores resultados hacen parte de un artículo que está en preparación [13].

1.2. Arreglos $g-$Golomb

En la actualidad existen varios conceptos que resultan ser generalizaciones o casos particulares de las reglas Golomb en diferentes contextos, pero no todos se enmarcan como tal, ver por ejemplo [10, 21, 38, 39]. Es por esto que en el Capítulo 4 reunimos todos estos conceptos en la definición de un arreglos $g-$Golomb, estos arreglos son básicamente reglas $g-$Golomb consideradas en un grupo abeliano cualquiera.

En primer lugar, al estudiar los arreglos $g-$Golomb en $\mathbb{Z}^d$, logramos establecer el comportamiento asintótico de la función que estudia el máximo cardinal que puede tener un arreglo $g-$Golomb contenido en la caja d dimensional $[1, n_1] \times \cdots \times [1, n_d]$. Es decir, demostramos que

$$F^-(g, n_1, \ldots, n_d) = (g^{1/2} + o(1))(n_1 n_2 \cdots n_d)^{1/2}, \tag{1.1}$$

resultado que generaliza lo encontrado por Caicedo, Martos y Trujillo en [6], Cilleruelo en [9] y Lindström en [28].

En segundo lugar, con el comportamiento asintótico de la función $F^-(g, n_1, \ldots, n_d)$, logramos demostrar que un arreglo $g-$Golomb óptimamente denso está bien distribuido cuando está contenido en el cubo d dimensional $[1, n]^d$ y en un látice o retícula particular. Estos resultados forman parte del artículo [13] que se encuentra en fase de preparación.

En tercer lugar, estudiamos un caso particular de los arreglos $1-$Golomb que se denominan secuencias sonar. Estas secuencias tienen gran aplicación en la detección radar y sonar. En el mismo Capítulo 4 establecemos dos nuevas construcciones de secuencias sonar extendidas. Estas construcciones las publicamos en el artículo [11].

Finalmente, mostramos una nueva construcción de reglas Golomb en $\mathbb{Z}$ a partir de arreglos $1-$Golomb en $\mathbb{Z}^2$. Este aporte fue motivado por un trabajo realizado por Kløve en [24] y mejora el que estableció Shearer en [44].

1.3. Números Sidon Ramsey

En el Capítulo 5 revisamos la teoría existente de los números Sidon Ramsey $SR(r)$, los cuales establecen qué tan grande debe ser un intervalo entero para que en toda $r-$coloración del mismo, se garantice la existencia de una solución monocromática no trivial de la ecuación de Sidon $x+y=z+w$. Para conocer un poco más de la Teoría de Ramsey y de los números Sidon Ramsey se puede consultar los libros [26, 52].

Aunque los números Sidon Ramsey son un punto de encuentro más entre la teoría de los conjuntos de Sidon y la teoría de Ramsey, esta nueva relación tiene una reciente acogida como se puede evidenciar en [19, 27, 52]. Además, se están encontrando nuevos espacios de investigación relacionados a $SR(r)$.

Nuestros principales descubrimientos se presentan al considerar los números Sidon Ramsey en grupos cíclicos, denotados por $\overline{SR}(r)$. En el Capítulo 5, obtuvimos cotas superiores de $\overline{SR}(r)$, una asintótica y otras para un número finito de valores de r. Buscando mejorar estas cotas, logramos dar nuevos resultados a la teoría de los conjuntos casi diferencia y de los conjuntos de Sidon modulares. Estos aportes mejoran en parte los establecidos en [53, 30].

También realizamos una búsqueda computacional para determinar cotas inferiores de valores particulares de $\overline{SR}(r)$, con dichas cotas logramos establecer seis valores exactos de $\overline{SR}(r)$. Por otra parte, finalizamos el Capítulo 5 dando una construcción de reglas Golomb disjuntas regulares con la cual se puede encontrar cotas inferiores de $SR(r)$ para infinitos valores de r. El Capítulo 5 hace parte del artículo [12] que está por someterse.

Capítulo 2

Preliminares

En este capítulo damos los conceptos, la notación y los resultados que usaremos en el desarrollo de nuestro trabajo. Presentamos los conjuntos de Sidon, reglas $g-$Golomb y energía aditiva, después revisamos las construcciones de los conjuntos de Sidon modulares, conjuntos casi diferencia, damos una introducción a la teoría de Ramsey y finalizamos con las reglas Golomb modulares disjuntas.

2.1. Definiciones básicas

Vamos a denotar el conjunto de número enteros con $\mathbb{Z}$, el conjunto de enteros positivos con $\mathbb{Z}^+$, el conjunto de los números reales con $\mathbb{R}$ y el anillo de enteros módulo n con $\mathbb{Z}_n$.

Consideremos G un grupo abeliano notado aditivamente, A y B subconjuntos de G y x un elemento de G. Definimos los siguientes conjuntos:

- Multiconjunto **A** contenido en el grupo G. Está compuesto por elementos del grupo G donde la repetición importa, es decir, cada elemento puede repetirse varias veces. Por ejemplo, el conjunto A puede ser $\{a, b, c\}$ mientras que el multiconjunto **A** se puede definir como $\{a, a, b, c, c, c\}$.

- Conjunto suma de A y B:

$$A + B := \{a + b : \ a \in A, b \in B\},$$
$$A \oplus B := \{a + b : \ a \in A, b \in B, \ a \neq b\}.$$

- Conjunto diferencia de A y B:

$$A - B := \{a - b : \ a \in A, b \in B\},$$
$$A \ominus B := \{a - b : \ a \in A, b \in B, \ a \neq b\}.$$

- Conjunto traslación de A por x:

$$x + A := \{x + a : \ a \in A\}.$$

- Conjunto dilatación de A, para todo entero positivo k:

$$k \cdot A := \{ka : \ a \in A\},$$

  donde $ka = \underbrace{a + \cdots + a}_{k \text{ veces}}$.

- Conjunto inverso de A:

$$A^{-1} := \{a^{-1} : \ a \in A\},$$

  donde a^{-1} denota el elemento inverso de $a \in G$. En este caso, como G es un grupo aditivo denotamos a^{-1} por $-a$.

En adelante, dado un conjunto finito A, denotamos con $|A|$ al número de elementos o cardinal del conjunto A. También denotamos el intervalo de los primeros n enteros positivos por $[1, n] := \{1, 2, \ldots, n\}$ y el número combinatorio $\binom{n}{m}$, el cual cuenta el número de subconjuntos de tamaño m tomados de un conjunto de cardinal n, para $n \geq m$. Uno de los aspecto de mayor interés es estudiar el cardinal del conjunto suma (o diferencia) sobre todo cuando éste es grande, es por esto que damos a continuación un resultado que muestra algunas cotas triviales para el cardinal de estos conjuntos [49].

Lema 1. Sean, G un grupo abeliano notado aditivamente, A, B subconjuntos de G y $x \in G$ no nulo. Entonces:

a) $|A + x| = |A| = |-A|$;

b) $\text{máx}\{|A|, |B|\} \leq |A + B|, \ |A - B| \leq |A||B|$;

c) $|A| \leq |A+A| \leq \dfrac{|A|(|A|+1)}{2}$;

d) $|A| \leq |A-A| \leq |A|^2 - |A| + 1$.

Demostración. Ver [49]. □

Si el conjunto suma o el conjunto diferencia de una colección dada A alcanza las cotas superiores de c) o d), se dice que A es un conjunto de Sidon, una regla Golomb o un conjunto B_2. Estos conjuntos son el principal objeto de estudio en nuestro trabajo.

Ahora, consideramos la función representación para introducir algunos conceptos que necesitamos más adelante. Esta función cuenta el número de formas de escribir cualquier elemento de un grupo aditivo G como suma o diferencia de los elementos de dos conjuntos A y B.

Definición 1. Sean, G un grupo abeliano notado aditivamente, A, B subconjuntos de G. Definimos la función representación suma y la función representación diferencia, con dominio en el grupo G y codominio el conjunto de enteros no negativos, de la siguiente manera:

$$R_{A+B}(x) := |\{(a,b) \in A \times B : \ a+b=x\}|, \tag{2.1}$$

$$R_{A-B}(x) := |\{(a,b) \in A \times B : \ a-b=x\}|, \tag{2.2}$$

para $x \in G$.

De la definición anterior se siguen las igualdades:

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

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

donde $x - B := \{x - b : \ b \in B\}$. Dado que por el momento estamos interesados en el estudio de subconjunto finitos de un grupo G, podemos observar que

$$\sum_{x \in G} R_{A+B}(x) = \sum_{x \in G} R_{A-B}(x) = |A||B|.$$

Note que la anterior suma se puede tomar sobre todo $x \in A+B$, puesto que $R_{A+B}(x) = 0$ para $x \notin A+B$. Igualmente sucede si trabajamos con $A - B$.

Finalmente damos a conocer la siguiente notación que será utilizada a lo largo del documento. Algunas veces vamos a describir la magnitud de una función asintóticamente.

Para este propósito mencionamos dos símbolos usados comúnmente, estos son llamados "o"pequeña y "O"grande.

Sean, $f(n)$ y $g(n)$ dos funciones que no son cero para todo n. Decimos que $f(n) = O(g(n))$ si existen constantes $c, m > 0$, independientes de n, tales que $0 < \left|\frac{f(n)}{g(n)}\right| \leq c$, para todo $n > m$. En otras palabras, $\lim_{n\to\infty} \left|\frac{f(n)}{g(n)}\right| \leq c$, si el límite existe.

Decimos que $f(n) = o(g(n))$ si para todo $c > 0$ existe una constante $m > 0$, independientes de n, tal que $\left|\frac{f(n)}{g(n)}\right| < c$, para todo $n > m$. En otras palabras, $\lim_{n\to\infty} \left|\frac{f(n)}{g(n)}\right| = 0$.

2.2. Reglas Golomb o conjuntos de Sidon

Como nuestro principal tema de estudio son las reglas Golomb, necesitamos establecer su equivalencia con los conjuntos de Sidon, para hacerlo procedemos a presentar algunas definiciones.

Definición 2. Sean, G un grupo abeliano notado aditivamente y $a, b, c, d \in G$. La ecuación $x + y = z + w$ la denominamos como ecuación Sidon. Decimos que (a, b, c, d) es una solución trivial de la ecuación de Sidon siempre que $a + b = c + d$ y $\{a, b\} = \{c, d\}$.

Definición 3. Sean, G un grupo abeliano notado aditivamente y $A = \{a_1, a_2, \ldots, a_k\}$ un subconjunto de G. Denominamos al conjunto A como un conjunto B_2 o conjunto de Sidon, si las únicas soluciones en A de la ecuación Sidon son triviales. Equivalentemente, A es un conjunto de Sidon en G, si para todo $x \in G$ no nulo, se cumple que $R_{A-A}(x) \leq 1$.

En otras palabras, un conjunto de Sidon, es aquel cuyas sumas de dos elementos son todas distintas salvo conmutatividad, o aquel que genera diferencias no nulas distintas.

El principal problema que se estudia en la teoría de los conjuntos B_2 en $\mathbb{Z}$ es determinar el mayor número de elementos que un conjunto de Sidon puede tener en el intervalo entero $[1, n]$. Por consiguiente, estudiamos la función

$$F(n) := \text{máx}\{|A| : A \subseteq [1, n],\ A \text{ es } B_2\}. \tag{2.3}$$

Cuando G es un grupo abeliano finito estudiamos la función

$$F(G) := \text{máx}\{|A| : A \subseteq G,\ A \text{ es } B_2\}. \tag{2.4}$$

Si se trabaja en el grupo de enteros modulares $G = \mathbb{Z}_n$, usamos la notación $F(\mathbb{Z}_n)$ y en este caso los conjuntos se denominan conjuntos de Sidon modulares.

Existen tres construcciones clásicas de conjuntos de Sidon modulares que resultan ser maximales; es decir, se conoce el valor exacto de la función $F(\mathbb{Z}_n)$ para infinitos valores de n. Sin embargo, no se conoce el valor exacto de dicha función para todo n, lo cual constituye un problema abierto sobre el cual se ha logrado avanzar muy poco. Las construcciones de los conjuntos de Sidon modulares las daremos más adelante.

Definimos a continuación los conjuntos $B_2^-[g]$ que generalizan el concepto de conjunto de Sidon, en cuanto a permitir la repetición en las diferencias generadas.

Definición 4. Sean, $g \in \mathbb{Z}^+$ y $A \subset \mathbb{Z}$ finito. Decimos que A es un conjunto $B_2^-[g]$ si $R_{A-A}(x) \leq g$, para todo $x \in \mathbb{Z}$ con $x \neq 0$.

Observamos fácilmente que si A es un $B_2^-[1]$ entonces A es un conjunto de Sidon. Los conjuntos $B_2^-[g]$ también se denominan reglas $g-$Golomb [6]. Cuando $g = 1$, la regla $1-$Golomb simplemente se denomina regla Golomb.

2.3. Energía aditiva

Sean, A, B subconjuntos de un grupo G que está notado aditivamente. La cantidad $\sum_{x\in G} R^2_{A+B}(x)$ se denomina la energía aditiva de A y B. Algunas veces se denota con $E(A, B)$ y cuenta el número de soluciones de la ecuación $a + b = a' + b'$ con $a, a' \in A$ y $b, b' \in B$, lo cual equivale a determinar el número de soluciones de la ecuación $a-a' = b'-b$ con $a, a' \in A$ y $b, b' \in B$. Así

$$E(A, B) = \sum_{x\in G} R^2_{A+B}(x) = \sum_{x\in G} R_{A-A}(x)R_{B-B}(x).$$

Para más propiedades y aplicaciones de la energía aditiva, ver [49]. La anterior igualdad se utiliza en la demostración del siguiente lema y más adelante para obtener resultados sobre las reglas $g-$Golomb y sus generalizaciones. A continuación introducimos un lema de Cilleruelo dado en [9] el cual es una aplicación de la energía aditiva y nos permite acotar el cardinal de un conjunto con ciertas propiedades dadas. Aunque Ruzsa [42] lo demostró primero para el caso $g = 1$, fue Cilleruelo quien lo generalizó para todo entero $g \geq 1$.

Lema 2. Sean, G un grupo notado aditivamente, $A, B \subseteq G$ y $g \in \mathbb{Z}^+$. Entonces

$$|A|^2 \leq \frac{|A+B|}{|B|^2} \sum_{x \in G} R_{A-A}(x) R_{B-B}(x). \tag{2.5}$$

En particular, si $R_{A-A}(x) \leq g$ para todo x no nulo, entonces

$$|A|^2 \leq |A+B|\Big(g + \frac{|A|-g}{|B|}\Big). \tag{2.6}$$

Demostración. Ver [9]. □

2.4. Conjuntos de Sidon modulares

La importancia de los conjuntos de Sidon modulares radica en que, en el contexto de los grupos cíclicos se encuentran las únicas construcciones conocidas. Inicialmente estudiamos las funciones relacionadas a los conjuntos de Sidon en $\mathbb{Z}_n$.

La siguiente función relaciona el menor entero positivo n, para el cual $\mathbb{Z}_n$ contiene un conjunto de Sidon de un tamaño fijo.

Definición 5. Sea $k \in \mathbb{Z}^+$. Definimos la función $f^*(k)$ como:

$$f^*(k) := \text{mín}\{n : \exists\ A \subseteq \mathbb{Z}_n, \quad A \quad es \quad Sidon \quad y \quad |A| = k\}. \tag{2.7}$$

Para esta función tenemos la siguiente cota inferior trivial. En $\mathbb{Z}_{f^*(k)}$ existe un conjunto de Sidon de cardinal k. Entonces como todas las diferencias generadas por el conjunto, incluyendo al cero, deben estar contenidas en el grupo, se tiene que:

$$k(k-1) + 1 \leq f^*(k).$$

Los valores conocidos de esta función $f^*(k)$ forman la secuencia $A004136$ en la Online Encyclopedia of Integers Sequences (OEIS) por sus siglas en inglés [47]. Sólo 18 valores de esta función se conocen actualmente y se muestran en la Tabla 2.1.

Por otro lado, tenemos la función $F(\mathbb{Z}_n)$ definida en (2.4) la cual muestra el máximo cardinal que puede tener un conjunto de Sidon en $\mathbb{Z}_n$ para un n fijo. Los valores conocidos de la función $F(\mathbb{Z}_n)$ forman la secuencia $A260999$ en la OEIS [47]. Hasta ahora se

k	1	2	3	4	5	6	7	8	9
$f^*(k)$	1	3	7	13	21	31	48	57	73
k	10	11	12	13	14	15	16	17	18
$f^*(k)$	91	120	133	168	183	255	255	273	307

Tabla 2.1: Valores conocidos de la función $f^*(k)$.

tienen los primeros 295 valores de esta secuencia, además de los valores particulares que proporcionan las tres construcciones de conjuntos de Sidon modulares. En el Capítulo 5 damos algunos aportes sobre la función $F(\mathbb{Z}_n)$.

Ahora, mostramos las construcciones que se conocen de conjuntos de Sidon en $\mathbb{Z}_n$ para infinitos valores de n, que además generan valores exactos de la función $F(\mathbb{Z}_n)$ al ser conjuntos maximales.

2.4.1. Construcción tipo Bose

La construcción de Bose [3], aunque no fue la primera que se conoció, es la más reconocida por su sencillez y permitirá luego mostrar una forma alternativa de construir nuevos conjuntos de Sidon llamados tipo Singer.

Teorema 1. Sean, q una potencia prima y θ un elemento primitivo del campo finito $\mathbb{F}_q^2$. Entonces

$$B(q,\theta) = \{\log_\theta(\theta + a) : a \in \mathbb{F}_q\},$$

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

Demostración. Ver [3]. □

Ejemplo 1. Sean, $q = 7$ y θ un elemento primitivo de $\mathbb{F}_{7^2}$. El conjunto

$$B(7,\theta) = \{1, 10, 29, 31, 35, 36, 46\}$$

es un conjunto de Sidon tipo Bose en el grupo aditivo $\mathbb{Z}_{48}$.

Propiedades de la construcción tipo Bose

Presentamos algunas propiedades que cumplen los conjuntos de Sidon tipo Bose.

Proposición 1. Sean, q una potencia prima, θ un elemento primitivo del campo finito $\mathbb{F}_q^2$ y $B = B(q,\theta)$ un conjunto de Sidon tipo Bose. Entonces

1. $a \not\equiv 0 \,(\text{mód } q+1)$, para todo $a \in B$.
2. Dados $a, b \in B$ distintos, entonces $a \not\equiv b \,(\text{mód } q+1)$.
3. $B \ominus B = \mathbb{Z}_{q^2-1} \setminus M_{q+1}$, donde $M_{q+1} = \{0, q+1, 2(q+1), \ldots, (q-2)(q-1)\}$.
4. $B \,(\text{mód } q+1) := \{a \,(\text{mód } q+1) : a \in B\} = [1, q]$.

Demostración. Ver [5]. □

2.4.2. Construcción tipo Singer

La construcción de Conjuntos de Sidon tipo Singer [46] apareció primero que la construcción tipo Bose [3], pero en este documento se va a presentar como una consecuencia de la construcción tipo Bose.

Teorema 2. Sean, q una potencia prima, θ un elemento primitivo del campo finito $\mathbb{F}_{q^3}$ y $n = q^2 + q + 1$. Entonces

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

es un conjunto de Sidon tipo Singer en $\mathbb{Z}_{q^2+q+1}$ con $q+1$ elementos.

Demostración. Ver [5] □

2.4.3. Construcción tipo Ruzsa

La construcción de conjuntos tipo Ruzsa es una de las construcciones algebraicas más conocidas, la cual apareció por primera vez en 1993 [42]. Esta construcción consiste en hallar primero un conjunto de Sidon en dos dimensiones y a partir de este hallar un conjunto en dimensión uno con $p-1$ elementos contenido en el grupo aditivo $\left(\mathbb{Z}_{p(p-1)}, +\right)$.

Teorema 3. Sean, p un primo y θ un elemento primitivo de $\mathbb{Z}_p$. El conjunto

$$R := \left\{\left(i, \theta^i\right) : 1 \leq i \leq p-1\right\},$$

es un conjunto de Sidon con $p-1$ elementos en el grupo aditivo $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$.

Demostración. Ver [42] □

Ahora por el isomorfismo inducido por el Teorema Chino de los Restos $\mathbb{Z}_{p-1} \times \mathbb{Z}_p \cong \mathbb{Z}_{p(p-1)}$, obtenemos un conjunto B_2 con $p-1$ elementos en el grupo $\mathbb{Z}_{p(p-1)}$. De donde tenemos el siguiente teorema.

Teorema 4. Sean, p un primo y θ un elemento primitivo de $\mathbb{Z}_p$, entonces el conjunto

$$R(\theta, p) := \left\{ x \equiv ip - \theta^i(p-1) \pmod{p^2 - p} : 1 \leq i \leq p-1 \right\},$$

es un conjunto de Sidon con $p-1$ elementos en el grupo aditivo $\mathbb{Z}_{p^2-p}$.

Demostración. Ver [42]. □

Ejemplo 2. Sean, $p = 11$ y $\theta = 2$ una raíz primitiva de $\mathbb{Z}_{11}$. El conjunto

$$R = \{(1,2), (2,4), (3,8), (4,5), (5,10), (6,9), (7,7), (8,3), (9,6), (10,1)\},$$

es un conjunto de Sidon en dos dimensiones en el grupo $\mathbb{Z}_{10} \times \mathbb{Z}_{11}$. Ahora aplicando el isomorfismo definido por el Teorema Chino de los Restos encontramos el conjunto

$$R(2, 11) = \{101,\ 92,\ 63,\ 104,\ 65,\ 86,\ 7,\ 58,\ 39,\ 100\},$$

el cual resulta ser un conjunto de Sidon tipo Ruzsa en el grupo aditivo $\mathbb{Z}_{110}$.

Propiedades de la Construcción tipo Ruzsa

Para el conjunto de Sidon tipo Ruzsa presentamos algunas propiedades. Sea p un número primo, entonces definimos los siguientes conjuntos:

$$M_p = \{x \in \mathbb{Z}_{p^2-p} : x \equiv 0 \pmod{p}\},$$
$$M_{p-1} = \{y \in \mathbb{Z}_{p^2-p} : y \equiv 0 \pmod{p-1}\}.$$

Proposición 2. Sean, p un número primo, θ un elemento primitivo de $\mathbb{Z}_p$ y $R(\theta, p)$ el conjunto de Sidon tipo Ruzsa definido anteriormente. Entonces

1. Si $r \in R(\theta, p)$ entonces $r \not\equiv 0 (\text{mód } p)$.
2. Si $r, r' \in R(\theta, p)$, con $r \neq r'$, entonces $r \not\equiv r' (\text{mód } p)$.

3. Si $r, r' \in R(\theta, p)$, con $r \neq r'$, entonces $r \not\equiv r' (\text{mód}\, p-1)$.
4. $(R(\theta,p) \ominus R(\theta,p)) = \mathbb{Z}_{p^2-p} \setminus (M_p \cup M_{p-1})$.
5. $R(\theta,p)(\text{mód}\, p) = [1, p-1]$.
6. $R(\theta,p)(\text{mód}\, p-1) = [0, p-2]$.

Demostración. Ver [5]. □

2.5. Conjuntos casi diferencia (CCD)

La definición de reglas Golomb o conjuntos de Sidon es muy amplia y por lo tanto, resultan ser casos particulares o generales de otros conceptos en teoría de números. Lo anterior permite generar relaciones con las teorías de dichos objetos y obtener nuevas herramientas para su estudio. Un ejemplo de la anterior afirmación son los Conjuntos Casi Diferencia (CCD), que en inglés se denominan Almost Difference Sets. Los CCD son objetos de interés combinatorio que tienen aplicaciones en varias áreas de ingeniería. En teoría de códigos ellos son empleados para construir códigos cíclicos, en criptografía son usados para construir funciones no-lineales óptimas y en comunicaciones por medio del Acceso Múltiple por División de Código o CDMA (por sus siglas en inglés), algunos CCD cíclicos producen secuencias con autocorrelación óptima [34]. En esta sección revisaremos parte de la teoría de los CCD que utilizaremos más adelante.

Para introducir los CCD recordemos que una regla Golomb se puede definir de la siguiente forma: Sea G un grupo abeliano notado aditivamente. Un subconjunto $D \subset G$ es una regla Golomb si y sólo si $R_{D-D}(x) \leq 1$ para todo $x \in G \setminus \{0\}$. En algunas ocasiones utilizaremos el término $k-$conjunto para referirnos a un conjunto de orden k.

Definición 6. Sean, $n, k \in \mathbb{Z}^+$, $\lambda, t \in \mathbb{Z}^+ \cup \{0\}$ y G un grupo aditivo de orden n. Un $k-$subconjunto $D \subseteq G$ se llama un (n, k, λ, t)-conjunto casi diferencia de G si el multi-conjunto $\{d_1 - d_2 : d_1, d_2 \in D, d_1 \neq d_2\}$ contiene t elementos no nulos de G cada uno exactamente λ veces y los restantes $n-1-t$ elementos no nulos, cada uno exactamente $\lambda+1$ veces.

En otras palabras, $D \subseteq G$ es un (n, k, λ, t)-conjunto casi diferencia ((n, k, λ, t)-CCD) si y sólo si $R_{D-D}(0) = k$ (lo cual significa que D es un k-conjunto), existe un t-conjunto $S \subseteq G \setminus \{0\}$ tal que para cada $x \in S$, $R_{D-D}(x) = \lambda$, y para cada $x \in G \setminus (S \cup \{0\})$ se

cumple que $R_{D-D}(x) = \lambda + 1$. Por definición, si D es un (n, k, λ, t)-CCD en G entonces necesariamente

$$k^2 - k = \lambda t + (\lambda + 1)(n - 1 - t),$$

de donde

$$t = (\lambda + 1)(n - 1) - k(k - 1). \tag{2.8}$$

También, notamos que una regla Golomb o conjunto de Sidon es un $(n, k, 0, t)$-CCD donde $t = (n - 1) - k(k - 1)$.

Ejemplo 3. El conjunto $D = \{0, 1, 3, 4, 14, 16\}$ es un $(21, 6, 1, 10) - CCD$ en $\mathbb{Z}_{21}$. Encontremos las diferencias que genera el conjunto D.

-	0	1	3	4	14	16
0	0	1	3	4	14	16
1	20	0	2	3	13	15
3	18	19	0	1	11	13
4	17	18	20	0	10	12
14	7	8	10	11	0	2
16	5	6	8	9	19	0

Observemos que $S = \{4, 5, 6, 7, 9, 12, 14, 15, 16, 17\}$ y por tanto, $R_{D-D}(x) = 1$ para todo $x \in S$. Mientras que $R_{D-D}(x) = 2$ para todo $x \in \mathbb{Z}_{21} \setminus (S \cup \{0\})$.

Para conocer un poco más sobre los conjuntos casi diferencia se puede consultar [34]. A continuación damos algunos resultados importantes de los CCD que vamos a utilizar a lo largo del Capítulo 5.

Teorema 5. Sean, $(G, +)$ un grupo abeliano de orden n y $D \subset G$ de cardinal k. D es un $(n, k, \lambda, t)-$CCD en G si y sólo si su complemento $D^* = G \setminus D$ es un $(n, n - k, n - 2k + \lambda, t)-$ CCD.

Demostración. Ver [53]. □

En el caso en el que $G = \mathbb{Z}_n$, tenemos el siguiente resultado.

Teorema 6. Sean, $a, b \in \mathbb{Z}_n$ con $mcd(a, n) = 1$. Si D es un (n, k, λ, t)-CCD en $\mathbb{Z}_n$, entonces, el conjunto $aD + b$ es nuevamente un (n, k, λ, t)-CCD.

Demostración. Ver [34] □

En [53], Zhang *et al.* estudiaron algunas condiciones necesarias para la existencia de conjuntos casi diferencia en $\mathbb{Z}_n$. Entre otros resultados, ellos proporcionaron un sistema de ecuaciones diofánticas que se deben satisfacer para que un CCD exista (ver Teorema 7 abajo). Con el fin de complementar el Teorema 7, exponemos la demostración dada en [53] de forma más detallada. Para poder hacerlo con la notación utilizada por ellos, hacemos uso de un anillo que introducimos a continuación. Para un grupo abeliano G sea $\mathbb{Z}[G]$ el anillo de polinomios con términos de la forma aX^g donde $a \in \mathbb{Z}$ y $g \in G$, es decir, resulta ser el anillo de sumas formales

$$\mathbb{Z}[G] = \left\{ \sum_{g \in G} a_g X^g \ : \ a_g \in \mathbb{Z} \right\},$$

donde X es una variable indeterminada. El anillo $\mathbb{Z}[G]$ está dotado de la operación adición dada por

$$\sum_{g \in G} a_g X^g + \sum_{g \in G} b_g X^g = \sum_{g \in G} (a_g + b_g) X^g$$

y la operación multiplicación definida por

$$\left(\sum_{g \in G} a_g X^g \right) \left(\sum_{g \in G} b_g X^g \right) = \sum_{h \in G} \left(\sum_{g \in G} a_g b_{h-g} \right) X^g.$$

Cuando escribimos X^0 estamos denotando con 0 al elemento neutro del grupo G. Luego el elemento neutro y la unidad de $\mathbb{Z}[G]$ son $\sum_{g \in G} 0X^g := 0$ y $X^0 := 1$, respectivamente. Para $D \subseteq G$, definimos

$$D(X) = \sum_{d \in D} X^d$$

y

$$D(X^{-1}) = \sum_{d \in D} X^{-d}$$

donde $-d$ es el elemento inverso de d en G.

Observemos que, por definición, un k-subconjunto $D \subset G$ es un (n, k, λ, t)-CCD si y sólo si

$$D(X)D(X^{-1}) = kX^0 + \lambda S(X) + (\lambda + 1)U(X),$$

donde S es el t-subconjunto de los elementos de G los cuales tienen λ representaciones como diferencias de los elementos en D, y $U = G \setminus (S \cup \{0\})$. Note que, en realidad,

$$D(X)D(X^{-1}) = k + \lambda S(X) + (\lambda + 1)(G(X) - S(X) - 1),$$

de donde podemos deducir que

$$D(X)D(X^{-1}) = k - (\lambda + 1) + (\lambda + 1)G(X) - S(X). \tag{2.9}$$

Ahora, introducimos algo de notación modular. Sea $G = \mathbb{Z}_n$ y consideremos un subgrupo normal $\mathbb{Z}_w$ de $\mathbb{Z}_n$, donde w es un entero positivo tal que $w|n$, y el grupo cociente $\mathbb{Z}_n/\mathbb{Z}_w \cong \mathbb{Z}_{n/w}$. Para cualquier subconjunto $D \subseteq \mathbb{Z}_n$, decimos que

$$D(X) \equiv D'(X) (\text{mód } w),$$

si $D'(X)$ es el polinomio obtenido de $D(X)$ al identificar X^w con $X^0 = 1$. Esta notación es muy útil ya que los coeficientes del polinomio módulo w indican el número de elementos de D en cada una de las clases laterales de $\mathbb{Z}_w$.

Ejemplo 4. Como vimos en el Ejemplo 3, el conjunto $D = \{0, 1, 3, 4, 14, 16\}$ es un $(21, 6, 1, 10)$-CCD en $\mathbb{Z}_{21}$. Aplicando la anterior notación tenemos que

$$D(X) = X^0 + X^1 + X^3 + X^4 + X^{14} + X^{16},$$

$$D(X^{-1}) = X^0 + X^{20} + X^{18} + X^{17} + X^7 + X^5.$$

Además, al calcular $D(X)D(X^{-1})$ obtenemos

$$D(X)D(X^{-1}) \equiv 6X^0 + 2(G(X) - X^0) - S(X) \text{ (mód } 21)$$

donde $S(X) = X^4 + X^5 + X^6 + X^7 + X^9 + X^{12} + X^{14} + X^{15} + X^{16} + X^{17}$.

Teorema 7 (Teorema 3.3 en [53])**.** Sean, $n, k \in \mathbb{Z}^+$ y $\lambda \in \mathbb{Z}^+ \cup \{0\}$. Si existe un (n, k, λ, t)-CCD en $\mathbb{Z}_n$ entonces, para cualquier entero positivo w tal que $w|n$, existen enteros no negativos $b_0, ..., b_{w-1}$ y $c_0, ..., c_{w-1}$, los cuales satisfacen el siguiente sistema de ecuaciones,

$$\sum_{i=0}^{w-1} b_i = k, \tag{2.10}$$

$$\sum_{i=0}^{w-1} c_i = t, \tag{2.11}$$

$$\sum_{i=0}^{w-1} b_i^2 = (k - \lambda - 1) + (\lambda + 1)\frac{n}{w} - c_0, \tag{2.12}$$

y, para cada $1 \leq j \leq w - 1$,

$$\sum_{i=0}^{w-1} b_i b_{j-i} = (\lambda+1)\frac{n}{w} - c_j, \tag{2.13}$$

donde los subíndices de b_{j-i} se toman módulo w.

Demostración. Sea $D = \{d_1, d_2, ..., d_k\}$ un (n, k, λ, t)-CCD en $\mathbb{Z}_n$, y sea $S = \{s_1, s_2, ..., s_t\}$ el conjunto de elementos en $\mathbb{Z}_n$ que aparecen λ veces como diferencia de los elementos en D. Sea

$$D(X) \equiv b_0X^0 + b_1X^1 + \cdots + b_{w-1}X^{w-1} \pmod{w},$$

y

$$S(X) \equiv c_0X^0 + c_1X^1 + \cdots + c_{w-1}X^{w-1} \pmod{w}.$$

Entonces, $b_i = |\{d \in D : d \equiv i \pmod{w}\}|$ y $c_i = |\{s \in S : s \equiv i \pmod{w}\}|$ para cada $0 \leq i \leq w-1$. Así las ecuaciones (2.10) y (2.11) se satisfacen.

Ahora, de (2.9), tenemos que

$$\begin{aligned} D(X)D(X^{-1}) &= k - (\lambda+1) + (\lambda+1)G(X) - S(X) \\ &\equiv k - (\lambda+1) + (\lambda+1)\frac{n}{w}\sum_{i=0}^{w-1} X^i - \sum_{i=0}^{w-1} c_iX^i \pmod{w} \\ &\equiv k - (\lambda+1) + (\lambda+1)\frac{n}{w} - c_0 + \sum_{j=1}^{w-1}\left((\lambda+1)\frac{n}{w} - c_j\right)X^j \pmod{w}. \end{aligned} \tag{2.14}$$

Para completar la demostración, notemos que

$$D(X^{-1}) \equiv b_0X^0 + b_1X^{-1} + \cdots + b_{w-1}X^{-(w-1)} \pmod{w},$$

por lo tanto

$$\begin{aligned} D(X)D(X^{-1}) &= \left(\sum_{i=0}^{w-1} b_iX^i\right)\left(\sum_{i=0}^{w-1} b_iX^{-i}\right) \pmod{w} \\ &\equiv \sum_{j=0}^{w-1}\left(\sum_{i=0}^{w-1} b_ib_{i-j}\right)X^j \pmod{w} \\ &\equiv \sum_{i=0}^{w-1} b_i^2X^0 + \sum_{j=1}^{w-1}\left(\sum_{i=0}^{w-1} b_ib_{i-j}\right)X^j \pmod{w}. \end{aligned} \tag{2.15}$$

La identificación de los coeficientes de (2.14) y (2.15) proporciona (2.12) y (2.13). □

Ejemplo 5. Retomando el $(21, 6, 1, 10)$-CCD en $\mathbb{Z}_{21}$ del Ejemplo 4 y si tomamos $w = 3$, al modular tenemos que

$$S(X) \equiv 4X^0 + 3X + 3X^2 \ (\text{mód } 3),$$

donde $c_0 = 4$, $c_1 = 3$ y $c_2 = 3$ satisfacen la ecuación (2.11). Para verificar que se cumplen todas las ecuaciones del Teorema 7 calculamos

$$D(X) \equiv 2X^0 + 3X + X^2 \ (\text{mód } 3),$$

donde $b_0 = 2$, $b_1 = 3$ y $b_2 = 1$, que claramente satisfacen (2.10), (2.12) y (2.13).

En conclusión, si fijamos los parámetro de un (n, k, λ, t)-CCD en el grupo $\mathbb{Z}_n$, por cada divisor de n obtenemos un sistema de ecuaciones dado por (2.10), (2.11), (2.12) y (2.13). Entonces, si dicho sistema no tiene soluciones enteras significa que el conjunto casi diferencia no existe.

Ejemplo 6. En $\mathbb{Z}_{80}$ no existe un $(80, 13, 1, 2)$-CCD. Para mostrar este resultado aplicamos el Teorema 7 con $w = 2$. Obtenemos entonces las ecuaciones

$$b_0 + b_1 = 13$$

$$c_0 + c_1 = 2$$

$$b_o^2 + b_1^2 = 13 - 2 + 2(40) - c_0 = 69 - c_0$$

$$2b_0b_1 = 80 - c_1.$$

Fácilmente chequeamos que el sistema anterior no tiene soluciones enteras no negativas. Así, por el Teorema 7 no existe dicho CCD.

Observación 1. Cuando $G = \mathbb{Z}_n$ con n par y $w = 2$, entonces en el sistema de ecuaciones del Teorema 7, tenemos que (2.10), (2.11), y (2.13) implican (2.12).

Para demostrar la anterior afirmación veamos que las ecuaciones diofánticas cuando $w = 2$ son las siguientes:

$$b_0 + b_1 = k, \tag{2.16}$$

$$c_0 + c_1 = t, \tag{2.17}$$

$$b_0^2 + b_1^2 = k - \lambda - 1 + (\lambda + 1)\frac{n}{2} - c_0, \tag{2.18}$$

$$2b_0b_1 = (\lambda + 1)\frac{n}{2} - c_1. \tag{2.19}$$

Ahora, vamos a mostrar que (2.18) se puede conseguir, a partir de (2.16), (2.17) y (2.19). Iniciamos elevando al cuadrado (2.16)

$$b_0^2 + 2b_0b_1 + b_1^2 = k^2,$$

de donde,

$$b_0^2 + b_1^2 = k^2 - 2b_0b_1.$$

Reemplazamos (2.19) en la anterior igualdad y tenemos

$$b_0^2 + b_1^2 = k^2 - (\lambda + 1)\frac{n}{2} + c_1.$$

De (2.17) tenemos que $c_1 = t - c_0$, por lo tanto

$$b_0^2 + b_1^2 = k^2 - (\lambda + 1)\frac{n}{2} + t - c_0,$$

finalmente reemplazamos $k^2 + t = (\lambda + 1)n - (\lambda + 1) + k$ que se obtiene de (2.8).

$$b_0^2 + b_1^2 = (\lambda + 1)n - (\lambda + 1) + k - (\lambda + 1)\frac{n}{2} - c_0$$

$$b_0^2 + b_1^2 = k - \lambda - 1 + (\lambda + 1)\frac{n}{2} - c_0.$$

Finalizando así la prueba de nuestra afirmación.

Otro concepto relacionado a los conjuntos casi diferencia y claramente a las reglas Golomb, es el de Conjuntos Diferencia.

Definición 7. Sea G un grupo notado aditivamente de orden n. Un $k-$subconjunto $D \subseteq G$ es llamado un (n, k, λ) conjunto diferencia si el multiconjunto $\{d_1 - d_2 : d_1, d_2 \in D, d_1 \neq d_2\}$ contiene cada elemento no nulo de G exactamente λ veces.

Claramente, si $t = n - 1$ o $t = 0$, un $(n, k, \lambda, t)-$CCD resulta ser un conjunto diferencia. Así, los conjuntos diferencia son casos particulares de los CCD. Si $\lambda = 1$, el conjunto diferencia es llamado planar, la construcción de conjuntos de Sidon tipo Singer demuestra la existencia de conjuntos diferencia planar cuando $k-1$ es una potencia prima. Conjuntos diferencia para $\lambda > 1$ han sido construidos por varios autores [34]. La Conjetura de Potencias Primas establece que: un entero $k \geq 2$ es el orden de un conjunto diferencia planar, si y solo si $k - 1$ es una potencia prima [22].

2.6. Teoría de Ramsey

La teoría de Ramsey recibe este nombre en honor al extraordinario matemático Frank Plumpton Ramsey quién probó en 1928 un teorema fundamental para esta rama de la matemática, dicho resultado fue publicado de forma póstuma en 1930. Pero Ramsey no creó ni desarrolló la teoría que lleva su nombre, que fue iniciada por Erdös y Szekeres en 1933. Tiempo después descubrieron la conexión con lo trabajos de Ramsey, que en este contexto habían pasado desapercibidos.

Aunque no existe una definición universalmente aceptada para la teoría de Ramsey, en algunos textos la describen como: La teoría de Ramsey es el estudio de la preservación de propiedades bajo particiones. En otras palabras, dado un conjunto S el cual tiene una propiedad P, es verdad que siempre que S sea particionado un número finito de veces en subconjuntos, uno de los subconjuntos debe también tener la propiedad P.

En está sección vamos a definir las bases para la investigación que desarrollamos en el Capítulo 5 que relaciona la teoría de Ramsey y los conjuntos de Sidon. Las particiones a las que nos referimos más adelante las vamos definir a continuación como coloraciones.

Definición 8. Sean, S un conjunto no vacío y $r \in \mathbb{Z}^+$. Una $r-$coloración del conjunto S es una función $\chi : S \to [1, r]$.

Podemos pensar en una $r-$coloración χ de un conjunto S como una partición de S en r subconjuntos $S_1, S_2, \ldots, S_r$, podemos definir cada subconjunto S_i como el conjunto $\{x \in S,\, \chi(x) = i\}$. Cada uno de los conjuntos S_i los denominamos clases cromáticas.

Definición 9. Sean, S un conjunto no vacío y χ una coloración de S. Decimos que χ es monocromática sobre el conjunto S si χ es constante sobre S.

En el Capítulo 5 vamos a hacer referencia a soluciones monocromáticas de una ecuación e incluso sistemas de ecuaciones. Si ξ representa una ecuación dada o un sistema de ecuaciones, llamaremos a $(x_1, x_2, \ldots, x_k)$ una solución monocromática de ξ si $x_1, x_2, \ldots, x_k$ tienen todas el mismo color, es decir, pertenecen a la misma clase cromática y satisfacen ξ. Las soluciones de una ecuación o un sistema de ecuaciones se diferencian en triviales y no triviales, esta característica depende del tipo de ecuación con la que se esté trabajando.

En el Capítulo 5 y en el caso de la ecuación Sidon vamos a considerar como soluciones triviales a aquellas que se establecieron en la Definición 2.

2.7. Reglas Golomb disjuntas (RGD)

El problema de encontrar reglas Golomb disjuntas, una generalización del problema de reglas Golomb, fue inicialmente considerado por Chen en la localización de radio-frecuencias móviles para una colección de áreas en las cuales se eliminaban las interferencias de intermodulación de tercer orden en cada área [7]. Actualmente las reglas Golomb disjuntas se utilizan en la construcción de códigos auto-ortogonales y códigos ortogonales ópticos. Decimos que una colección de v reglas Golomb disjuntas dos a dos (abreviadas como RGD) que están contenidas en el intervalo $[1, n]$ y cada una compuesta por w elementos, es una $(v, w)-$RGD.

Definición 10. Sean, $v, w \in \mathbb{Z}^+$ y $D_i \subseteq \mathbb{Z}$ para cada $i \in [1, v]$. Si los v conjuntos son disjuntos dos a dos y cada D_i es una regla Golomb con w marcas, entonces definimos a la colección

$$D := \{D_1, D_2, ..., D_v\},$$

como $(v, w)-$ Reglas Golomb Disjuntas. Si cada D_i es una regla Golomb modular, entonces D se denomina $(v, w)-$Reglas Golomb Modulares Disjuntas ($(v, w)-$RGMD).

Sea D una $(v, w)-$RGD, donde los $D_i = \{a_{ij} : \ 1 \leq j \leq w\}$, $1 \leq i \leq v$, entonces definimos

$$h = h(D) = \text{máx}\{a_{ij} : \ a_{ij} \in D_i, \ 1 \leq i \leq v, \ 1 \leq j \leq w\}.$$

Son de gran interés las reglas Golomb disjuntas con h lo más cercano posible a vw, es por esto que se estudia la siguiente función:

$$H(v, w) := \text{mín}\{h(D) : \quad D \text{ es una } (v, w) - RGD\}.$$

Si D es una $(v, w)-$RGD tal que $h(D) = H(v, w) = vw$, entonces D es llamada regular. En el caso modular una colección de $(v, w)-$RGMD, se denomina regular si resulta ser regular al ser considerada como un conjunto de RGD enteras. Kløve probó que existe una cota $\iota(w)$ que garantiza la existencia de una regla Golomb disjunta regular para todo $v \geq \iota(w)$, también propuso varias construcciones de RGD y mostró una tabla con valores exactos y cotas para $H(v, w)$ que pueden ser revisadas en [24]. Dichos valores fueron mejorados y extendidos por Shearer con asistencia computacional en [45]. Luego, nuevas construcciones de RGD regulares fueron proporcionadas por W. Chen, Z. Chen y Kløve en [7]. Finalmente, Liang et al proponen una serie de conjeturas sobre las RGD e intentan mejorar los valores de $\iota(w)$ en [51].

Nosotros establecemos cotas inferiores para el Número Sidon-Ramsey $SR(r)$, que será estudiado en el Capítulo 5, basados en resultados conocidos de RGD regulares. Por

ejemplo, si $H(v,w) = vw$, entonces $SR(v) \geq vw + 1$. Kløve en [24] propuso algunas construcciones de reglas Golomb disjuntas, entre las cuales está el siguiente teorema que permite construir RGD regulares.

Teorema 8. Sean, $w, n \in \mathbb{Z}^+$ y $A = \{a_1, a_2, \ldots, a_w\} \subseteq \mathbb{Z}_n$ un conjunto de Sidon. Se define $D := \{D_i, 1 \leq i \leq w\}$, donde

$$D_i := (A - a_i \,(\text{mód } n)) \setminus \{0\}.$$

Entonces, D es una $(w, w-1)-$RGMD y $h(D) \leq n - 1$.

Demostración. Ver [24]. □

Corolario 1. Sea q una potencia prima y A el conjunto diferencia planar de Singer en $\mathbb{Z}_{q^2+q+1}$. Entonces A proporciona una $(v,w)-$RGMD regular con $v = q+1$ y $w = q$, por lo tanto, $H(q+1, q) = q^2 + q$.

Demostración. Ver [24]. □

Ejemplo 7. Sea $q = 4$ y el conjunto $A = \{0, 1, 4, 14, 16\}$ un conjunto de Sidon tipo Singer en $\mathbb{Z}_{21}$. Ahora aplicando el Corolario 1 tenemos los siguientes conjuntos

$$\begin{aligned}
D_1 =& (A - 0 \pmod{21}) \setminus \{0\} = \{1, 4, 14, 16\} \\
D_2 =& (A - 1 \pmod{21}) \setminus \{0\} = \{20, 3, 13, 15\} \\
D_3 =& (A - 4 \pmod{21}) \setminus \{0\} = \{17, 18, 10, 12\} \\
D_4 =& (A - 14 \pmod{21}) \setminus \{0\} = \{7, 8, 11, 2\} \\
D_5 =& (A - 16 \pmod{21}) \setminus \{0\} = \{5, 6, 9, 19\}.
\end{aligned}$$

luego, $D = \{D_1, D_2, D_3, D_4, D_5\}$ es una $(5,4)-$RGMD que tiene $h(D) = 20 = H(5,4)$ y por lo tanto es una $(5,4)-$RGD regular.

Con ayuda de la construcción de conjuntos de Sidon de Ruzsa en el Capítulo 5, damos una nueva construcción de Reglas Golomb Disjuntas que resultan ser regulares.

Capítulo 3

Reglas g-Golomb

En este capítulo estudiamos la definición de reglas $g-$Golomb óptimamente densas y óptimamente cortas al igual que algunos resultados al respecto. Lo anterior con el propósito de mostrar que las reglas $g-$Golomb óptimamente densas se distribuyen bien en intervalos enteros y en clases residuales. También mostramos una cota superior para el cardinal de una regla $g-$Golomb contenida en progresiones aritméticas que tienen la misma diferencia. Con este resultado logramos proporcionar una cota superior para la máxima distancia que pueden tener dos elementos consecutivos de una regla $g-$Golomb.

A continuación ejemplificamos la Definición 4 de reglas $g-$Golomb.

Ejemplo 8. El siguiente conjunto es una regla $2-$Golomb,

$$A = \{0, 2, 3, 7, 9, 12, 13\}.$$

En la siguiente tabla verificamos que las diferencias generadas por elementos distintos de A se repiten a lo sumo 2 veces.

-	0	2	3	7	9	12	13
0	0	2	3	7	9	12	13
2	-2	0	1	5	7	10	11
3	-3	-1	0	4	6	9	10
7	-7	-5	-4	0	2	5	6
9	-9	-7	-6	-2	0	3	4
12	-12	-10	-9	-5	-3	0	1
13	-13	-11	-10	-6	-4	-1	0

No es difícil probar que la propiedad de ser regla g-Golomb se mantiene bajo traslación y dilatación por enteros.

Proposición 3. Sean, $u, t \in \mathbb{Z}$ con $u \neq 0$. Si A es una regla g-Golomb, entonces el conjunto $uA + t$ es también una regla g-Golomb.

La propiedad de traslación, permite suponer que una regla g-Golomb A tiene su primera marca en cero, $a_1 = 0$, y que su longitud es igual a su máximo elemento, $a_m = \ell(A)$. Estas se llaman reglas g-Golomb canónicas.

3.1. Reglas g-Golomb óptimas

Al igual que con las reglas Golomb existe un problema fundamental en el estudio de las reglas g-Golomb, en el cual se trata de hallar reglas óptimamente densas y óptimamente cortas. Estas reglas las definimos a continuación.

Definición 11. Sean, $n, m \in \mathbb{Z}^+$ y A una regla g-Golomb.

1. $A \subseteq [1, n]$ se llama óptimamente densa en $[1, n]$, si tiene el mayor número posible de marcas, es decir, todo subconjunto de $[1, n]$ de tamaño $|A| + 1$ no es una regla $g-$Golomb.
2. A se llama óptimamente corta si tiene la menor longitud posible para un número de marcas dado m.

En este capítulo vamos a mostrar características importantes que tienen las reglas $g-$Golomb óptimamente densas.

3.1.1. Reglas g-Golomb óptimamente cortas

En el caso de las reglas g-Golomb óptimamente cortas, es importante considerar la siguiente definición.

Definición 12. La mínima longitud de las reglas g-Golomb con m marcas, se define como

$$\mathfrak{G}(g, m) := \text{mín}\left\{\ell\left(A\right) : A \text{ es una regla } g\text{-Golomb}, |A| = m\right\}.$$

Encontrar valores exactos de la función $\mathfrak{G}(g,m)$ es un problema difícil, aún con la capacidad computacional actual. En cuanto a $\mathfrak{G}(1,m)$ hasta el momento se conocen valores exactos para todo $m \leq 27$, los cuales se han encontrado mediante búsqueda computacional [37]. Los algoritmos utilizados son básicamente exhaustivos ("fuerza bruta"), debido a que no existe hasta el momento una alternativa eficiente ni teórica ni computacional que permita calcular el valor exacto de $\mathfrak{G}(g,m)$. Así, la única forma para determinar si una regla g-Golomb es óptimamente corta consiste en presentar una regla g-Golomb candidata y después verificar mediante búsqueda computacional que no existen reglas g-Golomb de longitud menor para el número de marcas dado.

Debido a los pocos valores conocidos de la función $\mathfrak{G}(1,m)$ y a que la dificultad de encontrar nuevos valores se incrementa cada vez más, es importante determinar cotas superiores e inferiores para esta función, y en general para $\mathfrak{G}(g,m)$. Dimitromanolakis en el año 2002 probó computacionalmente que $\mathfrak{G}(1,m) \leq m^2$ para todo $m \leq 65000$ [14].

Una forma de obtener una cota superior para la función $\mathfrak{G}(g,m)$ es exhibir una regla g-Golomb A con m marcas. Note que si A es una regla $g-$Golomb canónica, entonces

$$\mathfrak{G}(g,m) \leq \max A = a_m.$$

Así, las cotas superiores para $\mathfrak{G}(g,m)$ se obtienen a partir de "buenas construcciones".

De otro lado, es fundamental determinar cotas inferiores para la función $\mathfrak{G}(g,m)$. Una cota inferior se obtiene contando diferencias. Si A es una regla g-Golomb canónica con m marcas, el mínimo número de diferencias positivas que se repiten hasta g veces es

$$\left\lfloor \frac{m(m-1)}{2g} \right\rfloor,$$

las cuales deben estar contenidas en el conjunto $\{1,2,\ldots,\ell(A)=a_m\}$. Entonces lo peor que puede ocurrir es que ese número de diferencias sea igual a a_m, esto es:

$$a_m \geq \left\lfloor \frac{m(m-1)}{2g} \right\rfloor.$$

Como se tomó una regla g-Golomb arbitraria, lo mismo es válido para la de menor longitud, esto es:

$$\mathfrak{G}(g,m) \geq \left\lfloor \frac{m(m-1)}{2g} \right\rfloor \text{ (cota trivial).}$$

Para el caso $g=1$, Atkinson, Santoro y Urrutia en [1] presentaron la cota inferior de la siguiente proposición.

Proposición 4. Sea $A = \{0, a_1, \ldots, a_m\}$ una regla Golomb con $m+1$ marcas. Entonces

$$a_m \geq m^2 - 2m\sqrt{m}.$$

Demostración. Ver [1]. □

En su tesis de maestría, Dimitromanolakis [14], utilizando la equivalencia entre el concepto de regla Golomb y conjunto de Sidon, estableció algunas relaciones entre reglas Golomb óptimamente cortas y conjuntos de Sidon óptimamente densos, y utilizando la cota superior para estos últimos dada en [18], mejoró la cota de la Proposición 4. Él demuestra que para todo entero positivo m

$$\mathfrak{G}(1, m) > m^2 - 2m\sqrt{m} + \sqrt{m} + 2.$$

Caicedo, Martos y Trujillo en [6] prueban la cota inferior dada por:

$$\mathfrak{G}(g, m) \geq \frac{m^2}{g} - \frac{2m\sqrt{m-g}}{g} + \frac{m}{g} - \frac{m}{\sqrt{m-g}} - 1.$$

También prueban que, para cada entero $g \geq 1$, se tiene

$$\lim_{m\to\infty} \frac{\mathfrak{G}(g, m)}{m^2} = \frac{1}{g}.$$

3.1.2. Reglas g-Golomb óptimamente densas

En el estudio de las reglas g-Golomb otro problema fundamental es hallar el mayor cardinal que puede tener una regla $g-$Golomb contenida en un intervalo entero $[1, n]$. Estas reglas se llaman óptimamente densa. En este caso vamos a estimar la función:

$$F^-(g, n) := \text{máx}\left\{|A| : A \subseteq [1, n]\,,\ \text{A es una regla } g\text{-Golomb}\right\}.$$

En cuanto a esta función es importante estudiar su comportamiento asintótico, esto es estudiar el límite

$$\lim_{n\to\infty} \frac{F^-(g, n)}{(gn)^{1/2}}.$$

En [6], [28] y [50] se prueba que

$$F^-(g,n) \leq (gn)^{\frac{1}{2}} + (gn)^{\frac{1}{4}} + 1, \tag{3.1}$$

además, en [6] y [50] logran demostrar que $F^-(g,n)$ se comporta asintóticamente como $(1+o(1))\sqrt{gn}$, es decir,

$$\lim_{n\to\infty} \frac{F^-(g,n)}{\sqrt{n}} = \sqrt{g}.$$

3.2. Distribución de las reglas $g-$Golomb óptimamente densas

Con ayuda de las cotas conocidas para la función $F^-(g,n)$, vamos a realizar un estudio sobre cómo se distribuyen las reglas $g-$Golomb óptimamente densas en el intervalo entero $[1,n]$. Dentro del estudio de las reglas $1-$Golomb surgió la pregunta de como se distribuían las reglas Golomb óptimamente densas contenidas en un intervalo entero. En 1991 Erdös y Freud [16] mostraron algunos teoremas sobre conjuntos de Sidon (reglas $1-$Golomb), dentro de los cuales está un lema que muestra la distribución uniforme de los conjuntos de Sidon maximales en el intervalo $[1,n]$. Luego Graham [23] obtuvo este mismo resultado pero de forma más precisa. Posteriormente Lindström [29], Kolountzakis [25], y Cilleruelo [9] mostraron con diferentes herramientas que los conjuntos de Sidon densos se distribuyen de manera uniforme sobre clases residuales. Todo lo anterior nos motivo a estudiar la distribución de reglas $g-$Golomb en intervalos enteros, en progresiones aritméticas disjuntas que tienen la misma diferencia y en clases residuales. A continuación mostramos nuestros resultados. Está sección hacen parte del artículo [13] que está en preparación.

En esta sección vamos a utilizar la siguiente observación.

Observación 2. Sean, $t \in \mathbb{Z}^+$ y $a, b \in \mathbb{Z}$.

i) Si e_a es el número de enteros m tales que $a \in m + [0,t]$, entonces

$$e_a = t + 1.$$

ii) Si $e_{a,b}$ es el número de enteros m tales que $a, b \in m + [0,t]$, entonces

$$e_{a,b} \leq \text{máx}\{t + 1 - |a-b|, 0\}.$$

El resultado sobre la distribución de conjuntos de Sidon maximales en $[0, n]$ que obtuvieron Erdös y Freud es el siguiente teorema.

Teorema 9 (Lema 1 en [16])**.** Sean, $n \in \mathbb{Z}^+$ y $c \in (0, 1)$. Para cualquier conjunto de Sidon $A \subset [0, n]$ con $|A| = (1 + o(1))n^{1/2}$, se tiene que

$$|A \cap [0, cn]| = (c + o(1))n^{1/2}.$$

Ahora mostramos nuestro resultado que resulta ser una generalización del Teorema 9 para reglas $g-$Golomb.

Teorema 10. Sean, $n \in \mathbb{Z}^+$ y $c \in (0, 1)$. Para cualquier regla $g-$Golomb $A \subset [0, n]$ con $|A| = (1 + o(1))(gn)^{1/2}$, se tiene que

$$|A \cap [0, cn]| = (c + o(1))(gn)^{1/2}.$$

Demostración. Sea $t = \left\lfloor \left(\dfrac{(cn)^{1/2}}{2g} \right)^{1/3} \right\rfloor$. Para todo $m \in \mathbb{Z}$ definimos

$$A_m := A \cap (m + [0, t]).$$

También, a partir de cada A_m, definimos el multiconjunto $\mathbf{B}_m = A_m \ominus A_m$, donde la repetición de los elementos importa. Por último denotamos

$$e = \sum_{m \in \mathbb{Z}} |\mathbf{B}_m|.$$

Para la demostración vamos a acotar e superiormente, luego inferiormente y de la comparación de las dos cotas vamos a obtener el resultado deseado.

Para cualquiera $a, b \in A$, sea $E_{a,b} := \{m \in \mathbb{Z} : \ a, b \in A_m\}$. De la Observación 2 *ii*), se sigue

$$|E_{a,b}| \leq \text{máx}\{t + 1 - |a - b|, 0\}. \tag{3.2}$$

Ahora, aunque A es una regla $g-$Golomb, cada pareja de elementos $a, b \in A$ distintos es única, y por tanto la diferencia generada por a y b, $a - b$, está contada en $\sum_{m \in \mathbb{Z}} |\mathbf{B}_m|$ el mismo número de elementos que tiene el conjunto $E_{a,b}$, es decir, $|E_{a,b}|$ por tanto

$$e = \sum_{m \in \mathbb{Z}} |\mathbf{B}_m| = \sum_{a,b \in A,\, a \neq b} |E_{a,b}|. \tag{3.3}$$

Sean, $a, b \in A$ distintos. Note que $|E_{a,b}| = 0$ a menos que $|a-b| \leq t$. Luego, si $|E_{a,b}| \neq 0$, la diferencia $a-b$ es un número entre $[-t, t]$. Reemplazando lo anterior en (3.2) obtenemos

$$\sum_{a,b\in A,\, a\neq b} |E_{a,b}| \leq \sum_{a,b\in A,\, a\neq b} \text{máx}\{t+1-|a-b|, 0\}.$$

Observemos ahora que cada diferencia no nula generada por un par de elementos de A, con $|a-b| \leq t$, se encuentra exactamente en $t+1-|a-b|$ traslaciones del intervalo $[0, t]$. Además, considerando que A es una regla $g-$Golomb, la diferencia $a-b$ se puede repetir hasta $g-$veces por lo tanto,

$$\begin{aligned}
\sum_{a,b\in A,\, a\neq b} \text{máx}\{t+1-|a-b|, 0\} &\leq \sum_{j\in[-t,t]} g(t+1-|j|) \\
&\leq \sum_{j\in[0,t+1]} 2g(t+1-j) \\
&= \sum_{j\in[0,t+1]} 2gj \\
&= g(t+1)(t+2) \\
&= (1+o(1))gt^2. \qquad (3.4)
\end{aligned}$$

De (3.3) y (3.4), concluimos que

$$e \leq (1+o(1))gt^2. \qquad (3.5)$$

Sea $I := \{m \in \mathbb{Z} : \ A_m \neq \emptyset\}$. Dado que estamos considerando los multiconjuntos $\mathbf{B}_m = A_m \ominus A_m$, entonces

$$\begin{aligned}
e &= \sum_{m\in\mathbb{Z}} |\mathbf{B}_m| \\
&= \sum_{m\in I} |\mathbf{B}_m| \\
&= \sum_{m\in I} |A_m|(|A_m|-1) \\
&= \left(\sum_{m\in I} |A_m|^2 - \sum_{m\in I} |A_m|\right) \\
&= (1+o(1)) \sum_{m\in I} |A_m|^2. \qquad (3.6)
\end{aligned}$$

Definimos ahora $q := \lfloor cn \rfloor$ y los conjuntos

$$\begin{aligned} J &:= [-t, q-t] & L &:= [-t, q] \\ K &:= [-t, n] \setminus [-t, q-t] & M &:= [-t, n] \setminus [-t, q]. \end{aligned}$$

Por un lado, debido a que $A \cap (J + [0,t]) \subseteq A \cap [0,q]$, tenemos que

$$\sum_{m \in J} |A_m| \leq (t+1)|A \cap [0,q]|.$$

Por otro lado, la Observación 2 *i)* y la inclusión $[0,q] \subseteq L + [0,t]$ implican que cada $a \in A \cap [0,q]$ puede estar en a lo más $t+1$ conjuntos A_m con $m \in L$ así

$$(t+1)|A \cap [0,q]| \leq \sum_{m \in L} |A_m|.$$

Lo mismo se puede hacer para $|A \cap ([0,n] \setminus [0,q])|$ obteniendo que

$$\begin{aligned} &\sum_{m \in J} |A_m| \leq (t+1)|A \cap [0,q]| \leq \sum_{m \in L} |A_m| \quad \text{y} \\ &\sum_{m \in M} |A_m| \leq (t+1)|A \cap ([0,n] \setminus [0,q])| \leq \sum_{m \in K} |A_m|. \end{aligned} \tag{3.7}$$

Ahora, definimos los conjuntos $C := [q-t+1, q] = L \setminus J$ y $D := C + [0,t]$. Si aplicamos nuevamente la Observación 2 i), concluimos que cada $a \in A \cap D$ puede estar en máximo $t+1$ conjuntos A_m con $m \in C$. Luego

$$\sum_{m \in C} |A_m| \leq (t+1)|A \cap D| \leq (t+1)(1+o(1))(2gt)^{1/2}. \tag{3.8}$$

La última desigualdad se cumple ya que $A \cap D$ es una regla $g-$Golomb contenida en el intervalo $[q-t+1, q+t]$.

Además, como $t \leq \left(\dfrac{q^{1/2}}{2g}\right)^{1/3}$, la anterior desigualdad nos lleva a

$$(t+1)(1+o(1))(2gt)^{1/2} \leq (1+o(1))(2g)^{1/2}\Big(\frac{q^{1/2}}{2g}\Big)^{1/2} = (1+o(1))q^{1/4}$$

y por lo tanto

$$\sum_{m \in L \setminus J} |A_m| = o(q^{1/2}). \tag{3.9}$$

De igual manera,

$$\sum_{m\in K\setminus M}|A_m| = o(q^{1/2}). \tag{3.10}$$

De (3.7), (3.9) y (3.10), obtenemos que

$$\begin{aligned}\sum_{m\in J}|A_m| &= (1+o(1))t|A\cap[0,q]|,\\ \sum_{m\in K}|A_m| &= (1+o(1))t|A\cap([0,n]\setminus[0,q])|.\end{aligned} \tag{3.11}$$

Sea $f := \dfrac{|A\cap[0,q]|}{(gn)^{1/2}}$, Entonces de (3.11) se sigue que

$$\begin{aligned}\sum_{m\in J}|A_m| &= (1+o(1))tf(gn)^{1/2},\\ \sum_{m\in K}|A_m| &= (1+o(1))t(1-f)(gn)^{1/2}.\end{aligned} \tag{3.12}$$

Dado que $A\subseteq[0,n]$, observamos que $I\subseteq J\cup K$. Además, por la definición de I y dado que $J\cap K=\emptyset$, entonces $\{m\in J : A_m\neq\emptyset\}\cup\{m\in K : A_m\neq\emptyset\} = I$. De lo anterior y de (3.6) tenemos que

$$\begin{aligned}e \geq&(1+o(1))\sum_{m\in I}|A_m|^2\\ =&(1+o(1))\left(\sum_{m\in J}|A_m|^2+\sum_{m\in K}|A_m|^2\right).\end{aligned} \tag{3.13}$$

Aplicando la desigualdad de Cauchy-Schwarz a las sumatorias de (3.13), encontramos que

$$\begin{aligned}\sum_{m\in J}|A_m|^2 &\geq \frac{(\sum_{m\in J}|A_m|)^2}{|J|},\\ \sum_{m\in K}|A_m|^2 &\geq \frac{(\sum_{m\in K}|A_m|)^2}{|K|},\end{aligned}$$

y por tanto (3.12) nos lleva a

$$\begin{aligned}\sum_{m\in J}|A_m|^2 &\geq (1+o(1))\frac{f^2}{c}gt^2,\\ \sum_{m\in K}|A_m|^2 &\geq (1+o(1))\frac{(1-f)^2}{(1-c)}gt^2.\end{aligned} \tag{3.14}$$

Usando (3.13) y (3.14), tenemos que

$$e \geq (1+o(1))gt^2\left(\frac{f^2}{c}+\frac{(1-f)^2}{(1-c)}\right). \tag{3.15}$$

Comparando (3.5) y (3.15) se sigue que

$$1 \geq \frac{f^2}{c}+\frac{(1-f)^2}{(1-c)},$$

luego

$$0 \geq f^2-2fc+c^2=(f-c)^2.$$

Por lo tanto, $c=f$ y esto concluye la demostración. □

Cilleruelo [8] logró aproximar la máxima distancia que pueden tener dos elementos consecutivos de dicha regla; ésta distancia se denomina el gap de la regla Golomb.

Definición 13. Sea $A=\{a_1,a_2,\ldots,a_k\}$ un conjunto finito contenido en $\mathbb{Z}$. Definimos la máxima distancia que separa dos elementos consecutivos de A como:

$$\mathfrak{g}(A)=\text{máx}_{i\in[2,k]}\{a_i-a_{i-1}\}.$$

Cilleruelo en [8] afirma que como consecuencia del Teorema B de Graham en [23], toda regla Golomb A contenida en $[1,n]$ de cardinal $n^{1/2}+O(n^{1/4})$ satisface la desigualdad $\mathfrak{g}(A)\ll n^{7/8}$. En el mismo trabajo Cilleruelo precisa más el Teorema 9 y como consecuencia de éste demuestra que: Si A es una regla Golomb contenida en $[1,n]$ de tamaño $|A|=n^{1/2}+O(n^{1/4})$, entonces $\mathfrak{g}(A)\ll n^{3/4}$.

En el año 2010, Cilleruelo [9] establece una cota superior para el cardinal de las reglas Golomb contenidas en progresiones aritméticas que tengan la misma diferencia y a partir de este resultado logró precisar de forma más acertada la cota superior para el gap de una regla Golomb.

Teorema 11 (Teorema 2 en [9])**.** Sean, A una regla Golomb y $P_1,P_2,\ldots,P_k$ progresiones aritméticas disjuntas de la misma diferencia con longitudes $n_1,n_2,\ldots,n_k$ respectivamente. Si se cumple que $A\subseteq\bigcup_{i=1}^{k}P_i$, entonces

$$|A|<(n_1+n_2+\cdots+n_k)^{1/2}+k^{1/2}(n_1+n_2+\cdots+n_k)^{1/4}+\frac{1}{2}.$$

El anterior resultado de Cilleruelo lo hemos logrado generalizar para reglas $g-$Golomb y lo mostramos a continuación.

Teorema 12. Sean, A una regla $g-$Golomb y $P_1, P_2, \ldots, P_k$ progresiones aritméticas disjuntas de la misma diferencia con longitudes $n_1, n_2, \ldots, n_k$ respectivamente. Si se cumple que $A \subseteq \bigcup_{i=1}^{k} P_i$, entonces

$$|A| < g^{1/2}(n_1 + n_2 + \cdots + n_k)^{1/2} + k^{1/2} g^{1/4}(n_1 + n_2 + \cdots + n_k)^{1/4} + \frac{1}{2}.$$

Demostración. Definimos $A_i := A \cap P_i$ para $i \in [1, k]$, luego

$$A = \bigcup_{i=1}^{k} A_i.$$

Sea d la diferencia común de las progresiones aritméticas y sea B el conjunto definido por $B := d[0, l]$ para algún entero positivo l que será fijado más adelante. Ahora vamos a aplicar la desigualdad (2.5) que nos permite relacionar los cardinales de los conjuntos A_i, B y $A_i + B$ de la siguiente forma. Para cada i tenemos que

$$|A_i|^2 \leq \frac{|A_i + B|}{|B|^2} \sum_{x \in (A_i - A_i) \cap (B - B)} R_{A_i - A_i}(x) R_{B-B}(x)$$
$$\frac{|A_i|^2}{|A_i + B|} \leq \frac{1}{|B|^2} \sum_{x \in (A_i - A_i) \cap (B - B)} R_{A_i - A_i}(x) R_{B-B}(x),$$

Sumando la desigualdad para todo $i \in [1, k]$

$$\begin{aligned}
\sum_{i=1}^{k} \frac{|A_i|^2}{|A_i + B|} &\leq \frac{1}{|B|^2} \sum_{x \in (A_i - A_i) \cap (B - B)} \sum_{i=1}^{k} R_{A_i - A_i}(x) R_{B-B}(x) \\
&= \frac{1}{|B|^2} \left(\sum_{i=1}^{k} R_{A_i - A_i}(0) R_{B-B}(0) + \sum_{\substack{x \in (A_i - A_i) \cap (B - B) \\ x \neq 0}} \sum_{i=1}^{k} R_{A_i - A_i}(x) R_{B-B}(x) \right) \\
&= \frac{1}{|B|^2} \left(\sum_{i=1}^{k} |A_i||B| + \sum_{\substack{x \in (A_i - A_i) \cap (B - B) \\ x \neq 0}} \sum_{i=1}^{k} R_{A_i - A_i}(x) R_{B-B}(x) \right).
\end{aligned}$$

Dado que $\sum_{i=1}^{k} R_{A_i - A_i}(x) \leq R_{A-A}(x) \leq g$ para todo $x \in \mathbb{Z} \setminus \{0\}$, ya que A es una regla

$g-$Golomb, se deduce que

$$\sum_{i=1}^{k}\frac{|A_i|^2}{|A_i+B|}\leq\frac{1}{|B|^2}\left(|A||B|+g\sum_{\substack{x\in B-B\\ x\neq 0}}R_{B-B}(x)\right),$$
$$\leq\frac{1}{|B|^2}\left(|A||B|+g(|B|^2-|B|)\right),$$
$$\leq g+\frac{|A|-g}{|B|}. \tag{3.16}$$

Por otra parte, observemos que

$$|A|^2=\left(\sum_{i=1}^{k}|A_i|\right)^2=\left(\sum_{i=1}^{k}\sqrt{|A_i+B|}\frac{|A_i|}{\sqrt{|A_i+B|}}\right)^2,$$

ahora si aplicamos la desigualdad de Cauchy-Schwarz tenemos

$$|A|^2\leq\sum_{i=1}^{k}|A_i+B|\sum_{i=1}^{k}\frac{|A_i|^2}{|A_i+B|},$$

y teniendo en cuenta (3.16) en la anterior desigualdad nos lleva a

$$|A|^2\leq\sum_{i=1}^{k}|A_i+B|\left(g+\frac{|A|-g}{|B|}\right)$$
$$\leq\sum_{i=1}^{k}|P_i+B|\left(g+\frac{|A|-g}{l+1}\right).$$

Ahora, para cada i, se cumple que P_i y B son progresiones aritméticas de la misma diferencia. Entonces, $|P_i+B|=n_i+l$ y además si denotamos $n=n_1+n_2+\cdots+n_k$, entonces tenemos que

$$|A|^2<(n+kl)\Big(g+\frac{|A|-g}{l+1}\Big)$$
$$<gn+gkl+n\Big(\frac{|A|-g}{l+1}\Big)+k(|A|-g). \tag{3.17}$$

Tomando $l=\left\lfloor\sqrt{\dfrac{n(|A|-g)}{gk}}\right\rfloor$ y reemplazando en (3.17) encontramos que

$$|A|^2<gn+2\sqrt{gnk(|A|-g)}+k(|A|-g)$$
$$|A|^2<\left(\sqrt{gn}+\sqrt{k(|A|-g)}\right)^2.$$

Por lo tanto,

$$|A| < \sqrt{gn} + \sqrt{k(|A| - g)}. \tag{3.18}$$

Ahora, si $|A| = (gn)^{1/2} + c(gn)^{1/4} + \frac{1}{2}$ y lo reemplazamos en (3.18), obtenemos

$$\Big((gn)^{1/2} + c(gn)^{1/4} + \frac{1}{2} - (gn)^{1/2}\Big)^2 < k\Big((gn)^{1/2} + c(gn)^{1/4} + \frac{1}{2} - g\Big)$$

$$\Big(c(gn)^{1/4} + \frac{1}{2}\Big)^2 < k\Big((gn)^{1/2} + c(gn)^{1/4} + \frac{1-2g}{2}\Big),$$

lo cual no se puede cumplir para $c \geq \sqrt{k}$ y de ahí se sigue el resultado. □

Como consecuencia del Teorema 12 establecemos a continuación una cota superior para la máxima distancia que pueden tener dos elementos consecutivos en una regla $g-$Golomb.

Corolario 2. Sean, $c, c_0 \in \mathbb{R}$ y A una regla $g-$Golomb contenida en el intervalo entero $[1, n]$. Entonces el gap de A, $\mathfrak{g}(A)$ satisface la desigualdad

$$\mathfrak{g}(A) < \frac{gn - |A|(|A|^{1/2} - \sqrt{2})^2}{g}.$$

En particular, si $c_0 < |A|$ y $|A| \geq (gn)^{1/2} + c(gn)^{1/4}$, entonces tenemos que

$$\mathfrak{g}(A) < \frac{2(2\sqrt{2} - c)(gn)^{3/4} + O(gn)^{1/2}}{g}.$$

Demostración. Supongamos que la máxima distancia que separa a dos elementos consecutivos de A es $l+1$. Consideremos el intervalo $[m,\ m+l+1]$ el cual contiene a dicho gap y las siguientes progresiones aritméticas de diferencia 1, $P_1 = [1, m]$ y $P_2 = [m+l+1, n]$ de longitudes $n_1 = m$ y $n_2 = n - m - l$ respectivamente. Por el Teorema 12 obtenemos

$$\begin{aligned} |A| &< g^{1/2}(n_1 + n_2)^{1/2} + g^{1/4}\sqrt{2}(n_1 + n_2)^{1/4} + \frac{1}{2} \\ &= g^{1/2}(n-l)^{1/2} + g^{1/4}\sqrt{2}(n-l)^{1/4} + \frac{1}{2} \\ &= \Big(g^{1/4}(n-l)^{1/4} + \frac{1}{\sqrt{2}}\Big)^2. \end{aligned}$$

Luego,

$$\begin{aligned}
|A|^{1/2} &< g^{1/4}(n-l)^{1/4} + \frac{1}{\sqrt{2}} \\
|A|^{1/2} - \frac{1}{\sqrt{2}} &< g^{1/4}(n-l)^{1/4} \\
\left(|A|^{1/2} - \frac{1}{\sqrt{2}}\right)^4 &< g(n-l) \\
\left(|A| - \sqrt{2}|A|^{1/2} + \frac{1}{2}\right)^2 &< g(n-l) \\
\left(|A|^{1/2}(|A|^{1/2} - \sqrt{2})\right)^2 &< g(n-l).
\end{aligned}$$

De donde

$$l < \frac{gn - |A|\left(|A|^{1/2} - \sqrt{2}\right)^2}{g}. \tag{3.19}$$

Queda entonces demostrada la primera parte del Corolario.

Por otra parte, denotamos $N = gn$. Por hipótesis $N^{1/2} + cN^{1/4} \leq |A|$. Reemplazando la desigualdad en (3.19) tenemos

$$\begin{aligned}
l &< \frac{N - (N^{1/2} + cN^{1/4})\left((N^{1/2} + cN^{1/4})^{1/2} - \sqrt{2}\right)^2}{g} \\
&= \frac{N - (N^{1/2} + cN^{1/4})\left((N^{1/2} + cN^{1/4}) - 2\sqrt{2}(N^{1/2} + cN^{1/4})^{1/2} + 2\right)}{g} \\
&= \frac{N - (N^{1/2} + cN^{1/4})^2 + 2\sqrt{2}(N^{1/2} + cN^{1/4})^{3/2} - 2(N^{1/2} + cN^{1/4})}{g},
\end{aligned}$$

por tanto

$$l < \frac{-2cN^{3/4} - c^2N^{1/2} + 2\sqrt{2}(N^{1/2} + cN^{1/4})^{3/2} - 2N^{1/2} - 2cN^{1/4}}{g}. \tag{3.20}$$

También por hipótesis tenemos que $c_0 < |A|$. Basta con tomar a c_0 suficientemente grande para que se cumpla la desigualdad $(N^{1/2} + cN^{1/4})^{3/2} \leq 2(N^{3/4} + cN^{3/8})$. Así, al

reemplazarla en (3.20) nos permite concluir que

$$\begin{aligned} l &\leq \frac{4\sqrt{2}(N^{3/4}+cN^{3/8})-2cN^{3/4}-(c^2+2)N^{1/2}-2cN^{1/4}}{g} \\ &= \frac{2(2\sqrt{2}-c)N^{3/4}-(c^2+2)N^{1/2}+4\sqrt{2}cN^{3/8}-2cN^{1/4}}{g}. \end{aligned}$$

De donde,

$$\mathfrak{g}(A) < \frac{2(2\sqrt{2}-c)(gn)^{3/4}+O(gn)^{1/2}}{g}.$$

□

El exponente 3/4 que se obtiene en el Corolario 2 se puede alcanzar en situaciones donde se cumplan sus hipótesis. Por ejemplo, de la construcción de reglas $g-$Golomb de Caicedo, Martos y Trujillo en el Teorema 3.5 de [6], conocemos que existen reglas de cardinal $(gn)^{1/2}$ contenidas en el intervalo $[1,n]$. Sea A una regla $g-$Golomb contenida en $[1,n]$ con $|A|=(gn)^{1/2}$. Si dividimos este intervalo en $n^{1/4}/c$ intervalos de longitud $cn^{3/4}$, tenemos que por lo menos uno de los subintervalos debe contener no más que $cg^{1/2}n^{1/4}$ elementos de la regla $g-$Golomb. Si quitamos estos elementos de A, obtenemos una nueva regla $g-$Golomb A' con $|A'|\geq (gn)^{1/2}-c'(gn)^{1/4}$, la cual tiene un gap de longitud $cn^{3/4}$. Cilleruelo también había notado esta observación con su resultado sobre gaps de reglas $1-$Golomb en [9].

El resultado más preciso sobre la buena distribución de las reglas Golomb en clases residuales se debe a Cilleruelo [9] y lo enunciamos a continuación. Este resultado mejora lo que obtuvieron Kolountzakis en [25] y Lindström en [29].

Teorema 13 (Teorema 3 en [9])**.** Sean, $n,q\in\mathbb{Z}^+$, $l\in\mathbb{Z}$, con $q<n^{1/2}$ y $A\subset[1,n]$ una regla Golomb con $|A|\geq n^{1/2}-l$. Si definimos $A_i:=\{a\in A\,:\,a\equiv i(\text{mód}\,q)\}$ con $i\in[1,q]$, entonces

i) $\displaystyle\sum_{i=1}^{q}\Big(|A_i|-\frac{|A|}{q}\Big)^2\leq\frac{4ln^{1/2}}{q}+\frac{8n^{3/4}}{q^{1/2}}.$

ii) $\displaystyle|A_i|=\frac{|A|}{q}+\theta\Big(\frac{\text{máx}\{0,l\}^{1/2}n^{1/4}}{q^{1/2}}+\frac{n^{3/8}}{q^{1/4}}\Big)$, para algún $\theta\in\mathbb{R}$ con $|\theta|<3$.

iii) Si $\displaystyle q<\frac{n^{1/6}}{100}$ y $l<n^{1/3}$, entonces A contiene todas las clases residuales módulo q.

En el siguiente resultado mostramos que las reglas $g-$Golomb también están bien distribuidas en clases residuales.

Teorema 14. Sean, $g, n, q \in \mathbb{Z}^+$, $l \in \mathbb{Z}$, con $q < (gn)^{1/2}$ y $A \subset [1, n]$ una regla $g-$Golomb con $|A| \geq (gn)^{1/2} - l$. Si definimos $A_i := \{a \in A : a \equiv i(\text{mód } q)\}$ con $i \in [1, q]$, entonces

i) $\displaystyle\sum_{i=1}^{q} \left(|A_i| - \frac{|A|}{q}\right)^2 \leq \frac{4l(gn)^{1/2}}{q} + \frac{8(gn)^{3/4}}{q^{1/2}}.$

ii) $\displaystyle|A_i| = \frac{|A|}{q} + \theta\Big(\frac{\text{máx}\{0, l\}^{1/2}(gn)^{1/4}}{q^{1/2}} + \frac{(gn)^{3/8}}{q^{1/4}}\Big)$, para algún $\theta \in \mathbb{R}$ con $|\theta| < 3$.

iii) Si $\displaystyle q < \frac{(gn)^{1/6}}{100}$ y $l < (gn)^{1/3}$, entonces A contiene todas las clases residuales módulo q.

Demostración. Inicialmente descomponemos la regla $g-$Golomb A en clases residuales distintas $A = \cup_{i=1}^{q} A_i$ donde

$$A_i = A \cap (q \cdot [0, \lfloor n/q \rfloor] + i), \quad i \in [1, q].$$

Ahora, sean $t \in \mathbb{Z}^+$ y $B = q \cdot [1, t]$. Note que $|A_i + B| \leq \lfloor n/q \rfloor + t$. Reemplazando los cardinales de los conjuntos A, B y $A_i + B$ con $i \in [1, q]$ en la desigualdad (3.16), tenemos

$$\sum_{i=1}^{q} |A_i|^2 \leq \left(\left\lfloor \frac{n}{q} \right\rfloor + t\right)\left(g + \frac{|A| - g}{t}\right). \tag{3.21}$$

Si tomamos $t = \left\lfloor \sqrt{\dfrac{|A|n}{gq}} \right\rfloor$ y reemplazamos su valor en (3.21) obtenemos

$$\sum_{i=1}^{q} |A_i|^2 < \frac{gn}{q} + 2\sqrt{\frac{gn|A|}{q}} + |A|. \tag{3.22}$$

Por otro lado, observemos que

$$\begin{aligned}\sum_{i=1}^{q} \left(|A_i| - \frac{|A|}{q}\right)^2 &= \sum_{i=1}^{q} \left(|A_i|^2 - 2\frac{|A_i||A|}{q} + \frac{|A|^2}{q^2}\right) \\ &= \sum_{i=1}^{q} |A_i|^2 - 2\frac{|A|}{q}\sum_{i=1}^{q} |A_i| + \sum_{i=1}^{q} \frac{|A|^2}{q^2} \\ &= \sum_{i=1}^{q} |A_i|^2 - 2\frac{|A|^2}{q} + \frac{|A|^2}{q}.\end{aligned}$$

Por tanto

$$\sum_{i=1}^{q}\left(|A_i|-\frac{|A|}{q}\right)^2=\sum_{i=1}^{q}|A_i|^2-\frac{|A|^2}{q}. \tag{3.23}$$

Reemplazamos (3.22) en (3.23) y encontramos

$$\sum_{i=1}^{q}\left(|A_i|-\frac{|A|}{q}\right)^2<\frac{gn-|A|^2}{q}+2\sqrt{\frac{gn|A|}{q}}+|A|.$$

Por hipótesis tenemos que $|A|\geq (gn)^{1/2}-l$, luego $-|A|^2\leq -gn+2l(gn)^{1/2}$. Como consecuencia de (3.1) podemos usar la estimación trivial $|A|<4(gn)^{1/2}$. Al reemplazar estos dos resultados en la anterior desigualdad obtenemos

$$\begin{aligned}\sum_{i=1}^{q}\left(|A_i|-\frac{|A|}{q}\right)^2&<\frac{4l(gn)^{1/2}}{q}+4\sqrt{\frac{(gn)^{3/2}}{q}}+4(gn)^{1/2}\\&<\frac{4l(gn)^{1/2}}{q}+\frac{8(gn)^{3/4}}{q^{1/2}}.\end{aligned}$$

La última desigualdad se cumple ya que $q<(gn)^{1/2}$. Así queda demostrado i).

Para probar ii) observamos inicialmente que

$$\left||A_i|-\frac{|A|}{q}\right|=\sqrt{\left(|A_i|-\frac{|A|}{q}\right)^2}$$

y entonces

$$\left||A_i|-\frac{|A|}{q}\right|\leq\sqrt{\sum_{i=1}^{q}\left(|A_i|-\frac{|A|}{q}\right)^2}. \tag{3.24}$$

Teniendo en cuenta que l puede ser negativo o positivo, podemos escribir la parte i) de la siguiente manera

$$\sum_{i=1}^{q}\left(|A_i|-\frac{|A|}{q}\right)^2<\frac{4\text{máx}\{0,l\}(gn)^{1/2}}{q}+\frac{8(gn)^{3/4}}{q^{1/2}}. \tag{3.25}$$

Reemplazando (3.25) en (3.24) encontramos que

$$\left||A_i|-\frac{|A|}{q}\right|\leq\left(\frac{4\text{máx}\{0,l\}(gn)^{1/2}}{q}+\frac{8(gn)^{3/4}}{q^{1/2}}\right)^{1/2}$$

$$\leq \frac{2\text{máx}\{0,\text{l}\}^{1/2}(gn)^{1/4}}{q^{1/2}} + \frac{2^{3/2}(gn)^{3/8}}{q^{1/4}}. \tag{3.26}$$

De lo anterior afirmamos que

$$\left||A_i| - \frac{|A|}{q}\right| = \theta\left(\frac{\text{máx}\{0,l\}^{1/2}(gn)^{1/4}}{q^{1/2}} + \frac{(gn)^{3/8}}{q^{1/4}}\right)$$

para algún $\theta \in \mathbb{R}$ con $|\theta| < 3$ y así queda demostrado *ii*).

Para probar *iii*) vamos a utilizar reducción al absurdo. Supongamos que tenemos al menos una clase residual A_i vacía. Se sigue entonces que

$$\frac{(gn)^{1/2} - l}{q} = \left|\frac{|A|}{q}\right| = \left||A_i| - \frac{|A|}{q}\right|.$$

Aplicamos ahora (3.26) y obtenemos

$$\frac{(gn)^{1/2} - l}{q} \leq \frac{2\,\text{máx}\{0,l\}^{1/2}(gn)^{1/4}}{q^{1/2}} + \frac{2^{3/2}(gn)^{3/8}}{q^{1/4}}.$$

Supongamos ahora que $\text{máx}\{0,l\} = l$ ya que en caso contrario la prueba se sigue de igual manera. Entonces

$$\begin{aligned}(gn)^{1/2} - l \leq& q^{1/4}\left(2l^{1/2}(gn)^{1/4}q^{1/4} + 2^{3/2}(gn)^{3/8}q^{1/2}\right)\\ =& 2l^{1/2}(gn)^{1/4}q^{1/2} + 2^{3/2}(gn)^{3/8}q^{3/4}.\end{aligned}$$

Ahora dado que $q < \dfrac{(gn)^{1/6}}{100}$ y $l < (gn)^{1/3}$, tenemos que

$$\begin{aligned}(gn)^{1/2} - (gn)^{1/3} &< 2(gn)^{1/6}(gn)^{1/4}\frac{(gn)^{1/12}}{10} + 2^{3/2}(gn)^{3/8}\frac{(gn)^{1/8}}{10^{3/2}}\\ &= \frac{(gn)^{1/2}}{5} + \frac{(gn)^{1/2}}{5^{3/2}}\\ &< \frac{2}{5}(gn)^{1/2}\end{aligned}$$

luego

$$\frac{3}{5}(gn)^{1/2} < (gn)^{1/3},$$

lo que claramente es una contradicción ya que $100 < (gn)^{1/6}$ como consecuencia de que $q \in \mathbb{Z}^+$ y $q < \dfrac{(gn)^{1/6}}{100}$. Quedando así demostrado *iii*). □

Observemos que el item *iii*) del Teorema 14 está ajustado a las constantes establecidas. Para ver esto, tomemos nuevamente una regla $g-$Golomb A de cardinal $(gn)^{1/2}$ en $[1,n]$. Ahora, consideremos el módulo $q=[(gn)^{1/6}]$. Entonces existe $r\in[0,q-1]$ tal que $A_r=\{a\in A\,:\,a\equiv r\,(\text{mód}\,q)\}$ y $|A_r|\leq(gn)^{1/3}$. Sea $A'=A\setminus A_r$. El conjunto A' es una regla $g-$Golomb y satisface que $|A'|\geq(gn)^{1/2}-(gn)^{1/3}$ pero una de las clases residuales módulo q, con $q\sim(gn)^{1/6}$ no aparece en los elementos de A'.

Capítulo 4

Arreglos g-Golomb

Aunque el concepto de regla Golomb fue establecido en el grupo de los números enteros se puede cambiar su grupo ambiente, no obstante observamos que su definición nuevamente coincide con la de un conjunto de Sidon. Pero al permitir la repetición de las diferencias generadas por un conjunto obtenemos un nuevo concepto que difiere de los conjuntos de Sidon y sus generalizaciones. Este es el caso por ejemplo, de las reglas $g-$Golomb que estudiamos en el capítulo anterior.

En la literatura encontramos que se han estudiado las reglas $g-$Golomb en grupos diferentes al de los números enteros. Pero la mayoría de trabajos no muestran relación alguna con las reglas $g-$Golomb como se puede evidenciar desde su denominación. Es por esto que consideramos oportuno unificar estos conceptos alrededor de los arreglos $g-$Golomb que fueron estudiados inicialmente por Robinson en [39].

En este capítulo establecemos la definición formal de los arreglos $g-$Golomb o reglas Golomb generalizadas contenidas en un grupo abeliano cualquiera. Con esta definición queremos mostrar que muchos conceptos particulares que existen en la literatura son en realidad arreglos $g-$Golomb. Adicionalmente mostramos algunos resultados que obtuvimos.

Definición 14. Sean, G un grupo abeliano notado aditivamente y $A \subseteq G$ no vacío. Decimos que A es un arreglo $g-$Golomb en G, si para todo $x \in G$ no nulo, se cumple que:

$$R_{A-A}(x) \leq g.$$

En otras palabras, cuando $G = \mathbb{Z}$ resulta que el arreglo $g-$Golomb es una regla $g-$Golomb. Mientras que cuando $g = 1$ estamos trabajando con un conjunto de Sidon contenido en el grupo G. Casos particulares de arreglos $g-$Golomb en $\mathbb{Z} \times \mathbb{Z}$ fueron introducidos por Costas en [10] y posteriormente por Golomb y Taylor en [21]; estos se denominaron arreglos Costas y secuencias sonar, respectivamente. El primer estudio de los arreglos $1-$Golomb en $\mathbb{Z} \times \mathbb{Z}$ fue realizado por Robinson en [38], en esta ocasión los denominó rectángulos Golomb. Más adelante el mismo Robinson introdujo el concepto de arreglo $1-$Golomb en el grupo $\mathbb{Z}^d$ [39]. Por otra parte, Zhang et al. en [53] dieron construcciones de casos particulares de arreglos $g-$Golomb en los grupos $\mathbb{Z}_4 \times \mathbb{F}_q$ y $\mathbb{F}_p \times \mathbb{F}_q$, pero bajo el nombre de conjuntos casi diferencia. Para estudiar más sobre los arreglos $g-$Golomb, puede consultar [1, 21, 39, 43].

4.1. Arreglos $g-$Golomb óptimos

En el caso de los arreglos $g-$Golomb encontramos que su problema fundamental se centra en determinar el máximo cardinal que puede tener un arreglo $g-$Golomb contenido en un subconjunto del grupo G.

Definición 15. Sean, G un grupo abeliano notado aditivamente, $D \subseteq G$ y $\mathcal{F}$ la familia de los arreglos $g-$Golomb contenidos en D. Decimos que $A \subseteq D$ es un arreglo g-Golomb óptimo en D si $|A| = \max_{F \in \mathcal{F}} |F|$.

Para el estudio de los arreglos $g-$Golomb óptimos contenidos en G, definimos a continuación la función $F^-(g, D)$ para $D \subseteq G$.

$$F^-(g, D) := \max \{|A| : A \subseteq D, \text{ A es un arreglo } g\text{-Golomb}\}.$$

4.2. Arreglos $g-$Golomb en $\mathbb{Z}^d$

En esta sección vamos a presentar los resultados que obtuvimos al estudiar los arreglos $g-$Golomb en $\mathbb{Z}^d$ donde encontramos como casos particulares los aportes que se conocen para $g = 1$. Iniciamos entonces con el estudio de la función $F^-(g, D)$ para $D = [1, n_1] \times \cdots \times [1, n_d]$, que será denotada $F^-(g, n_1, \ldots, n_d)$. En particular, cuando $D = [1, n]^d$ escribimos $F_d^-(g, n)$.

Teorema 15. Sean, $d, n_1, n_2, \ldots, n_d \in \mathbb{Z}^+$. Si A es un arreglo $g-$Golomb contenido en $[1, n_1] \times [1, n_2] \times \cdots \times [1, n_d]$, entonces $|A| \leq (g^{1/2} + o(1))(n_1 n_2 \cdots n_d)^{1/2}$.

Demostración. Si $B = [1, u_1] \times [1, u_2] \times \cdots \times [1, u_d]$, entonces $|B| = \prod_{i=1}^{d} u_i$. Además $A + B \subseteq [1, n_1 + u_1] \times [1, n_2 + u_2] \times \cdots \times [1, n_d + u_d]$ y por tanto $|A + B| \leq \prod_{i=1}^{d}(n_i + u_i)$. Denotamos $|A| = k$. Ahora aplicamos (2.6) del Lema 2 que nos permite relacionar los cardinales de los conjuntos A, $A + B$ y B de la siguiente manera:

$$\begin{aligned} k^2 \leq & \prod_{i=1}^{d}(n_i + u_i)\left(g + \frac{k-g}{\prod_{i=1}^{d} u_i}\right) \\ \leq & \prod_{i=1}^{d}(n_i + u_i)\left(g + \frac{k}{\prod_{i=1}^{d} u_i}\right) \\ \leq & g\prod_{i=1}^{d}(n_i + u_i) + \frac{k\prod_{i=1}^{d}(n_i + u_i)}{\prod_{i=1}^{d} u_i} \\ \leq & g\prod_{i=1}^{d}(n_i + u_i) + k\prod_{i=1}^{d}\left(\frac{n_i}{u_i} + 1\right). \end{aligned}$$

De lo anterior se sigue que

$$k^2 - k\prod_{i=1}^{d}\left(\frac{n_i}{u_i} + 1\right) \leq g\prod_{i=1}^{d}(n_i + u_i),$$

de donde

$$k^2 - \frac{1}{2}2k\prod_{i=1}^{d}\left(\frac{n_i}{u_i} + 1\right) + \frac{1}{4}\prod_{i=1}^{d}\left(\frac{n_i}{u_i} + 1\right)^2 \leq g\prod_{i=1}^{d}(n_i + u_i) + \frac{1}{4}\prod_{i=1}^{d}\left(\frac{n_i}{u_i} + 1\right)^2.$$

Por tanto

$$\left(k - \frac{1}{2}\prod_{i=1}^{d}\left(\frac{n_i}{u_i} + 1\right)\right)^2 \leq g\prod_{i=1}^{d}(n_i + u_i) + \frac{1}{4}\prod_{i=1}^{d}\left(\frac{n_i}{u_i} + 1\right)^2.$$

En consecuencia

$$k - \frac{1}{2}\prod_{i=1}^{d}\left(\frac{n_i}{u_i} + 1\right) \leq g^{1/2}\prod_{i=1}^{d}(n_i + u_i)^{1/2} + \frac{1}{2}\prod_{i=1}^{d}\left(\frac{n_i}{u_i} + 1\right),$$

lo cual implica

$$k \leq g^{1/2}\prod_{i=1}^{d}(n_i + u_i)^{1/2} + \prod_{i=1}^{d}\left(\frac{n_i}{u_i} + 1\right). \tag{4.1}$$

Tomando $u_i = n_i^{2/3}$ para $i \in [1, d]$, de (4.1) obtenemos que

$$k \leq g^{1/2} \prod_{i=1}^{d} (n_i + n_i^{2/3})^{1/2} + \prod_{i=1}^{d} \left(n_i^{1/3} + 1 \right),$$

de donde

$$k \leq g^{1/2}(1 + o(1)) \prod_{i=1}^{d} n_i^{1/2} = (g^{1/2} + o(1))(n_1 n_2 \cdots n_d)^{1/2}.$$

□

En otras palabras, del anterior teorema concluimos que

$$F^-(g, n_1, \ldots, n_d) \leq (g^{1/2} + o(1))(n_1 n_2 \cdots n_d)^{1/2}. \tag{4.2}$$

Observemos que con $d = 1$ tenemos la cota superior de las reglas $g-$Golomb que encontraron Caicedo et al. en [6], a saber

$$F^-(g, n) \leq (g^{1/2} + o(1))n^{1/2}.$$

Además, si $g = 1$, nuestro resultado se reduce a la cota superior

$$F^-(1, n_1, \ldots, n_d) \leq (1 + o(1))(n_1 n_2 \cdots n_d)^{1/2},$$

establecida por Cilleruelo en [9] para los conjunto de Sidon. Finalmente, cuando $g = 1$ y $n_1 = n_2 = \cdots = n_d = n$, se cumple que

$$F_d^-(1, n) \leq (1 + o(1))n^{d/2},$$

cota encontrada por Lindström en [28].

Por otro lado, se puede establecer una cota inferior de la función $F^-(g, n_1, n_2, \ldots, n_d)$ con una fácil generalización del Teorema 5 de Cilleruelo en [9] que utiliza un mapeo natural de reglas $1-$Golomb en $\mathbb{Z}$ hacia arreglos $1-$Golomb en $\mathbb{Z}^d$. Con la generalización del resultado se puede establecer que

$$F^-(g, n_1 n_2 \ldots n_d) \leq F^-(g, n_1, n_2, \ldots, n_d). \tag{4.3}$$

Como referenciamos en el Capítulo 3, en [6] se estableció el comportamiento asintótico de la función $F^-(g, n)$ y por tanto podemos decir que

$$F^-(g, n_1 n_2 \ldots n_d) = (g^{1/2} + o(1))(n_1 n_2 \ldots n_d)^{1/2}.$$

Reemplazando esta última igualdad en (4.3) tenemos que

$$(g^{1/2}+o(1))(n_1n_2\cdots n_d)^{1/2} \leq F^-(g,n_1,n_2,\ldots,n_d). \tag{4.4}$$

Ahora, de (4.2) y (4.4) concluimos que

$$F^-(g,n_1,n_2,\ldots,n_d) = (g^{1/2}+o(1))(n_1n_2\cdots n_d)^{1/2}. \tag{4.5}$$

En particular, cuando $n_1 = n_2 = \cdots = n_d = n$ tenemos que

$$F_d^-(g,n) = (g^{1/2}+o(1))n^{d/2}.$$

4.3. Distribución de los arreglos $g-$Golomb óptimos

En esta sección vamos a generalizar los resultados del Capítulo 3 sobre la distribución de las reglas $g-$Golomb óptimas, pero ahora para arreglos $g-$Golomb óptimos. Vamos a mostrar inicialmente que los arreglos $g-$Golomb óptimos se distribuyen bien en los cubos $d-$dimensionales $[0,n]^d$. Introducimos a continuación una observación que utilizamos más adelante.

Observación 3. Sean, $t,d \in \mathbb{Z}^+$ y $a=(a_1,a_2,\ldots,a_d)$, $b=(b_1,b_2,\ldots,b_d) \in \mathbb{Z}^d$.

i) Si e_a es el número de puntos $m \in \mathbb{Z}^d$ tales que $a \in m+[0,t]^d$, entonces

$$e_a = (t+1)^d.$$

ii) Si $e_{a,b}$ es el número de puntos $m \in \mathbb{Z}^d$ tales que $a,b \in m+[0,t]^d$, entonces

$$e_{a,b} \leq \prod_{i=1}^{d}(\text{máx}\{t+1-|a_i-b_i|,0\}).$$

Ahora mostramos nuestro resultado que resulta ser una generalización del Teorema 10 para arreglos $g-$Golomb.

Teorema 16. Sean, $n,d \in \mathbb{Z}^+$ y $c \in (0,1)$. Para cualquier arreglo $g-$Golomb $A \subset [0,n]^d$ con $|A| = (g^{1/2}+o(1))n^{d/2}$, se tiene que

$$|A \cap [0,cn]^d| = (g^{1/2}c^d+o(1))n^{d/2}.$$

Demostración. Sea $t = \left\lfloor \left(\frac{cn}{(2d)^4}\right)^{\frac{1}{4(d+1)}} \right\rfloor$. Para todo $m \in \mathbb{Z}^d$, definimos

$$A_m := A \cap (m + [0,t]^d).$$

También, a partir de cada A_m definimos el multiconjunto $\mathbf{B}_m = A_m \ominus A_m$. Por último denotamos

$$e = \sum_{m \in \mathbb{Z}^d} |\mathbf{B}_m|.$$

Para la demostración vamos a acotar e superiormente e inferiormente y de la comparación de las dos cotas obtenemos el resultado deseado. Para cualquiera $a = (a_1, a_2, \ldots, a_d),\ b = (b_1, b_2, \ldots, b_d) \in A$, sea $E_{a,b} := \{m \in \mathbb{Z}^d :\ a, b \in A_m\}$. De la Observación 3 *ii*), se sigue que

$$|E_{a,b}| \leq \prod_{i=1}^{d} (\text{máx}\{t + 1 - |a_i - b_i|, 0\}). \tag{4.6}$$

Ahora, aunque A es un arreglo $g-$Golomb cada pareja de elementos $a, b \in A$ distintos es única y por tanto el vector generado por a y b, $a - b$, está contado en $e = \sum_{m \in \mathbb{Z}^d} |\mathbf{B}_m|$ el mismo número de elementos que tiene el conjunto $E_{a,b}$, es decir, $|E_{a,b}|$. Así

$$e = \sum_{m \in \mathbb{Z}^d} |\mathbf{B}_m| = \sum_{a,b \in A,\, a \neq b} |E_{a,b}|. \tag{4.7}$$

Sean, $a = (a_1, a_2, \ldots, a_d),\ b = (b_1, b_2, \ldots, b_d) \in A$ distintos. Note que $|E_{a,b}| = 0$ a menos que $|a_i - b_i| \leq t$ para todo $i \in [1, d]$. Luego, si $|E_{a,b}| \neq 0$, la diferencia $a - b$ es un vector en $[-t, t]^d$. Si reemplazamos todo esto en (4.6) nos lleva a que

$$\sum_{a,b \in A,\, a \neq b} |E_{a,b}| \leq \sum_{a,b \in A,\, a \neq b} \prod_{i=1}^{d} (\text{máx}\{t + 1 - |a_i - b_i|, 0\}).$$

Observemos que cada vector no nulo generado por un par de elementos de A, con $|a_i - b_i| \leq t$ para $i \in [1, d]$, se encuentra exactamente en $\prod_{i=1}^{d}(t + 1 - |a_i - b_i|)$ traslaciones del intervalo $[0, t]^d$. Además, considerando que A es un arreglo $g-$Golomb el vector $a - b$ se puede repetir hasta $g-$veces, por lo tanto

$$\begin{aligned}\sum_{a,b\in A,\, a\neq b}\prod_{i=1}^{d}(\text{máx}\{t+1-|a_i-b_i|,0\}) &\leq \sum_{(c_1,c_2,\ldots,c_d)\in[-t,t]^d} g\prod_{i=1}^{d}(t+1-|c_i|)\\ &\leq \sum_{(c_1,c_2,\ldots,c_d)\in[-t-1,t+1]^d} g\prod_{i=1}^{d}|c_i|\\ &\leq g\left(\sum_{i=-t-1}^{t+1}|i|\right)^d\\ &\leq g((t+1)(t+2))^d\\ &= (1+o(1))gt^{2d}.\end{aligned} \tag{4.8}$$

De (4.7) y (4.8) obtenemos que

$$e \leq (1+o(1))gt^{2d}. \tag{4.9}$$

Sea $I := \{m \in \mathbb{Z}^d : \ A_m \neq \emptyset\}$. Dado que estamos considerando los multiconjuntos $\mathbf{B}_m = A_m \ominus A_m$ obtenemos que

$$\begin{aligned}e &= \sum_{m\in\mathbb{Z}^d}|\mathbf{B}_m|\\ &= \sum_{m\in I}|\mathbf{B}_m|\\ &= \sum_{m\in I}|A_m|(|A_m|-1)\\ &= \left(\sum_{m\in I}|A_m|^2 - \sum_{m\in I}|A_m|\right)\\ &= (1+o(1))\sum_{m\in I}|A_m|^2.\end{aligned} \tag{4.10}$$

Definimos ahora $q := \lfloor cn \rfloor$ y los conjuntos

$$\begin{aligned} J &:= [-t, q-t]^d & L &:= [-t,q]^d\\ K &:= [-t,n]^d \setminus [-t,q-t]^d & M &:= [-t,n]^d \setminus [-t,q]^d. \end{aligned}$$

Por un lado, debido a que $A \cap (J+[0,t]^d) \subseteq A \cap [0,q]^d$, tenemos que

$$\sum_{m\in J}|A_m| \leq (t+1)^d |A\cap[0,q]^d|.$$

Por otro lado, la Observación 3 i) y la inclusión $[0,q]^d \subseteq L + [0,t]^d$ implican que cada $a \in A \cap [0,q]^d$ puede estar en a lo más $(t+1)^d$ conjuntos A_m con $m \in L$, así

$$(t+1)^d |A \cap [0,q]^d| \leq \sum_{m \in L} |A_m|.$$

Lo mismo se puede hacer para $|A \cap ([0,n]^d \setminus [0,q]^d)|$ obteniendo que

$$\begin{aligned} \sum_{m \in J} |A_m| \leq (t+1)^d |A \cap [0,q]^d| \leq \sum_{m \in L} |A_m| \text{ y} \\ \sum_{m \in M} |A_m| \leq (t+1)^d |A \cap ([0,n]^d \setminus [0,q]^d)| \leq \sum_{m \in K} |A_m|. \end{aligned} \tag{4.11}$$

Ahora, definimos para cada $i \in [1,d]$

$$\begin{aligned} C_i &:= \overbrace{[-t,q] \times \cdots \times [-t,q]}^{i-1} \times [q-t+1,q] \times \overbrace{[-t,q] \times \cdots \times [-t,q]}^{d-i}, \\ D_i &:= C_i + [0,t]^d, \end{aligned}$$

y observamos que

$$L \setminus J = \bigcup_{i=1}^{d} C_i. \tag{4.12}$$

Para cada $i \in [1,d]$, la Observación 3 i) implica que cada $a \in A \cap D_i$ puede estar en máximo $(t+1)^d$ conjuntos A_m con $m \in C_i$, luego

$$\sum_{m \in C_i} |A_m| \leq (t+1)^d |A \cap D_i|. \tag{4.13}$$

Ahora, note que para todo $i \in [1,d]$ y $j \in [q-t+1, q+t]$,

$$A_{i,j} := A \cap \left(\overbrace{[-t,q+t] \times \cdots \times [-t,q+t]}^{i-1} \times \{j\} \times \overbrace{[-t,q+t] \times \cdots \times [-t,q+t]}^{d-i} \right)$$

es un arreglo $g-$Golomb contenido en

$$\overbrace{[-t,q+t] \times \cdots \times [-t,q+t]}^{i-1} \times \{j\} \times \overbrace{[-t,q+t] \times \cdots \times [-t,q+t]}^{d-i},$$

y dado que este conjunto es una traslación de $[0,q+2t]^{d-1}$, entonces de (4.5) se sigue que

$$|A_{i,j}| \leq (g^{1/2} + o(1))(q+2t)^{\frac{d-1}{2}}. \tag{4.14}$$

Aplicando (4.14) a cada $j \in [q-t+1, q+t]$, obtenemos que

$$|A \cap D_i| \leq (g^{1/2} + o(1))(q+2t)^{\frac{d-1}{2}} 2t. \tag{4.15}$$

Entonces,

$$\begin{aligned}
\sum_{m \in L \setminus J} |A_m| \leq & \sum_{i=1}^{d} \sum_{m \in C_i} |A_m| && \text{(por (4.12))} \\
\leq & \sum_{i=1}^{d} (t+1)^d |A \cap D_i| && \text{(por (4.13))} \\
\leq & (g^{1/2} + o(1)) d (q+2t)^{\frac{d-1}{2}} 2(t+1)^{d+1} && \text{(por (4.15))}
\end{aligned}$$

y ya que $t \leq \left(\frac{q}{(2d)^4}\right)^{\frac{1}{4(d+1)}}$, la desigualdad anterior nos lleva a

$$\begin{aligned}
(g^{1/2} + o(1)) d (q+2t)^{\frac{d-1}{2}} 2(t+1)^{d+1} &\leq (g^{1/2} + o(1)) 2 (q^{\frac{d-1}{2}} + (2t)^{\frac{d-1}{2}}) 2d (t)^{d+1} \\
&\leq (2g^{1/2} + o(1)) (q^{\frac{d-1}{2}} + (2t)^{\frac{d-1}{2}}) q^{1/4} \\
&\leq (2g^{1/2} + o(1)) \left(q^{\frac{d-1}{2}} + \left(2 \left(\frac{q}{(2d)^4} \right)^{\frac{1}{4(d+1)}} \right)^{\frac{d-1}{2}} \right) q^{1/4} \\
&\leq (2g^{1/2} + o(1))(1 + o(1)) q^{\frac{d-1}{2}} q^{1/4} \\
&= (2g^{1/2} + o(1)) q^{\frac{d}{2} - \frac{1}{4}},
\end{aligned}$$

y por lo tanto

$$\sum_{m \in L \setminus J} |A_m| = o\left(q^{\frac{d}{2}}\right). \tag{4.16}$$

De igual manera,

$$\sum_{m \in K \setminus M} |A_m| = o\left(q^{\frac{d}{2}}\right). \tag{4.17}$$

De (4.11), (4.16) y (4.17), deducimos que

$$\begin{aligned}
&\sum_{m \in J} |A_m| = (1 + o(1)) t^d |A \cap [0,q]^d| \text{ y} \\
&\sum_{m \in K} |A_m| = (1 + o(1)) t^d |A \cap ([0,n]^d \setminus [0,q]^d)|.
\end{aligned} \tag{4.18}$$

Sea $f := \dfrac{|A \cap [0,q]^d|}{g^{1/2} n^{d/2}}$. Luego de (4.18) se sigue que

$$\begin{aligned} \sum_{m \in J} |A_m| &= (1+o(1)) t^d f g^{1/2} n^{d/2} \text{ y} \\ \sum_{m \in K} |A_m| &= (1+o(1)) t^d (1-f) g^{1/2} n^{d/2}. \end{aligned} \tag{4.19}$$

Dado que $A \subseteq [0,n]^d$, observamos que $I \subseteq J \cup K$. Además, por la definición de I y dado que $J \cap K = \emptyset$, entonces $\{m \in J : A_m \neq \emptyset\} \cup \{m \in K : A_m \neq \emptyset\} = I$. Por lo tanto (4.10) implica que

$$\begin{aligned} e \geq & (1+o(1)) \sum_{m \in I} |A_m|^2 \\ = & (1+o(1)) \left(\sum_{m \in J} |A_m|^2 + \sum_{m \in K} |A_m|^2 \right). \end{aligned} \tag{4.20}$$

Aplicando la desigualdad de Cauchy-Schwarz a las sumatorias de (4.20), encontramos que

$$\begin{aligned} \sum_{m \in J} |A_m|^2 &\geq \frac{(\sum_{m \in J} |A_m|)^2}{|J|} \text{ y} \\ \sum_{m \in K} |A_m|^2 &\geq \frac{(\sum_{m \in K} |A_m|)^2}{|K|}. \end{aligned}$$

Por tanto (4.19) nos lleva a

$$\begin{aligned} \sum_{m \in J} |A_m|^2 &\geq (1+o(1)) \frac{f^2}{c^d} g t^{2d} \text{ y} \\ \sum_{m \in K} |A_m|^2 &\geq (1+o(1)) \frac{(1-f)^2}{(1-c^d)} g t^{2d}. \end{aligned} \tag{4.21}$$

Usando (4.20) y (4.21), tenemos que

$$e \geq (1+o(1)) g t^{2d} \left(\frac{f^2}{c^d} + \frac{(1-f)^2}{(1-c^d)} \right) \tag{4.22}$$

Comparando (4.9) y (4.22) se sigue que

$$1 \geq \frac{f^2}{c^d} + \frac{(1-f)^2}{(1-c^d)},$$

de donde

$$0 \geq f^2 - 2fc^d + c^{2d} = (f - c^d)^2.$$

Por lo tanto $f = c^d$, lo que concluye la demostración. □

La buena distribución de los arreglos $g-$Golomb no sólo se presenta en los cubos d-dimensionales, sino que también se puede evidenciar en látices de $\mathbb{Z}^d$. Para poder abordar este tema necesitamos la notación que definimos a continuación. Primero, escribimos a $\mathbf{0} = (\underbrace{0, 0, \ldots, 0}_{d})$.

Para cualquier $m_1, m_2, \ldots, m_d \in \mathbb{Z}^+$, denotamos

$$\Lambda(m_1, m_2, \ldots, m_d) := \{(n_1, n_2, \ldots, n_d) \in \mathbb{Z}^d \ : \ n_1 \in m_1\mathbb{Z}, n_2 \in m_2\mathbb{Z}, \ldots, n_d \in m_d\mathbb{Z}\},$$
$$\Delta(m_1, m_2, \ldots, m_d) := [0, m_1 - 1] \times [0, m_2 - 1] \times \cdots \times [0, m_d - 1].$$

Note que $\Delta(m_1, m_2, \ldots, m_d)$ es un dominio fundamental del látice $\Lambda(m_1, m_2, \ldots, m_d)$, es decir, $\mathbb{Z}^d = \Delta(m_1, m_2, \ldots, m_d) \oplus \Lambda(m_1, m_2, \ldots, m_d)$, para ampliar la información sobre látices puede consultar la sección 3.1.1 de [49]. Ahora mostramos que el Lema 2 se puede generalizar en el sentido en que se relaciona el cardinal de un conjunto B y los cardinales de cada uno de los elementos de una partición del conjunto A.

Lema 3. Sean, A y B subconjuntos de $\mathbb{Z}^d$ con A un arreglo $g-$Golomb. Supongamos que existe una colección $\{A_i\}_{i\in I}$ de conjuntos disjuntos dos a dos tales que $A = \bigcup_{i\in I} A_i$, es decir, la colección es una partición de A. Entonces

$$\sum_{i\in I} \frac{|A_i|^2}{|A_i + B|} \leq g + \frac{|A| - g}{|B|}.$$

Demostración. Para todo $i \in I$, A_i es un arreglo $g-$Golomb. Además por Lema 2 se cumple que

$$|A_i|^2 \leq \frac{|A_i + B|}{|B|^2} \sum_{\mathbf{c}\in\mathbb{Z}^d} R_{A_i - A_i}(\mathbf{c}) \cdot R_{B-B}(\mathbf{c}),$$

de donde

$$\frac{|A_i|^2}{|A_i + B|} \leq \frac{1}{|B|^2} \sum_{\mathbf{c}\in\mathbb{Z}^d} R_{A_i - A_i}(\mathbf{c}) \cdot R_{B-B}(\mathbf{c}). \tag{4.23}$$

Si sumamos (4.23) para cada $i \in I$, obtenemos

$$\begin{aligned}\sum_{i\in I}\frac{|A_i|^2}{|A_i+B|} &\leq \frac{1}{|B|^2}\sum_{i\in I}\sum_{\mathbf{c}\in\mathbb{Z}^d} R_{A_i-A_i}(\mathbf{c})\cdot R_{B-B}(\mathbf{c}) \\ &= \frac{1}{|B|^2}\left(\sum_{i\in I}|A_i||B| + \sum_{i\in I}\sum_{\mathbf{c}\in\mathbb{Z}^d\setminus\{\mathbf{0}\}} R_{A_i-A_i}(\mathbf{c})\cdot R_{B-B}(\mathbf{c})\right).\end{aligned} \tag{4.24}$$

Como los elementos de $\{A_i\}_{i\in I}$ son disjuntos dos a dos, tenemos que $|A| = \sum_{i\in I}|A_i|$. Usando esto en (4.24), deducimos que

$$\sum_{i\in I}\frac{|A_i|^2}{|A_i+B|} \leq \frac{1}{|B|^2}\left(|A||B| + \sum_{i\in I}\sum_{\mathbf{c}\in\mathbb{Z}^d\setminus\{\mathbf{0}\}} R_{A_i-A_i}(\mathbf{c})\cdot R_{B-B}(\mathbf{c})\right). \tag{4.25}$$

Ahora, ya que A es un arreglo $g-$Golomb, entonces $\sum_{i\in I} R_{A_i-A_i}(\mathbf{c}) \leq R_{A-A}(\mathbf{c}) \leq g$ para todo $\mathbf{c}\neq\mathbf{0}$. Al reemplazar esto en (4.25) se sigue que

$$\begin{aligned}\sum_{i\in I}\frac{|A_i|^2}{|A_i+B|} \leq& \frac{1}{|B|^2}\left(|A||B| + g\sum_{\mathbf{c}\in\mathbb{Z}^d\setminus\{\mathbf{0}\}} R_{B-B}(\mathbf{c})\right) \\ \leq& \frac{1}{|B|^2}\left(|A||B| + g|B|^2 - g|B|\right) \\ =& g + \frac{|A|-g}{|B|},\end{aligned}$$

lo cual concluye la demostración. □

Veamos ahora como se distribuye un arreglo $g-$Golomb en el látice $\Lambda(m_1, m_2, \ldots, m_d)$.

Teorema 17. Sean, $n, m_1, m_2, \ldots, m_d \in \mathbb{Z}^+$, $l \in \mathbb{Z}$, $\Lambda := \Lambda(m_1, m_2, \ldots, m_d)$, $\Delta := \Delta(m_1, m_2, \ldots, m_d)$, $m := \prod_{i=1}^d m_i$ y A un arreglo $g-$Golomb contenido en $[1, n]^d$ tal que $|A| = g^{1/2}n^{d/2} - l$. Denotamos $A_{\mathbf{c}} := A \cap (\mathbf{c} + \Lambda)$ para cada $\mathbf{c} \in \Delta$. Entonces

$$\sum_{\mathbf{c}\in\Delta}\left(|A_{\mathbf{c}}| - \frac{|A|}{m}\right)^2 \leq (1+o(1))\left(2\left(\frac{(g^{\frac{1}{2}}n^{\frac{d}{2}} - l)gn^d}{m}\right)^{\frac{1}{2}} + (g^{\frac{1}{2}}n^{\frac{d}{2}} - l) + \frac{2g^{\frac{1}{2}}n^{\frac{d}{2}}l}{m}\right).$$

En particular, para cada $\mathbf{c} \in \Delta$,

$$|A_{\mathbf{c}}| = (1+o(1))\frac{|A|}{m}.$$

Demostración. Sea $f := \left(\frac{|A|n^d m}{g}\right)^{\frac{1}{2d}}$ y

$$B := [1, f]^d \cap \Lambda.$$

Dado que A es un arreglo $g-$Golomb se cumple que cada elemento de $\{A_{\mathbf{c}}\}_{\mathbf{c}\in\Delta}$ es un arreglo $g-$Golomb. Además, cada $A_{\mathbf{c}}$ está contenido en una única clase lateral de $\mathbb{Z}^d/\Lambda$ y por tanto los elemento de $\{A_{\mathbf{c}}\}_{\mathbf{c}\in\Delta}$ son disjuntos dos a dos. Luego, los conjuntos A y B satisfacen las condiciones del Lema 3. Esto es

$$\sum_{\mathbf{c}\in\Delta} \frac{|A_{\mathbf{c}}|^2}{|A_{\mathbf{c}} + B|} \leq g + \frac{|A| - g}{|B|}. \tag{4.26}$$

Ahora, para cada $\mathbf{c} \in \Delta$ tenemos que $A_{\mathbf{c}} = A \cap (\mathbf{c} + \Lambda) \subseteq [1, n]^d \cap (\mathbf{c} + \Lambda)$ y como $B := [1, f]^d \cap \Lambda$, se sigue que

$$A_{\mathbf{c}} + B \subseteq [1, n + f]^d \cap (\mathbf{c} + \Lambda).$$

Como $\mathbb{Z}^d = \Delta \oplus \Lambda$, entonces cada traslación de Δ tiene un y sólo un representante de cada clase $\mathbf{b} + \Lambda$; si partimos a $[1, n + f]^d$ en traslaciones de Δ, obtenemos que las clases laterales $\{\mathbf{b} + \Lambda\}_{\mathbf{b}\in\Delta}$ están casi equidistribuidas en el cubo $[1, n + f]^d$, de lo anterior concluimos que

$$|A_{\mathbf{c}} + B| \leq \frac{|[1, n + f]^d|}{m} + o(1) = \frac{(n + f)^d}{m} + o(1). \tag{4.27}$$

De (4.26) y (4.27), notamos que

$$\frac{m}{(n + f)^d} \sum_{\mathbf{c}\in\Delta} |A_{\mathbf{c}}|^2 \leq \sum_{\mathbf{c}\in\Delta} \frac{|A_{\mathbf{c}}|^2}{|A_{\mathbf{c}} + B|} \leq g + \frac{|A| - g}{|B|},$$

de donde

$$\sum_{\mathbf{c}\in\Delta} |A_{\mathbf{c}}|^2 \leq \left(\frac{(n + f)^d}{m} + o(1)\right)\left(g + \frac{|A| - g}{|B|}\right). \tag{4.28}$$

Debido a que $B = [1, f]^d \cap \Lambda$, tenemos que $|B| = \frac{f^d}{m} + o(1)$, y entonces de (4.28) resulta

$$\sum_{\mathbf{c}\in\Delta} |A_{\mathbf{c}}|^2 \leq \left(\frac{(n + f)^d}{m}\right)\left(g + \frac{m(|A| - g)}{f^d}\right). \tag{4.29}$$

Finalmente,

$$\sum_{\mathbf{c}\in\Delta} |A_{\mathbf{c}}|^2 \leq (1 + o(1))\left(\frac{n^d + f^d}{m}\right)\left(g + \frac{m|A|}{f^d}\right). \tag{4.30}$$

Ahora, al reemplazar la definición de f en (4.30) nos lleva a

$$\sum_{\mathbf{c}\in\Delta}|A_{\mathbf{c}}|^2 \leq (1+o(1))\left(\frac{gn^d}{m}+2\left(\frac{|A|gn^d}{m}\right)^{1/2}+|A|\right). \tag{4.31}$$

Recordemos que $\{A_{\mathbf{c}}\}_{\mathbf{c}\in\Delta}$ es una partición de A y por lo tanto $|A|=\sum_{\mathbf{c}\in\Delta}|A_{\mathbf{c}}|$. Además, ya que $|\Delta|=m$, obtenemos que

$$\left(\sum_{\mathbf{c}\in\Delta}2|A_{\mathbf{c}}|\frac{|A|}{m}\right)-\left(\sum_{\mathbf{c}\in\Delta}\left(\frac{|A|}{m}\right)^2\right)=\frac{|A|^2}{m}.$$

Por lo tanto

$$\sum_{\mathbf{c}\in\Delta}\left(|A_{\mathbf{c}}|-\frac{|A|}{m}\right)^2=\left(\sum_{\mathbf{c}\in\Delta}|A_{\mathbf{c}}|^2\right)-\frac{|A|^2}{m}. \tag{4.32}$$

De (4.31) y (4.32), tenemos que

$$\begin{aligned}\sum_{\mathbf{c}\in\Delta}\left(|A_{\mathbf{c}}|-\frac{|A|}{m}\right)^2&=\left(\sum_{\mathbf{c}\in\Delta}|A_{\mathbf{c}}|^2\right)-\frac{|A|^2}{m}\\ &\leq(1+o(1))\left(\frac{gn^d}{m}+2\left(\frac{|A|gn^d}{m}\right)^{1/2}+|A|-\frac{|A|^2}{m}\right),\end{aligned} \tag{4.33}$$

y recordando que $|A|=g^{\frac{1}{2}}n^{\frac{d}{2}}-l$, se sigue que

$$\sum_{\mathbf{c}\in\Delta}\left(|A_{\mathbf{c}}|-\frac{|A|}{m}\right)^2\leq(1+o(1))\left(2\left(\frac{(g^{\frac{1}{2}}n^{\frac{d}{2}}-l)gn^d}{m}\right)^{\frac{1}{2}}+(g^{\frac{1}{2}}n^{\frac{d}{2}}-l)+\frac{2g^{\frac{1}{2}}n^{\frac{d}{2}}l}{m}\right).$$

Queda entonces demostrado la primera parte del teorema.

Por otro lado, tenemos que para todo $\mathbf{c}\in\Delta$ se cumple que

$$\left(|A_{\mathbf{c}}|-\frac{|A|}{m}\right)^2\leq\sum_{\mathbf{c}\in\Delta}\left(|A_{\mathbf{c}}|-\frac{|A|}{m}\right)^2. \tag{4.34}$$

De (4.33) y (4.34) se sigue que

$$\left(|A_{\mathbf{c}}|-\frac{|A|}{m}\right)^2\leq(1+o(1))\left(2\left(\frac{|A|gn^d}{m}\right)^{1/2}+|A|+\frac{2g^{\frac{1}{2}}n^{\frac{d}{2}}l-l^2}{m}\right).$$

En consecuencia

$$\left||A_{\mathbf{c}}| - \frac{|A|}{m}\right| \leq (1+o(1)) \left(\left(\frac{4|A|gn^d}{m} \right)^{\frac{1}{4}} + |A|^{\frac{1}{2}} + \left(\frac{2g^{\frac{1}{2}}n^{\frac{d}{2}}l - l^2}{m} \right)^{\frac{1}{2}} \right).$$

Finalmente, obtenemos que

$$\begin{aligned} |A_{\mathbf{c}}| \leq & (1+o(1)) \left(\frac{|A|}{m} + \left(\frac{4|A|gn^d}{m} \right)^{\frac{1}{4}} + |A|^{\frac{1}{2}} + \left(\frac{2g^{\frac{1}{2}}n^{\frac{d}{2}}l - l^2}{m} \right)^{\frac{1}{2}} \right) \\ = & (1+o(1))\frac{|A|}{m}. \end{aligned}$$

□

4.4. Secuencias sonar

Estudiando el problema de detección radar Costas encontró que cuando una señal (onda) está conformada por un arreglo de frecuencias que satisfacen la propiedad de diferencias distintas y es enviada hacia un objeto en movimiento, entonces la señal de regreso contiene suficiente información para determinar la velocidad y la distancia del objeto.

Los arreglos encontrados por Costas pueden ser representados por matrices con entradas en $\{0,1\}$, como un conjunto de puntos contenidos en una malla rectangular o como secuencias de números enteros; en cualquier caso sus elementos deben satisfacer la propiedad de diferencias distintas que definimos a continuación. En adelante vamos a denotar al conjunto de puntos $A = \{(1,a_1),(2,a_2),\ldots,(n,a_n)\}$ contenido en $[1,n]\times[1,m]$ como la secuencia $A = [a_1,a_2,\ldots,a_n]$.

Definición 16. Sea $A = [a_1,a_2,...,a_n]$ una secuencia de números enteros no negativos. Decimos que A satisface la *Propiedad de Diferencias Distintas (PDD)* si

$$a_{i+h} - a_i = a_{j+h} - a_j$$

con $1 \leq i < i+h \leq n$; $1 \leq j < j+h \leq n$, implica que $i = j$.

En otras palabras, la propiedad de diferencias distintas es equivalente a la condición que satisfacen los arreglos $1-$Golomb en $\mathbb{Z}\times\mathbb{Z}$. Costas construía la señal a enviar a partir de

un arreglo de puntos. Relacionaba las primeras componentes con intervalos de tiempo consecutivos y las segundas componentes con la frecuencia que la onda debía tener. En los arreglos Costas las frecuencias pueden ser utilizadas una sola vez y en cada intervalo de tiempo debe haber siempre una única frecuencia. Posteriormente Golomb y Taylor mostraron que la primer condición no es necesaria, es decir permitieron que el arreglo tenga una frecuencia en cada intervalo de tiempo, pero que las frecuencias puedan ser usadas más de una vez y siempre satisfaciendo la PDD. Estos nuevos arreglos fueron llamados secuencias sonar y presentaron mejores resultados en su aplicación ya que con el mismo número de frecuencias (ancho de banda) se puede construir una secuencia con más elementos que un arreglo Costas y por ende generar una señal de regreso con más información [21].

Definición 17. Sea $A = [a_1, a_2, ..., a_n]$ una secuencia contenida en $[1, n] \times [0, m-1]$. Decimos que A es una (m, n) secuencia sonar, si satisface la propiedad de diferencias distintas. Cuando la PDD se satisface considerando las diferencias módulo m, entonces se llama una (m, n) secuencia sonar módular (SSM).

El problema fundamental en el estudio de las secuencias sonar establece que: "En una malla con m filas, se requiere encontrar el mayor número de columnas n para el cual existe una (m, n) secuencia sonar" o equivalentemente estudiar la siguiente función:

$$S(m) := \text{máx}\{n : \text{existe una } (m, n) \text{ secuencia sonar}\}.$$

Definición 18. Sean, $m, n \in \mathbb{Z}^+$ y A una secuencia sonar contenida en $[1, n] \times [1, m]$. A se denomina la mejor secuencia sonar con n elementos y contenida en una malla de m filas, si $S(m) = n$.

Por ejemplo, la $(3, 6)$ secuencia sonar dada en la Figura 4.1 es la mejor secuencia sonar contenida en tres filas ($m = 3$). Esto se cumple ya que no existe una secuencia sonar de cardinal 7 que pueda estar contenida en un rectángulo de 3 filas, es decir $S(3) = 6$; cualquier otra $(3, 6)$ secuencia sonar contenida en $[1, 6] \times [1, 3]$ se considera equivalente.

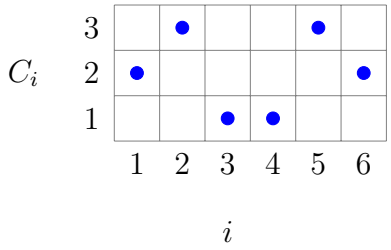


Figura 4.1: $(3, 6)$ Secuencia Sonar.

Moreno, Games y Taylor [32] estudiaron la función $S(m)$ y encontraron valores cercanamente óptimos de n mediante una búsqueda computacional para $m \leq 100$. Por otro lado, Osorio, Ruiz y Trujillo en [36] estudiaron dicha función para valores pequeños de m y establecieron la siguiente conjetura

$$\lim_{m\to\infty} \frac{S(m)}{m} = 1.$$

Se puede encontrar fácilmente una cota superior trivial de la función $S(m)$ contando el número de diferencias distintas que produce una secuencia sonar en un rectángulo de m filas, así

$$S(m) \leq 2m.$$

Algunos investigadores han mejorado dicha cota trivial con los siguientes resultados:

- $S(m) \leq m + 5m^{2/3}$, (Erdös, Graham, Ruzsa y Taylor [17]).
- $S(m) \leq m + 3,78m^{2/3} + 4,76m^{1/3} + 2$, (Caicedo [5]).

Estas cotas superiores muestran que para m grande una (m, n) secuencia sonar tiene a $S(m)$ más cercana a m que a $2m$.

4.4.1. Construcciones de secuencias sonar

En cuanto al estudio de las secuencias sonar encontramos que Moreno, Games y Taylor en [32] dieron las primeras construcciones que mostramos en la Tabla 4.1 con sus respectivos parámetros.

Nombre de la Costrucción	Parámetros
Cuadrática	$(p, p+1)$
Shift	$(q-1, q)$
Welch Exponencial	$(p, p-1)$
Welch Logarítmica	$(p-1, p-1)$
Golomb	$(q-1, q-2)$

Tabla 4.1: Construcciones de SSM con p primo y q una potencia prima.

Con estas construcciones Moreno, Games y Taylor [32] obtuvieron una tabla con los parámetros de las secuencias sonar candidatas a ser las mejores en un ancho de banda de hasta 100 frecuencias.

A continuación presentamos las construcciones de secuencias sonar provenientes de conjuntos de Sidon modulares. Estas construcciones fueron introducidas por Ruiz, Trujillo y Caicedo en [40] y son diferentes de las dadas en la Tabla 4.1 aunque tienen los mismos parámetros.

El Teorema 18 dado en [40] proporciona secuencias sonar a partir de conjuntos de Sidon modulares que tengan características particulares.

Teorema 18. Sean, $n, m, b \in \mathbb{Z}^+$, $B = \{b_1, b_2, ..., b_n\}$ un conjunto de Sidon en $\mathbb{Z}_{mb}$, tal que $B \,(\text{mód}\, b) = [1, n]$. Si B está ordenado de forma que $b_i \equiv i \,(\text{mód}\, b)$, entonces la secuencia definida por

$$a_i = \left\lfloor \frac{b_i}{b} \right\rfloor \tag{4.35}$$

para $i \in [1, n]$, resulta ser una (m, n) secuencia sonar modular.

Conjuntos de Sidon modulares que cumplen la hipótesis del Teorema 18 son aquellos provenientes de dos construcciones estudiadas en el Capítulo 2, estas son la construcción de Bose y la construcción de Ruzsa. Con estos resultados en [40] obtuvieron tres construcciones de secuencias sonar a partir de los conjuntos de Sidon tipo Bose y tipo Ruzsa que nosotros presentamos a continuación.

Corolario 3. (**sonar Bose**). Sea $B(q, \theta)$ un conjunto de Sidon tipo Bose del Teorema 1. La secuencia definida por

$$a_i = \left\lfloor \frac{b_i}{q+1} \right\rfloor \tag{4.36}$$

donde $b_i \in B(q, \theta)$ es el único elemento tal que $b_i \equiv i \,(\text{mód}\, q+1)$ es una $(q-1, q)$ secuencia sonar modular.

Ejemplo 9. Sean, $q = 11$ y $\theta = 2x + 5$ un elemento primitivo de $\mathbb{F}_{q^2}$. Entonces, del Teorema 1 obtenemos inicialmente el conjunto tipo Bose

$$B(11, \theta) = \{8, 13, 15, 19, 28, 29, 46, 54, 83, 86, 105\}$$

contenido en $\mathbb{Z}_{120}$. Ahora aplicamos (4.36) del Corolario 3 y obtenemos la siguiente secuencia $[1, 7, 1, 2, 2, 4, 1, 0, 8, 3, 6]$ que resulta ser una $(10, 11)$ secuencia sonar modular.

Corolario 4. (**sonar Ruzsa 1**). Sea $R(\theta, p)$ el conjunto de Sidon tipo Ruzsa del Teorema 4. La secuencia definida por

$$a_i = \left\lfloor \frac{b_i}{p} \right\rfloor \tag{4.37}$$

donde $b_i \in R(\theta, p)$ es el único elemento tal que $b_i \equiv i \,(\text{mód}\, p)$ es una $(p-1, p-1)$ secuencia sonar modular.

Ejemplo 10. Sean, $p = 11$ y $\alpha = 2$ una raíz primitiva módulo 11. Entonces, del Teorema 4 obtenemos inicialmente el conjunto de Sidon tipo Ruzsa

$$R(2, 11) = \{7, 39, 58, 63, 65, 86, 92, 100, 101, 104\},$$

contenido en $\mathbb{Z}_{110}$. Posteriormente aplicamos (4.37) del Corolario 4 para obtener la siguiente $(10, 10)$ secuencia sonar modular:

$$[9, 9, 5, 8, 9, 3, 0, 5, 7, 5].$$

Corolario 5. (**sonar Ruzsa 2**). Sea $R(\theta, p)$ el conjunto de Sidon tipo Ruzsa del Teorema 4. La secuencia definida por

$$a_i = \left\lfloor \frac{b_i}{p-1} \right\rfloor \tag{4.38}$$

donde $b_i \in R(\theta, p)$ es el único elemento tal que $b_i \equiv \ i \pmod{p-1}$ es una $(p, p-1)$ secuencia sonar modular.

Ejemplo 11. Sean, $p = 11$ y $\alpha = 2$ una raíz primitiva módulo 11. Del Teorema 4 obtenemos el conjunto

$$R(2, 11) = \{7, 39, 58, 63, 65, 86, 92, 100, 101, 104\}$$

el cual es un conjunto de Sidon contenido en $\mathbb{Z}_{110}$. Posteriormente aplicamos (4.38) del Corolario 5 y encontramos una $(11, 10)$ secuencia sonar modular:

$$[10, 10, 9, 6, 10, 6, 8, 0, 5, 3].$$

4.4.2. Secuencias sonar extendidas

Cuando Golomb y Taylor introducen el concepto de secuencia sonar implícitamente están demostrando que la característica fundamental que debe tener una secuencia para ser utilizada en la detección sonar es que cumpla la propiedad de las diferencias distintas. Teniendo en cuenta la anterior conclusión Moreno, Golomb y Corrada [33] observaron el comportamiento de la señal de retorno y encontraron que siempre contenía espacios de tiempo sin frecuencia, es decir espacios en blanco generados por el ruido que se encuentra en el ambiente.

Como resultado de su observación Moreno, Golomb y Corrada [33] introducen una generalización de las secuencias sonar. En estos nuevos arreglos se permite que cada columna

tenga máximo un punto; esto permite incluir columnas en blanco. Estos arreglos fueron denominados Secuencias Sonar Extendidas (SSE) y han tenido gran acogida ya que presentan un mejor desempeño al ser utilizadas en detección sonar. La mejora se presenta ya que en m filas (ancho de banda fijo) una SSE siempre puede tener más columnas que una secuencia sonar, esto se traduce en más datos que permiten realizar una mejor aproximación. También en [33] se dan construcciones de SSE y una lista de SSE cercanamente óptimas con $m \leq 10$.

En esta sección presentamos un contexto más detallado de las SSE y las nuevas construcciones de secuencias sonar extendidas que publicamos en [11].

En adelante, para denotar las columnas vacías (espacios de tiempo en blanco) vamos a utilizar el símbolo $*$, es decir el arreglo $A = \{(1,2),(2,3),(4,1),(5,3)\}$ se puede escribir como la secuencia $[2,3,*,1,3]$.

Definición 19. Sea $A = [a_1, a_2, ..., a_{n+k}]$ una secuencia contenida en $[1, n+k] \times [1, m]$, con k columnas en blanco, es decir, k asteriscos $(*)$ y $|A| = n$. Si los elementos de A satisfacen la propiedad de diferencias distintas, entonces dicha secuencia se denomina una (m, n, k) *Secuencia Sonar Extendida (SSE).*

Para mostrar las construcciones que obtuvimos de SSE necesitamos conocer las Secuencias Sonar Extendidas Circulares SSEC y por tanto las definimos a continuación:

Definición 20. Sean, $c \in \mathbb{Z}$, $d \in \mathbb{Z}^+$ y $A := [a_1, a_2, \ldots, a_n, a_{n+1}, \ldots, a_{2n+1}]$ con $a_{n+1} = *$ y $a_{k+n+1} \equiv a_k + c \,(\text{mód}\, d)$ para $1 \leq k \leq n$. Si para cada $h \in [1, n]$ se cumple que las diferencias $a_{i+h} - a_i$ con $i \in [1, n]$ e $i + h \neq n + 1$ son distintas módulo d, entonces la secuencia inicial es denominada como una *secuencia sonar extendida circular* (SSEC).

Las únicas construcciones de SSEC que se conocen hasta ahora fueron proporcionadas por Moreno, Golomb y Corrada en [33], a continuación mostramos dichas construcciones.

Teorema 19. (**Welch Logarítmica Extendida Circular**). Sean, p un primo y α un elemento primitivo de $\mathbb{F}_p$. La secuencia definida por

$$a_i = \begin{cases} \log_\alpha i, & i \in [1, p-1]. \\ *, & i = p. \\ \log_\alpha (i-p), & i \in [p+1, 2p-1], \end{cases}$$

donde $1 \leq a_i \leq p-1$ resulta ser una secuencia sonar extendida circular con $n = p-1$, $d = p-1$ y $c = 0$.

Teorema 20. (**Shift Extendida Circular**). Sean, p un primo, α una raíz primitiva de $\mathbb{F}_{p^{2r}}$ y β una raíz primitiva de $\mathbb{F}_{p^r}$. Para $p = 2$ definimos la secuencia por

$$a_i = \begin{cases} \log_\beta((\alpha^i)^{p^r} + \alpha^i), & i \in [1, 2p^r + 1], i \neq p^r + 1. \\ *, & i = p^r + 1. \end{cases}$$

donde $1 \leq a_i \leq p^r + 1$. Mientras que para p impar, se define a_i de forma similar excepto que

$$a_i = \begin{cases} \log_\beta((\alpha^i)^{p^r} + \alpha^i), & i \in \left[\frac{-(p^r-1)}{2}, \frac{3p^r+1}{2}\right] \quad con \;\; i \neq \frac{p^r+1}{2}. \\ *, & i = \frac{p^r+1}{2}. \end{cases}$$

Entonces, el resultado es una secuencia sonar extendida circular con $n = p^r$, $d = p^r - 1$ y $c \neq 0$.

Teorema 21. (**Golomb-Lempel Extendida Circular**). Sean, $p^r > 2$ una potencia prima, α y β raíces primitivas de $\mathbb{F}_{p^r}$. La secuencia definida por

$$a_i = \begin{cases} j, & \text{sí y sólo si } \alpha^i + \beta^j = 1 \\ & \text{donde } \; i \in [1, 2p^r - 3], \quad i \neq p^r - 1. \\ *, & i = p^r - 1, \end{cases}$$

donde $1 \leq a_i \leq p^r - 2$. El resultado es una secuencia sonar extendida circular con $n = p^r - 2$, $d = p^r - 1$ y $c = 0$.

También en [33] se demuestra el siguiente teorema que permite obtener secuencias sonar extendidas a partir de SSEC, aunque el resultado es de fácil comprensión hasta el momento es el único camino que se conoce para poder obtener construcciones generales de SSE.

Teorema 22. Sean, $d \in \mathbb{Z}^+$ y $[a_1, a_2, \ldots, a_{2n+1}]$ una secuencia sonar extendida circular con módulo d. Para cada $k \in [0, n-1]$ definimos la secuencia

$$[a_{k+1}, a_{k+2}, \ldots, a_{k+n+2}],$$

que resulta ser una $(d, n+1, 1)$ secuencia sonar extendida .

Más adelante vamos a trabajar con el Teorema 22, por ahora vamos a mostrar las nuevas construcciones de SSEC que encontramos a partir de conjuntos de Sidon.

El Teorema 23 permite construir SSEC a partir de conjuntos de Sidon modulares con características particulares. Con dichas secuencias posteriormente encontraremos las secuencias sonar extendidas que es nuestro objetivo principal en esta sección.

Teorema 23. Sean, $n, m \in \mathbb{Z}^+$ y $B = \{b_1, b_2, ..., b_n\}$ un conjunto de Sidon en $\mathbb{Z}_{m(n+1)}$ tal que $B(\text{mód } n+1) = [1, n]$. Si B está ordenado de tal forma que $b_i \equiv i \ (\text{mód } n+1)$, entonces la secuencia definida por

$$a_i = \begin{cases} \left\lfloor \dfrac{b_i}{n+1} \right\rfloor, & i \in [1, n]. \\ *, & i = n+1. \\ \left(\left\lfloor \dfrac{b_{i-(n+1)}}{n+1} \right\rfloor - 1 \right) (\text{mód } m), & i \in [n+2, 2n+1], \end{cases} \tag{4.39}$$

es una secuencia sonar extendida circular con $c = -1$ y $d = m$.

Demostración. Sean, h, i, j enteros tales que $1 \leq h, i, j \leq n$ con $i + h \neq n+1$ y $j + h \neq n+1$. Al suponer que

$$a_{i+h} - a_i \equiv a_{j+h} - a_j \ (\text{mód } m),$$

encontramos cuatro casos:

1. Si $i + h < n + 1$ y $j + h < n + 1$. Entonces de (4.39),

$$\left\lfloor \frac{b_{i+h}}{n+1} \right\rfloor - \left\lfloor \frac{b_i}{n+1} \right\rfloor \equiv \left\lfloor \frac{b_{j+h}}{n+1} \right\rfloor - \left\lfloor \frac{b_j}{n+1} \right\rfloor (\text{mód } m).$$

Así, existe un entero t tal que

$$\left\lfloor \frac{b_{i+h}}{n+1} \right\rfloor - \left\lfloor \frac{b_i}{n+1} \right\rfloor = \left\lfloor \frac{b_{j+h}}{n+1} \right\rfloor - \left\lfloor \frac{b_j}{n+1} \right\rfloor + tm.$$

Ahora, multiplicando la anterior igualdad por $n+1$ obtenemos

$$\begin{aligned} &(n+1) \left\lfloor \frac{b_{i+h}}{n+1} \right\rfloor - (n+1) \left\lfloor \frac{b_i}{n+1} \right\rfloor = \\ &(n+1) \left\lfloor \frac{b_{j+h}}{n+1} \right\rfloor - (n+1) \left\lfloor \frac{b_j}{n+1} \right\rfloor + tm(n+1). \end{aligned}$$

Si además añadimos $h = (i+h) - i = (j+h) - j$ a ambos lados de la ecuación tenemos que

$$\begin{aligned}&\left[(n+1)\left\lfloor\frac{b_{i+h}}{n+1}\right\rfloor + (i+h)\right] - \left[(n+1)\left\lfloor\frac{b_i}{n+1}\right\rfloor + i\right]\\ &= \left[(n+1)\left\lfloor\frac{b_{j+h}}{n+1}\right\rfloor + (j+h)\right]\\ &- \left[(n+1)\left\lfloor\frac{b_j}{n+1}\right\rfloor + j\right] + tm(n+1).\end{aligned}$$

$$b_{i+h} - b_i - b_{j+h} + b_j = tm(n+1),$$

lo cual implica

$$b_{i+h} + b_j \equiv b_{j+h} + b_i \,(\text{mód } m(n+1)).$$

Pero B es un conjunto de Sidon en $\mathbb{Z}_{m(n+1)}$, entonces $\{i+h, j\} = \{j+h, i\}$, y así $i = j$.

2. Si $i + h > n + 1$ y $j + h < n + 1$. Entonces de (4.39),

$$\left\lfloor\frac{b_{i+h-(n+1)}}{n+1}\right\rfloor - 1 - \left\lfloor\frac{b_i}{n+1}\right\rfloor \equiv \left\lfloor\frac{b_{j+h}}{n+1}\right\rfloor - \left\lfloor\frac{b_j}{n+1}\right\rfloor \,(\text{mód } m).$$

Luego, existe un entero t tal que

$$\left\lfloor\frac{b_{i+h-(n+1)}}{n+1}\right\rfloor - 1 - \left\lfloor\frac{b_i}{n+1}\right\rfloor = \left\lfloor\frac{b_{j+h}}{n+1}\right\rfloor - \left\lfloor\frac{b_j}{n+1}\right\rfloor + tm.$$

Ahora, multiplicando la anterior igualdad por $n + 1$, obtenemos

$$\begin{aligned}&(n+1)\left(\left\lfloor\frac{b_{i+h-(n+1)}}{n+1}\right\rfloor - 1\right) - (n+1)\left\lfloor\frac{b_i}{n+1}\right\rfloor =\\ &(n+1)\left\lfloor\frac{b_{j+h}}{n+1}\right\rfloor - (n+1)\left\lfloor\frac{b_j}{n+1}\right\rfloor + tm(n+1).\end{aligned}$$

Si ahora añadimos $h = (i+h) - i = (j+h) - j$ a ambos lados de la ecuación, tenemos

$$\begin{aligned}&(n+1)\left(\left\lfloor\frac{b_{i+h-(n+1)}}{n+1}\right\rfloor - 1\right) + (i+h) - \left[(n+1)\left\lfloor\frac{b_i}{n+1}\right\rfloor + i\right] = (n+1)\left\lfloor\frac{b_{j+h}}{n+1}\right\rfloor\\ &+ (j+h) - \left[(n+1)\left\lfloor\frac{b_j}{n+1}\right\rfloor + j\right] + tm(n+1).\end{aligned}$$

Ya que $i+h > n+1$, entonces, reemplazando $i+h = k+(n+1)$.

$$(n+1)\left(\left\lfloor \frac{b_{k+(n+1)-(n+1)}}{n+1} \right\rfloor - 1\right) + k + (n+1) - b_i = b_{j+h} - b_j + tm(n+1).$$

$$(n+1)\left\lfloor \frac{b_k}{n+1} \right\rfloor + k - b_i = b_{j+h} - b_j + tm(n+1).$$

$$b_k - b_i - b_{j+h} + b_j = tm(n+1),$$

esto implica que,

$$b_k + b_j \equiv b_{j+h} + b_i \,(\text{mód } m(n+1)).$$

Pero como B es un conjunto de Sidon en $\mathbb{Z}_{m(n+1)}$, entonces $\{k,j\} = \{j+h,i\}$. Pero claramente, $j \neq j+h$ y por hipótesis $j < i$ por tanto llegamos a una contradicción ya que este caso nunca se puede presentar.

3. Si $i+h < n+1$ y $j+h > n+1$. Entonces al seguir los mismos pasos como en el caso anterior llegamos a una nueva contradicción dado que este caso es imposible.

4. Si $i+h > n+1$ y $j+h > n+1$. Entonces, se sigue de (4.39) las siguientes igualdades $a_{i+h} - a_i = a_{i+h-(n+1)} - 1 - a_i$ y $a_{j+h} - a_j = a_{j+h-(n+1)} - 1 - a_j$, cuando reemplazamos esta información en la congruencia inicial llegamos al Caso 1, de donde se sigue la misma conclusión.

De todo lo anterior concluimos que la secuencia es una secuencia sonar extendida circular. □

Una consecuencia de la Proposición 1, la Proposición 2 y el Teorema 23, son las siguientes construcciones de secuencias sonar extendidas circulares. La demostración se sigue inmediatamente del Teorema 23.

Corolario 6. (**Secuencia Bose Extendida Circular**). Sea $B(q,\theta)$ el conjunto de Sidon tipo Bose dado en el Teorema 1. Entonces la secuencia definida por:

$$a_i = \begin{cases} \left\lfloor \dfrac{b_i}{q+1} \right\rfloor, & i \in [1,q]. \\ *, & i = q+1. \\ \left\lfloor \dfrac{b_{i-(q+1)}}{q+1} \right\rfloor - 1 \,(\text{mód } q-1), & i \in [q+2, 2q+1]. \end{cases} \tag{4.40}$$

donde $b_i \in B(q,\theta)$ es el único elemento tal que $b_i \equiv \ i \,(\text{mód } q+1)$, es una secuencia sonar extendida circular que además es modular, con $c=-1$, $d=q-1$ y $n=q$.

Corolario 7. (**Secuencia sonar Ruzsa extendida circular**). Sea $R(\theta, p)$ el conjunto de Sidon tipo Ruzsa dado en el Teorema 4. Entonces la secuencia definida por:

$$a_i = \begin{cases} \left\lfloor \frac{b_i}{p} \right\rfloor, & i \in [1, p-1]. \\ *, & i = p. \\ \left\lfloor \frac{b_{i-p}}{p} \right\rfloor - 1 \,(\text{mód}\, p-1), & i \in [p+1, 2p-1]. \end{cases} \tag{4.41}$$

donde $b_i \in R(\theta, p)$ es el único elemento tal que $b_i \equiv \ i \,(\text{mód}\, p)$, es una secuencia sonar extendida circular que además resulta ser modular con $c = -1$, $d = n = p - 1$.

Como consecuencia del Teorema 22 y los anteriores resultados proporcionamos las siguientes construcciones de secuencias sonar extendidas:

Corolario 8. (**Secuencia Bose extendida**). Sean, q una potencia prima y $[a_1, \ldots, a_{2q+1}]$ una secuencia sonar extendida circular tipo Bose como la dada en el Corolario 6. Entonces cada secuencia establecida de la siguiente forma

$$[a_{k+1}, a_{k+2}, ..., a_{k+q+2}],$$

es una $(q-1, q+1, 1)$ secuencia sonar extendida para $k \in [0, q-1]$.

Ejemplo 12. Sean, $q = 11$ y $B(11, \theta)$ el conjunto de Sidon en $\mathbb{Z}_{120}$ del Ejemplo 9. Ahora aplicando el Corolario 6 encontramos la siguiente secuencia sonar extendida circular con $d = 10$, $m = 11$.

$$[1, 7, 1, 2, 2, 4, 1, 0, 8, 3, 6, *, 0, 6, 0, 1, 1, 3, 0, 9, 7, 2, 5].$$

Finalmente, del Corolario 8 podemos encontrar las secuencias sonar extendidas con parámetros $(10, 12, 1)$ que mostramos en la Tabla 4.2.

[1	7	1	2	2	4	1	0	8	3	6	∗	0]
[7	1	2	2	4	1	0	8	3	6	∗	0	6]
[1	2	2	4	1	0	8	3	6	∗	0	6	0]
[2	2	4	1	0	8	3	6	∗	0	6	0	1]
[2	4	1	0	8	3	6	∗	0	6	0	1	1]
[4	1	0	8	3	6	∗	0	6	0	1	1	3]
[1	0	8	3	6	∗	0	6	0	1	1	3	0]
[0	8	3	6	∗	0	6	0	1	1	3	0	9]
[8	3	6	∗	0	6	0	1	1	3	0	9	7]
[3	6	∗	0	6	0	1	1	3	0	9	7	2]
[6	∗	0	6	0	1	1	3	0	9	7	2	5]

Tabla 4.2: Secuencias sonar extendidas de parámetros (10, 12, 1)

Corolario 9. (**Secuencia Ruzsa extendida**). Sean, p primo y $[a_1, \ldots, a_{2p-1}]$ una secuencia sonar Ruzsa extendida circular dada en el Corolario 7. Entonces cada secuencia

$$[a_{k+1}, a_{k+2}, ..., a_{k+p+1}],$$

es una $(p-1, p, 1)$ secuencia sonar extendida para $k \in [0, p-2]$.

Ejemplo 13. Sea $p = 11$ y $R(2, 11)$ el conjunto de Sidon en $\mathbb{Z}_{110}$ del Ejemplo 10. Ahora aplicando el Corolario 7 al conjunto dado obtenemos la siguiente secuencia sonar extendida circular con $d = m = 10$.

$$[9, 9, 5, 8, 9, 3, 0, 5, 7, 5, *, 8, 8, 4, 7, 8, 2, 9, 4, 6, 4].$$

Finalmente, del Corolario 9 encontramos las $(10, 11, 1)$ secuencias sonar extendidas que damos en la Tabla 4.3.

[9	9	5	8	9	3	0	5	7	5	∗	8]
[9	5	8	9	3	0	5	7	5	∗	8	8]
[5	8	9	3	0	5	7	5	∗	8	8	4]
[8	9	3	0	5	7	5	∗	8	8	4	7]
[9	3	0	5	7	5	∗	8	8	4	7	8]
[3	0	5	7	5	∗	8	8	4	7	8	2]
[0	5	7	5	∗	8	8	4	7	8	2	9]
[5	7	5	∗	8	8	4	7	8	2	9	4]
[7	5	∗	8	8	4	7	8	2	9	4	6]
[5	∗	8	8	4	7	8	2	9	4	6	4]

Tabla 4.3: Secuencias sonar extendidas con parámetros $(10, 11, 1)$

En la Figura 4.2 mostramos la $(10, 11, 1)$ secuencia sonar extendida dada por

$$[9, 9, 5, 8, 9, 3, 0, 5, 7, 5, *, 8].$$

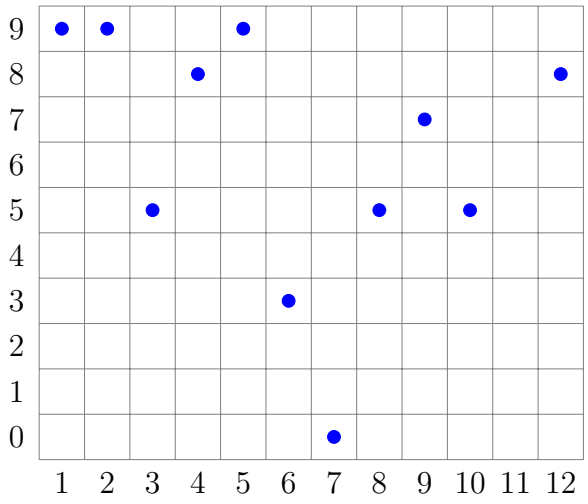


Figura 4.2: $(10, 11, 1)$ Secuencia sonar extendida.

4.5. Reglas Golomb a partir de arreglos 1−Golomb

En esta sección vamos a estudiar un resultado que nos permite obtener reglas Golomb a partir de arreglos 1−Golomb contenidos en $\mathbb{Z}\times\mathbb{Z}$. Kløve en [24] muestra una construcción de reglas Golomb disjuntas a partir de secuencias sonar. A continuación damos una generalización de este resultado que nos permite encontrar reglas Golomb partiendo de un arreglo 1−Golomb cualquiera.

Sean, $n, m \in \mathbb{Z}^+$ y $A = \{(a_1, b_1), (a_2, b_2), \ldots, (a_k, b_k)\}$ un arreglo 1−Golomb contenido en la malla rectangular $[1, n] \times [1, m]$. Definimos entonces

$$\delta_A := \text{máx}\{(b_{j'}-b_{l'})-(b_j-b_l) \ : \ a_j-a_l = a_{j'}-a_{l'}+1 \ y \ (a_j, b_j), (a_l, b_l), (a_{j'}, b_{j'}), (a_{l'}, b_{l'}) \in A\}.$$

Lema 4. Sean, $n, m, t \in \mathbb{Z}^+$ y $A \subseteq [1, n] \times [1, m]$ un arreglo 1−Golomb. Para todo $(a_j, b_j), (a_l, b_l), (a_{j'}, b_{j'}), (a_{l'}, b_{l'}) \in A$ con $a_j - a_l = a_{j'} - a_{l'} + t$, se cumple que

$$(b_{j'} - b_{l'}) - (b_j - b_l) \leq t\delta_A.$$

Demostración. Sean,

$$M_h = \text{máx}\{b_{j'} - b_{l'} \ : \ a_{j'} - a_{l'} = h\},$$

$$m_h = \text{mín}\{b_j - b_l \ : \ a_j - a_l = h\}.$$

Fácilmente observamos que,

$$\begin{aligned} M_h - m_{h+t} &= \sum_{u=0}^{t-1}(M_{h+u} - m_{h+u+1}) - \sum_{u=1}^{t-1}(M_{h+u} - m_{h+u}) \\ &\leq \sum_{u=0}^{t-1}(M_{h+u} - m_{h+u+1}) \\ &\leq \sum_{u=0}^{t-1}\delta_A = t\delta_A. \end{aligned}$$

□

Teorema 24. Sean, $n, m, q \in \mathbb{Z}^+$ y $A = \{(a_1, b_1), (a_2, b_2), \ldots, (a_k, b_k)\}$ un arreglo $1-$Golomb contenido en $[1, n] \times [1, m]$. Definimos el conjunto R de la siguiente forma

$$R := \{c_j = (a_j - 1)q + b_j \ : \quad (a_j, b_j) \in A\}.$$

Si $q > \delta_A$, entonces R es una regla Golomb con k marcas en $[1, (n-1)q + m]$.

Demostración. Veamos que todas las diferencias que provienen del conjunto R son distintas. Sean, $c_j, c_l, c_{j'}, c_{l'} \in R$. Definimos ahora

$$d = c_j - c_l = (a_j - a_l)q + b_j - b_l,$$

$$d' = c_{j'} - c_{l'} = (a_{j'} - a_{l'})q + b_{j'} - b_{l'}.$$

Entonces, $d - d' = [(a_j - a_l) - (a_{j'} - a_{l'})]q + (b_j - b_l) - (b_{j'} - b_{l'})$. Supongamos que $d = d'$ y que $a_j - a_l = a_{j'} - a_{l'} + t$, luego

$$0 = d - d' = tq + (b_j - b_l) - (b_{j'} - b_{l'}) \geq t(q - \delta_A). \tag{4.42}$$

Como $q > \delta_A$ entonces, $t = 0$. En consecuencia tenemos que $a_j - a_l = a_{j'} - a_{l'}$. Reemplazando esto en (4.42) se sigue que $b_j - b_l = b_{j'} - b_{l'}$, lo cual es imposible debido a que A es un arreglo $1-$Golomb. Por lo tanto, el único caso en el cual se generen diferencias iguales se presenta cuando $(a_j, b_j) = (a_{j'}, b_{j'})$ y $(a_l, b_l) = (a_{l'}, b_{l'})$, lo que significa $c_j = c_{j'}$ y $c_l = c_{l'}$. De todo lo anterior concluimos que R es una regla Golomb. □

Ejemplo 14. Sea A un arreglo 1− Golomb o en este caso un rectángulo Golomb contenido en $[1,4]\times[1,13]$ que se define de la siguiente manera:

$$A=\{(1,4),(1,12),(1,13),(2,1),(3,2),(3,7),(3,9),(4,1),(4,5),(4,11)\}.$$

En la Figura 4.3 representamos al conjunto A.

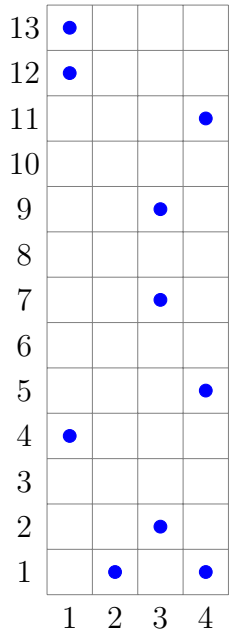


Figura 4.3: Representación de A en $\mathbb{Z}\times\mathbb{Z}$.

Para determinar δ_A necesitamos primero encontrar las siguientes diferencias:

Cuando $a_j-a_l=0$, las diferencias son $\{1,2,4,5,6,7,8,9,10\}$. En este caso $M_0=10$.

Para $a_j-a_l=1$, las diferencias son $\{-12,-11,-8,-6,-4,-3,-2,-1,1,2,3,4,6,8,9\}$. De donde $M_1=9$ y $m_1=-12$.

Para $a_j-a_l=2$, las diferencias son $\{-11,-10,-6,-5,-4,-3,-2,3,4,5,10\}$. De donde $M_2=10$ y $m_2=-11$.

Para $a_j-a_l=3$, las diferencias son $\{-12,-11,-8,-7,-3,-2,-1,1,7\}$. De donde $M_3=7$ y $m_3=-12$. Luego, $\delta_A=\text{máx}\{10-(-12),9-(-11),10-(-12)\}=\text{máx}\{20,22\}=22$.

Si aplicamos el Teorema 24 con $q=23$ tenemos la siguiente regla Golomb

$$R=\{4,12,13,24,48,53,55,70,74,80\},$$

que tiene longitud 76. Shearer propuso en [44] una construcción para transformar arreglos $1-$Golomb en reglas Golomb pero utilizando su resultado tenemos que $q = 2m - 1 = 2(13) - 1 = 25$ y encontramos la regla Golomb R' de longitud 82:

$$R' = \{4, 12, 13, 26, 52, 57, 59, 76, 80, 86\}.$$

Capítulo 5

Número Sidon Ramsey

En la Teoría de Ramsey encontramos el teorema de Schur como uno de los primeros resultados: para cada $r, n \in \mathbb{Z}^+$, con n suficientemente grande, toda $r-$coloración de $[1, n]$ contiene una solución monocromática de la ecuación $x + y = z$ [26]. Otro resultado clásico se debe a Van der Waerden: para todo $m, r \in \mathbb{Z}^+$ existe un entero $N_0 = N_0(m, r)$, tal que cada $r-$coloración de $[1, n]$ con $n \geq N_0$ contiene una progresión aritmética monocromática con m términos [26]. Los anteriores resultados involucran ecuaciones lineales que tienen una característica particular que definimos a continuación.

Definición 21. Sea $r \geq 1$. Una ecuación lineal ξ se llama $r-$regular si existe un entero positivo $n = n(\xi, r)$ tal que para cada $r-$coloración de $[1, n]$ existe una solución monocromática de ξ. La ecuación se llama regular si es $r-$regular para todo $r \geq 1$.

En una serie de artículos alrededor de 1930 Richard Rado, un estudiante doctoral de Schur, determinó las condiciones que debe cumplir una ecuación lineal homogénea para que tenga soluciones monocromáticas bajo cualquier coloración finita del intervalo entero [26]. En el caso de los sistemas de ecuaciones lineales homogéneos encontramos el Teorema completo de Rado, resultado muy importante que proporciona una poderosa herramienta que determina cuando existen soluciones monocromáticas de un sistema dado. Para establecer de forma clara dicho teorema requerimos la siguiente definición.

Definición 22. Sea $C = \begin{pmatrix} \vec{c_1} & \vec{c_2} & \dots & \vec{c_n} \end{pmatrix}$ una matriz $m \times n$, donde $\vec{c_i} \in \mathbb{Z}^m$ para $1 \leq i \leq n$. Decimos que C satisface la condición de las Columnas si sus columnas pueden ser particionadas como $C_1 \cup C_2 \cup \cdots \cup C_k$, donde cada C_i es un conjunto de vectores columnas provenientes de C, tales que las siguientes condiciones se cumplen para $\vec{s_j} = \sum_{\vec{c_i} \in C_j} \vec{c_i}$ $(1 \leq j \leq k)$:

1. $\vec{s_1} = \vec{0}$.
2. $\vec{s_j}$ puede ser escrito como una combinación lineal de los vectores del conjunto $C_1 \cup C_2 \cup \cdots \cup C_{j-1}$ para $2 \leq j \leq k$.

Ahora estamos listos para establecer el Teorema de Rado. Para conocer más sobre el resultado de Rado se puede consultar [26].

Teorema 25. [**Teorema completo de Rado**]. Sea $\mathcal{S}$ un sistema de ecuaciones lineales homogéneo. Escribamos a $\mathcal{S}$ como $A\vec{x} = \vec{0}$. $\mathcal{S}$ es regular, si y sólo si la matriz A satisface la condición de las Columnas. Además, $\mathcal{S}$ tiene una solución monocromática de distintos enteros positivos, si y sólo si $\mathcal{S}$ es regular y existen distintos enteros (no necesariamente monocromáticos) que satisfacen $\mathcal{S}$.

Aplicando el Teorema 25 podemos comprobar la existencia de soluciones monocromáticas no triviales para la ecuación Sidon, $x + y = z + w$, es decir, dicha ecuación resulta ser regular. Para esto, basta considerar la siguiente matriz

$$C = \begin{pmatrix} 1 & 1 & -1 & -1 & 0 & 0 \\ 1 & 0 & -1 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 & 0 & 1 \end{pmatrix} \tag{5.1}$$

donde se han incluido dos nuevas variables y dos nuevas ecuaciones con el fin de asegurar que las soluciones consideradas sean no triviales. Sea $C_1 = \{\vec{c_1}, \vec{c_2}, \vec{c_3}, \vec{c_4}\}$ y $C_2 = \{\vec{c_5}, \vec{c_6}\}$. Entonces tenemos que $\vec{s_1} = \vec{0}$ y $\vec{s_2} = \vec{c_5} + \vec{c_6} = 2\vec{c_1} + \vec{c_3} + \vec{c_4}$, por lo que C satisface la condición de las columnas.

La anterior observación sobre la ecuación Sidon fue dada inicialmente por Liang, Li, Xiu y Xu [27] en el año 2013 utilizando otras herramientas. Con este hallazgo introdujeron un nuevo número tipo Ramsey que denominaron Número Sidon-Ramsey.

Definición 23. Sea $r \in \mathbb{Z}^+$. El Número Sidon-Ramsey de r, denotado por $SR(r)$, se define como el menor entero positivo n tal que en toda r-coloración de $[1, n]$ existe al menos una solución monocromática (no trivial) de la ecuación $x + y = z + w$.

En otras palabras, el número Sidon-Ramsey $SR(r)$ es el mínimo entero para el cual no existe una r-coloración del intervalo $[1, SR(r)]$ donde cada clase cromática sea un conjunto de Sidon.

Liang et al. en [27] y Xu et al. en [52] encontraron valores exactos de $SR(r)$ para $r \leq 5$ y dieron cotas específicas para $r \leq 19$ con asistencia computacional. Ellos notaron

que $SR(r)$ puede ser acotado por arriba al usar las cotas conocidas del máximo cardinal de un conjunto de Sidon y el principio de las casillas. En particular, ellos mostraron los siguientes resultados

Teorema 26. Sean, $r, t \in \mathbb{Z}^+$, con $r, t \geq 2$ y $F(t)$ la función definida en (2.3). Siempre que se satisfaga la desigualdad $(F(t)-1)/(t-1) > r$, se sigue que

$$SR(r) \leq (t-1)r + 1.$$

Demostración. Ver [27]. □

Mientras que para las cotas inferiores de $SR(r)$ construyeron la siguiente cota recursiva

$$SR(a+b) \geq SR(a) + SR(b) + b - 1$$

siempre que $b \leq a$.

Por otra parte, en 2021 Espinosa et al. [19] mostraron el comportamiento asintótico de $SR(r) = (1+o(1))r^2$ en el siguiente resultado:

Teorema 27. Sea $r \in \mathbb{Z}^+$. Entonces

$$r^2 - O(r^{5/3}) \leq SR(r) \leq r^2 + Cr^{3/2} + O(r),$$

donde C puede ser cercano a 1,996 y depende de la mejor cota superior que se conozca para el máximo cardinal de un conjunto de Sidon.

También en [19] trasladaron las ideas del número Sidon-Ramsey en los enteros al grupo $G = \mathbb{Z}^d$ considerando la caja $d-$dimensional $X = \prod_{i \leq d}[1, n_i]$ estableciendo así un parámetro relacionado con $SR(r)$, para el parámetro que introdujeron lograron obtener cotas superiores e inferiores.

5.1. Número Sidon-Ramsey en $\mathbb{Z}_n$

En esta sección vamos a realizar el estudio de los números $SR(r)$ en grupos cíclicos debido a que en este contexto la teoría de los conjuntos de Sidon tiene resultados importantes que nos permitieron avanzar de forma eficaz. El punto de partida de esta investigación es entonces la definición de $SR(r)$ en $\mathbb{Z}_n$. Los resultados que mostramos en esta sección hacen parte del preprint [12].

Definición 24. Sea $r \in \mathbb{Z}^+$ con $r \geq 2$. El número Sidon-Ramsey de r para grupos cíclicos, se denota por $\overline{SR}(r)$ y se define como el menor entero positivo n tal que en toda r-coloración de $\mathbb{Z}_n$ existe al menos una solución monocromática (no trivial) de la ecuación $x + y = z + w$.

Claramente se cumple que $\overline{SR}(r) \leq SR(r)$ y así queda demostrada la existencia de $\overline{SR}(r)$. A continuación mostramos los resultados que obtuvimos en el estudio de $\overline{SR}(r)$ en cuanto a cotas y valores exactos.

5.1.1. Cotas superiores

Muchos autores coinciden en la importancia de entender más el comportamiento de la función $F(\mathbb{Z}_n)$, definida en (2.4), para poder avanzar en el estudio de la función análoga en el caso entero [30]. Hasta la fecha se conoce muy poco del comportamiento de la función $F(\mathbb{Z}_n)$, por ejemplo en cuanto a cotas superiores solo se conoce que $F(\mathbb{Z}_n) \leq n^{1/2} + 1$ resultado de Martin y O'Bryant en [30], con esta información vamos a encontrar nuestra primer cota superior de $\overline{SR}(r)$.

Teorema 28. Sea $r \in \mathbb{Z}^+$ con $r \geq 2$, entonces $\overline{SR}(r) \leq r^2 + O(r)$.

Demostración. La mejor cota superior conocida para el cardinal de un conjunto de Sidon modular en $\mathbb{Z}_n$ es $F(\mathbb{Z}_n) \leq n^{1/2} + 1$. De lo anterior y usando el principio de las casillas deducimos que el grupo $\mathbb{Z}_n$ no puede ser particionado en menos de

$$r \geq \frac{n}{F(\mathbb{Z}_n)} \geq \frac{n}{n^{1/2} + 1}$$

conjuntos de Sidon. Lo anterior se puede simplificar usando las series geométricas

$$\begin{aligned} r &\geq \frac{n^{1/2}}{1 + n^{-1/2}} \\ &\geq n^{1/2}(1 - O(n^{-1/2})) \\ &\geq n^{1/2} - O(1), \end{aligned}$$

de donde al despejar $n^{1/2}$ tenemos

$$n^{1/2} \leq r + O(1).$$

Finalmente concluimos que

$$n \leq r^2 + O(r).$$

□

Un resultado más preciso pero así mismo más limitado que el del Teorema 28 lo encontramos de la misma forma que Liang et al. en [27] cuando ellos estudiaban $SR(r)$. Para establecer cotas superiores de $\overline{SR}(r)$ utilizamos valores exactos de la función $f^*(k)$ que fue definida en (2.7). Estos valores deben cumplir una desigualdad en relación a un valor fijo de r. Por lo anterior vamos a tener presente la Tabla 2.1.

Teorema 29. Sean, $r, k \in \mathbb{Z}^+$. Para r fijo, si k es el menor valor para el cual

$$f^*(k) > r(k-1)+1,$$

entonces $\overline{SR}(r) \leq (k-1)r+1$.

Demostración. Por hipótesis tenemos que si $m = r(k-1)+1$, entonces en $\mathbb{Z}_m$ no existe un conjunto de Sidon de cardinal k. Además, por el principio de las casillas toda $r-$coloración de $\mathbb{Z}_m$ tendrá una clase cromática de tamaño mayor o igual a k, claramente dicha clase cromática debe contener la solución no trivial de la ecuación $x+y=z+w$ ya que no puede ser un conjunto de Sidon, por lo tanto $\overline{SR}(r) \leq (k-1)r+1$. □

Ejemplo 15. Para $r=5$ tenemos que $k=6$ satisface $f^*(6)=31 > 5(6-1)+1=26$. Así, del Teorema 29 se sigue la cota superior $\overline{SR}(5) \leq 26$.

Aplicando el Teorema 29 establecemos en la Tabla 5.1 las cotas superiores de $\overline{SR}(r)$ para $2 \leq r \leq 18$.

r	2	3	4	5	6	7	8	9	10
$\overline{SR}(r) \leq$	5	10	17	26	37	43	65	82	101
r	11	12	13	14	15	16	17	18	
$\overline{SR}(r) \leq$	111	145	157	197	211	225	239	253	

Tabla 5.1: Cotas superiores de $\overline{SR}(r)$ aplicando el Teorema 29.

Aplicando el Teorema 29 encontramos la limitación de que los valores conocidos de la función $f^*(k)$ son pocos; en el caso entero se presento la misma dificultad y hasta ahora no se conoce un resultado alternativo. En nuestro caso, con el fin de encontrar una solución a esta limitación, buscamos alternativas en la teoría de los conjuntos de Sidon y conceptos relacionados. Después de varios intentos logramos utilizar parte de la teoría de los conjuntos casi diferencia en nuestra investigación y conseguimos generar infinitas cotas superiores para $\overline{SR}(r)$, cotas que en algunos casos mejoran las de la Tabla 5.1. La forma en que aplicamos la teoría de los CCD en nuestro estudio la ejemplificamos a continuación.

Ejemplo 16. Recordemos que al aplicar el Teorema 29 encontramos $\overline{SR}(5) \leq 26$. Ahora afirmamos que $\overline{SR}(5) \leq 22$.

En efecto, como consecuencia del principio de las casillas tenemos que toda $5-$coloración de $\mathbb{Z}_{22}$ contiene una clase cromática de tamaño al menos 5. Vamos a probar que esta clase es la que contiene la solución no trivial de la ecuación de Sidon. Para esto, denotamos con A dicha clase. El objetivo es mostrar que A no puede ser un conjunto de Sidon.

Si $|A| > 5$, entonces A no puede ser Sidon ya que $f^*(6) = 31$. Por lo tanto, de ahora en adelante suponemos que $|A| = 5$. Observemos que:

- Como el cardinal de $\mathbb{Z}_{22}$ es par, se cumple que si $A \subseteq \mathbb{Z}_{22}$ es un conjunto de Sidon, entonces $11 \notin A - A$.
- Si $A \subseteq \mathbb{Z}_{22}$ es un conjunto de Sidon con $|A| = 5$, entonces $A - A = \mathbb{Z}_{22} \setminus \{11\}$. Además, al considerar $A-A$ como un multiconjunto encontramos que los elementos de $\mathbb{Z}_{22} \setminus \{0, 11\}$ tienen única representación, el 0 cinco representaciones y el 11 ninguna.

Luego, el conjunto A satisface la Definición 6 y por consiguiente es un $(22, 5, 0, 1)-$conjunto casi diferencia en $\mathbb{Z}_{22}$. Por lo tanto, probar que A no es un conjunto de Sidon equivale a mostrar que A no es un $(22, 5, 0, 1)$-CCD. Para esto, hacemos uso de las condiciones necesarias para la existencia de CCD dadas en el Teorema 7.

Las ecuaciones diofánticas del Teorema 7 con $n = 22$, $k = 5$, $\lambda = 0$, $t = 1$, $w = 2$ son:

$$b_0 + b_1 = 5,$$

$$c_0 + c_1 = 1,$$

$$b_0^2 + b_1^2 = 15 - c_0,$$

$$2b_0b_1 = 11 - c_1.$$

Note que $c_0 = 0$ y $c_1 = 1$ ya que $S(X) = X^{11}$. Luego, $2b_0b_1 = 10$ de donde se sigue que $b_0b_1 = 5$. Luego la única solución en enteros positivos es $\{1, 5\}$ lo cual contradice con $b_0 + b_1 = 5$. Así el sistema de ecuaciones diofánticas no tiene solución en $\mathbb{Z}$. Por lo tanto, la clase cromática A no puede ser un $(22, 5, 0, 1)$-CCD, esto equivale a decir que A debe contener una solución monocromática no trivial de la ecuación de Sidon. Como esto se satisface para cualquier $5-$coloración de $\mathbb{Z}_{22}$, concluimos que $\overline{SR}(5) \leq 22$.

Después de generalizar las ideas del Ejemplo 16 logramos encontrar el Teorema 30 que establece condiciones para la existencia de los conjuntos casi diferencia en $G = \mathbb{Z}_n$ con n par. A partir del Teorema 30 establecemos el resultado más importante de nuestra investigación sobre $\overline{SR}(r)$ enunciado en el Corolario 10 que aparece abajo. Dicho aporte permite encontrar infinitas cotas superiores para $\overline{SR}(r)$ y tiene implicaciones directas a la teoría de los conjuntos de Sidon. Después de revisar la literatura encontramos que el Teorema 30 se estableció en [53] por Zhang *et al.* Este trabajo se especializa exclusivamente al estudio de los CCD en diferentes grupos, pero consideramos importante resaltar que la demostración del Teorema 30 utiliza teoría de carácteres mientras que nuestra prueba es combinatoria.

Teorema 30 (Teorema 3.7 en [53])**.** Sean $k, \lambda, t \in \mathbb{Z}^+$, con $k > 2$ y n par. En $\mathbb{Z}_n$ no existe un (n, k, λ, t)-conjunto casi diferencia en los siguientes casos

i) Cuando t sea par y $k+t-\lambda-4i-1$ no sea un cuadrado para todo $i \in \left[0, \dfrac{t-1}{2}\right)$.

ii) Cuando t sea impar, $n \equiv 0(\text{mód}4)$ y $k+t-\lambda-4i-3$ no sea un cuadrado para todo $i \in \left[0, \dfrac{t-1}{2}\right]$.

iii) Cuando t sea impar, $n \equiv 2(\text{mód}4)$ y $k+t-\lambda-4i-1$ no sea un cuadrado para todo $i \in \left[0, \dfrac{t-1}{2}\right]$.

Demostración. Para mostrar la no existencia del (n, k, λ, t)-CCD vamos a utilizar las siguientes ecuaciones diofánticas que resultan del Teorema 7 con $w = 2$:

$$c_0 + c_1 = t,$$

$$b_0 + b_1 = k,$$

$$2b_0b_1 = (\lambda+1)\frac{n}{2} - c_1.$$

No escribimos la ecuación (2.12) ya que en la Observación 1 mostramos que proviene de las otras tres. Las anteriores ecuaciones no tienen soluciones enteras positivas en los casos i), ii) y iii) como lo vamos a demostrar a continuación.

Recordemos que el conjunto S está conformado por los elementos del grupo que tienen λ representaciones como diferencia de los elementos del CCD. Es claro que si $a \in S$, entonces $-a \in S$. Por otra parte, dado que n es par se cumplen que:

Si $X^a \equiv X^j(\text{mód}\,2)$, entonces $X^{-a} \equiv X^j(\text{mód}\,2)$ para $j \in \{0, 1\}$.

Finalmente, recordemos que los parámetros de un (n, k, λ, t)-CCD deben satisfacer siempre la siguiente igualdad (2.8) que es

$$t = (\lambda + 1)(n - 1) - k(k - 1).$$

i) Supongamos ahora que t es par. De la ecuación (2.8) se sigue que λ debe ser impar. Como el elemento $n/2 \in \mathbb{Z}_n$ tiene un número par de representaciones como diferencia de elementos del CCD, entonces $n/2 \notin S$. Si

$$S(X) \equiv c_0 X^0 + c_1 X (\text{mód } 2),$$

entonces los posibles valores de c_0 y c_1 son de la forma, $c_0 = 2i$ y $c_1 = t - 2i$ con $i \in \left[0, \frac{t-1}{2}\right)$. Por otra parte, de (2.8) se sigue que $(\lambda+1)n = k(k-1)+t+\lambda+1$. Reemplazando estos valores en las ecuaciones iniciales encontramos:

$$b_0 + b_1 = k, \tag{5.2}$$

$$b_0 b_1 = \frac{k^2 - k - t + \lambda + 4i + 1}{4}. \tag{5.3}$$

Por otro lado, resulta que b_0 y b_1 también son soluciones de la ecuación cuadrática $x^2 - (b_0 + b_1)x + b_0 b_1 = 0$ y como necesitamos que b_0 y b_1 sean soluciones enteras de (5.2) y (5.3), esto equivale a que la ecuación cuadrática tenga raíces enteras. Por lo tanto, es necesario que el discriminante

$$k^2 - 4\frac{k^2 - k - t + \lambda + 4i + 1}{4},$$

sea un cuadrado, es decir, que $k + t - \lambda - 4i - 1$ sea un cuadrado para algún $i \in \left[0, \frac{t-1}{2}\right)$. Pero por hipótesis ninguno de estos valores es un cuadrado, luego las ecuaciones (5.2) y (5.3) no tienen solución en $\mathbb{Z}^+$. Concluimos así que no puede existir el $(n, k, \lambda, t)-$CCD.

ii) Para t impar, se sigue de la ecuación (2.8) que λ debe ser par y por tanto $n/2 \in S$. Además, dado que $n \equiv 0 (\text{mód } 4)$, entonces $X^{n/2} \equiv X^0 (\text{mód } 2)$. Por lo tanto, si

$$S(X) \equiv c_0 X^0 + c_1 X (\text{mód } 2),$$

entonces los posibles valores de c_0 y c_1 son de la forma $c_0 = 1 + 2i$ y $c_1 = t - 1 - 2i$ para $i \in \left[0, \frac{t-1}{2}\right]$. Reemplazando estos valores y $(\lambda + 1)n = k(k-1) + t + \lambda + 1$ en las ecuaciones iniciales encontramos:

$$b_0 + b_1 = k, \tag{5.4}$$

$$b_0 b_1 = \frac{k^2 - k - t + \lambda + 4i + 3}{4}. \tag{5.5}$$

Igual que en el caso anterior, observamos que b_0 y b_1 son soluciones de la ecuación cuadrática $x^2 - (b_0 + b_1)x + b_0 b_1 = 0$ y como necesitamos que b_0 y b_1 sean soluciones enteras de (5.4) y (5.5), esto es equivalente a que la ecuación cuadrática tenga raíces enteras. Para que se cumpla esto es necesario que el discriminante

$$k^2 - 4\Big(\frac{k^2 - k - t + \lambda + 4i + 3}{4}\Big),$$

sea un cuadrado, es decir, que $k + t - \lambda - 4i - 3$ sea un cuadrado para algún $i \in \left[0, \frac{t-1}{2}\right]$. Pero por hipótesis ninguno de estos valores es un cuadrado, por lo que las ecuaciones (5.4) y (5.5) no tienen solución en $\mathbb{Z}^+$. De ahí se sigue la no existencia del $(n, k, \lambda, t)-$CCD.

iii) Por otro lado, si t es impar, nuevamente λ debe ser par y $n/2 \in S$. Pero, si suponemos que $n \equiv 2 \,(\text{mód } 4)$, entonces $X^{n/2} \equiv X^1 (\text{mód } X^2 - 1)$. Luego, si

$$S(X) \equiv c_0 X^0 + c_1 X \,(\text{mód } 2),$$

entonces los posibles valores de c_0 y c_1 son de la forma, $c_0 = 2i$ y $c_1 = t - 2i$ llegando nuevamente al caso i) y por tanto al tener las mismas condiciones se sigue que las ecuaciones iniciales no tienen soluciones enteras completando así la prueba del teorema.

□

En el siguiente ejemplo evidenciamos que el Teorema 30 también resulta ser un aporte a la teoría de las reglas g-Golomb modulares. Es fácil evidenciar que el Teorema 30 es más fuerte que el resultado de no existencia sobre reglas Golomb de Buratti y Stinson en [4].

Ejemplo 17. En $\mathbb{Z}_{68}$ no puede existir una regla $2-$Golomb de cardinal 12 con la siguiente condición: Las diferencias generadas por la regla $2-$Golomb representan a dos elementos del grupo de forma única y a los demás elementos no nulos con dos representaciones. Lo anterior es equivalente a demostrar que no existe un $(68, 12, 1, 2)$-CCD, lo cual se concluye fácilmente al aplicar el caso i) del Teorema 30 ya que $t = 2$ y $k + t - \lambda - 1 = 12$ no es un cuadrado.

Claramente el Teorema 30 también permite demostrar la no existencia de algunos conjuntos de Sidon modulares.

Ejemplo 18. En $\mathbb{Z}_{424}$ no existe un conjunto de Sidon de cardinal 21. En efecto, al considerar las diferencias generadas por los elementos del conjunto de Sidon siempre quedarán 3 elementos no nulos sin representación. Por lo tanto, demostrar que no existe un conjunto de Sidon equivale a demostrar la no existencia de un $(424, 21, 0, 3)$-CCD, lo cual se sigue fácilmente de la parte *ii)* del Teorema 30 dado que $424 \equiv 0\,(\text{mód}\,4)$ y los números $k + t - 3 = 21$ y $k + t - 4 - 3 = 17$ no son cuadrados.

A continuación mostramos el aporte más importante de esta sección que inicialmente fue la motivación que nos llevó a estudiar los CCD. El Corolario 10 nos permite encontrar cotas superiores de $\overline{SR}(r)$ para infinitos valores de r, con lo cual logramos superar la limitación del Teorema 29 e incluso mejorar algunos de sus resultados.

Corolario 10. Sean, $r \in \mathbb{Z}^+$ mayor que 2 y $n = r(r-1) + 2$, entonces $\overline{SR}(r) \leq n$ siempre que se cumpla alguno de los siguientes casos:

i) $n \equiv 0\,(\text{mód}\,4)$ y $r - 2$ no sea un cuadrado.

ii) $n \equiv 2\,(\text{mód}\,4)$ y r no sea un cuadrado.

Demostración. Para demostrar que toda $r-$coloración de $\mathbb{Z}_n$ siempre contiene una solución monocromática no trivial de la ecuación $x + y = z + w$ observemos que por el principio de las casillas en toda $r-$coloración de $\mathbb{Z}_n$ tenemos una clase cromática con al menos r elementos. La idea es mostrar que esta clase no puede ser un conjunto de Sidon, lo cual equivale a probar la no existencia de un $(n, r, 0, 1)$ conjunto casi diferencia en $\mathbb{Z}_n$.

i) En el caso en que $n \equiv 0\,(\text{mód}\,4)$ y $r - 2$ no es un cuadrado podemos aplicar la parte ii) del Teorema 30 con $t = 1$ y $k = r$ de donde se concluye la no existencia del $(n, r, 0, 1)$-CCD.

ii) Mientras que cuando $n \equiv 2\,(\text{mód}\,4)$ y r no sea un cuadrado podemos aplicar la parte iii) del Teorema 30 con $t = 1$ y $k = r$ para concluir la no existencia del $(n, r, 0, 1)$-CCD en $\mathbb{Z}_n$. Finalizando así la demostración del corolario.

□

Recordemos que al aplicar el Teorema 29 encontramos de acuerdo a la Tabla 5.1 que $\overline{SR}(8) \leq 65$. Con ayuda del Corolario 10 vamos a mejorar esta cota superior.

Ejemplo 19. Sean, $r = 8$ y $n = 58$. Dado que $58 \equiv 2\,(\text{mód}\,4)$ y que $r = 8$ no es cuadrado, entonces por la parte *ii)* del Corolario 10 se concluye que $\overline{SR}(8) \leq 58$.

En la Tabla 5.2 mostramos cotas superiores de $\overline{SR}(r)$ para $5 \leq r \leq 45$ que se obtienen del Corolario 10. Con negrita resaltamos los resultados mejorados con respecto a la Tabla 5.1.

r	5	7	8	10	12	13	14	15
$\overline{SR}(r) \leq$	**22**	44	**58**	**92**	**134**	158	**184**	212
r	17	19	20	21	22	23	24	26
$\overline{SR}(r) \leq$	274	**344**	**382**	**422**	**464**	**508**	**554**	**652**
r	28	29	30	31	32	33	34	35
$\overline{SR}(r) \leq$	**758**	**814**	**872**	**932**	**994**	**1058**	**1124**	**1192**
r	37	39	40	41	42	43	44	45
$\overline{SR}(r) \leq$	**1334**	**1484**	**1562**	**1642**	**1724**	**1808**	**1894**	**1982**

Tabla 5.2: Cotas superiores que provienen del Corolario 10

Los resultados derivados del Teorema 30 son consecuencia de que nuestra investigación inició en el estudio de $\overline{SR}(r)$ y por haber establecido la relación entre los conjuntos de Sidon y los conjuntos casi diferencia. A continuación damos un resultado que proporciona una cota superior de la función $F(\mathbb{Z}_n)$ para algunos valores de n. Esta cota mejora la establecida en [30] por Martin y O'Bryant.

Corolario 11. Sean, $k, t \in \mathbb{Z}^+$, con $k > 2$, t impar y $n = k(k-1) + 1 + t$. Se tiene la cota superior $F(\mathbb{Z}_n) < k$ en los siguientes casos:

i) Cuando $n \equiv 0\,(\text{mód}\,4)$ y $k + t - 4i - 3$ no sea cuadrado para todo $i \in \left[0, \dfrac{t-1}{2}\right]$.

ii) Cuando $n \equiv 2\,(\text{mód}\,4)$ y $k + t - 4i - 1$ no sea un cuadrado para todo $i \in \left[0, \dfrac{t-1}{2}\right]$.

Demostración. Si aplicamos las hipótesis de la parte *i)* en el Teorema 30 item *ii)*, entonces queda garantizado que en $\mathbb{Z}_n$ no existe un conjunto de Sidon de cardinal k, por lo tanto $F(\mathbb{Z}_n) < k$.

De igual manera, las hipótesis de la parte *ii)* aplicadas en el Teorema 30 item *iii)* garantizan la no existencia de un conjunto de Sidon con cardinal k en $\mathbb{Z}_n$, luego $F(\mathbb{Z}_n) < k$. □

Según Martin y O'Bryant [30] existe un consenso entre investigadores del problema Sidon de que un progreso substancial sobre el crecimiento de $F(n)$ requiere una mayor comprensión de la función $F(\mathbb{Z}_n)$ que exhibe la importancia del Corolario 11. Adicionalmente, cuando las hipótesis del Corolario 11 se cumplan con k y t cada vez más grandes, podemos inferir que la cota superior de la función F evaluada en los grupos $\mathbb{Z}_{k(k-1)+i+1}$ donde $i \in \{1, 3, 5, \ldots, t\}$ es la misma, es decir, $F(\mathbb{Z}_{k(k-1)+i+1}) \leq k-1$.

Ejemplo 20. Recordemos que $F(\mathbb{Z}_{273}) = 17$ como consecuencia de la construcción de Singer. Mostramos a continuación que el valor de la función F en los grupos $\mathbb{Z}_{274}$, $\mathbb{Z}_{276}$ y $\mathbb{Z}_{278}$, es menor a 17.

- Sean, $k = 17$, $t = 1$ y $n = 17(16) + 2 = 274$. Como $n \not\equiv 0 (\text{mód } 4)$ y $k = 17$ no es un cuadrado, entonces por el caso $i)$ del Corolario 11 se tiene que $F(\mathbb{Z}_{274}) \leq 16$.
- Si $k = 17$, $t_1 = 3$ y $n_1 = 17(16) + 4 = 276$, tenemos que $n_1 \equiv 0 (\text{mód } 4)$, $k = 17$ y $k - 4 = 13$ no son cuadrados. Entonces por el caso $i)$ del Corolario 11 se tiene que $F(\mathbb{Z}_{276}) \leq 16$.
- Finalmente, sean $k = 17$, $t_2 = 5$ y $n_2 = 17(16)+6 = 278$. Dado que $n_2 \equiv 2 (\text{ mód } 4)$, $k + 4 = 21$, $k = 17$ y $k - 4 = 13$ no son cuadrados, entonces por el caso $ii)$ del Corolario 11 se tiene que $F(\mathbb{Z}_{278}) \leq 16$.

Al igual que en el anterior ejemplo nuestro siguiente resultado muestra que la función $F(\mathbb{Z}_n)$ tiene la misma cota superior para todos los valores de n pares, que pertenezcan a intervalos arbitrariamente grandes.

Corolario 12. Sean, $m, t \in \mathbb{Z}^+$ con m mayor que uno, t impar y tales que $t \leq 2m$. En $\mathbb{Z}_{m^4+m^2+1+t}$ no existe un $(m^4 + m^2 + 1 + t, m^2 + 1, 0, t)-$conjunto casi diferencia y por tanto, $F(\mathbb{Z}_{m^4+m^2+1+t}) \leq m^2$.

Demostración. Para la prueba aplicamos el Teorema 30 con $n = m^4 + m^2 + 1 + t$ que claramente es par, con $k = m^2 + 1$ y los parámetros dados en la hipótesis.

Observemos que los cuadrados más cercanos a $m^2 + 1$ son precisamente $(m-1)^2$ y m^2; además, sin importar la congruencia de n módulo 4 únicamente tres términos de las condiciones del Teorema 30 que damos a continuación pueden ser estos cuadrados. Por todo lo anterior, la no existencia del conjunto casi diferencia queda garantizada si mostramos que $k+t-3$ y $k+t-1$ no son m^2 y que $k-t+1$ no es $(m-1)^2$. En efecto, dado que t es un número impar, se cumple que $k+t-3 \neq m^2$ y $k+t-1 \neq m^2$. Además, la distancia de m^2 a $k-t+1$ es $t-2$, pero por hipótesis esta distancia es menor que $2m-1$ y en consecuencia $k-t+1 \neq (m-1)^2$, quedando así demostrado el corolario. □

Del anterior resultado es fácil observar que cuando $m = p^2$ con p primo, se satisface la siguiente desigualdad $F(\mathbb{Z}_{m^2+m+2}) < F(\mathbb{Z}_{m^2+m+1})$. Esto debido a que $F(\mathbb{Z}_{m^2+m+1}) = m+1$ por la construcción de Singer y $F(\mathbb{Z}_{m^2+m+2}) < m+1$ como resultado del Corolario 12.

Corolario 13. Sea $r-1$ un cuadrado mayor o igual que 4. Entonces $\overline{SR}(r) \leq r^2 - r + 2$.

Demostración. Del principio de las casillas se sigue que toda $r-$coloración de $\mathbb{Z}_{r^2-r+2}$ tiene una clase cromática con al menos r elementos. Afirmamos que esta clase no puede ser un conjunto de Sidon. En efecto, aplicando el Corolario 12 con $n = r-1$, tenemos que $F(\mathbb{Z}_{r^2-r+2}) < r$. Por lo tanto, $\overline{SR}(r) \leq r^2 - r + 2$. □

Nuestro siguiente resultado muestra otra familia infinita de grupos para los cuales no existe un conjunto de Sidon con un cardinal determinado y por ende se establece de inmediato una cota superior de la función $F(\mathbb{Z}_n)$ evaluada en estos grupos.

Corolario 14. Sean, $p \equiv 3\,(\text{mód}\,4)$ un número primo, $r \in \mathbb{Z}^+ \cup \{0\}$ y $q = p^{2r+1}$ con $q \neq 3$. En $\mathbb{Z}_{q^2+q+2}$ no existe un $(q^2+q+2, q+1, 0, 1)-$conjunto casi diferencia y por tanto $F(\mathbb{Z}_{q^2+q+2}) \leq q$.

Demostración. Claramente $n = q^2 + q + 2$ es par y dado que $p \equiv 3\,(\text{mód}\,4)$, entonces $n \equiv 2\,(\text{mód}\ 4)$. Lo anterior nos permite aplicar el item *iii)* del Teorema 30 con $k = q+1$, $\lambda = 0$ y $t = 1$.

En este caso, la no existencia del conjunto casi diferencia está garantizada si $q+1$ no es un cuadrado. La prueba la vamos a realizar por contradicción. Supongamos que existe $a \in \mathbb{Z}$ tal que $q + 1 = a^2$. Por lo tanto, $(a+1)(a-1) = p^{2r+1}$, de donde se sigue que la descomposición de $a+1$ y $a-1$ en factores primos debe ser de la forma $a+1 = p^l$ y $a-1 = p^m$ con $l + m = 2r+1$. Además, $|a+1-(a-1)| = |p^l - p^m| = 2$. Lo cual es una contradición dado que el único caso en el que se pueden cumplir estas condiciones es cuando $p = 3$ y $r = 0$. □

Aunque algunos de los anteriores resultado proporcionan cotas superiores de $\overline{SR}(r)$ para casi todos los valores de r, existen casos muy puntuales donde el Corolario 10 no puede ser usado a pesar de tener casi todas las condiciones del mismo; en estos casos es necesario aplicar otras herramientas.

Ejemplo 21. Del Teorema 29 tenemos que $\overline{SR}(6) \leq 37$. A continuación mostramos que $\overline{SR}(6) \leq 32$.

En $\mathbb{Z}_{32}$ toda 6−coloración contiene una clase cromática de tamaño al menos 6. Cumpliéndose así las primeras condiciones del Corolario 10 con $r = 6$ y $t = 1$, pero debido a que $32 \equiv 0 \,(\text{mód}\, 4)$ y $r - 2 = 4$ es un cuadrado, entonces no se puede aplicar dicho corolario. Afortunadamente Zhang, Lei y Zhang en [53] mostraron por medio de asistencia computacional la no existencia de un (32,6,0,1)-CCD en $\mathbb{Z}_{32}$. Por lo tanto, concluimos que $\overline{SR}(6) \leq 32$.

En la Tabla 5.3 damos las mejores cotas superiores que encontramos para $\overline{SR}(r)$ donde $r \in [2, 19]$.

r	$\overline{SR}(r) \leq$	Resultado Aplicado	r	$\overline{SR}(r) \leq$	Resultado Aplicado
2	5	Teorema 29	11	111	Teorema 29
3	10	Teorema 29	12	134	Corolario 10
4	17	Teorema 29	13	157	Teorema 29
5	22	Corolario 10	14	184	Corolario 10
6	32	Zhang, Lei y Zhang en [53]	15	211	Teorema 29
7	43	Teorema 29	16	225	Teorema 29
8	58	Corolario 10	17	239	Teorema 29
9	82	Teorema 29	18	253	Teorema 29
10	92	Corolario 10	19	344	Corolario 10

Tabla 5.3: Las mejores cotas superiores para $\overline{SR}(r)$.

Para finalizar el estudio de las cotas superiores de $\overline{SR}(r)$ con ayuda de la conjetura de las Potencias Primas [22] establecemos la siguiente conjetura:

Conjetura 1. Sean, $r \in \mathbb{Z}^+$, $r > 2$ y $n = r(r-1)+1$. Si $r-1$ no es una potencia prima, entonces $\overline{SR}(r) \leq n$.

Observemos que la Conjetura 1 es una consecuencia directa de la Conjetura de las Potencias Primas, esto debido a que la hipótesis de la Conjetura 1 mediante la Conjetura de Potencias Primas se traduce en la no existencia en $\mathbb{Z}_n$ de un conjunto diferencia planar de orden $r-1$ o equivalentemente un conjunto de Sidon de cardinal r. Además, aplicando el principio de las casillas toda r−coloración de $\mathbb{Z}_n$ tienen una clase cromática de cardinal r y por la anterior conclusión tenemos que esta clase cromática es la que contiene la solución no trivial de la ecuación de Sidon. Mostrándose así que $\overline{SR}(r) \leq n$.

5.1.2. Cotas inferiores

En el caso de las cotas inferiores de $\overline{SR}(r)$ el proceso es totalmente distinto a lo realizado en la anterior sección. Por ejemplo, para establecer $\overline{SR}(r) \geq m$ con r fijo se debe exhibir r-coloraciones de $\mathbb{Z}_n$ donde todas las clases cromáticas sean conjuntos de Sidon para todo $n \leq m$. Es claro que una r-coloración de $\mathbb{Z}_n$ con todas sus clases cromáticas Sidon garantiza la existencia de una $(r+1)$-coloración de $\mathbb{Z}_n$ en las mismas condiciones, es decir, $\overline{SR}(r) \leq \overline{SR}(r+1)$.

Ejemplo 22. Enseguida mostramos la mejor cota inferior para $\overline{SR}(6)$. Partimos de que $\overline{SR}(5) = 22 \leq \overline{SR}(6)$. La búsqueda la realizamos empleando los programas computacionales MatLab y SAGE [48] empleando "fuerza bruta", iniciamos en $\mathbb{Z}_{22}$.

- Para $\mathbb{Z}_{22}$ encontramos la 6−coloración $\{0, 13, 15\}$, $\{1, 2, 6, 21\}$, $\{3, 5, 17, 20\}$, $\{4, 7, 8, 14\}$, $\{9, 11, 12, 19\}$, $\{10, 16, 18\}$, donde cada clase cromática es un conjunto de Sidon, luego $22 < \overline{SR}(6)$.

- En $\mathbb{Z}_{23}$ encontramos la 6−coloración $\{4, 7, 8, 14, 16\}$, $\{2, 13, 15, 18\}$, $\{3, 5, 17, 20\}$, $\{9, 11, 12, 19\}$, $\{1, 6, 21, 22\}$, $\{0, 10\}$, donde cada clase cromática es un conjunto de Sidon, luego $23 < \overline{SR}(6)$.

- En $\mathbb{Z}_{24}$ encontramos la 6−coloración $\{3, 4, 8, 11, 17\}$, $\{0, 7, 13, 16\}$, $\{1, 12, 20, 21\}$, $\{6, 9, 10, 23\}$, $\{5, 14, 15, 18\}$, $\{2, 19, 22\}$, donde cada clase cromática es un conjunto de Sidon, luego $24 < \overline{SR}(6)$.

- En $\mathbb{Z}_{25}$ encontramos la 6−coloración $\{8, 12, 13, 19, 21\}$, $\{2, 3, 5, 10, 14\}$, $\{1, 11, 15, 18, 20\}$, $\{6, 9, 16, 17, 22\}$, $\{4, 7, 23, 24\}$, $\{0\}$, donde cada clase cromática es un conjunto de Sidon, luego $25 < \overline{SR}(6)$.

- En $\mathbb{Z}_{26}$ encontramos la 6−coloración $\{0, 5, 6, 8, 15\}$, $\{4, 7, 19, 23, 24\}$, $\{10, 12, 17, 20, 21\}$, $\{2, 3, 9, 11, 25\}$, $\{1, 13, 16, 18\}$, $\{14, 22\}$, donde cada clase cromática es un conjunto de Sidon, luego $26 < \overline{SR}(6)$.

- En $\mathbb{Z}_{27}$ encontramos la 6−coloración $\{9, 11, 19, 20, 24\}$, $\{10, 14, 16, 17, 26\}$, $\{0, 4, 5, 12, 21\}$, $\{1, 7, 8, 23, 25\}$, $\{6, 13, 18, 22\}$, $\{2, 3, 15\}$, donde cada clase cromática es un conjunto de Sidon, luego $27 < \overline{SR}(6)$.

- En $\mathbb{Z}_{28}$ encontramos la 6−coloración $\{1, 6, 18, 21, 27\}$, $\{2, 8, 10, 11, 15\}$, $\{0, 4, 17, 25, 26\}$, $\{3, 7, 12, 13, 20\}$, $\{14, 19, 22, 23\}$, $\{5, 9, 16, 24\}$, donde cada clase cromática es un conjunto de Sidon, luego $28 < \overline{SR}(6)$.

- En $\mathbb{Z}_{29}$ encontramos la 6−coloración $\{2, 5, 20, 22, 26\}$, $\{13, 19, 21, 24, 28\}$, $\{0, 6, 8, 9, 25\}$, $\{3, 4, 11, 15, 17\}$, $\{10, 12, 18, 23, 27\}$, $\{1, 7, 14, 16\}$, donde cada clase cromática es un conjunto de Sidon, luego $29 < \overline{SR}(6)$.
- En $\mathbb{Z}_{30}$ encontramos la 6−coloración $\{2, 3, 20, 22, 28\}$, $\{4, 5, 9, 15, 18\}$, $\{8, 13, 14, 17, 27\}$, $\{10, 11, 16, 19, 29\}$, $\{1, 7, 12, 21, 24\}$, $\{0, 6, 23, 25, 26\}$, donde cada clase cromática es un conjunto de Sidon, luego $30 < \overline{SR}(6)$.
- En $\mathbb{Z}_{31}$ encontramos la 6−coloración $\{3, 5, 6, 19, 25, 29\}$, $\{9, 10, 14, 28, 30\}$, $\{1, 11, 15, 23, 26\}$, $\{0, 7, 8, 17, 20\}$, $\{2, 12, 13, 16, 21\}$, $\{4, 18, 22, 24, 27\}$, donde cada clase cromática es un conjunto de Sidon.

Por lo tanto, la mejor cota inferior que logramos establecer para $r = 6$ fue $31 < \overline{SR}(6)$.

Al igual que en el anterior ejemplo, todas las cotas inferiores de $\overline{SR}(r)$ se encontraron con asistencia computacional haciendo uso de los programas MatLab y SAGE [48]. Los resultados de la búsqueda los consignamos en la Tabla 5.4 para $r \in [2, 9]$.

r	2	3	4	5	6	7	8	9
$\overline{SR}(r) \geq$	5	10	17	22	32	43	56	66

Tabla 5.4: Mejores cotas inferiores para $\overline{SR}(r)$.

Como consecuencia del trabajo realizado con cotas superiores e inferiores para $\overline{SR}(r)$, que están consignadas en las Tabla 5.3 y Tabla 5.4, establecimos seis valores para $\overline{SR}(r)$ que mostramos en la Tabla 5.5.

r	2	3	4	5	6	7
$\overline{SR}(r)$	5	10	17	22	32	43

Tabla 5.5: Valores conocidos de $\overline{SR}(r)$.

Una alternativa para encontrar cotas inferiores de $\overline{SR}(r)$ es mediante construcciones de reglas Golomb modulares disjuntas (RGMD) que sean además regulares. Pero debido a que la existencia de $r-$ RGDM regulares en $\mathbb{Z}_m$ no implica la existencia de $r-$ RGDM también regulares en $\mathbb{Z}_{m'}$ para $m' < m$, entonces esta opción no es viable en el contexto modular. Mientras que en el caso entero ocurre lo contrario; establecer $r-$RGD regulares en $[1, n]$ garantiza que $SR(r) > n$. Enseguida mostramos un resultado que obtuvimos a partir de la construcción de Ruzsa, el cual proporciona RGD regulares.

Teorema 31. Sean, p un primo impar y R un conjunto de Sidon tipo Ruzsa en $\mathbb{Z}_{p^2-p}$. La colección $R_0, R_1, \ldots, R_{p-1}$, donde

$$R_t = [R + t(p-1)](\text{mód } p^2 - p),$$

para $t \in [0, p-1]$, es una $(p, p-1)$-RGMD en $\mathbb{Z}_{p^2-p}$ y además, $H(p, p-1) = p^2 - p$.

Antes de demostrar el Teorema 31 necesitamos algunas herramientas. Por ejemplo, el conjunto R hace referencia a $R = R(\theta, p)$ que es el conjunto de Sidon tipo Ruzsa definido en el Capítulo 2.

Además, con M_p y M_{p-1} denotamos los siguientes conjuntos

$$\begin{aligned} M_p &= \{x \in \mathbb{Z}_{p^2-p} : x \equiv 0(\text{mód } p)\}, \\ M_{p-1} &= \{y \in \mathbb{Z}_{p^2-p} : y \equiv 0(\text{mód } p-1)\}. \end{aligned}$$

Caicedo en [5] demostró la siguiente proposición con respecto a $R = R(\theta, p)$.

Proposición 5. El conjunto de Sidon tipo Ruzsa $R(\theta, p)$ satisface las siguiente propiedad:

$$R(\theta, p) \ominus R(\theta, p) = \mathbb{Z}_{p^2-p} \setminus (M_p \cup M_{p-1}).$$

Ahora estamos listos para demostrar el Teorema 31.

Demostración. Demostración del Teorema 31.

Denotemos con $R = R(\theta, p)$ y sea $t \in [0, p-1]$. Definimos las siguientes traslaciones de R como:

$$R_t := [R + t(p-1)](\text{mód } p^2 - p).$$

Claramente, cada R_t es un conjunto de Sidon en $\mathbb{Z}_{p^2-p}$ con $p-1$ elementos. Veamos que los conjuntos $R_0, R_1, \ldots, R_{p-1}$ son disjuntos. Supongamos por contradicción que existe un $x \in R_i \cap R_j$ para $i \neq j$. Entonces $x = r + i(p-1) = r' + j(p-1)$ donde $r, r' \in R$ y $r \neq r'$, así que $r - r' = (j-i)(p-1)$. Pero por la Proposición 5 tenemos que esto es imposible.

Por lo tanto, $R_0, R_1, \ldots, R_{p-1}$ son p conjuntos de Sidon disjuntos y cada uno con $p-1$ elementos, es decir, esta colección es una $(p, p-1)$-RGMD en $\mathbb{Z}_{p^2-p}$. Además, fácilmente se observa que $H(p, p-1) = p^2 - p$. □

Ejemplo 23. En el Ejemplo 2 encontramos en $\mathbb{Z}_{110}$ el conjunto de Sidon tipo Ruzsa $R(\theta, p)$ con $p = 11$ y $\theta = 2$ raíz primitiva de $\mathbb{F}_{11}$, donde

$$R = R(2, 11) = \{7, 39, 58, 63, 65, 86, 92, 100, 101, 104\}.$$

Vamos a aplicar el Teorema 31 para encontrar una $(11, 10)$-RGMD que resulta ser regular. Iniciamos encontrando

$$\begin{aligned}
R_0 =& [R + 0(10)](\text{mód } 110) = \{7, 39, 58, 63, 65, 86, 92, 100, 101, 104\},\\
R_1 =& [R + 1(10)](\text{mód } 110) = \{17, 49, 68, 73, 75, 96, 102, 0, 1, 4\},\\
R_2 =& [R + 2(10)](\text{mód } 110) = \{27, 59, 78, 83, 85, 106, 2, 10, 11, 14\},\\
R_3 =& [R + 3(10)](\text{mód } 110) = \{37, 69, 88, 93, 95, 6, 12, 20, 21, 24\},\\
R_4 =& [R + 4(10)](\text{mód } 110) = \{47, 79, 98, 103, 105, 16, 22, 30, 31, 34\},\\
R_5 =& [R + 5(10)](\text{mód } 110) = \{57, 89, 108, 3, 5, 26, 32, 40, 41, 44\},\\
R_6 =& [R + 6(10)](\text{mód } 110) = \{67, 99, 8, 13, 15, 36, 42, 50, 51, 54\},\\
R_7 =& [R + 7(10)](\text{mód } 110) = \{77, 109, 18, 23, 25, 46, 52, 60, 61, 64\},\\
R_8 =& [R + 8(10)](\text{mód } 110) = \{87, 9, 28, 33, 35, 56, 62, 70, 71, 74\},\\
R_9 =& [R + 9(10)](\text{mód } 110) = \{97, 19, 38, 43, 45, 66, 72, 80, 81, 84\},\\
R_{10} =& [R + 10(10)](\text{mód } 110) = \{107, 29, 48, 53, 55, 76, 82, 90, 91, 94\}.
\end{aligned}$$

Como se mostró en el Teorema 31, la colección $R_0, R_1, \ldots, R_{10}$ es una $(11, 10)$-RGMD en $\mathbb{Z}_{110}$; al ser consideradas en $\mathbb{Z}$ trasladando todos los conjuntos una unidad se obtiene que dicha colección cumple con $H(11, 10) = 110$, por lo tanto, es una $(11, 10)$-RGD regular. De lo anterior concluimos que $110 < SR(11)$. Liang et al. en [52] lograron construir una 11-partición de $[1, 132]$ con asistencia computacional, estableciendo la mejor cota inferior conocida en $SR(11) > 132$, pero nosotros tenemos la ventaja de utilizar nuestro resultado para obtener infinitas cotas inferiores de $SR(r)$ mejorando incluso algunas de las que se conocen actualmente.

Corolario 15. Sea p un primo impar. Entonces $p^2 - p + 1 \leq SR(p)$.

Demostración. Aplicando el Teorema 31 tenemos que $H(p, p-1) = p^2 - p$, esto significa que existe una $p-$coloración del intervalo entero $[1, p^2 - p]$ donde todas las clases cromáticas son reglas Golomb, es decir, conjuntos de Sidon. De lo anterior se concluye que $p^2 - p + 1 \leq SR(p)$. □

Ejemplo 24. Sea $p = 17$, del Corolario 15 se obtiene la siguiente cota inferior

$$273 \leq SR(17).$$

Esta cota es mucho mejor a la actualmente conocida $229 \leq SR(17)$, que fue dada por Liang et al. en [52]. Si ahora tomamos $p = 19$ y aplicamos nuevamente el Corolario 15 encontramos que $343 \leq SR(19)$ estableciendo así la primer cota inferior conocida para $SR(19)$.

Capítulo 6

Conclusiones

1. La característica sobre la buena distribución de conjuntos de Sidon en un intervalo entero que Erdös y Freud mostraron en [16] y que posteriormente precisó Graham en [23], la logramos demostrar para reglas $g-$Golomb en el Teorema 10. En este sentido, mostramos en el Teorema 14 que las reglas $g-$Golomb se distribuyen bien en clases residuales.

2. En el Corolario 2 logramos establecer una cota superior para la máxima distancia que puede separar a dos elementos consecutivos pertenecientes a una regla $g-$Golomb. Este resultado generaliza las establecidas por Cilleruelo en [8] y [9]. Además observamos que la cota que establecimos se puede alcanzar.

3. En el Capítulo 4 mostramos que en $\mathbb{Z}^d$ los arreglos $g-$Golomb tiene una buena distribución en cajas d dimensionales (Teorema 16) y también en el látice $\Lambda(m_1, m_2, \ldots, m_d)$ (Teorema 17). Estos resultados se basan en el comportamiento asintótico de la función $F^-(g, n_1, n_2, \ldots, n_d)$, a saber

$$F^-(g, n_1, n_2, \ldots, n_d) = (g^{1/2} + o(1))(n_1 n_2 \ldots n_d)^{1/2}.$$

4. También en el Capítulo 4 damos un resultado que permite construir secuencias sonar extendidas circulares (Teorema 23). Gracias a las construcciones de conjuntos de Sidon tipo Bose y Ruzsa junto con el Teorema 23 obtuvimos dos construcciones prácticas de secuencias sonar extendidas Corolarios 8 y 9. Estos resultado fueron publicados en nuestro artículo [11].

5. En el Teorema 24 damos una nueva construcción de regla Golomb a partir de cualquier arreglo $1-$Golomb que esté en $\mathbb{Z}^2$. Además observamos que esta construcción

mejora las ideas de Shearer en [44].

6. Observamos en el Capítulo 5 que en el estudio de los números Sidon Ramsey es necesario una mayor comprensión de los conjuntos de Sidon en el grupo ambiente en que se esté trabajando. Además, muchos resultados de $SR(r)$ y $\overline{SR}(r)$ tienen consecuencias inmediatas en la teoría de los conjuntos de Sidon.

7. Consideramos que el Teorema 30 tiene aún muchas más consecuencias, muestra de ello está en el contexto de los conjuntos casi diferencia que encontramos en el trabajo de Zhang, Lei y Zhang en [53], pero además en cuanto a reglas Golomb modulares en la investigación de Buratti y Stinson en [4]. Las ideas de estos trabajos se pueden ampliar en distintas direcciones y encontrar consecuencias para varios conceptos combinatorios que están relacionados.

8. El Corolario 11 permite establecer cotas superiores de la función $F(\mathbb{Z}_n)$ para infinitos valores de n pero se necesita realizar un trabajo previo. Mientras que los Corolarios 12 y 14 establecen cotas superiores de $F(\mathbb{Z}_n)$ para valores de n ya establecidos. Además, observemos que el Corolario 12 garantiza que la función $F(\mathbb{Z}_n)$ tiene la misma cota superior para todos los valores de n pares que estén en un intervalo particular. Este intervalo puede llegar a ser arbitrariamente grande. Las implicaciones que estos resultados tienen en la teoría de los conjuntos de Sidon cobran importancia si tenemos en cuenta las observaciones que Martin y O'Bryant dan en [30].

9. Los resultados que obtuvimos sobre $\overline{SR}(r)$ nos permitieron establecer infinitas cotas superiores y seis valores exactos, pero con una mejor búsqueda computacional se puede llegar más lejos. Gracias al trabajo que realizamos hemos podido estudiar conceptos relacionados y aportar nuevos resultados a su teoría.

A continuación damos una lista de posibles trabajos futuros a realizar.

1. Consideramos que los resultados que conseguimos en el Capítulo 3 se pueden traducir a otros contextos en los cuales se estudian las reglas $g-$Golomb, por ejemplo en grupos cíclicos.

2. Los resultados que obtuvimos sobre los arreglos $g-$Golomb en $\mathbb{Z}^d$ muestran que existe una estrecha relación con las reglas $g-$Golomb en $\mathbb{Z}$, es por esto que consideramos interesante extender la función $\mathfrak{G}(g,n)$ a $\mathbb{Z}^d$ y estudiar su comportamiento.

3. La construcción de Cilleruelo en [9] de arreglos $1-$Golomb en $\mathbb{Z}^d$ a partir de reglas Golomb se puede extender a arreglos $g-$Golomb pero no resulta ser práctica.

Además, no se conocen construcciones generales de arreglos $g-$Golomb directamente en $\mathbb{Z}^d$, es por esto que sería un buen trabajo de investigación avanzar en este problema. En este sentido, aunque las construcciones que damos sobre secuencias sonar extendidas son una herramienta importante aún falta establecer más construcciones donde se pueda incluir más columnas vacías de una forma apropiada en términos de su aplicación.

4. Encontrar nuevas condiciones necesarias para la existencia de conjuntos casi diferencia tienen un valor cada vez mayor cuando se revisan trabajos como los de Buratti y Stinson en [4]. Es por esto que consideramos importante profundizar más en las implicaciones que tienen nuestros resultados del Capítulo 5 e intentar extenderlos a nuevas familias infinitas de parámetros.

Bibliografía

[1] M. D. Atkinson, N. Santoro, and J. Urrutia, *Integer sets with distinct sums and differences and carrier frequency assignments for nonlinear repeaters*, IEEE Transactions on Communications **34** (1986), no. 6, 614 – 617.

[2] W. C. Babcock, *Intermodulation interference in radio systems frequency of occurence and control by channel selection*, The Bell System Technical Journal **32** (1953), no. 1, 63 – 73.

[3] R. C. Bose, *An affine analogue of Singer's theorem*, The Journal of the Indian Mathematical Society **6** (1942), 1 – 15.

[4] M. Buratti and R. Stinson, *New results on modular golomb rulers, optical orthogonal codes and related structures*, ARS Mathematica Contemporanea **20** (2020), 1 – 27.

[5] Y. Caicedo, *Conjuntos de sidon en dimensión dos*, Tesis de doctorado, Universidad del Valle, Marzo 2016.

[6] Y. Caicedo, C. Martos, and C. Trujillo, *$g-$Golomb rulers*, Revista Integración, Temas de Matemáticas **33** (2015), no. 2, 161 – 172.

[7] W. Chen, Z. Chen, and T. Klø ve, *New constructions of disjoint distinct difference sets*, Designs, Codes and Cryptography **15** (1998), 157 – 165.

[8] J. Cilleruelo, *Gaps in dense Sidon sets*, Integers: Electronic Journal of Combinatorial Number Theory **11** (2000), no. A11, 1 – 6.

[9] _____, *Sidon sets in N^d*, Journal of Combinatorial Theory, series A **117** (2010), no. 7, 857 – 871.

[10] J. Costas, *A study of a class of detection waveforms having nearly ideal range—doppler ambiguity properties*, Proceedings of the IEEE **72** (1984), no. 8, 996 – 1009.

[11] L. Delgado, C. Martos, and C. Trujillo, *New constructions of extended sonar sequences from Sidon sets*, IEEE Access **10** (2021), 3343 – 3350.

[12] L. Delgado, A. Montejano, H. Ruiz, and C. Trujillo, *Sidon ramsey numbers and almost difference sets*, Preprint (2022).

[13] L. Delgado and C. Trujillo, *Generalized golomb rulers in Z^d*, Preprint (2023).

[14] A. Dimitromanolakis, *Analysis of the Golomb ruler and the Sidon sets problems, and determination of large, near-optimal golomb ruler*, Tesis de maestría, Universidad Tecnica de Creta, Junio 2002.

[15] K. Drakakis, *A review of the available construction methods for Golomb rulers*, Advances in Mathematics of Communications **3** (2009), no. 3, 235 – 250.

[16] P. Erdös and R. Freud, *On sums of a Sidon sequence*, Journal Number Theory **38** (1991), no. 2, 196 – 205.

[17] P. Erdös, R. Graham, I. Ruzsa, and H. Taylor, *Bounds for arrays of dots with distinct slopes or lengths*, Combinatorica **12** (1992), no. 1, 39 – 44.

[18] P. Erdös and P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*, Journal of London Mathematical Society **16** (1941), no. 4, 212 – 215.

[19] M. Espinosa-Garcia, A. Montejano, E. Roldan-Pensado, and D. Suarez, *A note on Sidon-Ramsey numbers*, arXiv preprint arXiv (2021), 1 – 9.

[20] S. Golomb, *How to number a graph*, Graph Theory and Computing. Academic press. (1972), 23 – 37.

[21] S. Golomb and H. Taylor, *Two-dimensional synchronization patterns for minimum ambiguity*, IEEE Transactions on Information Theory **28** (1982), 600 – 604.

[22] D. Gordon, *The prime power conjecture is true for $n <$ 2,000,000*, The Electronic Journal of Combinatorics **1** (1994), 1 – 7.

[23] S. Graham, *B_h sequences*, Proceedings of a Conference in Honor of Heini Halberstam (1996), 337 – 355.

[24] T. Klø ve, *Bounds and constructions of disjoint sets of distinct difference sets*, IEEE Transactions on Information Theory **36** (1990), 184 – 190.

[25] M. Kolountzakis, *On the uniform distribution in residue classes of dense sets of integers with distinct sums*, Journal of Number Theory **76** (1999), no. 1, 147 – 153.

[26] B. Landman and A. Robertson, *Ramsey theory on the integers*, second ed., American Mathematical Society, 2014.

[27] M. Liang, Xi. Li, B. Xiu, and X. Xu, *On sidon-ramsey numbers*, Journal of Computational and Theoretical Nanoscience **10** (2013), no. 4, 884 – 887.

[28] B. Lindström, *An inequality for B_2-sequences*, Journal of Combinatorial Theory **6** (1969), 211 – 212.

[29] ———, *Well distribution of Sidon sets in residue classes*, Journal of Number Theory **69** (1998), no. 2, 197 – 200.

[30] G. Martin and K. O'Bryant, *Constructions of generalized sidon sets*, Journal of Combinatorial Theory **113** (2006), 591 – 607.

[31] C. Martos, *Conjuntos B_h y reglas $g-$Golomb cortas*, Tesis de doctorado, Universidad del Valle, Abril 2020.

[32] O. Moreno, R. Games, and H. Taylor, *Sonar sequences from costas arrays and the best known sonar sequences with up to 100 symbols*, IEEE Transactions on Information Theory **39** (1993), no. 6, 1985 – 1987.

[33] O. Moreno, S. Golomb, and C. Corrada, *Extended sonar sequences*, IEEE Transactions on Information Theory **43** (1997), no. 6, 1999 – 2005.

[34] K Nowak, *A survey on almost difference sets*, arXiv Preprint arXiv:1409.0114 (2014), 1 – 31.

[35] K. O'Bryant, *A complete annotated bibliography of work related to Sidon sequences*, Electronic Journal of Combinatorics **11** (2004), 1 – 39.

[36] R. Osorio, D. Ruiz, and C. Trujillo, *Sonar sequences and sidon sets*, Revista de Ciencias **18** (2014), no. 1, 33 – 42.

[37] P. Robinson, *Optimum golomb rulers*, IEEE Transactions on Computers **C-28** (1979), no. 12, 943 – 944.

[38] ———, *Golomb rectangles*, IEEE Transactions on Information Theory **31** (1985), no. 6, 781 – 787.

[39] ———, *Golomb rectangles as folded rulers*, IEEE Transactions on Information Theory **43** (1997), no. 1, 290 – 293.

[40] D. Ruiz, C. Trujillo, and Y. Caicedo, *New constructions of sonar sequences*, arXiv Preprint arXiv:1311.1679 (2013), 1 – 12.

[41] H. Ruiz, L. Delgado, and C. Trujillo, *A new construction of optimal optical orthogonal codes from Sidon sets*, IEEE Access **8** (2020), 100749 – 100753.

[42] I. Ruzsa, *Solving a linear equation in a set of integers*, Acta Arithmetica **65** (1993), no. 3, 259 – 282.

[43] Z. Shao, J. Zhou, M. Liang, F. Lang, and X. Xu, *Some new Golomb rectangles*, Journal of Computational and Theoretical Nanoscience **10** (2013), 66 – 68.

[44] J. B. Shearer, *Some new optimum Golomb rectangles*, The Electronic Journal of Combinatorics **2** (1995), no. R12, 1 – 9.

[45] ———, *Some new disjoint Golomb rulers*, IEEE Transactions on Information Theory **44** (1998), no. 7, 3151 – 3153.

[46] J. 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.

[47] N. Sloane, https://www.oeis.org/, 1964.

[48] W. Stein, https://www.sagemath.org/, 2005.

[49] T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge University Press, 2006.

[50] C. Trujillo, G. García, and J. M. Velásquez, $B_2^-[g]$ *finite sets*, JP Journal of Algebra Number Theory and Appications **4** (2004), no. 3, 593 – 604.

[51] B. Xiu, C. Fan, and M. Liang, *On disjoint Golomb rulers*, arXiv preprint arXiv:1405.4535 (2014), 1 – 12.

[52] X. Xu, M. Liang, and H. Lou, *Ramsey theory: unsolved problems and results*, Walter de Gruyter GmbH Co KG, 2018.

[53] Y. Zhang, J. Lei, and S. Zhang, *A new family of almost difference sets and some necessary conditions*, IEEE Transactions on Information Theory **52** (2006), no. 5, 2052 – 2061.