

CONJUNTOS DE SIDON EN DIMENSIÓN DOS

NIDIA YADIRA CAICEDO BRAVO



UNIVERSIDAD DEL VALLE
FACULTAD DE CIENCIAS NATURALES Y EXACTAS
DEPARTAMENTO DE MATEMÁTICAS
DOCTORADO EN CIENCIAS MATEMÁTICAS
SANTIAGO DE CALI
2016

CONJUNTOS DE SIDON EN DIMENSIÓN DOS

NIDIA YADIRA CAICEDO BRAVO

TESIS DOCTORAL PRESENTADA COMO REQUISITO PARA OPTAR AL
TÍTULO DE DOCTOR EN CIENCIAS MATEMÁTICAS

DIRIGIDO POR:
CARLOS ALBERTO TRUJILLO SOLARTE, PH. D.



UNIVERSIDAD DEL VALLE
FACULTAD DE CIENCIAS NATURALES Y EXACTAS
DEPARTAMENTO DE MATEMÁTICAS
DOCTORADO EN CIENCIAS MATEMÁTICAS
SANTIAGO DE CALI
2016

*A las personas más importantes de mi vida,
mi madre Lilia, mis hermanos Ayda Lilia, Jairo Adrián
y a mi padre Jairo, que desde el cielo siempre me acompaña y protege.*

Agradecimientos

Le doy gracias a Dios por iluminar mi camino y darme la sabiduría para culminar este proyecto de vida.

Agradezco a mi madre Lilia Bravo, a mis hermanos Jairo Adrián y Ayda Lilia por creer en mi, apoyarme incondicionalmente en todos los proyectos que emprendo, por darme siempre fortaleza, por estar presentes cuando más los necesito y sobre todo por el amor que me brindan cada día.

Infinitas gracias al Dr. Carlos Alberto Trujillo, docente de la Universidad del Cauca y director de este trabajo de investigación, por su paciencia, motivación, guía, apoyo, y todo su tiempo dedicado para que esta tesis finalice de manera satisfactoria. Ha sido un privilegio conocer al profesor Carlos por inducirme en el camino investigador y por todas sus enseñanzas que serán muy útiles en mi labor como docente.

A la Universidad del Valle, por darme la oportunidad de continuar mis estudios de nivel superior y apoyarme en la financiación a través de su programa de asistencias de docencia.

A los docentes del Departamento de Matemáticas que contribuyeron en mi formación tanto académica como investigativa, durante mi permanencia en el Programa de Doctorado en Ciencias Matemáticas.

A los evaluadores de este trabajo por el tiempo dedicado en la revisión, sus comentarios y sugerencias fueron muy valiosos.

A los compañeros del posgrado que compartieron conmigo muchos momentos académicos e hicieron que mi vida en la ciudad de Cali sea

agradable.

Finalmente, agradezco a mis familiares y amigos que desde la distancia me apoyaron y me dieron su voz de aliento en los momentos más difíciles.

Santiago de Cali, Marzo 10 de 2016

Índice general

Resumen	XI
Abstract	XIII
Introducción	XV
1. Preliminares	1
2. Energía Aditiva y algunas aplicaciones	15
2.1. Energía Aditiva	15
2.2. Aplicación de la Energía Aditiva para la función $F_2^-(n, g)$. . .	25
2.3. Aplicaciones de Energía Aditiva a Reglas g -Golomb para la función $G(g, m)$	28
2.4. Aplicación de Energía Aditiva a Conjuntos de Sidon en $\mathbb{Z} \times \mathbb{Z}$. . .	30
2.5. Aplicación de Energía Aditiva a Conjuntos de Sidon en $\mathbb{Z}^d$. . .	33
2.6. Aplicación de Energía Aditiva a Secuencias Sonar.	36
3. Construcciones de conjuntos de Sidon en una dimensión	39
3.1. Construcción de conjuntos B_2 tipo Bose	40

3.1.1.	Propiedades de la construcción de conjuntos B_2 tipo Bose.	42
3.2.	Construcción de conjuntos B_2 tipo Singer.	44
3.2.1.	Propiedades de la construcción de conjuntos B_2 tipo Singer.	46
3.3.	Construcción de conjuntos B_2 tipo Ruzsa.	49
3.3.1.	Propiedades de la construcción de conjuntos B_2 tipo Ruzsa.	51
4.	Construcciones de conjuntos de Sidon en dos dimensiones	55
4.1.	Algunas construcciones generales.	55
4.1.1.	Propiedades del conjunto $\mathcal{C}$	61
4.1.2.	Propiedades del conjunto $\mathcal{I}$	62
4.1.3.	Propiedades del conjunto $\mathcal{I}_a$	67
4.1.4.	Propiedades del conjunto $\mathcal{I}_{ext}$	69
4.2.	Función Sidon, Secuencias Sonar y Arreglos Costas.	71
4.3.	Nuevas Construcciones de Secuencias Sonar.	75
5.	Construcciones de conjuntos B_h en d dimensiones	81
5.1.	Construcción de conjunto B_h tipo Bose y Chowla.	82
5.2.	Construcción de conjunto B_h tipo Singer generalizada.	84
5.3.	Construcción de conjunto B_{h+1} en dimensión dos.	89
5.4.	Construcción de conjunto B_{h+2} en dimensión tres.	91
5.5.	Construcción de conjunto B_{h+2} en $h + 1$ dimensiones	94
5.6.	Consecuencias de las construcciones para la función f_h	100

ÍNDICE GENERAL

6. Resultados obtenidos y trabajos futuros	103
Bibliografía	107
Anexo	111

x

Resumen

Un subconjunto A de enteros positivos se denomina conjunto de Sidon si todas las sumas de dos elementos son distintas, excepto cuando coinciden por conmutatividad. Si en lugar de tomar sumas de dos elementos, consideramos sumas de h elementos, los conjuntos se denominan B_h . Esta definición también se puede extender a un grupo abeliano arbitrario.

En esta tesis realizamos un amplio estudio sobre las construcciones de conjuntos de Sidon en una y dos dimensiones. En el caso de conjuntos de Sidon en dos dimensiones, presentamos tres construcciones que son subconjuntos de los grupos provenientes de un campo arbitrario. Además, analizamos sus propiedades y describimos algunas propiedades que no se conocían. Como las secuencias sonar corresponden a funciones cuyo grafo es un conjunto de Sidon, uno de nuestros aportes más importante (en el caso de conjuntos de Sidon en dos dimensiones) es el diseño de nuevas construcciones de secuencias sonar obtenidas a partir de conjuntos de Sidon en una dimensión.

Uno de los problemas principales en el estudio de conjuntos de Sidon en una o varias dimensiones es encontrar conjuntos de Sidon maximales; es decir, se busca el valor exacto de la función

$$F_2^d(n) := \max\{|A| : A \subseteq [1, n]^d, A \text{ es un conjunto de Sidon en } \mathbb{Z}^d\},$$

para todo n entero positivo, donde $[1, n] = \{1, 2, \dots, n\}$ y $d \geq 1$ entero.

En este sentido, analizamos las funciones extremas relacionadas con los principales problemas de conjuntos de Sidon y logramos mejores cotas en algunos casos, usando energía aditiva entre dos conjuntos, una herramienta de Teoría de Números Combinatoria. Finalmente, como los conjuntos de

Sidon son generalizables a conjuntos B_h obtuvimos nuevas construcciones de conjuntos B_h en varias dimensiones.

Palabras clave: conjunto de Sidon, secuencias Sonar, arreglos Costas, reglas Golomb, conjuntos B_h .

Abstract

A subset A of positive integers is a Sidon set if all the sums of two of its elements are different, except when they coincide by commutativity. If instead of taking sums of two elements, we consider sums of h elements, the sets are called B_h . This definition can be extended to an arbitrary abelian group.

In this thesis, we conduct an extensive study on the construction of Sidon sets in one and two dimensions. In the case of Sidon sets in two dimensions, we present three constructions arising from subsets of groups in a arbitrary field. Besides, we analyze their properties and describe some properties that were unknown. As sonar sequences correspond to functions whose graph is a Sidon set, one of our most important contribution (in the case of Sidon sets in two dimensions) has been the design of new constructions of sonar sequences from Sidon sets in one dimension.

One of the main problems concerning Sidon sets, in one or more dimensions, is to find maximal Sidon sets. That is to say, we seek the exact value of the function

$$F_2^d(n) := \max\{|A| : A \subseteq [1, n]^d, A \text{ is a Sidon set in } \mathbb{Z}^d\},$$

for every positive integer n , where $[1, n] = \{1, 2, \dots, n\}$ and $d \geq 1$ integer.

In this respect, we analyze extreme functions related to the main problems of Sidon sets and improve the bounds in some cases by using the concept of additive energy between two sets, a tool of Combinatorial Number Theory. Finally, as Sidon sets are generalized into B_h sets, we obtain new constructions of B_h sets in several dimensions.

Keywords: Sidon sets, Sonar sequences, Costas arrays, Golomb rulers, B_h sets.

Introducción

En 1932, Simon Sidon le plantea a Paul Erdős el problema de encontrar conjuntos de enteros positivos con la propiedad que todas las sumas de dos elementos sean distintas. Estos conjuntos surgen en conexión con el trabajo que Sidon realizaba en el contexto del análisis Fourier [17]; el problema llamó mucho la atención de Erdős por su relación con la aritmética y la combinatoria, convirtiéndose en uno de sus temas de investigación de mucho interés en Teoría de Números y Combinatoria. A estos conjuntos hoy en día se les conoce con el nombre de *conjuntos de Sidon*.

En 1950, W. C. Babcock [2] consideró conjuntos de enteros positivos con la propiedad que todas las diferencias no nulas son distintas. Éstos conjuntos los encontró en su estudio sobre la distorsión de intermodulación de las bandas de radio-frecuencia, mientras analizaba el posicionamiento de canales de radio en el espectro de frecuencias. A éstos conjuntos se los conoce con el nombre de *reglas Golomb*. Sin embargo, las reglas Golomb derivan su nombre de Solomon Golomb quien fue uno de los primeros en estudiar sus construcciones en relación a la Combinatoria, Teoría de Códigos y Comunicaciones.

Dado que analizar diferencias distintas es equivalente a analizar sumas distintas, puesto que $a + b = c + d$ si y sólo si $a - d = c - b$, el estudio de conjuntos de Sidon es equivalente al estudio de las reglas Golomb. Por tal razón nos referimos a estos dos tipos de conjuntos simplemente como conjuntos B_2 . Sin embargo, los problemas principales de estudio en estos dos tipos de conjuntos son distintos. En el caso de conjuntos de Sidon se busca el mayor cardinal que un conjunto B_2 puede tener entre los primeros N enteros positivos, y para el caso de reglas Golomb se busca construir un conjunto B_2 de longitud lo más corta posible con un número fijo de marcas o elementos

dado, en este caso se denomina longitud a la mayor diferencia que existe entre los elementos del conjunto B_2 .

El concepto de conjuntos de Sidon o reglas Golomb en principio se estudió en el caso cuando el grupo ambiente eran los enteros, aunque es posible extender este concepto a cualquier grupo abeliano en general, e incluso a varias dimensiones. En el caso de dimensión dos, aparecen las Secuencias Sonar, los Arreglos Costas y los Rectángulos Golomb, que son un tipo particular de conjuntos B_2 .

Las secuencias sonar fueron introducidas por Golomb y Taylor [22] como ejemplos de patrones de sincronización dos dimensional de mínima ambigüedad. Una *secuencia sonar* $m \times n$ es un arreglo de puntos y espacios que tienen m filas y exactamente un punto en cada una de sus n columnas, sujeto a la restricción que cada par de puntos determinan vectores distintos.

El problema de estudio actualmente de las secuencias sonar es el siguiente: *para m fijo encontrar el mayor n para el cual existe una secuencia sonar $m \times n$;*

Un *arreglo Costas de orden n* se puede considerar geométricamente como un conjunto de n puntos situados en los cuadrados de un tablero de ajedrez de tamaño $n \times n$, tales que cada fila o columna contiene sólo un punto, y que todos los $\binom{n}{2} = \frac{n(n-1)}{2}$ vectores de desplazamiento entre cada par de puntos son distintos.

Los arreglos Costas aparecen por primera vez en 1965 en el contexto de la detección sonar [11] cuando J. P. Costas decepcionado por los malos resultados de los sistemas sonar, los usó para describir un nuevo patrón de saltos de frecuencia [26] para los sistemas sonar con óptimas propiedades de autocorrelación. J. P. Costas manualmente encontró arreglos Costas hasta de orden 12, pero no pudo continuar para órdenes mayores ni tampoco pudo encontrar una técnica general de construcción de los mismos. Golomb desarrolló dos técnicas de generación de arreglos Costas, ambas basadas en la teoría de Campos Finitos, conocidos hoy en día como Método Welch y Método Golomb [15, 21, 20]. Además, éstas construcciones son las únicas que se conocen en la actualidad, pese a los esfuerzos de muchos investigadores.

Los arreglos Costas se han estudiado durante varios años y muchas de

las preguntas básicas referentes a su construcción aún permanecen abiertas. Por ejemplo, la generación de algunos métodos produce arreglos Costas para infinitos n , pero no para todo n . La primera pregunta planteada por J. P. Costas, que aún sigue abierta, es la siguiente:

¿Existen arreglos Costas de orden n , para todo n ?

Los dos primeros n para los cuales no se conoce la existencia de arreglos Costas son $n = 32$ y $n = 33$.

Por último mencionamos el caso de conjuntos de Sidon d dimensionales; es decir, conjuntos de Sidon contenidos en $\mathbb{Z}^d$, en particular, para el estudio de conjuntos de Sidon maximales se consideran como subconjuntos de $[1, n]^d$. Más generalmente, dados los grupos aditivos G_i , para $i = 1, \dots, d$, si consideramos el producto directo $G = G_1 \times \dots \times G_d$, se dice que un conjunto $A \subseteq G$ es de Sidon si todas las sumas de vectores de la forma

$$(a_1, \dots, a_d) + (a'_1, \dots, a'_d) = (a_1 + a'_1, \dots, a_d + a'_d),$$

para todo $(a_1, \dots, a_d), (a'_1, \dots, a'_d) \in A$, son distintas, salvo permutaciones de los sumandos.

La distribución de los temas en esta tesis es la siguiente. En el Capítulo 1, presentamos la notación que vamos a usar durante todo el trabajo, algunas definiciones, por ejemplo la de conjunto de Sidon en un grupo abeliano arbitrario, regla g -Golomb, conjunto B_h , entre otros; así como también los problemas principales relacionados con este tipo de conjuntos, las funciones maximales o minimales, según sea el caso, y algunas cotas conocidas de dichas funciones.

En el Capítulo 2, presentamos la definición de Energía Aditiva entre dos conjuntos, propiedades y algunas aplicaciones a problemas relacionados con conjuntos de Sidon, conjuntos $B_2^-[g]$ o reglas g -Golomb, conjuntos de Sidon en dimensión dos, en dimensión d y secuencias sonar. Destacamos en este capítulo que el uso de la energía aditiva nos permitió mejorar algunas cotas conocidas, por ejemplo para el caso de conjuntos de Sidon en dos y d dimensiones, logramos encontrar constantes explícitas para las cotas de las funciones relacionadas con el problema.

En el Capítulo 3, presentamos en detalle las construcciones de conjuntos de Sidon modulares clásicas tipo Bose, Singer y Ruzsa, junto con algunas

propiedades que satisfacen, las cuales nos permitieron encontrar nuevas construcciones de secuencias sonar que presentamos en el siguiente capítulo.

En el Capítulo 4, realizamos un estudio de construcciones sobre conjuntos de Sidon en dimensión dos, en el producto directo de los grupos que provienen de un campo. En particular, analizamos algunas propiedades de dichos conjuntos cuando consideramos el campo finito $\mathbb{F}_p$, donde p es un número primo. También presentamos nuevas construcciones de secuencias sonar, que son un tipo especial de conjuntos de Sidon en dimensión dos.

En el Capítulo 5, describimos en detalle las construcciones clásicas de conjuntos B_h tipo Bose-Chowla y Singer generalizada, y luego usando algunas ideas de estas construcciones presentamos nuevas construcciones de conjuntos B_h en d dimensiones, para algunos valores de d , cuyas componentes son elementos de un campo arbitrario o alguna extensión adecuada de dicho campo. Destacamos que las construcciones que presentamos en este capítulo permiten construir familias de conjuntos B_h que son densos.

En el Capítulo 6 presentamos los resultados obtenidos en este trabajo de investigación, así como posibles trabajos futuros que se pueden realizar teniendo como base los logros alcanzados.

El documento termina con las referencias bibliográficas y un anexo en el que mencionamos los eventos en que participamos con ponencias relacionadas con el tema de investigación.

Capítulo 1

Preliminares

En este capítulo, presentamos la notación que usamos a lo largo del desarrollo de este trabajo, además algunas definiciones de conjuntos con ciertas propiedades, problemas relacionados con estos conjuntos y cotas triviales.

Consideremos G un grupo notado aditivamente, A, B subconjuntos de G y x un elemento no nulo de G . Definimos los siguientes conjuntos:

- Conjunto suma de A y B :

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

- Conjunto diferencia de A y B :

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

- Conjunto suma iterada de A , k veces, donde $k \in \mathbb{Z}^+$:

$$kA := \{a_1 + \cdots + a_k : a_i \in A, i = 1, \dots, k\},$$

es decir, $kA = \underbrace{A + \cdots + A}_{k \text{ veces}}$.

- Conjunto traslación de A por x :

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

- 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 en G . En este caso, como G es un grupo aditivo, representamos a^{-1} por $-a$.

Claramente, tenemos que $k \cdot A \subseteq kA$. Además, se cumplen las siguientes propiedades:

- $A - B \neq A \setminus B$.
- $A + B - B \neq A$, en lugar de esto se tiene que $A \subseteq A + B - B$.
- Para $m, n \in \mathbb{Z}^+$ tales que $m < n$ entonces $(n - m)A \subseteq nA - mA$.

Consideremos el siguiente ejemplo en el cual podemos observar que las anteriores propiedades se cumplen.

Ejemplo 1. Sean $(\mathbb{Z}, +)$ un grupo, $A = \{1, 2, 3\}$, $B = \{2, 4\}$ subconjuntos de $\mathbb{Z}$, y los enteros $n = 5$, $m = 2$. Tenemos los siguientes conjuntos.

$$A - B = \{-3, -2, -1, 0, 1\},$$

$$A \setminus B = \{1, 3\},$$

$$A + B - B = \{-1, 0, 1, 2, 3, 4, 5\},$$

$$3A = \{3, 4, 5, 6, 7, 8, 9\},$$

$$3 \cdot A = \{3, 6, 9\},$$

$$5A - 2A = \{-1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}.$$

En lo que sigue, dado un conjunto finito A , denotamos $|A|$ como el número de elementos o cardinal del conjunto. Además, suponemos que todos los subconjuntos del grupo G son finitos, pues son de gran interés para nuestro estudio, aunque algunas definiciones y resultados se pueden extender para conjuntos infinitos o grupos no abelianos.

También definimos el intervalo entero de los primeros n enteros positivos por: $[1, n] := \{1, 2, \dots, n\}$ y el número combinatorio denotado por $\binom{n}{m}$, que cuenta el número de subconjuntos de tamaño m tomados de un conjunto con n elementos, para $n \geq m$.

Uno de los aspectos de mayor interés para nosotros, es estudiar el cardinal del conjunto suma (o diferencia), sobre todo cuando éste es grande; por tal razón es posible preguntarnos: ¿Bajo que condiciones el tamaño del conjunto suma (o diferencia) es grande?. O en algunas ocasiones, es pertinente preguntarnos: ¿Bajo que condiciones el tamaño del conjunto suma (o diferencia) es pequeño?.

El siguiente resultado nos muestra algunas cotas triviales para los conjuntos mencionados [40].

Lema 1.0.1. *Sean G un grupo abeliano aditivo, A, B subconjuntos de G y $x \in G$ no nulo, entonces:*

$$(a) \quad |A + x| = |A| = |-A|;$$

$$(b) \quad \max(|A|, |B|) \leq |A + B|, |A - B| \leq |A| |B|;$$

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

$$(d) \quad |A| \leq |A - A| \leq |A|^2 - |A| + 1;$$

$$(e) \quad \text{Para cualquier entero } n \geq 1 \text{ se tiene que } |nA| \leq |(n+1)A| \text{ y}$$

$$|nA| \leq \binom{|A| + n - 1}{n} = \frac{|A|(|A| + 1) \cdots (|A| + n - 1)}{n!}.$$

Si el conjunto suma o el conjunto diferencia de un conjunto dado A , alcanzan las cotas superiores de (c) o (d), se dice que A es un conjunto B_2 . Si el conjunto nA alcanza la cota superior en la propiedad (e), para

$n \geq 2$, el conjunto se denomina B_n . Estos conjuntos son el objeto principal de nuestro trabajo.

Ahora, definimos la función de representación para introducir algunos conceptos que necesitamos más adelante; esta función cuenta el número de formas de escribir cualquier elemento del grupo aditivo G , como suma (o diferencia) de los elementos de A y B .

Definición 1.0.2. Sean G un grupo abeliano aditivo, A, B subconjuntos de G , definimos la funciones de representación con dominio el grupo G y codominio los enteros no negativos como:

$$R_{A+B}(x) := |\{(a, b) \in A \times B : a + b = x\}|, \quad (1.1)$$

$$R_{A-B}(x) := |\{(a, b) \in A \times B : a - b = x\}|, \quad (1.2)$$

para todo $x \in G$.

De la definición anterior podemos notar que las siguientes igualdades se tienen:

$$R_{A+B}(x) = |A \cap (x - B)|, \quad (1.3)$$

$$R_{A-B}(x) = |A \cap (x + B)|, \quad (1.4)$$

donde $x - B := \{x - b : b \in B\}$.

Verificamos sólo (1.3), pues (1.4) se prueba de manera similar. En efecto, tenemos

$$\begin{aligned} R_{A+B}(x) &= |\{(a, b) \in A \times B : a + b = x\}| \\ &= |\{(a, b) \in A \times B : a = x - b\}| \\ &= |\{y \in G : \exists a \in A, \exists b \in B, y = a \wedge y = x - b\}| \\ &= |A \cap (x - B)|. \end{aligned}$$

Dado que por el momento estamos interesados en el estudio de subconjuntos finitos de un grupo G , podemos notar que

$$\sum_{x \in G} R_{A+B}(x) = \sum_{x \in G} R_{A-B}(x) = |A| |B|. \quad (1.5)$$

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 $A - B$.

Verifiquemos que se cumple (1.5). En efecto, de (1.1) tenemos que

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

Para efectos de conteo, las sumas entre los conjuntos $A = \{a_1, a_2, \dots, a_n\}$ y $B = \{b_1, b_2, \dots, b_m\}$, las realizamos como ilustra la siguiente tabla:

+	a_1	a_2	$\cdots$	a_n
b_1	$a_1 + b_1$	$a_2 + b_1$	$\cdots$	$a_n + b_1$
b_2	$a_1 + b_2$	$a_2 + b_2$	$\cdots$	$a_n + b_2$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
b_m	$a_1 + b_m$	$a_2 + b_m$	$\cdots$	$a_n + b_m$

Cuadro 1.1: Conjunto Suma $A + B$.

Tenemos además las siguientes cotas triviales para la función de representación:

$$0 \leq R_{A+B}(x), R_{A-B}(x) \leq \min(|A|, |B|), \quad (1.6)$$

donde la cota superior es fácil de obtener, en este caso como todos los elementos del conjunto A son distintos, si observamos en la Tabla 1.1, por cada fila que tenemos del conjunto suma $A + B$, un elemento se puede repetir a los más una sola vez en cada fila y tenemos m filas; de manera análoga sucede si observamos los elementos del conjunto suma $A + B$ por columnas, un elemento se puede repetir a los más una sola vez en cada columna y tenemos n columnas pues los elementos del conjunto B también son todos distintos, esto se debe a que estamos trabajando en un grupo, por tal razón tomando el $\min\{m, n\}$ se tiene la cota superior.

En particular, si $|A| = |B| = k$ entonces $0 \leq R_{A+B}(x), R_{A-B}(x) \leq k$ y además

$$\sum_{x \in A+B} R_{A+B}(x) = \sum_{x \in A-B} R_{A-B}(x) = k^2. \quad (1.7)$$

De otro lado, como nuestro tema de estudio principal son los conjuntos de Sidon, presentamos algunas definiciones y problemas.

Definición 1.0.3. *Un conjunto A de enteros positivos es un **conjunto de Sidon** o un **conjunto B_2** si todas las sumas $a+b$ son distintas, para $a, b \in A$, excepto cuando coinciden por la conmutatividad.*

De manera natural esta definición es equivalente a decir que $A \subset \mathbb{Z}$ es un conjunto de Sidon si todas las diferencias no nulas $a - b$ son distintas, para todo $a, b \in A$, $a \neq b$, puesto que $a + b = c + d$ si y sólo si $a - d = c - b$.

El estudio de los conjuntos de Sidon inicia en 1932, con S. Sidon y su problema principal es encontrar conjuntos de enteros positivos maximales con la propiedad que todas las sumas de dos elementos sean distintas; es decir, conjuntos de Sidon enteros con la mayor cantidad de elementos hasta un cierto número n dado, con n entero positivo. Aunque este problema apareció en principio en los enteros, más adelante es extendido a cualquier grupo abeliano G , además no sólo se consideran sumas de dos elementos sino más bien sumas de h elementos.

Definimos a continuación un conjunto B_h , para $h \geq 2$ entero, que generaliza la definición de conjunto de Sidon.

Definición 1.0.4. *Sean G un grupo abeliano aditivo, A un subconjunto de G con k elementos y $h \geq 2$ un entero. Se dice que A es un **conjunto B_h** en G o A pertenece a la clase B_h en G , si para todo $x \in G$, la ecuación*

$$x = x_{i_1} + \cdots + x_{i_h},$$

con $x_{j_i} \in A$, tiene a lo más una solución en A , salvo permutaciones de los sumandos.

Si $h = 2$ los conjuntos B_2 son exactamente los conjuntos de Sidon.

Si $G = G_1 \times \cdots \times G_d$ es el producto directo de d grupos abelianos, decimos que A es un conjunto B_h d -dimensional.

Como se mencionó anteriormente, el concepto de conjunto de Sidon se puede generalizar a cualquier grupo $(G, *)$. Presentamos a continuación algunas definiciones equivalentes de conjunto de Sidon.

Definición 1.0.5. *A es un conjunto de Sidon en el grupo $(G, *)$ si y sólo si*

(a) *Para todo $a, b, c, d \in A$ se cumple*

$$a * b = c * d \Rightarrow \{a, b\} = \{c, d\}.$$

(b) *$|A * A| = \binom{|A|+1}{2}$.*

(c) *Para todo $x \in G$, se cumple que $R_{A*A}(x) \leq 2$.*

Ahora describimos algunas de las propiedades que satisfacen los conjuntos B_h en un grupo G .

Lema 1.0.6. *Si A es un conjunto B_h en G entonces A es un conjunto B_t en G , para todo t con $2 \leq t \leq h - 1$.*

Lema 1.0.7. *Sean $(G_1, \star)$, $(G_2, \bullet)$ grupos abelianos y A un conjunto B_h en G_1 . Si φ es un monomorfismo de G_1 en G_2 entonces $\varphi(A) = \{\varphi(a) : a \in A\}$ es un conjunto B_h en $\varphi(G_1)$.*

Como lo describimos anteriormente, el problema de estudio de conjuntos B_h surge en el caso cuando $h = 2$; algunas definiciones y resultados los enunciaremos en el caso general para conjuntos B_h , aunque nuestro principal interés de estudio son los conjuntos B_2 . En general, el problema principal de estudio para conjuntos B_h enteros es determinar el mayor número de elementos que un conjunto B_h puede tener, cuando está contenido en el conjunto de los primeros n números enteros positivos. Es decir, estudiar la función

$$F_h(n) := \max \{|A| : A \subseteq [1, n], A \text{ es } B_h \text{ en } \mathbb{Z}\}. \quad (1.8)$$

Para el caso cuando G es un grupo abeliano finito, se estudia la función

$$f_h(G) := \max \{|A| : A \subseteq G, A \text{ es } B_h \text{ en } G\}. \quad (1.9)$$

Si se trabaja en el grupo de los enteros modulares $G = \mathbb{Z}_N$, usamos la notación $f_h(N)$ y en este caso hablamos de conjuntos B_h modulares.

Como todo conjunto B_h en $\mathbb{Z}_N$ puede proyectarse por el Lema 1.0.7 a un conjunto B_h contenido en el intervalo entero $[1, N]$ entonces las funciones $f_h(N)$ y $F_h(N)$ tienen la siguiente relación:

$$f_h(N) \leq F_h(N). \quad (1.10)$$

Las cotas inferiores de dichas funciones se encuentran por medio de construcciones y las cotas superiores por medio de conteo. Para el caso $h = 2$, mencionamos una cuenta sencilla, que nos proporciona una cota superior de la función $F_2(N)$. En efecto, consideremos un conjunto B_2 en $[1, N]$, denotado por A , con $|A| = k$, el número de diferencias no nulas $a_i - a_j$, $a_i, a_j \in A$, es $2\binom{k}{2} = k(k-1)$ y como todas las diferencias son menores que N y $A \ominus A \subseteq [1-N, N-1]$ tenemos que

$$k(k-1) \leq 2N-2.$$

Así, $(k-1)^2 \leq k(k-1) \leq 2N-2 \leq 2N \iff k-1 \leq \sqrt{2N} \iff k \leq \sqrt{2N}+1$. Como esta desigualdad es válida para cualquier conjunto B_2 en $[1, N]$, tenemos que $F_2(N) \leq \sqrt{2N}+1$.

En general para cualquier grupo aditivo finito G , una cota superior trivial para la función $f_2(G)$ se obtiene de la siguiente manera: supongamos que A es un conjunto B_2 en $(G, +)$, así $A + A \subseteq G$ y por lo tanto

$$\frac{|A|(|A|+1)}{2} = |A + A| \leq |G|,$$

lo que implica que

$$f_2(G) \leq \sqrt{2|G|}. \quad (1.11)$$

Además, existen tres construcciones clásicas de conjuntos de Sidon modulares maximales; es decir, para este caso conocemos el valor exacto de la función $f_2(N)$ para infinitos valores de N . Sin embargo, no se conoce el valor exacto de dicha función para todo N , el cual sigue siendo aún un problema abierto. Tampoco se conoce el valor exacto de las funciones descritas anteriormente para el caso $h \geq 2$ aunque se conocen algunas estimaciones.

Las tres construcciones clásicas son:

- (1938) Construcción de Singer [39]: permite establecer que para todo q potencia de un primo, $f_2(q^2 + q + 1) = q + 1$.
- (1942,) Construcción de Bose [3]: permite establecer que para todo q potencia de un primo, $f_2(q^2 - 1) = q$.
- (1993) Construcción de Ruzsa [38]: permite establecer que para todo p primo, $f_2(p^2 - p) = p - 1$.

En consecuencia, para todo q potencia de un primo y todo primo p se tiene:

- $q + 1 \leq F_2(q^2 + q + 1)$,
- $q \leq F_2(q^2 - 1)$,
- $p - 1 \leq F_2(p^2 - p)$.

Otra generalización de los conjuntos de Sidon enteros es cuando se permite que cada suma de h elementos del conjunto se repite a lo más g veces. A estos conjuntos se les conoce con el nombre de conjuntos $B_h[g]$ enteros. Además, en lugar de considerar conjuntos de enteros también se pueden estudiar los conjuntos $B_h[g]$ en cualquier grupo abeliano G . Presentamos a continuación la definición formal de un conjunto $B_h[g]$ en un grupo abeliano G .

Definición 1.0.8. *Sea G un grupo abeliano finito notado aditivamente. Se dice que $A \subset G$ es un conjunto $B_h[g]$ en G si para todo $x \in G$, la ecuación*

$$x = x_1 + \cdots + x_h,$$

$x_i \in A$, tiene a lo más g soluciones distintas, salvo permutaciones de los sumandos.

En este caso también se busca encontrar conjuntos $B_h[g]$ maximales en un grupo abeliano finito G . Para ello se estudian las funciones:

- En el caso entero:

$$F_h(n, g) := \max\{|A| : A \subseteq [1, n], A \text{ es } B_h[g]\}, \quad (1.12)$$

- En el caso de un grupo finito:

$$f_h(G, g) := \max\{|A| : A \subseteq G, A \text{ es } B_h[g]\}. \quad (1.13)$$

A continuación, para el caso cuando $G = \mathbb{Z}$ y $h = 2$ definimos los siguientes conjuntos.

Definición 1.0.9. Sean g un entero positivo y A un conjunto de enteros positivos.

- A pertenece a la clase $B_2^+[g]$ si $R_{A+A}^*(x) \leq g$, para todo $x \in \mathbb{Z}^+$, donde $R_{A+A}^*(x) := |\{(a, b) \in A \times A : a + b = x, a \leq b\}|$.
- A pertenece a la clase $B_2^-[g]$ si $R_{A-A}(x) \leq g$, para todo $x \in \mathbb{Z}^+$.
- A pertenece a la clase $B_2^\pm[g]$ si $A \in B_2^+[g] \cap B_2^-[g]$.

Si $g = 1$, se tiene que $B_2^+[1] = B_2^-[1] = B_2^\pm[1]$ y en este caso los conjuntos mencionados son exactamente los conjuntos de Sidon.

En el caso finito, se estudia el comportamiento asintótico de las siguientes funciones:

$$F_2^+(n, g) := \max\{|A| : A \subseteq [1, n], A \in B_2^+[g]\}, \quad (1.14)$$

$$F_2^-(n, g) := \max\{|A| : A \subseteq [1, n], A \in B_2^-[g]\}, \quad (1.15)$$

$$F_2^\pm(n, g) := \max\{|A| : A \subseteq [1, n], A \in B_2^\pm[g]\}. \quad (1.16)$$

De las definiciones anteriores tenemos que

$$F_2^\pm(n, g) \leq \min\{F_2^+(n, g), F_2^-(n, g)\}. \quad (1.17)$$

En particular, si $g = 1$ estamos en el caso de conjuntos de Sidon y la función $F_2^\pm(n, 1)$ coincide con $F_2(n)$.

Los conjuntos $B_2^-[g]$ también se denominan reglas g -Golomb [7]. Cuando $g = 1$, la regla 1-Golomb es un conjunto de Sidon entero y simplemente se denomina regla Golomb.

Históricamente, las reglas Golomb aparecieron en 1950 con W. C. Babcock [2]; él consideró conjuntos de enteros positivos con la propiedad que todas las diferencias no nulas sean distintas. Sin embargo, las reglas Golomb derivan su nombre del profesor Solomon W. Golomb quien fué uno de los primeros en estudiar sus construcciones.

Definición 1.0.10. *Un conjunto de enteros positivos A es una regla Golomb si todas las diferencias no nulas $a - b$ son distintas, para todo a, b en A y $a \neq b$.*

Se denominan *orden* de la regla al cardinal del conjunto, *longitud* de la regla a la máxima diferencia entre dos elementos del conjunto y se denota por $\ell(A)$ y los elementos del conjunto se denominan *marcas*.

Definiciones equivalentes de regla Golomb son las siguientes.

Definición 1.0.11. *A es una regla Golomb si*

(a) *Para todo $a, b, c, d \in A$ con $a \neq b, c \neq d$ se cumple*

$$a - b = c - d \Rightarrow a = c, b = d.$$

(b) $|A \ominus A| = 2\binom{|A|}{2} = |A|^2 - |A|$.

Dado que el concepto de conjunto de Sidon entero es equivalente al concepto de regla Golomb, tenemos el siguiente resultado.

Lema 1.0.12. *Dado un conjunto $A \subseteq \mathbb{Z}$ entonces A es un conjunto de Sidon si y sólo si A es una regla Golomb.*

Además, existen dos preguntas interesantes referentes a las reglas Golomb:

¿Dada una longitud n , cuál es la mayor cantidad de marcas posible, todas menores que n , que puede tener una Regla Golomb?

¿Dado el orden m , se puede construir una regla Golomb de longitud n lo mas corta posible con m marcas?

Dicho de otra manera, una regla Golomb de orden m con longitud n se dice que es óptima en cualquiera de los dos casos:

- Puede ser óptimamente densa, exhibiendo un m máximo para un valor específico de n .
- Puede ser óptimamente corta, exhibiendo un n mínimo para un valor específico de m .

En el primer caso, el problema de optimización coincide con el estudio de la función $F_2(n)$ para los conjuntos de Sidon. Sin embargo, el término general de regla Golomb óptima es usado para referirse al segundo tipo de optimización; es decir, una regla Golomb óptima es aquella que tiene la menor longitud posible para un número fijo de marcas [13].

Para el estudio de este tipo de reglas consideramos la función

$$G(m) := \min\{\ell(A) : A \text{ es una regla Golomb, } |A| = m\}.$$

Por ejemplo, $G(6) = 17$ y además existen cuatro reglas óptimas de orden 6 y longitud 17, éstas son: $\{0, 1, 4, 10, 12, 17\}$, $\{0, 1, 4, 10, 15, 17\}$, $\{0, 1, 8, 11, 13, 17\}$, y $\{0, 1, 8, 12, 14, 17\}$.

Lo interesante de la función $G(m)$ es que no se conoce mucho al respecto; de hecho, la mayor parte de la investigación reciente sobre las reglas Golomb es sobre la acotación de la función $G(m)$. Incluso usando un cálculo computacional, hasta la fecha, sólo se conoce el valor exacto de $G(m)$ para valores de $m \leq 27$, más información sobre los valores de $G(m)$ conocidos se pueden encontrar en [14].

Algunas cotas inferiores conocidas de la función $G(m)$ son las siguientes:

- $G(m) \geq \frac{m(m-1)}{2}$ (cota trivial).
- $G(m) > m^2 - 2m\sqrt{m}$ (en [1]).
- $G(m) > m^2 - 2m\sqrt{m} + \sqrt{m} - 2$ (en [13]).
- $G(m) \geq m^2 - 2m\sqrt{m-1} + m - \frac{m}{\sqrt{m-1}} - 1$ (en [7]).

Una pregunta abierta interesante es saber si se tiene o no la desigualdad $G(m) < m^2$, para todo m .

Usando las construcciones conocidas de conjuntos de Sidon finitos, varios investigadores [1] las han manipulado para crear nuevas reglas Golomb cercanas a la óptima. Por ejemplo, a partir de las construcciones de Ruzsa, Bose y Singer se sigue que:

$$\begin{aligned} G(p-1) &\leq p^2 - p, \text{ para todo } p \text{ primo,} \\ G(q) &\leq q^2 - 1, \text{ para todo } q \text{ potencia prima,} \\ G(q+1) &\leq q^2 + q + 1, \text{ para todo } q \text{ potencia prima.} \end{aligned}$$

Erdős conjeturó que $G(m) \leq m^2 + c$, donde $c \in \mathbb{R}$ es una constante. Conjetura que hasta hoy no ha sido demostrada ni refutada. Dimitromanolakis [13] calculó reglas Golomb relativamente cortas y demostró con ayuda computacional que $G(m) < m^2$, para $m \leq 65000$.

De otra parte, dado que una regla Golomb A es un conjunto con la propiedad que todas las diferencias no nulas de dos de sus elementos son distintas, es posible generalizar este concepto al caso cuando las diferencias de dicho conjunto se repiten a lo más g veces, es decir, estamos hablando de conjuntos $B_2^-[g]$. Así, tenemos la siguiente definición de regla g -Golomb.

Definición 1.0.13. *Una regla g -Golomb o conjunto $B_2^-[g]$ es un conjunto A de enteros positivos tal que*

$$R_{A-A}(x) \leq g, \text{ para todo } x \in \mathbb{Z}, x \neq 0.$$

Por otro lado, es importante considerar una extensión de la función $G(m)$ para el caso de una regla g -Golomb A con m marcas, por lo cual definimos la función $G(g, m)$, como

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

El problema fundamental en el estudio de la función $G(g, m)$ es encontrar el valor exacto para todo g y todo m enteros positivos.

Además, de acuerdo al Lema 1.0.12 es posible mejorar la cota superior trivial (1.11) para el caso cuando A es un conjunto B_2 en un grupo aditivo G contando las diferencias, esto es: dado A un conjunto B_2 en el grupo

$(G, +)$ entonces por el Lema 1.0.12, A es una regla Golomb, por lo tanto $A \ominus A \subseteq G \setminus \{e\}$, donde e es el elemento neutro de G , $|A| = k$, y $|G| = N$. Así,

$$k(k-1) = |A \ominus A| \leq N-1,$$

lo que implica que

$$f_2(G) \leq \sqrt{N-1} + 1. \tag{1.18}$$

Capítulo 2

Energía Aditiva y algunas aplicaciones

En este capítulo, presentamos el concepto de Energía Aditiva entre dos conjuntos y algunas aplicaciones a problemas relacionados con conjuntos de Sidon en una, dos y d dimensiones, así como también a reglas g -Golomb o conjuntos $B_2^-[g]$ y secuencias sonar.

2.1. Energía Aditiva

La *energía aditiva* entre dos conjuntos permite medir qué tanta estructura aditiva común tienen los conjuntos; es decir, la energía aditiva es una de las medidas de estructura aditiva de conjuntos. El ejemplo más sobresaliente es la conclusión de los Teoremas de Balog-Szemerédi-Gowers y Freiman-Ruzsa [40], los cuales dicen que conjuntos con energía aditiva grande tienen partes grandes que son casi progresiones aritméticas generalizadas. Pero para el caso de conjuntos con energía aditiva pequeña no hay una descripción similar, aunque se han hecho algunos intentos para encontrar una. Los conjuntos de Sidon, que son el objeto principal de nuestro estudio, tienen energía aditiva pequeña.

Definición 2.1.1. Sean G un grupo abeliano aditivo, A, B subconjuntos de

G , definimos la energía aditiva entre A y B por:

$$E(A, B) := |\{(a, a', b, b') \in A \times A \times B \times B : a + b = a' + b'\}|. \quad (2.1)$$

Denotamos por $E(A)$ en el caso cuando $A = B$.

De la definición de energía aditiva, podemos observar las siguientes equivalencias.

$$E(A, B) = |\{(a, a', b, b') \in A \times A \times B \times B : a - b' = a' - b\}|, \quad (2.2)$$

$$E(A, B) = |\{(a, a', b, b') \in A \times A \times B \times B : a - a' = b' - b\}|. \quad (2.3)$$

Además, tenemos las siguientes cotas triviales:

$$|A| |B| \leq E(A, B) \leq |A| |B| \min(|A|, |B|), \quad (2.4)$$

donde la cota inferior se sigue del hecho que si $(a, b) = (a', b')$ entonces $a + b = a' + b'$, luego $|A \times B| = |A| |B| \leq E(A, B)$.

Para la cota superior, notemos que al fijar a, a', b tenemos que b' queda completamente determinado por $b' = a - a' + b$, de esto se sigue que $E(A, B) \leq |A \times A \times B| = |A|^2 |B|$. Similarmente, si fijamos a', b, b' , a queda completamente determinado por $a = a' - b + b'$, así

$$E(A, B) \leq |A \times B \times B| = |A| |B|^2.$$

En el caso cuando $|A| = |B| = n$, tenemos:

$$n^2 \leq E(A, B) \leq \frac{2}{3}n^3 + \frac{n}{3}, \quad (2.5)$$

donde la cota superior se alcanza para $A = B = \{1, 2, \dots, n\}$.

Además, la energía aditiva satisface las siguientes propiedades:

- (a) *Propiedad de simetría*, $E(A, B) = E(B, A)$.
- (b) *Propiedad de invarianza bajo traslaciones*, $E(A + x, B + y) = E(A, B)$, para todo $x, y \in G$. En este caso, notemos que

$$(a + x) + (b + y) = (a' + x) + (b' + y) \iff a + b = a' + b'.$$

(c) $E(A, B) = E(A, -B)$, puesto que $a + b = a' + b' \iff a - b' = a' - b$.

(d) $E(A, B) = E(-A, B)$, puesto que $a + b = a' + b' \iff -a' + b = -a + b'$.

El siguiente lema nos muestra la relación que tiene la energía aditiva con la función de representación [40].

Lema 2.1.2. *Sea G un grupo abeliano aditivo, A, B subconjuntos de G , entonces*

$$E(A, B) = \sum_{x \in A+B} R_{A+B}^2(x), \quad (2.6)$$

$$E(A, B) = \sum_{y \in A-B} R_{A-B}^2(y), \quad (2.7)$$

$$E(A, B) = \sum_{z \in (A-A) \cap (B-B)} R_{A-A}(z) R_{B-B}(z). \quad (2.8)$$

Demostración.

$$\begin{aligned} E(A, B) &= |\{(a, a', b, b') \in A \times A \times B \times B : a + b = a' + b'\}| \\ &= \sum_{x \in A+B} |\{(a, a', b, b') \in A \times A \times B \times B : a + b = a' + b' = x\}| \\ &= \sum_{x \in A+B} |\{(a, b) \in A \times B : a + b = x\}| |\{(a', b') \in A \times B : a' + b' = x\}| \\ &= \sum_{x \in A+B} |\{(a, b) \in A \times B : a + b = x\}|^2 \\ &= \sum_{x \in A+B} R_{A+B}^2(x). \end{aligned}$$

De manera análoga se demuestra la igualdad (2.7).

Para la igualdad (2.8), tenemos

$$\begin{aligned}
E(A, B) &= |\{(a, a', b, b') \in A \times A \times B \times B : a + b' = a' + b\}| \\
&= |\{(a, a', b, b') \in A \times A \times B \times B : a - a' = b - b'\}| \\
&= \sum_{z \in (A-A) \cap (B-B)} |\{(a, a', b, b') \in A \times A \times B \times B : a - a' = b - b' = z\}| \\
&= \sum_{z \in (A-A) \cap (B-B)} |\{(a, a') \in A \times A : a - a' = z\}| |\{(b, b') \in B \times B : b - b' = z\}| \\
&= \sum_{z \in (A-A) \cap (B-B)} R_{A-A}(z) R_{B-B}(z).
\end{aligned}$$

□

Presentamos a continuación algunos ejemplos del cálculo de la energía aditiva entre dos conjuntos.

Ejemplo 2. Sean $A = B = \{1, 2, \dots, n\}$, observemos la tabla de sumas.

+	1	2	3	...	$n-2$	$n-1$	n
1	2	3	4	...	$n-1$	n	$n+1$
2	3	4	5	...	n	$n+1$	$n+2$
3	4	5	6	...	$n+1$	$n+2$	$n+3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$
$n-2$	$n-1$	n	$n+1$	...	$2n-4$	$2n-3$	$2n-2$
$n-1$	n	$n+1$	$n+2$	...	$2n-3$	$2n-2$	$2n-1$
n	$n+1$	$n+2$	$n+3$	...	$2n-2$	$2n-1$	$2n$

Cuadro 2.1: Conjunto Suma $A + A$, para $A = \{1, 2, \dots, n\}$.

Hagamos $R_{A+A} = R$, luego de la Tabla 2.1, tenemos que

$$\begin{array}{lll}
 R(2) = 1 & R(n-1) = n-2 & \vdots \\
 R(3) = 2 & R(n) = n-1 & R(2n-2) = 3 \\
 R(4) = 3 & R(n+1) = n & R(2n-1) = 2 \\
 \vdots & R(n+2) = n-1 & R(2n) = 1 \\
 & R(n+3) = n-2 &
 \end{array}$$

Así,

$$\begin{aligned}
 E(A) &= R^2(2) + R^2(3) + R^2(4) + \cdots + R^2(n-1) + R^2(n) + R^2(n+1) \\
 &\quad + R^2(n+2) + R^2(n+3) + \cdots + R^2(2n-2) + R^2(2n-1) + R^2(2n) \\
 &= 1^2 + 2^2 + 3^2 + \cdots + (n-2)^2 + (n-1)^2 + n^2 \\
 &\quad + (n-1)^2 + (n-2)^2 + \cdots + 3^2 + 2^2 + 1^2 \\
 &= 2(1^2 + 2^2 + 3^2 + \cdots + (n-2)^2 + (n-1)^2) + n^2 \\
 &= 2 \left(\sum_{i=1}^{n-1} i^2 \right) + n^2 \\
 &= 2 \left(\frac{(n-1)n(2(n-1)+1)}{6} \right) + n^2 \\
 &= \frac{(n^2-n)(2n-1)}{3} + n^2 \\
 &= \frac{2n^3+n}{3}
 \end{aligned}$$

En este ejemplo podemos notar que la cota superior en (2.5) se alcanza.

De otra parte, si consideramos un conjunto de Sidon A entero con $|A| = n$, tenemos que

$$\begin{aligned}
 E(A) &= \sum_{x \in A-A} R_{A-A}^2(x) \\
 &= R_{A-A}^2(0) + \sum_{x \in A \ominus A} R_{A-A}^2(x) \\
 &= n^2 + \sum_{x \in A \ominus A} 1 \\
 &= n^2 + 2 \binom{n}{2} \\
 &= 2n^2 - n.
 \end{aligned}$$

Ejemplo 3. Sean $A = \{1, 6, 18, 20, 21, 27, 31\}$, $|A| = 7$, $B = \{1, 10, 14, 15, 17\}$, $|B| = 5$; observemos las tablas de $A + B$ y $A - B$.

+	1	6	18	20	21	27	31
1	2	7	19	21	22	28	32
10	11	16	28	30	31	37	41
14	15	20	32	34	35	41	45
15	16	21	33	35	36	42	46
17	18	23	35	37	38	44	48

Cuadro 2.2: Ejemplo 3 Conjunto Suma $A + B$.

−	1	6	18	20	21	27	31
1	0	5	17	19	20	26	30
10	-9	-4	8	10	11	17	21
14	-13	-8	4	6	7	13	17
15	-14	-9	3	5	6	12	16
17	-16	-11	1	3	4	10	14

Cuadro 2.3: Ejemplo 3 Conjunto Diferencia $A - B$.

En la Tabla 2.2, tenemos que $R_{A+B}(x) = 1$, para todo $x \in \{2, 7, 11, 15, 18, 19, 20, 22, 23, 30, 31, 33, 34, 36, 38, 42, 44, 45, 46, 48\}$, también $R_{A+B}(x) = 2$, para todo $x \in \{16, 21, 28, 32, 37, 41\}$ y $R_{A+B}(35) = 3$.

Luego, $E(A, B) = 20(1^2) + 6(2^2) + 1(3^2) = 20 + 24 + 9 = 53$.

En la Tabla 2.3, tenemos que $R_{A-B}(x) = 1$, para todo $x \in \{-16, -14, -13, -11, -8, -4, 0, 1, 7, 8, 11, 12, 13, 14, 16, 19, 20, 21, 26, 30\}$, también $R_{A-B}(x) = 2$, para todo $x \in \{-9, 3, 4, 5, 6, 10\}$ y $R_{A-B}(17) = 3$.

Luego, $E(A, B) = 20(1^2) + 6(2^2) + 1(3^2) = 20 + 24 + 9 = 53$.

Por último, tenemos las tablas de $A - A$ y $B - B$, respectivamente:

—	1	6	18	20	21	27	31
1	0	5	17	19	20	26	30
6	-5	0	12	14	15	21	25
18	-17	-12	0	2	3	9	13
20	-19	-14	-2	0	1	7	11
21	-20	-15	-3	-1	0	6	10
27	-26	-21	-9	-7	-6	0	4
31	-30	-25	-13	-11	-10	-4	0

Cuadro 2.4: Ejemplo 3 Conjunto Diferencia $A - A$.

—	1	10	14	15	17
1	0	9	13	14	16
10	-9	0	4	5	7
14	-13	-4	0	1	3
15	-14	-5	-1	0	2
17	-16	-7	-3	-2	0

Cuadro 2.5: Ejemplo 3 Conjunto Diferencia $B - B$.

Llamemos $C = (A - A) \cap (B - B)$, entonces tenemos

$$C = \{-14, -13, -9, -7, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 7, 9, 13, 14\},$$

luego $R_{A-A}(x) = R_{B-B}(x) = 1$, para todo $x \in (A - A) \cap (B - B)$, $x \neq 0$, además $R_{A-A}(0) = 7$ y $R_{B-B}(0) = 5$.

Así, $E(A, B) = 18(1^2) + R_{A-A}(0)R_{B-B}(0) = 18 + 7(5) = 18 + 35 = 53$.

Con este ejemplo podemos observar que se satisfacen las identidades del Lema 2.1.2.

De otro lado, como consecuencia del Lema 2.1.2, se tienen las siguientes desigualdades.

Corolario 2.1.3. *Sean A y B subconjuntos de un grupo abeliano aditivo G , entonces existen $x \in A + B$, $y \in A - B$ tales que:*

$$\frac{|A| |B|}{|A \pm B|} \leq \frac{E(A, B)}{|A| |B|} \leq |A \cap (x - B)|, |A \cap (B + y)|. \quad (2.9)$$

En particular, $|A \cap (x - B)| \leq |(A - A) \cap (B - B)|$.

Demostración. De (1.5) tenemos que

$$|A|^2 |B|^2 = \left(\sum_{x \in A+B} R_{A+B}(x) \right)^2,$$

luego aplicando la desigualdad de Cauchy-Schwarz en $\mathbb{R}$ obtenemos que

$$\begin{aligned} |A|^2 |B|^2 &= \left(\sum_{x \in A+B} R_{A+B}(x) \cdot 1 \right)^2 \\ &\leq \left(\sum_{x \in A+B} R_{A+B}^2(x) \right) \left(\sum_{x \in A+B} 1 \right) \\ &= E(A, B) |A + B|. \end{aligned}$$

Por lo tanto, $\frac{|A| |B|}{|A+B|} \leq \frac{E(A, B)}{|A| |B|}$.

Análogamente, obtenemos

$$\frac{|A| |B|}{|A - B|} \leq \frac{E(A, B)}{|A| |B|},$$

o simplemente cambiando B por $-B$ y usando la simetría de la energía aditiva.

Por otro lado, tenemos

$$\begin{aligned}
 E(A, B) &= \sum_{x \in A+B} R_{A+B}^2(x) \\
 &= \sum_{x \in A+B} R_{A+B}(x) R_{A+B}(x), \text{ dado que } |A+B| \text{ es finito,} \\
 &\leq \sum_{x \in A+B} R_{A+B}(x) \left(\max_{x \in A+B} \{R_{A+B}(x)\} \right).
 \end{aligned}$$

Si $R_{A+B}(x_0) = \max_{x \in A+B} \{R_{A+B}(x)\}$ entonces

$$E(A, B) \leq |A| |B| |A \cap (x_0 - B)|.$$

En consecuencia, $\frac{E(A,B)}{|A||B|} \leq |A \cap (x_0 - B)|$, para algún $x_0 \in A + B$.

Análogamente, podemos verificar que $\frac{E(A,B)}{|A||B|} \leq |A \cap (B + y_0)|$, para algún $y_0 \in A - B$.

Adicionalmente, queremos probar que $|A \cap (x - B)| \leq |(A - A) \cap (B - B)|$. Para ello demostramos que $A \cap (x - B) \subseteq z + (A - A) \cap (B - B)$, para algún $z \in A$ y dado que $|z + C| = |C|$, de esta manera obtenemos el resultado deseado.

En efecto, sea $a \in A \cap (x - B)$, entonces existe $b \in B$ tal que

$$a = x - b, \tag{2.10}$$

y como $x \in A + B$, existen $a' \in A$, $b' \in B$ tales que

$$x = a' + b', \tag{2.11}$$

luego reemplazando (2.11) en (2.10) tenemos $a = a' + b' - b$, lo que implica

$$a - a' = b' - b \in (A - A) \cap (B - B).$$

Así, $a \in a' + (A - A) \cap (B - B)$ y tomando $z = a'$, obtenemos el resultado. $\square$

Corolario 2.1.4. Desigualdad de Cauchy-Schwarz

$$E(A, B) \leq E(A, A)^{1/2} E(B, B)^{1/2}.$$

Demostración. Usamos la desigualdad de Cauchy-Schwarz en $\mathbb{R}$ tenemos

$$\begin{aligned} E(A, B) &= \sum_{x \in (A-A) \cap (B-B)} R_{A-A}(x) R_{B-B}(x) \\ &\leq \left(\sum_{x \in (A-A) \cap (B-B)} R_{A-A}^2(x) \right)^{1/2} \left(\sum_{x \in (A-A) \cap (B-B)} R_{B-B}^2(x) \right)^{1/2} \\ &\leq \left(\sum_{x \in A-A} R_{A-A}^2(x) \right)^{1/2} \left(\sum_{x \in B-B} R_{B-B}^2(x) \right)^{1/2} \\ &= E(A, A)^{1/2} E(B, B)^{1/2}. \end{aligned}$$

□

A continuación introducimos un lema de J. Cilleruelo [10] el cual es una aplicación de la energía aditiva y nos permite acotar el cardinal de un conjunto con ciertas propiedades dadas. Aunque Ruzsa [38] lo demostró primero para el caso de $g = 1$, luego J. Cilleruelo lo generalizó para todo entero $g \geq 1$.

Lema 2.1.5. *Sean G un grupo aditivo, A, B subconjuntos de G y g un entero positivo. Si $R_{A-A}(x) \leq g$, para todo $x \neq 0$ en G , entonces*

$$|A|^2 \leq |A + B| \left(g + \frac{|A| - g}{|B|} \right). \quad (2.12)$$

Demostración. Si $R_{A-A}(x) \leq g$ para todo $x \neq 0$ en G , usando (2.8) tenemos

$$\begin{aligned}
 E(A, B) &= \sum_{x \in (A-A) \cap (B-B)} R_{A-A}(x) R_{B-B}(x) \\
 &= R_{A-A}(0) R_{B-B}(0) + \sum_{\substack{x \in (A-A) \cap (B-B) \\ x \neq 0}} R_{A-A}(x) R_{B-B}(x) \\
 &= |A||B| + \sum_{\substack{x \in (A-A) \cap (B-B) \\ x \neq 0}} R_{A-A}(x) R_{B-B}(x) \\
 &\leq |A||B| + \sum_{\substack{x \in (A-A) \cap (B-B) \\ x \neq 0}} g R_{B-B}(x) \\
 &\leq |A||B| + g \sum_{\substack{x \in (B-B) \\ x \neq 0}} R_{B-B}(x) \\
 &= |A||B| + g(|B|^2 - |B|),
 \end{aligned}$$

luego usando la desigualdad (2.9) y la anterior desigualdad tenemos que

$$\begin{aligned}
 |A|^2 &\leq \frac{|A+B|}{|B|^2} E(A, B) \\
 &\leq \frac{|A+B|}{|B|^2} [|A||B| + g(|B|^2 - |B|)] \\
 &= |A+B| \left(\frac{|A|}{|B|} + g - \frac{g}{|B|} \right) \\
 &= |A+B| \left(g + \frac{|A| - g}{|B|} \right).
 \end{aligned}$$

□

2.2. Aplicación de la Energía Aditiva para la función $F_2^-(n, g)$.

Usando energía aditiva entre dos conjuntos es posible demostrar una cota superior de la función $F_2^-(n, g)$ [7], en particular usando la desigualdad (2.12)

del Lema 2.1.5. Sin embargo, esta cota fue demostrada por Lindström en [28] para el caso $g = 1$ y también fue demostrada para el caso general por Trujillo-García-Velásquez en [41], usando otros argumentos.

Teorema 2.2.1. *Sea g un entero positivo y $A \subseteq [1, n]$ un conjunto $B_2^-[g]$ entero, entonces*

$$|A| \leq (gn)^{1/2} + (gn)^{1/4} + 1. \quad (2.13)$$

Demostración. Consideremos el conjunto de enteros $B = [0, u]$, $|B| = u + 1$. Como A es un conjunto en la clase $B_2^-[g]$ se tiene que $R_{A-A}(x) \leq g$ para todo $x \neq 0$ en A , además $A + B \subseteq [1, u + n]$, luego $|A + B| \leq u + n$, así aplicando la desigualdad (2.12) del Lema 2.1.5 tenemos

$$\begin{aligned} |A|^2 &\leq |A + B| \left(g + \frac{|A| - g}{|B|} \right) \\ &\leq (u + n) \left(g + \frac{|A| - g}{u + 1} \right) \\ &= \frac{(u + n)(gu + |A|)}{u + 1}, \end{aligned}$$

ahora tomamos $u = \left\lfloor \sqrt[4]{\frac{n^3}{g}} \right\rfloor$, donde $\lfloor x \rfloor$ denota la parte entera del número real x , y por las propiedades de la función parte entera obtenemos

$$\begin{aligned} |A|^2 &\leq \frac{\left[\left(\frac{n^3}{g} \right)^{1/4} + n \right] \left[g \left(\frac{n^3}{g} \right)^{1/4} + |A| \right]}{\left(\frac{n^3}{g} \right)^{1/4}} \\ &= [(gn)^{1/4} + 1]|A| + gn + (gn)^{3/4}, \end{aligned}$$

luego

$$|A|^2 - [(gn)^{1/4} + 1]|A| \leq gn + (gn)^{3/4},$$

completando cuadrados en el lado izquierdo obtenemos que

$$\left(|A| - \frac{(gn)^{1/4} + 1}{2} \right)^2 \leq gn + (gn)^{3/4} + \left(\frac{(gn)^{1/4} + 1}{2} \right)^2,$$

y ahora completando cuadrados en el lado derecho tenemos

$$\begin{aligned} \left(|A| - \frac{(gn)^{1/4} + 1}{2} \right)^2 &\leq \left((gn)^{1/2} + \frac{(gn)^{1/4} + 1}{2} \right)^2 + (gn)^{3/4} - (gn)^{1/2}((gn)^{1/4} + 1) \\ &= \left((gn)^{1/2} + \frac{(gn)^{1/4} + 1}{2} \right)^2 - (gn)^{1/2} \\ &\leq \left((gn)^{1/2} + \frac{(gn)^{1/4} + 1}{2} \right)^2, \end{aligned}$$

ahora bien, si $|A| \geq \frac{(gn)^{1/4} + 1}{2}$, entonces

$$|A| - \frac{(gn)^{1/4} + 1}{2} \leq (gn)^{1/2} + \frac{(gn)^{1/4} + 1}{2}.$$

Así,

$$|A| \leq (gn)^{1/2} + (gn)^{1/4} + 1.$$

□

Como la desigualdad (2.13) es válida para todo A en la clase $B_2^-[g]$, $A \subseteq [1, n]$, podemos concluir que

$$F_2^-(n, g) \leq (gn)^{1/2} + (gn)^{1/4} + 1. \quad (2.14)$$

En la demostración anterior en lugar de tomar $u = \left\lfloor \sqrt[4]{\frac{n^3}{g}} \right\rfloor$, si consideramos $u = \left\lfloor \frac{\sqrt[4]{n^3}}{\sqrt{g}} \right\rfloor$, mejoramos un poco la cota (2.14) para valores pequeños de g , y de esta manera obtenemos

$$|A| \leq \sqrt{gn + g^{1/2}n^{3/4} + \left(\frac{g^{1/2}n^{1/4}}{2} + \frac{1}{2} \right)^2} + \frac{g^{1/2}n^{1/4}}{2} + \frac{1}{2}. \quad (2.15)$$

Como consecuencia del Teorema 2.2.1, se tiene el siguiente resultado para el caso de conjuntos de Sidon o B_2 enteros.

Corolario 2.2.2. *Para todo número natural n ,*

$$F_2(n) \leq n^{1/2} + n^{1/4} + 1.$$

Sin embargo, con un argumento similar usando energía aditiva, J. Cilleruelo [10] demuestra que

$$|A| \leq (gn)^{1/2} + (gn)^{1/4} + 1/2,$$

para cada número natural g y cada $A \subseteq [1, n]$ que pertenece a la clase $B_2^-[g]$. Esto implica

$$F_2^-(n, g) \leq (gn)^{1/2} + (gn)^{1/4} + 1/2, \quad (2.16)$$

para todo g y n enteros positivos.

En el caso $g = 1$, la mejor cota conocida en la actualidad es la dada por Cilleruelo [10]; es decir, para todo $n \in \mathbb{N}$,

$$F_2(n) \leq n^{1/2} + n^{1/4} + 1/2.$$

En consecuencia de (2.16) se obtiene el siguiente resultado.

Corolario 2.2.3.

$$\limsup_{n \rightarrow \infty} \frac{F_2^-(n, g)}{\sqrt{n}} \leq \sqrt{g}. \quad (2.17)$$

2.3. Aplicaciones de Energía Aditiva a Reglas g -Golomb para la función $G(g, m)$.

Otro ejemplo donde se usa la energía aditiva es para un problema relacionado con conjuntos $B_2^-[g]$ o también llamados reglas g -Golomb [7], en el cual es posible encontrar una cota inferior de la función $G(g, m)$.

Teorema 2.3.1. *Si g y m son enteros positivos arbitrarios, entonces*

$$G(g, m) \geq \frac{m^2}{g} - \frac{2m\sqrt{m-g}}{g} + \frac{m}{g} - \frac{m}{\sqrt{m-g}} - 1. \quad (2.18)$$

Demostración. Sea $A = \{a_i : 1 \leq i \leq m\}$ una regla g -Golomb con m marcas tal que $0 = a_1 < a_2 < \dots < a_m$ y longitud $\ell(A) = a_m$, entonces $R_{A-A}(x) \leq g$, para todo entero x no nulo. Consideremos el conjunto $B = [0, u]$, $|B| = u + 1$.

Además, $A + B \subset [0, a_m + u]$, $|A + B| \leq a_m + u + 1$, entonces por el Lema 2.1.5 tenemos que

$$\begin{aligned} m^2 &\leq (a_m + u + 1) \left(g + \frac{m - g}{u + 1} \right) \\ &= \frac{(a_m + u + 1)(gu + m)}{u + 1}, \end{aligned}$$

de aquí que

$$\begin{aligned} a_m &\geq \frac{m^2(u + 1)}{gu + m} - u - 1 \\ &= (u + 1) \left[\frac{m^2}{gu + m} - 1 \right], \end{aligned}$$

si tomamos $u = \lfloor \frac{m\sqrt{m-g}}{g} - \frac{m}{g} \rfloor$, $u \leq \frac{m\sqrt{m-g}}{g} - \frac{m}{g} \leq u + 1$, entonces

$$\begin{aligned} a_m &\geq \frac{m^2(\frac{m\sqrt{m-g}}{g} - \frac{m}{g})}{m\sqrt{m-g}} - \left(\frac{m\sqrt{m-g}}{g} - \frac{m}{g} \right) - 1 \\ &= \frac{m^2}{g} - \frac{m^2}{g\sqrt{m-g}} - \frac{m\sqrt{m-g}}{g} + \frac{m}{g} - 1 \\ &= \frac{m^2}{g} - \left(\frac{2m^2 - gm}{g\sqrt{m-g}} \right) + \frac{m}{g} - 1 \\ &= \frac{m^2}{g} - m \left(\frac{2(m-g)}{g\sqrt{m-g}} + \frac{gm}{g\sqrt{m-g}} \right) + \frac{m}{g} - 1 \\ &= \frac{m^2}{g} - \frac{2m\sqrt{m-g}}{g} - \frac{m}{\sqrt{m-g}} + \frac{m}{g} - 1. \end{aligned}$$

Esto es,

$$a_m \geq \frac{m^2}{g} - \frac{2m\sqrt{m-g}}{g} - \frac{m}{\sqrt{m-g}} + \frac{m}{g} - 1.$$

Como la desigualdad anterior se cumple para cualquier regla g -Golomb de longitud a_m , en particular se cumple para la regla g -Golomb de menor

longitud, por lo tanto,

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

□

Corolario 2.3.2. *Para todo entero m se cumple*

$$G(m) \geq m^2 - 2m\sqrt{m-1} + m - \frac{m}{\sqrt{m-1}} - 1. \quad (2.19)$$

Demostración. Tomar $g = 1$ en el Teorema 2.3.1. □

Además, del Teorema 2.3.1 se tiene el siguiente resultado.

Corolario 2.3.3. *Para todo g entero positivo, se cumple que*

$$\liminf_{m \rightarrow \infty} \frac{G(g, m)}{m^2} \geq \frac{1}{g}. \quad (2.20)$$

2.4. Aplicación de Energía Aditiva a Conjuntos de Sidon en $\mathbb{Z} \times \mathbb{Z}$.

A. Córdoba y P. Fernández en [18] consideran el siguiente problema: “Dada una malla $N \times N$ de $\mathbb{Z} \times \mathbb{Z}$, ¿cuántos puntos se pueden colocar en ella de manera que no existan dos vectores diferencia iguales?”. Esta pregunta es equivalente a buscar conjuntos de Sidon pero en dos dimensiones; de esta manera, los conjuntos de Sidon tienen una interesante interpretación geométrica: se pueden ver como aquellos que tienen la propiedad especial que no es posible “dibujar” un paralelogramo usando sus puntos como vértices [42].

En este caso, de acuerdo a la interpretación geométrica queremos saber cuál es el mayor número de puntos de coordenadas enteras que se pueden dibujar en el cuadrado $[1, N] \times [1, N]$ de tal manera que nunca cuatro de ellos formen un paralelogramo, para todo $N \in \mathbb{Z}^+$.

Análogamente al caso de conjuntos B_2 , definimos la función $F_2^2(n)$ para el caso de conjuntos B_2 en $\mathbb{Z} \times \mathbb{Z}$.

$$F_2^2(n) := \max\{|A| : A \subseteq [1, n] \times [1, n], A \text{ es un conjunto } B_2 \text{ en } \mathbb{Z} \times \mathbb{Z}\}. \quad (2.21)$$

Lindström [30] obtuvo una cota superior para $F_2^2(n)$,

$$F_2^2(n) \leq n + O(n^{\frac{2}{3}}). \quad (2.22)$$

Usando energía aditiva entre dos conjuntos, demostramos la cota dada por Lindström, pero en este caso, mostramos las constantes explícitas.

Teorema 2.4.1. *Si $A \subseteq [1, n] \times [1, n]$ es un conjunto B_2 en $\mathbb{Z} \times \mathbb{Z}$, entonces*

$$|A| \leq n + 3 \left(\frac{n}{2}\right)^{2/3} + (4n)^{1/3} + 1. \quad (2.23)$$

Demostración. Consideremos el conjunto $B = [0, u] \times [0, u]$, donde $1 \leq u \leq n$, $|B| = (u+1)^2$; además, tenemos que $A+B \subseteq [1, n+u] \times [1, n+u]$, $|A+B| \leq (n+u)^2$. Como A es un conjunto B_2 en $\mathbb{Z} \times \mathbb{Z}$, sabemos que $R_{A-A}(x) \leq 1$, para todo $x \in \mathbb{Z} \times \mathbb{Z}$ no nulo y denotemos por $|A| = k$, así aplicando el Lema 2.1.5 tenemos que

$$\begin{aligned} k^2 &\leq (n+u)^2 \left(1 + \frac{k-1}{(u+1)^2}\right) \\ &\leq (n+u)^2 \left(1 + \frac{k}{(u+1)^2}\right) \\ &= (n+u)^2 + \frac{(n+u)^2}{(u+1)^2} k, \end{aligned}$$

luego

$$k^2 - \frac{(n+u)^2}{(u+1)^2} k \leq (n+u)^2.$$

Ahora completamos cuadrados en el lado izquierdo

$$\left(k - \frac{1}{2} \left(\frac{n+u}{u+1}\right)^2\right)^2 \leq (n+u)^2 + \frac{1}{4} \left(\frac{n+u}{u+1}\right)^4.$$

Así, si $k \geq \frac{1}{2} \left(\frac{n+u}{u+1} \right)^2$ tenemos

$$\begin{aligned} k - \frac{1}{2} \left(\frac{n+u}{u+1} \right)^2 &\leq \sqrt{(n+u)^2 + \frac{1}{4} \left(\frac{n+u}{u+1} \right)^4} \\ &\leq (n+u) + \frac{1}{2} \left(\frac{n+u}{u+1} \right)^2, \end{aligned}$$

luego

$$\begin{aligned} k &\leq (n+u) + \frac{1}{2} \left(\frac{n+u}{u+1} \right)^2 + \frac{1}{2} \left(\frac{n+u}{u+1} \right)^2 \\ &= (n+u) + \left(\frac{n+u}{u+1} \right)^2. \end{aligned}$$

Si tomamos $u = \lfloor cn^{2/3} \rfloor$ tenemos que $cn^{2/3} - 1 \leq u \leq cn^{2/3} \leq u+1$ y así

$$\begin{aligned} k &\leq n + cn^{2/3} + \left(\frac{n + cn^{2/3}}{cn^{2/3}} \right)^2 \\ &= n + cn^{2/3} + \left(\frac{n^{1/3}}{c} + 1 \right)^2 \\ &= n + \left(c + \frac{1}{c^2} \right) n^{2/3} + \frac{2}{c} n^{1/3} + 1. \end{aligned}$$

En resumen, tenemos que

$$k \leq n + \left(c + \frac{1}{c^2} \right) n^{2/3} + \frac{2}{c} n^{1/3} + 1. \quad (2.24)$$

Si consideramos la función $h(c) = c + \frac{1}{c^2}$ tenemos que en $c = 2^{1/3}$ dicha función alcanza su valor mínimo absoluto. De esta manera, si usamos este valor de c y lo reemplazamos en (2.24) obtenemos

$$|A| = k \leq n + 3 \left(\frac{n}{2} \right)^{2/3} + (4n)^{1/3} + 1.$$

□

En consecuencia, para todo número natural n se cumple

$$F_2^2(n) \leq n + 1,9 n^{2/3} + 1,6 n^{1/3} + 1. \quad (2.25)$$

De la anterior desigualdad (2.25) se tiene el siguiente resultado.

Corolario 2.4.2.

$$\limsup_{n \rightarrow \infty} \frac{F_2^2(n)}{n} \leq 1. \quad (2.26)$$

2.5. Aplicación de Energía Aditiva a Conjuntos de Sidon en $\mathbb{Z}^d$.

Otra extensión de los conjuntos de Sidon es al caso d dimensional, para todo d entero positivo. Es decir, se estudian conjuntos de Sidon contenidos en $\mathbb{Z}^d$. El problema de estudio es igual que en el caso unidimensional, se buscan conjuntos de Sidon maximales contenidos en el hipercubo d dimensional; para ello, se define la siguiente función:

$$F_2^d(n) := \max\{|A| : A \subseteq [1, n]^d, A \text{ es un conjunto } B_2 \text{ en } \mathbb{Z}^d\}, \quad (2.27)$$

donde $[1, n]^d$ es el producto cartesiano del intervalo entero $[1, n]$, d veces. La cota dada por Lindström [30] para el caso de dimensión dos que se mencionó en la sección anterior, en realidad él la obtuvo para el caso d dimensional, con $d \geq 2$, la cota es

$$F_2^d(n) \leq n^{\frac{d}{2}} + O(n^{\frac{d^2}{2d+2}}). \quad (2.28)$$

Usando energía aditiva entre dos conjuntos, demostramos una cota superior explícita para la función $F_2^d(n)$ en el caso d par.

Teorema 2.5.1. *Si $A \subseteq [1, n]^d$, A un conjunto B_2 en $\mathbb{Z}^d$ y d es un entero positivo par, entonces*

$$F_2^d(n) \leq \sum_{i=0}^{d/2} \binom{d/2}{i} n^{\alpha(d/2)+i(1-\alpha)} + \sum_{j=0}^d \binom{d}{j} n^{(1-\alpha)(d-j)} \quad (2.29)$$

donde $\alpha = \frac{d+2}{2d+2}$.

Demostración. Consideremos el conjunto $B = [0, u]^d$, donde $1 \leq u \leq n$, $|B| = (u+1)^d$; además, tenemos que $A + B \subseteq [1, n+u]^d$, $|A + B| \leq (n+u)^d$. Como A es un conjunto B_2 en $\mathbb{Z}^d$, sabemos que $R_{A-A}(x) \leq 1$, para todo $x \in \mathbb{Z}^d$, $x \in \mathbb{Z}^d$ no nulo y denotemos por $|A| = k$, así aplicando el Lema 2.1.5 tenemos que

$$\begin{aligned} k^2 &\leq (n+u)^d \left(1 + \frac{k-1}{(u+1)^d} \right) \\ &\leq (n+u)^d + \left(\frac{n+u}{u+1} \right)^d k, \end{aligned}$$

luego

$$k^2 - \left(\frac{n+u}{u+1} \right)^d k \leq (n+u)^d.$$

Ahora completamos cuadrados en el lado izquierdo

$$\left(k - \frac{1}{2} \left(\frac{n+u}{u+1} \right)^d \right)^2 \leq (n+u)^d + \frac{1}{4} \left(\frac{n+u}{u+1} \right)^{2d}.$$

Así, si $k \geq \frac{1}{2} \left(\frac{n+u}{u+1} \right)^d$ tenemos

$$\begin{aligned} k - \frac{1}{2} \left(\frac{n+u}{u+1} \right)^d &\leq \sqrt{(n+u)^d + \frac{1}{4} \left(\frac{n+u}{u+1} \right)^{2d}} \\ &\leq (n+u)^{\frac{d}{2}} + \frac{1}{2} \left(\frac{n+u}{u+1} \right)^d, \end{aligned}$$

luego

$$k \leq (n+u)^{\frac{d}{2}} + \left(\frac{n+u}{u+1} \right)^d,$$

$$k \leq (n+u)^{\frac{d}{2}} + \left(\frac{n}{u+1} + 1 \right)^d.$$

Si tomamos $u = \lfloor n^\alpha \rfloor$, donde el valor de α lo damos más adelante, tenemos que $n^\alpha - 1 \leq u \leq n^\alpha \leq u + 1$ y así

$$\begin{aligned} k &\leq (n + n^\alpha)^{\frac{d}{2}} + \left(\frac{1}{n^{\alpha-1}} + 1 \right)^d \\ &= \frac{(n + n^\alpha)^{\frac{d}{2}} n^{(\alpha-1)d} + (1 + n^{\alpha-1})^d}{n^{(\alpha-1)d}} \end{aligned}$$

Si d es par, tenemos que

$$k \leq \frac{\sum_{i=0}^{d/2} \binom{d/2}{i} n^{i+\alpha(d/2-i)+(\alpha-1)d} + \sum_{j=0}^d \binom{d}{j} n^{(\alpha-1)j}}{n^{(\alpha-1)d}}.$$

Así,

$$k \leq \sum_{i=0}^{d/2} \binom{d/2}{i} n^{\alpha(d/2)+i(1-\alpha)} + \sum_{j=0}^d \binom{d}{j} n^{(1-\alpha)(d-j)}.$$

Tomando $\alpha = \frac{d^2}{2d+2} - \frac{d}{2} + 1 = \frac{d+2}{2d+2}$, como el conjunto A se escogió arbitrariamente obtenemos para todo n entero positivo y d par que

$$F_2^d(n) \leq \sum_{i=0}^{d/2} \binom{d/2}{i} n^{\alpha(d/2)+i(1-\alpha)} + \sum_{j=0}^d \binom{d}{j} n^{(1-\alpha)(d-j)}.$$

□

Con el resultado anterior obtenemos la cota (2.28) dada por Lindström [30], sin embargo en nuestro caso es posible obtener las constantes explícitas para cuando d es par. Presentamos a continuación dos ejemplos como aplicación del Teorema anterior en el caso cuando $d = 2$ y $d = 4$.

Ejemplo 4. Tomando $d = 2$, tenemos que $\alpha = \frac{2}{3}$, así:

$$F_2^2(n) \leq \sum_{i=0}^1 \binom{1}{i} n^{\frac{2}{3}+\frac{1}{3}i} + \sum_{j=0}^2 \binom{2}{j} n^{\frac{1}{3}(2-j)} = n + 2n^{\frac{2}{3}} + 2n^{\frac{1}{3}} + 1.$$

Podemos notar que la cota dada en (2.25) es mejor que la cota anterior cuando $d = 2$.

Ejemplo 5. Tomando $d = 4$, tenemos que $\alpha = \frac{3}{5}$, así:

$$F_2^4(n) \leq \sum_{i=0}^2 \binom{2}{i} n^{\frac{6}{5} + \frac{2}{5}i} + \sum_{j=0}^4 \binom{4}{j} n^{\frac{2}{5}(4-j)} = n^2 + 3n^{\frac{8}{5}} + 5n^{\frac{6}{5}} + 6n^{\frac{4}{5}} + 4n^{\frac{2}{5}} + 1.$$

2.6. Aplicación de Energía Aditiva a Secuencias Sonar.

Algunos conjuntos de Sidon en dimensión dos se pueden definir en términos de funciones, como se menciona a continuación.

Definición 2.6.1. Sean $n, m \in \mathbb{N}$ y $f : [1, n] \rightarrow [1, m]$ una función. Se dice que f tiene la propiedad de diferencias distintas si para todo i, j, k tales que $1 \leq k \leq n - 1$, $1 \leq i, j \leq n - k$ se cumple:

$$f(i + k) - f(i) = f(j + k) - f(j) \Rightarrow i = j. \quad (2.30)$$

Equivalentemente, si el grafo de f ,

$$G_f = \{(x, f(x)) : x \in [1, n]\} \subseteq [1, n] \times [1, m]$$

es un conjunto de Sidon en el grupo aditivo $\mathbb{Z} \times \mathbb{Z}$. Este tipo de funciones se denominan funciones Sidon.

Las secuencias sonar fueron introducidas por Golomb y Taylor [22] como ejemplos de patrones de sincronización dos dimensional de mínima ambigüedad. Una secuencia sonar $m \times n$ es un arreglo de puntos y espacios que tienen m filas y exactamente un punto en cada una de sus n columnas, sujeto a la restricción que cada par de puntos determinan vectores distintos. Se define a continuación una secuencia sonar en términos de función.

Definición 2.6.2. Una secuencia sonar de orden $m \times n$ es una función $f : [1, n] \rightarrow [1, m]$ que tiene la propiedad de diferencias distintas; dicho de otro modo, una secuencia sonar es una función Sidon de $[1, n]$ en $[1, m]$.

Actualmente, el problema de estudio de las secuencias sonar es el siguiente: para m fijo encontrar el mayor n para el cual existe una secuencia sonar $m \times n$; es decir, se estudia la función definida por:

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

Una cota trivial de $S(m)$ es $S(m) \leq 2m$. Como se describe en [16] la cota de Erdős y Turán puede adaptarse para probar que una secuencia sonar $m \times n$ debe cumplir que

$$S(m) < m + 3m^{2/3} + 2m^{1/3} + 9.$$

Esta cota muestra que para m grande, una secuencia sonar $m \times n$ tiene a $S(m)$ más cercano a m que a $2m$.

Aunque en este mismo artículo [16], los autores prueban que si una secuencia sonar $m \times n$ existe entonces $S(m) < m + 5m^{2/3}$.

Otro ejemplo del uso de la energía aditiva es para encontrar una cota superior de $S(m)$ [43]; esto muestra la eficacia de esta herramienta en otro problema relacionado con conjuntos de Sidon.

Teorema 2.6.3. *Si $f : [1, n] \rightarrow [1, m]$ define una secuencia sonar entonces*

$$S(m) < m + 3,78m^{2/3} + 4,76m^{1/3} + 2. \quad (2.31)$$

Demostración. Dado que f define una secuencia sonar, entonces su grafo G_f es un conjunto de Sidon en $[1, n] \times [1, m]$. Además, $|G_f| = n$.

Consideremos el conjunto $B = [0, u] \times [0, u]$, entonces $|B| = (u + 1)^2$, $G_f + B \subseteq [1, n + u] \times [1, m + u]$ y $|G_f + B| \leq (n + u)(m + u)$. Dado que G_f es un conjunto de Sidon entonces $R_{G_f + G_f}(x) \leq 1$, para todo $x \neq (0, 0)$, aplicando el Lema 2.1.5 tenemos que

$$\begin{aligned} |G_f|^2 &\leq |G_f + B| \left(1 + \frac{|G_f| - 1}{|B|} \right) \\ n^2 &\leq (n + u)(m + u) \left(1 + \frac{n - 1}{(u + 1)^2} \right). \end{aligned}$$

Dividimos a cada lado por n y tenemos que

$$n \leq \left(1 + \frac{u}{n}\right) (m + u) \left(1 + \frac{n-1}{(u+1)^2}\right).$$

Tomamos $u = \lfloor cm^{2/3} \rfloor$ y dado que $m \leq n \leq 2m$ entonces tenemos que

$$\begin{aligned} n &\leq \left(1 + \frac{cm^{2/3}}{m}\right) (m + cm^{2/3}) \left(1 + \frac{2m}{(cm^{2/3})^2}\right) \\ &= \left(1 + \frac{c}{m^{1/3}}\right) (m + cm^{2/3}) \left(1 + \frac{2}{c^2 m^{1/3}}\right) \\ &= (m + 2cm^{2/3} + c^2 m^{1/3}) \left(1 + \frac{2}{c^2 m^{1/3}}\right) \\ &= m + 2cm^{2/3} + c^2 m^{1/3} + \frac{2m^{2/3}}{c^2} + \frac{4m^{1/3}}{c} + 2 \\ &= m + \left(\frac{2c^3 + 2}{c^2}\right) m^{2/3} + \left(\frac{c^3 + 4}{c}\right) m^{1/3} + 2 \end{aligned}$$

Si consideramos la función $h(c) = \frac{2c^3+2}{c^2}$ tenemos que en $c = \sqrt[3]{2}$ dicha función alcanza su valor mínimo absoluto. De esta manera, si tomamos este valor de c y lo reemplazamos en la anterior desigualdad tenemos que

$$n \leq m + \left(\frac{6}{2^{2/3}}\right) m^{2/3} + \left(\frac{6}{2^{1/3}}\right) m^{1/3} + 2.$$

Dado que esto es válido para cualquier secuencia sonar $f : [1, n] \rightarrow [1, m]$ entonces

$$S(m) < m + 3,78m^{2/3} + 4,76m^{1/3} + 2.$$

□

Capítulo 3

Construcciones de conjuntos de Sidon en una dimensión

En este capítulo presentamos las tres construcciones de conjuntos de Sidon modulares maximales conocidas, desde una perspectiva diferente a la original. En primer lugar, describimos la construcción de conjuntos B_2 tipo Bose, para ello construimos un conjunto de Sidon multiplicativo y como la propiedad de conjunto de Sidon se preserva bajo isomorfismos, usamos el isomorfismo adecuado para construir el conjunto de Sidon modular tipo Bose en el grupo aditivo $\mathbb{Z}_{q^2-1}$, donde q es una potencia de un primo. En segundo lugar, para la construcción de un conjunto B_2 tipo Singer, construimos un conjunto B_3 en el grupo aditivo $\mathbb{Z}_{q^3-1}$ con q elementos y luego hacemos la reducción módulo $q^2 + q + 1$, éste nuevo conjunto es un conjunto de Sidon; lo interesante de esta construcción es que al hacer la reducción se preserva el número de elementos. Luego al conjunto resultante le agregamos un elemento adecuado para obtener el conjunto de Sidon con $q + 1$ elementos en el grupo aditivo $\mathbb{Z}_{q^2+q+1}$. En tercer lugar, presentamos la construcción de un conjunto B_2 tipo Ruzsa, la demostración es análoga a la original, donde primero construimos un conjunto de Sidon en dos dimensiones y luego por el isomorfismo del Teorema Chino el Residuo obtenemos el conjunto deseado.

Además, en cada una de las construcciones, presentamos algunas propiedades que satisfacen estos conjuntos.

3.1. Construcción de conjuntos B_2 tipo Bose

Históricamente, la construcción de conjuntos de Sidon tipo Singer [39] aparece en el año de 1938 en su estudio relacionado con Geometría Proyectiva y la construcción de Bose [3] aparece en el año 1941, donde Bose prueba un análogo al Teorema de Singer. Sin embargo, nosotros presentamos primero la construcción de Bose de conjuntos B_2 , la cual puede ser generalizada a conjunto B_h y luego presentamos la construcción de Singer a partir de un conjunto B_3 .

Teorema 3.1.1. *Sea $(F, +, \cdot)$ un campo, E una extensión algebraica de grado 2 sobre F con elemento algebraico α , $E = F(\alpha)$, y θ un elemento primitivo de E . El conjunto*

$$A(\alpha) = \alpha + F := \{\alpha + a : a \in F\}$$

es un conjunto B_2 en el grupo multiplicativo E^ .*

Demostración. Claramente, $A(\alpha) \neq \emptyset$ pues $\alpha = \alpha + 0 \in A(\alpha)$, para $0 \in F$.

Además, todos los elementos de $A(\alpha)$ son distintos, pues si tomamos $\alpha + a = \alpha + b$, con $a, b \in F$ entonces $a = b$.

Ahora, supongamos que existen $a, b, c, d \in F$ tales que

$$(\alpha + a)(\alpha + b) = (\alpha + c)(\alpha + d),$$

desarrollando los productos y eliminando el término α^2 obtenemos

$$(a + b)\alpha + ab = (c + d)\alpha + cd,$$

luego

$$[a + b - (c + d)]\alpha + ab - cd = 0.$$

De esto se sigue que α es raíz del polinomio de grado uno,

$$P(x) = [a + b - (c + d)]x + ab - cd \in F[x],$$

pero como α es algebraico sobre F de grado 2, su polinomio minimal también tiene grado 2, así que el polinomio $P(x)$ debe ser el polinomio nulo. Esto implica que

$$\begin{aligned} a + b &= c + d, \\ ab &= cd. \end{aligned}$$

Si tomamos el polinomio $P(x) = x^2 + Sx + P \in F[x]$, donde $S = a+b = c+d$ y $P = ab = cd$, podemos notar que éste se factoriza como

$$x^2 + Sx + P = x^2 + (a+b)x + ab = (x+a)(x+b),$$

o también como

$$x^2 + Sx + P = x^2 + (c+d)x + cd = (x+c)(x+d),$$

y dado que los ceros de un polinomio son únicos entonces $\{a, b\} = \{c, d\}$, lo que implica que $\{\alpha + a, \alpha + b\} = \{\alpha + c, \alpha + d\}$.

□

Ahora bien, si consideramos F el campo finito $\mathbb{F}_q$, q potencia prima, α un elemento de grado 2 sobre $\mathbb{F}_q$ y θ un elemento primitivo del campo de extensión $\mathbb{F}_{q^2}$, podemos obtener un conjunto B_2 tipo Bose en el grupo $(\mathbb{Z}_{q^2-1}, +)$ con q elementos, usando el isomorfismo del logaritmo discreto en la base θ entre los grupos $(\mathbb{F}_{q^2}^*, \cdot)$ y $(\mathbb{Z}_{q^2-1}, +)$ definido por:

$$\begin{aligned} \log_\theta : (\mathbb{F}_{q^2}^*, \cdot) &\rightarrow (\mathbb{Z}_{q^2-1}, +) \\ \theta^k &\mapsto \log_\theta(\theta^k) = k. \end{aligned}$$

Teorema 3.1.2. *Con la notación anterior, se tiene que el conjunto*

$$A = \log_\theta A(\alpha) = \log_\theta(\alpha + \mathbb{F}_q) := \{\log_\theta(\alpha + a) : a \in \mathbb{F}_q\} \subseteq \mathbb{Z}_{q^2-1}$$

es un conjunto B_2 en $\mathbb{Z}_{q^2-1}$, con q elementos.

Demostración. Se sigue del Teorema 3.1.1 y el Lema 1.0.7.

□

De otro lado, tenemos que los conjuntos de Sidon tipo Bose, dependen de la potencia prima q , el elemento primitivo θ y el elemento α de grado 2 sobre $\mathbb{F}_q$. Así que denotamos al conjunto $\log_\theta A(\alpha)$ por $\mathcal{B}(q, \alpha, \theta)$.

Ejemplo 6. Sea $p = 7$, θ un elemento primitivo de $\mathbb{F}_{7^2}$, con polinomio minimal sobre $\mathbb{F}_7$, $\min_{\mathbb{F}_7}(\theta) = 2x^2 + x + 3$ y tomemos $\alpha = \theta$ de grado 2 sobre $\mathbb{F}_7$. El conjunto

$$\begin{aligned} A(\theta) &= \{\theta, \theta + 1, \theta + 2, \theta + 3, \theta + 4, \theta + 5, \theta + 6\} \\ &= \{\theta, \theta^{46}, \theta^{36}, \theta^{10}, \theta^{31}, \theta^{35}, \theta^{29}\}, \end{aligned}$$

es un conjunto B_2 en el grupo multiplicativo $\mathbb{F}_{49}^*$. Usando el isomorfismo del logaritmo discreto en la base θ tenemos que el conjunto

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

es un conjunto B_2 en el grupo aditivo $\mathbb{Z}_{48}$.

3.1.1. Propiedades de la construcción de conjuntos B_2 tipo Bose.

Presentamos algunas propiedades que satisfacen los conjuntos B_2 tipo Bose. Como antes, θ es un elemento primitivo de $\mathbb{F}_{q^2}$, $\alpha \in \mathbb{F}_{q^2}$ un elemento de grado 2 sobre $\mathbb{F}_q$ y $\mathcal{B} = B(q, \alpha, \theta) = \{\log_\theta(\alpha + a) : a \in \mathbb{F}_q\}$.

Proposición 3.1.3. *Sea $\mathcal{B}$ un conjunto de Sidon tipo Bose definido como antes, las siguientes propiedades se satisfacen.*

(B1) *Si $a \in \mathcal{B}$ entonces $a \not\equiv 0 \pmod{q+1}$.*

(B2) $|\mathcal{B}| = q$.

(B3) *Dados $a, b \in \mathcal{B}$ distintos, entonces $a \not\equiv b \pmod{q+1}$.*

(B4) $\mathcal{B} \pmod{q+1} = \{a \pmod{q+1} : a \in \mathcal{B}\} = [1, q]$.

(B5) $\mathcal{B} \ominus \mathcal{B} = \mathbb{Z}_{q^2-1} \setminus M_{q+1}$,

donde $M_{q+1} = \{0, q+1, 2(q+1), \dots, (q-2)(q+1)\} \cong \mathbb{Z}_{q-1}$.

Demostración. (B1) En efecto, dado $a \in \mathcal{B}$ existe $k \in \mathbb{F}_q$ tal que $a = \log_\theta(\alpha + k)$, de esto se sigue que $\theta^a = \alpha + k$ y como $\alpha \notin \mathbb{F}_q^* = \langle \theta^{q+1} \rangle$ tenemos que $\theta^a \notin \mathbb{F}_q^*$. Por lo tanto $q+1$ no divide a a y así tenemos el resultado.

- (B2) $|\mathcal{B}| = q$ por la definición de $\mathcal{B}$ pues $\alpha \notin \mathbb{F}_q$, $|\alpha + \mathbb{F}_q| = q$ y la función logaritmo discreto es inyectiva.
- (B3) Verifiquemos esta propiedad por contradicción, para ello supongamos que $a \equiv b \pmod{q+1}$, luego existe $t \in \mathbb{Z}$ tal que $a - b = t(q+1)$. De aquí que $\theta^{a-b} = \theta^{t(q+1)}$ y como $\mathbb{F}_q^* = \langle \theta^{q+1} \rangle$ se sigue que $\theta^{a-b} \in \mathbb{F}_q^*$. De otro lado, dado que $a, b \in \mathcal{B}$ existen k_1 y k_2 en $\mathbb{F}_q$ distintos tales que $a = \log_\theta(\alpha + k_1)$ y $b = \log_\theta(\alpha + k_2)$, lo que implica que $\theta^a = \alpha + k_1$ y $\theta^b = \alpha + k_2$; luego $\theta^{a-b} = \frac{\alpha+k_1}{\alpha+k_2}$. Como $\theta^{a-b} \in \mathbb{F}_q^*$, existe $c \in \mathbb{F}_q^*$ tal que $\frac{\alpha+k_1}{\alpha+k_2} = c$. Dado que $k_1 \neq k_2$ tenemos que $c \neq 1$, luego $\alpha + k_1 = c(\alpha + k_2)$ lo que es equivalente a $(1-c)\alpha = ck_2 - k_1$ y por lo tanto tenemos que $\alpha = (ck_2 - k_1)(1-c)^{-1} \in \mathbb{F}_q^*$ lo cual es una contradicción; así, $a \not\equiv b \pmod{q+1}$. De esto se sigue que $(\mathcal{B} \ominus \mathcal{B}) \cap M_{q+1} = \emptyset$, donde $\mathcal{B} \ominus \mathcal{B} = (\mathcal{B} - \mathcal{B}) \setminus \{0\}$.

(B4) Esta propiedad se sigue de (B1) y (B3).

- (B5) Dado que $\mathcal{B}$ es un conjunto de Sidon y $|\mathcal{B}| = q$, entonces tenemos que $|\mathcal{B} \ominus \mathcal{B}| = 2\binom{q}{2} = q(q-1) = q^2 - q$. Además, $(\mathcal{B} \ominus \mathcal{B}) \cap M_{q+1} = \emptyset$, luego $|\mathbb{Z}_{q^2-1}| - |M_{q+1}| = q^2 - 1 - (q-1) = q^2 - q = |\mathcal{B} \ominus \mathcal{B}|$.

□

De la propiedad (B5) podemos notar que no importa el valor que tomen α y θ , el conjunto diferencia de $\mathcal{B}$ siempre es el mismo. Es decir, el conjunto diferencia de un conjunto B_2 tipo Bose es independiente de la escogencia del elemento primitivo de $\mathbb{F}_{q^2}$ y el elemento α de grado 2 sobre $\mathbb{F}_q$.

Observación 3.1.4. La construcción de conjuntos B_2 tipo Bose, es posible extenderla a conjuntos B_h , de manera similar; éstos son los conjuntos B_h tipo Bose-Chowla, los detalles se presentan en el Capítulo 5.

3.2. Construcción de conjuntos B_2 tipo Singer.

Aunque en principio la construcción de Singer apareció primero que la construcción de Bose-Chowla, en esta versión presentamos la construcción de Singer como una consecuencia de la construcción de Bose-Chowla.

Sea q una potencia de un primo, consideremos el campo finito $\mathbb{F}_{q^3}$ con elemento primitivo θ y sea $\alpha \in \mathbb{F}_{q^3}$ un elemento de grado 3 sobre $\mathbb{F}_q$. Construimos el conjunto $A(\alpha) = \alpha + \mathbb{F}_q$, el cual es un conjunto B_3 en el grupo multiplicativo de $\mathbb{F}_{q^3}$. La demostración es análoga a la del Teorema 3.1.1.

Dado que los grupos $(\mathbb{F}_{q^3}^*, \cdot)$ y $(\mathbb{Z}_{q^3-1}, +)$ son isomorfos por medio del isomorfismo del logaritmo discreto, tenemos que el conjunto

$$\mathcal{A} = \log_\theta(A(\alpha)) := \{\alpha + u : u \in \mathbb{F}_q\}$$

es un conjunto B_3 en $\mathbb{Z}_{q^3-1}$ con q elementos.

Llamemos $n_q = q^2 + q + 1 = \frac{q^3-1}{q-1}$. Por el isomorfismo mencionado entre los grupos $\mathbb{F}_{q^3}^*$ y $\mathbb{Z}_{q^3-1}$, entonces para cada elemento $\alpha + u_i \in A(\alpha)$ existe un único elemento $a_i \in \mathcal{A}$ tal que

$$\log_\theta(\alpha + u_i) = a_i,$$

y definimos $\mathcal{S} =: \mathcal{A}(\text{mód } n_q)$.

Teorema 3.2.1. *Con la notación anterior, se tiene que el conjunto $\mathcal{S}_0 = \mathcal{S} \cup \{0\}$ es un conjunto B_2 en $\mathbb{Z}_{q^2+q+1}$ con $q+1$ elementos.*

Demostración. Con la notación anterior consideremos el conjunto $\mathcal{A} = \log_\theta(\alpha + \mathbb{F}_q)$. Si modulamos el conjunto $\mathcal{A}$ módulo n_q , obtenemos un nuevo conjunto que llamamos $\mathcal{S} = \mathcal{A}(\text{mód } n_q)$. Ahora verifiquemos que $\mathcal{S}$ es un conjunto B_2 en $\mathbb{Z}_{q^2+q+1}$.

En efecto, sean a_1, a_2, a_3, a_4 en $\mathcal{S}$ tales que

$$a_1 + a_2 \equiv a_3 + a_4 \pmod{n_q}$$

entonces existe $r \in \mathbb{Z}$ tal que

$$a_1 + a_2 = a_3 + a_4 + rn_q.$$

Como para cada $a_i \in \mathcal{A} = \log_\theta(\alpha + \mathbb{F}_q)$, $i = 1, 2, 3, 4$, existe un único $u_i \in \mathbb{F}_q$ tal que $a_i = \log_\theta(\alpha + u_i)$ entonces

$$\log_\theta(\alpha + u_1) + \log_\theta(\alpha + u_2) = \log_\theta(\alpha + u_3) + \log_\theta(\alpha + u_4) + rn_q,$$

lo que implica que

$$(\alpha + u_1)(\alpha + u_2)(\alpha + u_3)^{-1}(\alpha + u_4)^{-1} = \theta^{rn_q},$$

y como $\theta^{rn_q} \in \mathbb{F}_q^* = \langle \theta^{n_q} \rangle$ tenemos que

$$(\alpha + u_1)(\alpha + u_2)(\alpha + u_3)^{-1}(\alpha + u_4)^{-1} = v,$$

donde $v = \theta^{rn_q}$. Esto es equivalente a

$$(\alpha + u_1)(\alpha + u_2) = v(\alpha + u_3)(\alpha + u_4).$$

Así, α satisface el polinomio

$$P(x) = (1 - v)x^2 + (u_1 + u_2 - v(u_3 + u_4))x + (u_1u_2 - vu_3u_4) \in \mathbb{F}_q[x],$$

pero como α es un elemento de grado 3 sobre $\mathbb{F}_q$ entonces $P(x)$ debe ser el polinomio nulo, luego $1 - v = 0$, $u_1 + u_2 - v(u_3 + u_4) = 0$ y $u_1u_2 - vu_3u_4 = 0$. Lo que implica que

$$\{u_1, u_2\} = \{u_3, u_4\}.$$

En consecuencia,

$$\{a_1, a_2\} = \{a_3, a_4\}.$$

Así, $\mathcal{S}$ es un conjunto B_2 en $\mathbb{Z}_{n_q}$ con q elementos.

Ahora, consideremos el conjunto $\mathcal{S}_0 := \mathcal{S} \cup \{0\}$. Para verificar que $\mathcal{S}_0$ es un conjunto B_2 , como $|\mathcal{S}_0| = q+1$, vamos a probar que $|\mathcal{S}_0 - \mathcal{S}_0| = |\mathcal{S}_0|^2 - |\mathcal{S}_0| + 1$. En efecto, como

$$\begin{aligned} \mathcal{S}_0 - \mathcal{S}_0 &= (\mathcal{S} - \mathcal{S}) \cup (\mathcal{S} - \{0\}) \cup (\{0\} - \mathcal{S}) \cup (\{0\} - \{0\}) \\ &= (\mathcal{S} - \mathcal{S}) \cup \mathcal{S} \cup (-\mathcal{S}), \end{aligned}$$

donde la última igualdad se sigue porque $\{0\} \subset \mathcal{S} - \mathcal{S}$. Además, por las propiedades que demostramos en la siguiente sección, tenemos que

$$(\mathcal{S} - \mathcal{S}) \cap \mathcal{S} = (\mathcal{S} - \mathcal{S}) \cap (-\mathcal{S}) = \mathcal{S} \cap (-\mathcal{S}) = \emptyset,$$

por lo tanto

$$\begin{aligned} |\mathcal{S}_0 - \mathcal{S}_0| &= |(\mathcal{S} - \mathcal{S}) \cup \mathcal{S} \cup (-\mathcal{S})| \\ &= |(\mathcal{S} - \mathcal{S})| + |\mathcal{S}| + |(-\mathcal{S})| \\ &= (q^2 - q + 1) + q + q. \end{aligned}$$

Así, $|\mathcal{S}_0 - \mathcal{S}_0| = q^2 + q + 1$ entonces $\mathcal{S}_0$ es un conjunto B_2 en $\mathbb{Z}_{n_q}$ con $q + 1$ elementos. $\square$

3.2.1. Propiedades de la construcción de conjuntos B_2 tipo Singer.

Presentamos algunas propiedades de los conjuntos B_2 módulo $q^2 + q + 1$ tipo Singer. Recordemos $\mathbb{F}_{q^3}^* = \langle \theta \rangle$, $\mathbb{F}_q^* = \langle \theta^{q^2+q+1} \rangle$, $\alpha \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ un elemento de grado 3 sobre $\mathbb{F}_q$, y consideramos los conjuntos $A(\alpha) = \alpha + \mathbb{F}_q$, $\mathcal{A} = \log_\theta A(\alpha)$, $\mathcal{S} = A(\text{mód } n_q)$ y $\mathcal{S}_0 = \mathcal{S} \cup \{0\}$, donde $n_q = q^2 + q + 1$.

Proposición 3.2.2. *Sea $\mathcal{S}$ un conjunto de Sidon tipo Singer definido como antes, las siguientes propiedades se satisfacen:*

- (S1) $0 \notin \mathcal{S}$.
- (S2) $|\mathcal{S}| = q$.
- (S3) $\mathcal{S} \cap (-\mathcal{S}) = \emptyset$.
- (S4) $\mathcal{S} \cap (\mathcal{S} - \mathcal{S}) = \emptyset$.
- (S5) $(-\mathcal{S}) \cap (\mathcal{S} - \mathcal{S}) = \emptyset$.
- (S6) $\mathbb{Z}_{q^2+q+1} \setminus \{0\} = (\mathcal{S} \ominus \mathcal{S}) \cup \mathcal{S} \cup (-\mathcal{S})$.
- (S7) $\mathcal{S}_0 \ominus \mathcal{S}_0 = \mathbb{Z}_{n_q} \setminus \{0\}$.

Demostración. (S1) $0 \notin \mathcal{S}$, pues si esto no es así, existe $a \in \mathcal{A}$ tal que $a \equiv 0 \pmod{n_q}$ y como $a \in \mathcal{A}$, existe $b \in \mathbb{F}_q$ tal que $a = \log_\theta(\alpha + b)$, luego

$$a = \log_\theta(\alpha + b) \equiv 0 \pmod{n_q},$$

así, existe $r \in \mathbb{Z}$ tal que $\log_\theta(\alpha + b) = rn_q$, lo que implica que $\alpha + b = \theta^{rn_q}$ y como $\mathbb{F}_q^* = \langle \theta^{n_q} \rangle$, se sigue que $\alpha + b \in \mathbb{F}_q^*$, luego $\alpha \in \mathbb{F}_q^*$ lo que es una contradicción.

(S2) Supongamos que existen $s, r \in \mathcal{S}$ tales que $s \equiv r \pmod{n_q}$, luego existen $s_1, r_1 \in \mathbb{F}_q$ y $t \in \mathbb{Z}$ tales que $s = \log_\theta(\alpha + s_1)$, $r = \log_\theta(\alpha + r_1)$, luego

$$\log_\theta(\alpha + s_1) = \log_\theta(\alpha + r_1) + n_q t.$$

De esta última igualdad se sigue que $(\alpha + s_1) = \theta^{n_q t}(\alpha + r_1)$ y como $\mathbb{F}_q^* = \langle \theta^{n_q} \rangle$, entonces $(\alpha + s_1) = c(\alpha + r_1)$, donde $c = \theta^{n_q t} \in \mathbb{F}_q^*$, lo que implica que α es raíz del polinomio

$$P(x) = (1 - c)x + s_1 - cr_1 \in \mathbb{F}_q[x],$$

pero como α es de grado 3 sobre $\mathbb{F}_q$, entonces $P(x)$ debe ser el polinomio nulo, lo que implica que $c = 1$ y por lo tanto $s_1 = r_1$. En consecuencia, $s = r$ y por lo tanto $|\mathcal{S}| = q$.

(S3) Supongamos que existen $s, s' \in \mathcal{S}$ tales que $s \equiv -s' \pmod{n_q}$ luego existen $a, a' \in \mathbb{F}_q$ y $r \in \mathbb{Z}$ tales que $s = \log_\theta(\alpha + a)$, $s' = \log_\theta(\alpha + a')$ luego

$$s + s' = \log_\theta(\alpha + a) + \log_\theta(\alpha + a') = rn_q,$$

así,

$$\log_\theta((\alpha + a)(\alpha + a')) = rn_q,$$

lo que implica

$$\alpha^2 + (a + a')\alpha + aa' = \theta^{rn_q},$$

si llamamos $v = \theta^{rn_q} \in \mathbb{F}_q^* = \langle \theta^{n_q} \rangle$ tenemos que α es raíz del polinomio

$$Q(x) = x^2 + (a + a')x + aa' - v$$

con coeficientes en $\mathbb{F}_q$, pero como α es de grado 3 sobre $\mathbb{F}_q$, entonces $Q(x)$ debe ser el polinomio nulo; lo cual no puede ser posible puesto que el coeficiente de x^2 es 1. De esta manera obtenemos el resultado.

- (S4) Supongamos que existen $s, r, t \in \mathcal{S}$ tales que $s \equiv r - t \pmod{n_q}$, luego existen $a, b, c \in \mathbb{F}_q$ y $r \in \mathbb{Z}$ tales que $s = \log_\theta(\alpha + a)$, $r = \log_\theta(\alpha + b)$ y $t = \log_\theta(\alpha + c)$ y

$$s - r + t = \log_\theta(\alpha + a) - \log_\theta(\alpha + b) + \log_\theta(\alpha + c) = rn_q,$$

lo que implica que

$$\frac{(\alpha + a)(\alpha + c)}{(\alpha + b)} = \theta^{rn_q}$$

si llamamos $v = \theta^{rn_q} \in \mathbb{F}_q^* = \langle \theta^{n_q} \rangle$ tenemos que α es raíz del polinomio

$$R(x) = x^2 + (a + c - v)x + ac - bv$$

con coeficientes en $\mathbb{F}_q$, pero como α es de grado 3 sobre $\mathbb{F}_q$, entonces $R(x)$ debe ser el polinomio nulo; lo cual no puede ser posible puesto que el coeficiente de x^2 es 1, así se sigue el resultado.

- (S5) La demostración es análoga a (S4).

- (S6) Dado que $|\mathbb{Z}_{q^2+q+1} \setminus \{0\}| = q^2 + q$, $|\mathcal{S} \ominus \mathcal{S}| = q^2 - q$, $|\mathcal{S}| = |-\mathcal{S}| = q$, $\mathcal{S} \ominus \mathcal{S}$, $\mathcal{S}$, $(-\mathcal{S})$ son subconjuntos de $\mathbb{Z}_{q^2+q+1}$ y disjuntos dos a dos, entonces

$$\begin{aligned} |\mathbb{Z}_{q^2+q+1} \setminus \{0\}| &= q^2 + q \\ &= (q^2 - q) + q + q \\ &= |\mathcal{S} \ominus \mathcal{S}| + |\mathcal{S}| + |-\mathcal{S}|. \end{aligned}$$

En consecuencia, $\mathbb{Z}_{q^2+q+1} \setminus \{0\} = (\mathcal{S} \ominus \mathcal{S}) \cup \mathcal{S} \cup (-\mathcal{S})$.

(S7) Se sigue del hecho que $0 \in \mathcal{S}_0$ y $\mathcal{S}_0 \ominus \mathcal{S}_0 = (\mathcal{S} \ominus \mathcal{S}) \cup \mathcal{S} \cup (-\mathcal{S})$.

□

3.3. Construcción de conjuntos B_2 tipo Ruzsa.

Otra construcción muy conocida de conjuntos de Sidon modulares es la construcción de Ruzsa [38], que aparece en el año 1993, la cual también nos proporciona un conjunto de Sidon maximal en el caso modular. Presentamos en esta sección dicha construcción, primero construimos un conjunto de Sidon en dos dimensiones y luego por medio del isomorfismo del Teorema Chino del Residuo, obtenemos un conjunto de Sidon con $p-1$ en el grupo aditivo $\mathbb{Z}_{p^2-p}$.

En adelante, p es un número primo y $\mathbb{Z}_p$ el campo finito con p elementos.

Teorema 3.3.1. *Para cualquier elemento primitivo θ de $\mathbb{Z}_p$, el conjunto*

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

es un conjunto B_2 con $p-1$ elementos en el grupo abeliano aditivo $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$.

Demostración. Sean $(i, \theta^i), (j, \theta^j), (k, \theta^k), (\ell, \theta^\ell)$ elementos de $\mathcal{R}$ tales que

$$(i, \theta^i) + (j, \theta^j) = (k, \theta^k) + (\ell, \theta^\ell). \quad (3.1)$$

De (3.1) tenemos que

$$i + j \equiv k + \ell \pmod{p-1} \quad (3.2)$$

$$\theta^i + \theta^j = \theta^k + \theta^\ell \text{ en } \mathbb{Z}_p \quad (3.3)$$

Dado que θ es un elemento primitivo de $\mathbb{Z}_p$, entonces de (3.2) se sigue que $\theta^i \theta^j = \theta^k \theta^\ell$.

Luego tenemos el sistema

$$\begin{aligned}\theta^i + \theta^j &= \theta^k + \theta^\ell, \\ \theta^i \theta^j &= \theta^k \theta^\ell,\end{aligned}$$

y usando el mismo argumento que en la demostración del Teorema 3.1.1, obtenemos que $\{\theta^i, \theta^j\} = \{\theta^k, \theta^\ell\}$ y así $\{i, j\} = \{k, l\}$. Por lo tanto,

$$\{(i, \theta^i), (j, \theta^j)\} = \{(k, \theta^k), (\ell, \theta^\ell)\},$$

es decir, $\mathcal{R}$ es un conjunto B_2 en el grupo abeliano aditivo $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$. $\square$

Ahora, consideremos $\varphi : \mathbb{Z}_{p-1} \times \mathbb{Z}_p \rightarrow \mathbb{Z}_{p(p-1)}$ el isomorfismo definido por el Teorema Chino del Residuo, entonces cuando se restringe φ al conjunto $\mathcal{R}$ definido en el Teorema 3.3.1 obtenemos el siguiente sistema de congruencias

$$\begin{aligned}\varphi(i, \theta^i) &\equiv i \pmod{p-1}, \\ \varphi(i, \theta^i) &\equiv \theta^i \pmod{p},\end{aligned}$$

para todo $(i, \theta^i) \in \mathcal{R}$.

Para resolver este sistema, llamemos $x := \varphi(i, \theta^i)$, de esta manera,

$$x \equiv i \pmod{p-1}, \tag{3.4}$$

$$x \equiv \theta^i \pmod{p}, \tag{3.5}$$

De (3.4), existe $t \in \mathbb{Z}$ tal que $x = i + t(p-1)$. Reemplazando x en (3.5) obtenemos

$$\begin{aligned}i + t(p-1) &\equiv \theta^i \pmod{p} \\ t &\equiv i - \theta^i \pmod{p}\end{aligned}$$

lo que implica que existe $s \in \mathbb{Z}$ tal que $t = i - \theta^i + sp$.

Así, $x = ip - \theta^i(p-1) + sp(p-1)$ y dado que $x \in \mathbb{Z}_{p^2-p}$ tenemos $x = ip - \theta^i(p-1)$.

Por lo tanto, la imagen de $\mathcal{R}$ por medio de φ es

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

Teorema 3.3.2. *Sea θ un elemento primitivo del campo finito $\mathbb{Z}_p$. Entonces el conjunto*

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

es un conjunto B_2 con $p-1$ elementos en el grupo aditivo $\mathbb{Z}_{p^2-p}$.

Demostración. Por el Teorema 3.3.1 sabemos que

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

es un conjunto B_2 con $p-1$ elementos en el grupo aditivo $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$. Por el isomorfismo entre $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$ y $\mathbb{Z}_{p(p-1)}$ y el Lema 1.0.7 tenemos que $\mathcal{R}(p, \theta)$ es un conjunto B_2 en el grupo aditivo $\mathbb{Z}_{p^2-p}$, con $p-1$ elementos. $\square$

3.3.1. Propiedades de la construcción de conjuntos B_2 tipo Ruzsa.

Para el conjunto B_2 tipo Ruzsa dado en el Teorema 3.3.2, presentamos algunas propiedades que satisfacen estos conjuntos. Sea p un número primo, consideremos el conjunto de Sidon tipo Ruzsa

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

y los conjuntos

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

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

Proposición 3.3.3. *El conjunto de Sidon tipo Ruzsa $\mathcal{R}(p, \theta)$ definido como antes, satisface las siguientes propiedades:*

- (R1) *Si $r \in \mathcal{R}(p, \theta)$ entonces $r \not\equiv 0 \pmod{p}$.*
- (R2) *Si $r, r' \in \mathcal{R}(p, \theta)$ con $r \neq r'$, entonces $r \not\equiv r' \pmod{p}$.*
- (R3) *Si $r, r' \in \mathcal{R}(p, \theta)$ con $r \neq r'$, entonces $r \not\equiv r' \pmod{p-1}$.*

$$(R4) \quad \mathcal{R}(p, \theta) \ominus \mathcal{R}(p, \theta) = \mathbb{Z}_{p^2-p} \setminus (M_p \cup M_{p-1}).$$

$$(R5) \quad \mathcal{R}(p, \theta) \pmod{p} = [1, p-1].$$

$$(R6) \quad \mathcal{R}(p, \theta) \pmod{p-1} = [0, p-2].$$

Demostración. (R1) Supongamos que existe $r \in \mathcal{R}(p, \theta)$ tal que satisface $r \equiv 0 \pmod{p}$, entonces existen $(i, \theta^i) \in \mathcal{R}$ y t entero, $1 \leq t \leq p-1$, tales que $\varphi(i, \theta^i) = pt$, por el Teorema Chino del Residuo tenemos que $\varphi(t, 0) = pt$, luego $\varphi(i, \theta^i) = \varphi(t, 0)$ y como φ es inyectiva tenemos que $(i, \theta^i) = (t, 0)$ lo que implica $i \equiv t \pmod{p-1}$ y $\theta^i \equiv 0 \pmod{p}$.

Pero como θ es un generador de $\mathbb{F}_p$ entonces no es posible que $\theta^i = 0$ en $\mathbb{F}_p$, para cualquier $1 \leq i \leq p-1$, luego $r \not\equiv 0 \pmod{p}$. Esto implica además que $\mathcal{R}(p, \theta) \cap M_p = \emptyset$.

(R2) Sean $r, r' \in \mathcal{R}(p, \theta)$, entonces existen $(i, \theta^i), (j, \theta^j) \in \mathcal{R}$ tales que $\varphi(i, \theta^i) = r$, $\varphi(j, \theta^j) = r'$, y supongamos que $r \equiv r' \pmod{p}$. Esto es, $r - r' = \varphi(i - j, \theta^i - \theta^j) = pl$, para algún entero ℓ tal que $1 \leq \ell \leq p-1$; por el Teorema Chino del Residuo tenemos $\varphi(\ell, 0) = pl$, luego $\varphi(i - j, \theta^i - \theta^j) = \varphi(\ell, 0)$ y como φ es inyectiva entonces $(i - j, \theta^i - \theta^j) = (\ell, 0)$ lo que implica que $\ell \equiv i - j \pmod{p-1}$ y $\theta^i - \theta^j \equiv 0 \pmod{p}$. Como $r \neq r'$ entonces $i \neq j$, así $\ell \not\equiv 0 \pmod{p-1}$.

Pero como $\theta^i \equiv \theta^j \pmod{p}$, y la función exponencial discreta es inyectiva tenemos que $i \equiv j \pmod{p-1}$, lo cual no puede ser posible. Así, $r \not\equiv r' \pmod{p}$.

En consecuencia, tenemos que $(\mathcal{R}(p, \theta) \ominus \mathcal{R}(p, \theta)) \cap M_p = \emptyset$.

(R3) Como en (R2) tenemos que $\varphi(i, \theta^i) = r$, $\varphi(j, \theta^j) = r'$ y supongamos que $r \equiv r' \pmod{p-1}$. Esto es, $r - r' = \varphi(i - j, \theta^i - \theta^j) = (p-1)k$, para algún entero k , $1 \leq k \leq p$; por el Teorema Chino del Residuo tenemos que $\varphi(0, k) = (p-1)k$, luego $\varphi(i - j, \theta^i - \theta^j) = \varphi(0, k)$ y como φ es inyectiva entonces $(i - j, \theta^i - \theta^j) = (0, k)$ lo que implica que $i \equiv j \pmod{p-1}$ lo cual no puede ser posible porque $r \neq r'$.

En consecuencia, tenemos que $(\mathcal{R}(p, \theta) \ominus \mathcal{R}(p, \theta)) \cap M_{p-1} = \emptyset$.

(R4) Dado que M_p y M_{p-1} son subconjuntos de $\mathbb{Z}_{p^2-p}$ tenemos que $M_p \cap M_{p-1} = \{p(p-1)\}$; además sabemos que $|M_p| = p-1$ y $|M_{p-1}| = p$, luego

$$|M_p \cup M_{p-1}| = |M_p| + |M_{p-1}| - |M_p \cap M_{p-1}| = 2(p-1).$$

De otro lado, como $\mathcal{R}(p, \theta)$ es un conjunto B_2 con $p-1$ elementos en $\mathbb{Z}_{p^2-p}$, sabemos que $|\mathcal{R}(p, \theta) \ominus \mathcal{R}(p, \theta)| = p^2 - 3p + 2 = p^2 - p - 2(p-1)$. Luego como $\mathcal{R}(p, \theta) \ominus \mathcal{R}(p, \theta) \subseteq \mathbb{Z}_{p^2-p}$, por (R2) y (R3) tenemos que $(\mathcal{R}(p, \theta) \ominus \mathcal{R}(p, \theta)) \cap M_p = \emptyset$ y además $(\mathcal{R}(p, \theta) \ominus \mathcal{R}(p, \theta)) \cap M_{p-1} = \emptyset$ entonces

$$(\mathcal{R}(p, \theta) \ominus \mathcal{R}(p, \theta)) \cap (M_p \cup M_{p-1}) = \emptyset,$$

por lo tanto $\mathcal{R}(p, \theta) \ominus \mathcal{R}(p, \theta) = \mathbb{Z}_{p^2-p} \setminus (M_p \cup M_{p-1})$.

(R5) $\mathcal{R}(p, \theta) \pmod{p} = [1, p-1]$.

En efecto, notemos que

$$\begin{aligned} \mathcal{R}(p, \theta) \pmod{p} &= \{-\theta^i(p-1) \pmod{p} : 1 \leq i \leq p-1\} \\ &= \{\theta^i \pmod{p} : 1 \leq i \leq p-1\} \\ &= [1, p-1]. \end{aligned}$$

(R6) $\mathcal{R}(p, \theta) \pmod{p-1} = [0, p-2]$.

Como en (R1) notemos que

$$\begin{aligned} \mathcal{R}(p, \theta) \pmod{p-1} &= \{ip \pmod{p-1} : 1 \leq i \leq p-1\} \\ &= \{i : 1 \leq i \leq p-1\} \\ &= [0, p-2]. \end{aligned}$$

□

Capítulo 4

Construcciones de conjuntos de Sidon en dos dimensiones

El estudio de conjuntos de Sidon aparece originalmente en el grupo aditivo de los enteros, pero claramente es posible definirlos en otros grupos, el caso más natural de conjuntos de Sidon en otros grupos es cuando se considera el conjunto $\mathbb{Z} \times \mathbb{Z}$ o en general en el producto directo de dos grupos. En este capítulo presentamos algunas construcciones de conjuntos de Sidon en dos dimensiones, principalmente, en el caso del producto de los grupos provenientes de un campo, analizamos algunas propiedades que satisfacen estos conjuntos cuando el campo es $\mathbb{Z}_p$, con p primo. Como caso particular de conjuntos de Sidon en dos dimensiones, presentamos nuevas construcciones de secuencias sonar, que provienen de analizar las propiedades que satisfacen los conjuntos de Sidon modulares tipo Bose y Ruzsa en una dimensión.

4.1. Algunas construcciones generales.

Para obtener conjuntos de Sidon en dos dimensiones, la primera idea que llega a la mente, es pensar si el producto cartesiano $A \times B$ de dos conjuntos de Sidon A, B enteros de nuevo es un conjunto de Sidon; sin embargo, esto

es falso, puesto que para todo $a, c \in A$ y $b, d \in B$ la igualdad

$$(a, b) + (c, d) = (a, d) + (c, b),$$

prohibe tal construcción [42].

Pero de forma natural, si se puede construir un conjunto de Sidon en dimensión dos a partir de un conjunto de Sidon en dimensión uno conocido, de la siguiente manera:

Proposición 4.1.1. *Sea $A \subseteq \mathbb{Z} \times \mathbb{Z}$, llamemos A_1 al conjunto de las primeras componentes de A y A_2 al conjunto de las segundas componentes de A . Si A_1 (o A_2) es un conjunto de Sidon y si todas las primeras (o segundas) componentes de A son distintas entonces A es un conjunto de Sidon en dimensión dos.*

En la construcción anterior de conjuntos de Sidon es posible notar que las segundas componentes pueden ser independientes de las primeras o recíprocamente.

C. A. Trujillo [42] en su tesis doctoral, logra obtener una manera de construir conjuntos de Sidon en dimensión dos a partir de un conjuntos de Sidon en dimensión uno; en su construcción sí hay una relación más estrecha entre las dos componentes de los elementos del conjunto de Sidon en $\mathbb{Z} \times \mathbb{Z}$. Para ello se considera $A \subseteq \mathbb{Z}$ un conjunto de Sidon y b un entero positivo llamado base tal que $b^2 - 1 \geq \max\{a : a \in A\}$, además se define el siguiente conjunto:

$$[A]_b := \{[a]_b : a \in A\},$$

donde $[a]_b = (\lfloor \frac{a}{b} \rfloor, a(\text{mód } b)) \in \mathbb{Z} \times \mathbb{Z}$.

Con estas observaciones Trujillo obtiene el siguiente resultado:

Teorema 4.1.2. *Si $A \subseteq [0, b^2 - 1]$ es un conjunto de Sidon en dimensión uno, entonces $[A]_b = \{(\lfloor \frac{a}{b} \rfloor, a(\text{mód } b)) : a \in A\}$ es un conjunto de Sidon en dimensión dos y es tal que*

$$|[A]_b| = |A| \quad y \quad [A]_b \subseteq [0, b - 1] \times [0, b - 1].$$

Demostración. Sean $[a_i]_b, [a_j]_b, [a_k]_b, [a_l]_b$ en $[A]_b$ tales que

$$[a_i]_b + [a_j]_b = [a_k]_b + [a_l]_b.$$

Equivalentemente,

$$\begin{aligned} \left(\left\lfloor \frac{a_i}{b} \right\rfloor, a_i(\text{mód } b) \right) + \left(\left\lfloor \frac{a_j}{b} \right\rfloor, a_j(\text{mód } b) \right) &= \left(\left\lfloor \frac{a_k}{b} \right\rfloor, a_k(\text{mód } b) \right) + \left(\left\lfloor \frac{a_l}{b} \right\rfloor, a_l(\text{mód } b) \right), \\ \left(\left\lfloor \frac{a_i}{b} \right\rfloor + \left\lfloor \frac{a_j}{b} \right\rfloor, a_i(\text{mód } b) + a_j(\text{mód } b) \right) &= \left(\left\lfloor \frac{a_k}{b} \right\rfloor + \left\lfloor \frac{a_l}{b} \right\rfloor, a_k(\text{mód } b) + a_l(\text{mód } b) \right). \end{aligned}$$

Esto implica que

$$\left\lfloor \frac{a_i}{b} \right\rfloor + \left\lfloor \frac{a_j}{b} \right\rfloor = \left\lfloor \frac{a_k}{b} \right\rfloor + \left\lfloor \frac{a_l}{b} \right\rfloor \quad y \quad (4.1)$$

$$a_i(\text{mód } b) + a_j(\text{mód } b) = a_k(\text{mód } b) + a_l(\text{mód } b). \quad (4.2)$$

Si multiplicamos (4.1) por b y sumamos con (4.2) obtenemos

$$a_i + a_j = a_k + a_l.$$

Como a_i, a_j, a_k, a_l son elementos de A y éste es un conjunto de Sidon, entonces

$$\{a_i, a_j\} = \{a_k, a_l\}.$$

En consecuencia,

$$\{[a_i]_b, [a_j]_b\} = \{[a_k]_b, [a_l]_b\},$$

por lo tanto $[A]_b$ es un conjunto de Sidon contenido en $[0, b-1] \times [0, b-1]$ y $|[A]_b| = |A|$ pues para cualquier par de elementos en $[A]_b$ tales que

$$\left(\left\lfloor \frac{a_i}{b} \right\rfloor, a_i(\text{mód } b) \right) = \left(\left\lfloor \frac{a_j}{b} \right\rfloor, a_j(\text{mód } b) \right)$$

entonces

$$\left\lfloor \frac{a_i}{b} \right\rfloor = \left\lfloor \frac{a_j}{b} \right\rfloor \quad y \quad a_i(\text{mód } b) = a_j(\text{mód } b),$$

de esto se sigue que $a_i = a_j$. □

Ahora presentamos algunas construcciones de conjuntos de Sidon en dimensión dos en algunos grupos particulares, aunque primero vamos a presentar las construcciones en ciertos grupos producto que provienen de un campo F .

Dado cualquier campo F con las operaciones de adición y multiplicación $(F, +, \cdot)$ tenemos dos grupos $(F, +)$ y $(F^*, \cdot)$, donde $F^* = F \setminus \{0\}$, donde 0 representa el elemento identidad de F con la operación $+$.

Con éstos dos grupos podemos formar los siguientes grupos producto:

1. $(F, +) \times (F, +) = (F \times F, +)$,
2. $(F, +) \times (F^*, \cdot) \cong (F^*, \cdot) \times (F, +)$,
3. $(F^*, \cdot) \times (F^*, \cdot) = (F^* \times F^*, \cdot)$.

Observación 4.1.3. En el caso del grupo $(F, +) \times (F^*, \cdot)$ denotamos la operación por $\star$, es decir, $(F, +) \times (F^*, \cdot) = (F \times F^*, \star)$.

En estos grupos es posible construir algunos conjuntos de Sidon, como mencionamos a continuación.

1. $\mathcal{C} = \{(x, x^2) : x \in F\} \subset (F \times F, +)$,
2. $\mathcal{I} = \{(x, x) : x \in F^*\} \subset (F \times F^*, \star)$,
3. $\mathcal{I}_a = \{(x - a, x) : x \in F^*, x \neq a, a \in F^*\} \subset (F^* \times F^*, \cdot)$.

La verificación de que cada uno de los anteriores conjuntos es un conjunto B_2 en su grupo respectivo no es difícil, presentamos a continuación la prueba de uno de ellos, pues las demás pruebas son similares.

Teorema 4.1.4. *Dado el campo $(F, +, \cdot)$, con característica diferente de 2, entonces los siguientes son conjuntos B_2 en sus grupos respectivos:*

$$\mathcal{C} = \{(x, x^2) : x \in F\} \subseteq (F \times F, +); \quad (4.3)$$

$$\mathcal{I} = \{(x, x) : x \in F^*\} \subseteq (F, +) \times (F^*, \cdot) = (F \times F^*, \star); \quad (4.4)$$

$$\mathcal{I}_a = \{(x - a, x) : x \in F^*, x \neq a \neq 0\} \subseteq (F^* \times F^*, \cdot), \quad (4.5)$$

donde $a \in F^*$.

Demostración. Demostramos únicamente que el conjunto $\mathcal{C}$ es un conjunto B_2 en el grupo $(F \times F, +)$, la prueba de los otros casos se hace de manera análoga.

Sean $(a, a^2), (b, b^2), (c, c^2), (d, d^2)$ en $\mathcal{C}$ tales que

$$(a, a^2) + (b, b^2) = (c, c^2) + (d, d^2), \quad (4.6)$$

lo que implica

$$a + b = c + d, \quad (4.7)$$

$$a^2 + b^2 = c^2 + d^2. \quad (4.8)$$

De (4.7) tenemos que $(a + b)^2 = (c + d)^2$, luego usando la igualdad (4.8) y dado que la característica de F es diferente de 2, obtenemos que $ab = cd$. Así, podemos considerar el siguiente sistema de ecuaciones

$$\begin{aligned} a + b &= c + d, \\ ab &= cd. \end{aligned}$$

Si tomamos el polinomio $P(x) = x^2 + Sx + P \in F[x]$, donde $S = a + b = c + d$ y $P = ab = cd$, podemos notar que éste se factoriza como

$$x^2 + Sx + P = x^2 + (a + b)x + ab = (x + a)(x + b),$$

o también como

$$x^2 + Sx + P = x^2 + (c + d)x + cd = (x + c)(x + d),$$

y dado que el número de ceros de un polinomio, con coeficientes en un campo, no puede exceder a su grado entonces $\{a, b\} = \{c, d\}$, lo que implica que

$$\{(a, a^2), (b, b^2)\} = \{(c, c^2), (d, d^2)\}.$$

□

Además, el conjunto $\mathcal{I}$ se puede extender o generalizar ya que la propiedad de conjunto de Sidon se preserva bajo traslaciones y multiplicación por unidad.

Corolario 4.1.5. *Sean $(F, +, \cdot)$ un campo, $u_1, u_2 \in F^*$ y $h_1, h_2 \in F$, entonces el conjunto*

$$\mathcal{I}_{ext} = \{(u_1x + h_1, u_2x + h_2) : x \in F^*\}$$

es un conjunto de Sidon en $(F, +) \times (F^, \cdot)$.*

Por otro lado, como la propiedad de conjunto de Sidon se preserva bajo isomorfismos, en el caso cuando consideramos el campo finito $F = \mathbb{F}_q$, para q potencia de un primo impar, y dado que $(\mathbb{F}_q^*, \cdot) \cong (\mathbb{Z}_{q-1}, +)$, los conjuntos $\mathcal{C}$, $\mathcal{I}$ y $\mathcal{I}_a$, los podemos ver como conjuntos Sidon en los siguientes grupos, respectivamente.

1. $\mathcal{C} = \{(x, x^2) : x \in \mathbb{F}_q\} \subset (\mathbb{F}_q \times \mathbb{F}_q, +)$,
2. $\mathcal{I} = \{(x, \log_\theta x) : x \in \mathbb{F}_q^*\} \subset (\mathbb{F}_q \times \mathbb{Z}_{q-1}, +)$, isomorfo al conjunto
 $\mathcal{I}' = \{(k, \theta^k) : k \in \mathbb{Z}_{q-1}^*\} \subset (\mathbb{Z}_{q-1} \times \mathbb{F}_q, +)$,
3. $\mathcal{I}_a = \{(\log_\theta(\theta^k - a), k) : k \in \mathbb{Z}_{q-1}\} \subset (\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}, +)$.

Aquí, θ es un elemento primitivo del campo finito $\mathbb{F}_q$.

Mencionamos a continuación algunas propiedades que satisfacen los conjuntos $\mathcal{C}$, $\mathcal{I}$ y $\mathcal{I}_a$ en el caso cuando consideramos el campo finito $\mathbb{F}_p = \mathbb{Z}_p$, con p un número primo. Aunque las propiedades también son válidas sobre el campo $\mathbb{F}_q$, con q potencia prima. Denotamos al conjunto de los residuos cuadráticos módulo p , incluido el cero, por $\mathcal{RC}(p)$.

Observación 4.1.6. Antes de describir las propiedades que satisfacen los conjuntos mencionados, vamos a definir el concepto de base, ya que ciertos conjuntos satisfacen esta propiedad.

Definición 4.1.7. Dado un subconjunto A de un grupo $(G, +)$, se dice que A es una base de orden k , si todo elemento $x \in G$ se puede escribir de la forma

$$x = a_1 + \cdots + a_k,$$

para algunos $a_1, \dots, a_k \in A$, no necesariamente distintos.

4.1.1. Propiedades del conjunto $\mathcal{C}$.

El conjunto $\mathcal{C} = \{(x, x^2) : x \in \mathbb{Z}_p\} \subseteq (\mathbb{Z}_p, +) \times (\mathbb{Z}_p, +)$ satisface las siguientes propiedades.

$$(a.) \mathcal{C} \ominus \mathcal{C} = \mathbb{Z}_p \times \mathbb{Z}_p \setminus \{(0, x) : x \in \mathbb{Z}_p\}.$$

En efecto, por definición tenemos que

$$\begin{aligned} \mathcal{C} \ominus \mathcal{C} &= \{(x, x^2) - (y, y^2) : x, y \in \mathbb{Z}_p, (x, x^2) \neq (y, y^2)\} \\ &= \{(x - y, x^2 - y^2) : x, y \in \mathbb{Z}_p, (x, x^2) \neq (y, y^2)\}. \end{aligned}$$

Como $(x, x^2) \neq (y, y^2)$ entonces $x \neq y$ o $x^2 \neq y^2$, pero esto es equivalente a decir que $x \neq y$, puesto que si $x^2 \neq y^2$ implica que $x^2 - y^2 \neq 0$, equivalentemente $(x - y)(x + y) \neq 0$ y como $\mathbb{Z}_p$ es un dominio de integridad entonces $x \neq y$ y $x \neq -y$. Luego los elementos que no pertenecen a este conjunto, son de la forma $(0, z)$, donde $z \in \mathbb{F}_q$.

Para ver que son todos, contemos: $|\mathbb{Z}_p \times \mathbb{Z}_p| = p^2$, $|\mathcal{C}| = p$, además $|\{(0, z) : z \in \mathbb{Z}_p\}| = p$ y como $\mathcal{C}$ es conjunto de Sidon entonces

$$\begin{aligned} |\mathcal{C} \ominus \mathcal{C}| &= 2 \binom{p}{2} \\ &= p(p - 1) \\ &= p^2 - p, \end{aligned}$$

de esto se sigue el resultado.

$$(b.) \mathcal{C} + \mathcal{C} = \{(u, v) \in \mathbb{Z}_p \times \mathbb{Z}_p : 2v - u^2 \in \mathcal{RC}(p)\}.$$

En efecto, por definición tenemos que

$$\mathcal{C} + \mathcal{C} = \{(x + y, x^2 + y^2) : x, y \in \mathbb{Z}_p\},$$

pero como $\mathcal{C} + \mathcal{C} \subseteq \mathbb{Z}_p \times \mathbb{Z}_p$ entonces $(x + y, x^2 + y^2) = (u, v)$, para algún u y algún v en $\mathbb{Z}_p$. Luego,

$$x + y = u \tag{4.9}$$

$$x^2 + y^2 = v. \tag{4.10}$$

Si despejamos y en (4.9) y lo reemplazamos en (4.10) obtenemos la siguiente ecuación

$$2x^2 - 2ux + u^2 - v = 0, \quad (4.11)$$

la cual tiene solución en $\mathbb{Z}_p$ si y sólo si el discriminante de la ecuación cuadrática $(-2u)^2 - 4(2)(u^2 - v)$ es un cuadrado. Pero esto es equivalente a determinar la solución de la ecuación cuadrática (4.11) la cual esta dada por

$$\begin{aligned} x &= \frac{2u \pm \sqrt{4u^2 - 8(u^2 - v)}}{4} \\ &= \frac{u \pm \sqrt{2v - u^2}}{2} \end{aligned}$$

y existe si y sólo si $2v - u^2$ es un cuadrado en $\mathbb{Z}_p$. De esto se sigue el resultado.

(c.) $\mathcal{C} \cup \{(0, z) : z \in \mathbb{Z}_p\}$ es base de orden 2 para $(\mathbb{Z}_p \times \mathbb{Z}_p, +)$.

En efecto, sea $H = \{(0, z) : z \in \mathbb{Z}_p\}$ y hagamos $B = \mathcal{C} \cup H$. Podemos notar que H es un subgrupo de $\mathbb{Z}_p \times \mathbb{Z}_p$. Además,

$$B + B = (\mathcal{C} + \mathcal{C}) \cup (\mathcal{C} + H) \cup (H + H),$$

pero $\mathcal{C} + H \subseteq B + B$, y $|\mathcal{C} + H| = p^2 = |\mathbb{Z}_p \times \mathbb{Z}_p|$, porque $\mathcal{C}, H \subseteq \mathbb{Z}_p \times \mathbb{Z}_p$ y todos los elementos del conjunto $\mathcal{C} + H$ son distintos, pues si existen dos iguales, digamos $c_1 + h_1 = c_2 + h_2$ implica que $c_1 - c_2 = h_2 - h_1 \in H$ lo cual es una contradicción por la propiedad (a.).

Luego como $B + B \subseteq \mathbb{Z}_p \times \mathbb{Z}_p$ y $|B + B| \geq p^2$ se sigue que

$$B + B = \mathbb{Z}_p \times \mathbb{Z}_p.$$

4.1.2. Propiedades del conjunto $\mathcal{I}$.

El conjunto $\mathcal{I} = \{(x, x) : x \in \mathbb{Z}_p^*\} \subseteq (\mathbb{Z}_p, +) \times (\mathbb{Z}_p^*, \cdot)$ satisface las siguientes propiedades. Denotamos por $\mathcal{I} \ominus \mathcal{I}$ al conjunto

$$\{(x, x) * (y, y)^{-1} : x, y \in \mathbb{Z}_p^*, (x, x) \neq (y, y)\}.$$

(a.) $\mathcal{I} \ominus \mathcal{I} = \mathbb{Z}_p \times \mathbb{Z}_p^* \setminus (A_1 \cup A_2)$, donde $A_1 = \{(0, z) : z \in \mathbb{Z}_p^*\}$ y $A_2 = \{(z, 1) : z \in \mathbb{Z}_p^*\}$.

En efecto, por definición

$$\mathcal{I} \ominus \mathcal{I} = \{(x, x) * (y, y)^{-1} : x, y \in \mathbb{Z}_p^*, (x, x) \neq (y, y)\},$$

pero $(x, x) * (y, y)^{-1} = (x - y, xy^{-1})$ y además como $(x, x) \neq (y, y)$ esto implica que $x \neq y$, luego los elementos del conjunto diferencia nunca tienen en la primera componente al elemento 0, así $(x - y, xy^{-1}) \neq (0, z)$, con $z \in \mathbb{Z}_p^*$. Además, como $x \neq y$ y $y \neq 0$ entonces $xy^{-1} \neq 1$ y así los elementos de la forma $(z, 1)$, con $z \in \mathbb{Z}_p^*$ tampoco pertenecen al conjunto.

De otro lado, tenemos que $|\mathbb{Z}_p \times \mathbb{Z}_p^*| = p(p-1)$, $|A_1| = p-1$, $|A_2| = p-1$ y como $A_1 \cap A_2 = \emptyset$ entonces $|A_1 \cup A_2| = 2(p-1)$, además $|\mathcal{I}| = p-1$ entonces

$$\begin{aligned} |\mathcal{I} \ominus \mathcal{I}| &= 2 \binom{p-1}{2} \\ &= (p-1)(p-2) \\ &= p^2 - 3p + 2 \\ &= p(p-1) - 2(p-1), \end{aligned}$$

de esto se sigue el resultado.

(b.) $\mathcal{I} * \mathcal{I} = \{(u, v) \in \mathbb{Z}_p \times \mathbb{Z}_p^* : u^2 - 4v \in \mathcal{RC}(p)\}$.

En efecto, sea $\mathcal{I} * \mathcal{I} = \{(x + y, xy) : x, y \in \mathbb{Z}_p^*\}$ y como $\mathcal{I} * \mathcal{I} \subseteq \mathbb{Z}_p \times \mathbb{Z}_p^*$ entonces existen $u \in \mathbb{Z}_p$, $v \in \mathbb{Z}_p^*$ tales que $(x + y, xy) = (u, v)$. Luego,

$$x + y = u, \tag{4.12}$$

$$xy = v. \tag{4.13}$$

Si despejamos y en (4.12) y lo reemplazamos en (4.13) obtenemos la ecuación

$$x^2 - ux + v = 0, \tag{4.14}$$

la cual tiene solución en $\mathbb{Z}_p$ si y sólo si el discriminante de la ecuación cuadrática $u^2 - 4v$ es un cuadrado. De ésto se sigue el resultado.

Como en (a.) consideremos el conjunto $A_1 = \{(0, z) : z \in \mathbb{Z}_p^*\}$, notemos que A_1 es un subgrupo de $(\mathbb{Z}_p, +) \times (\mathbb{Z}_p^*, \cdot) = (\mathbb{Z}_p \times \mathbb{Z}_p^*, *)$.

(c.) $(\mathcal{I} * A_1) \cap A_1 = \emptyset$, $|\mathcal{I} * A_1| = (p-1)^2$ y en consecuencia

$$(\mathcal{I} * A_1) = \mathbb{Z}_p \times \mathbb{Z}_p^* \setminus A_1.$$

Supongamos que existe $(u, v) \in (\mathcal{I} * A_1) \cap A_1$ entonces existen $x, y, z \in \mathbb{Z}_p^*$

$$\begin{aligned} (u, v) &= (x, x) * (0, y) \\ &= (0, z), \end{aligned}$$

esto implica que $x = 0$, $xy = z$; lo cual no puede ser posible porque $x \neq 0$. Así, $(\mathcal{I} * A_1) \cap A_1 = \emptyset$.

Ahora, supongamos que existen dos elementos iguales en $\mathcal{I} * A_1$, digamos $i_1 * a_1 = i_2 * a_2$, donde $i_1, i_2 \in \mathcal{I}$ y $a_1, a_2 \in A_1$, de esta igualdad se sigue que $i_1 * i_2^{-1} = a_2 * a_1^{-1} \in A_1$, lo cual no puede ser posible porque $\mathcal{I} \ominus \mathcal{I} \cap A_1 = \emptyset$ por la propiedad (a.), luego $|\mathcal{I} * A_1| = |\mathcal{I}| |A_1| = (p-1)^2$.

(d.) $(\mathcal{I} * A_1) \cap \mathcal{I} = \mathcal{I}$.

Dado $(x, x) \in \mathcal{I}$ entonces

$$(x, x) = (x + 0, x \cdot 1) = (x, x) * (0, 1) \in \mathcal{I} * A_1,$$

luego, $\mathcal{I} \subseteq \mathcal{I} * A_1$ y así se obtiene el resultado.

(e.) $(\mathcal{I} * \mathcal{I}) \cap A_1 = B$, donde

$$B = \begin{cases} \{(0, z) \in \mathbb{Z}_p \times \mathbb{Z}_p^* : z \notin \mathcal{RC}(p)\} & \text{si } p \equiv 3 \pmod{4} \\ \{(0, z) \in \mathbb{Z}_p \times \mathbb{Z}_p^* : z \in \mathcal{RC}(p)\} & \text{si } p \equiv 1 \pmod{4} \end{cases}$$

En efecto, $(0, z) \in \mathcal{I} * \mathcal{I}$ si y sólo si $-4z \in \mathcal{RC}(p)$, esto implica que $-z \in \mathcal{RC}(p)$, por el símbolo de Legendre tenemos

$$\left(\frac{-1}{p}\right) = -1 \text{ y } \left(\frac{z}{p}\right) = -1$$

o

$$\left(\frac{-1}{p}\right) = 1 \text{ y } \left(\frac{z}{p}\right) = 1,$$

pero

$$\left(\frac{-1}{p}\right) = \begin{cases} -1 & \text{si } p \equiv 3(\text{mód } 4) \\ 1 & \text{si } p \equiv 1(\text{mód } 4) \end{cases}$$

Luego si $p \equiv 3(\text{mód } 4)$ entonces $\left(\frac{-1}{p}\right) = -1$ lo que implica que $z \notin \mathcal{RC}(p)$, y si $p \equiv 1(\text{mód } 4)$ entonces $\left(\frac{-1}{p}\right) = 1$ lo que implica que $z \in \mathcal{RC}(p)$.

En este caso como $z \neq 0$ entonces $|B| = \frac{p-1}{2}$.

(f.) $(\mathcal{I} * A_1) \cap (\mathcal{I} * \mathcal{I}) = (\mathcal{I} * \mathcal{I}) \setminus B$, donde B es el conjunto del item anterior.

Como $\mathcal{I} * A_1 = \mathbb{Z}_p \times \mathbb{Z}_p^* \setminus A_1$ entonces

$$\begin{aligned} (\mathcal{I} * A_1) \cap (\mathcal{I} * \mathcal{I}) &= (\mathbb{Z}_p \times \mathbb{Z}_p^* \setminus A_1) \cap (\mathcal{I} * \mathcal{I}) \\ &= (\mathbb{Z}_p \times \mathbb{Z}_p^* \cap (\mathcal{I} * \mathcal{I})) \setminus (A_1 \cap (\mathcal{I} * \mathcal{I})) \\ &= (\mathcal{I} * \mathcal{I}) \setminus B. \end{aligned}$$

(g.) $\mathcal{I} \cup A_1$ es base de orden 2 para $(\mathbb{Z}_p, +) \times (\mathbb{Z}_p^*, \cdot)$.

En efecto, sea $R = \mathcal{I} \cup A_1$ entonces

$$R * R = (\mathcal{I} * \mathcal{I}) \cup (\mathcal{I} * A_1) \cup A_1,$$

luego

$$\begin{aligned} |R * R| &= |(\mathcal{I} * \mathcal{I}) \cup (\mathcal{I} * A_1) \cup A_1| \\ &= |(\mathcal{I} * \mathcal{I})| + |(\mathcal{I} * A_1)| + |A_1| - |(\mathcal{I} * \mathcal{I}) \cap (\mathcal{I} * A_1)| \\ &\quad - |(\mathcal{I} * \mathcal{I}) \cap A_1| - |(\mathcal{I} * A_1) \cap A_1| + |(\mathcal{I} * \mathcal{I}) \cap (\mathcal{I} * A_1) \cap A_1| \\ &= \frac{p(p-1)}{2} + (p-1)^2 + (p-1) \\ &\quad - \left[\frac{p(p-1)}{2} - \frac{p-1}{2} \right] - \frac{p-1}{2} - 0 + 0 \\ &= p^2 - p. \end{aligned}$$

De esta última igualdad se sigue el resultado.

Como en (a.) consideremos el conjunto $A_2 = \{(z, 1) : z \in \mathbb{Z}_p^*\}$.

(h.) $(\mathcal{I} * A_2) \cap \mathcal{I} = \emptyset$, $|\mathcal{I} * A_2| = (p-1)^2$ y en consecuencia $\mathcal{I} * A_2 = \mathbb{Z}_p \times \mathbb{Z}_p^* \setminus \mathcal{I}$.

En efecto, supongamos que existe $(u, v) \in (\mathcal{I} * A_2) \cap \mathcal{I}$ entonces existen $x, y, z \in \mathbb{Z}_p^*$ tales que $(u, v) = (x, x) * (z, 1) = (y, y)$, esto implica que

$$u = x + z = y$$

$$v = x = y$$

luego $z = 0$ lo cual es una contradicción. Así, $(\mathcal{I} * A_2) \cap \mathcal{I} = \emptyset$.

Ahora, supongamos que existen dos elementos en $\mathcal{I} * A_2$ iguales, digamos $i_1 * a_1 = i_2 * a_2$, donde $i_1, i_2 \in \mathcal{I}$, $a_1, a_2 \in A_2$. De esta igualdad se sigue que $i_1 * i_2^{-1} = a_2 * a_1^{-1} \in (A_2 \cup \{(0, 1)\})$, lo cual no puede ser posible porque $\mathcal{I} \ominus \mathcal{I} \cap (A_2 \cup \{(0, 1)\}) = \emptyset$ por la propiedad (a.), luego $|\mathcal{I} * A_2| = |\mathcal{I}| |A_2| = (p-1)^2$.

(i.) $(\mathcal{I} * A_2) \cap A_2 = A_2 \setminus \{(1, 1)\}$.

en efecto, dado $(z, 1) \in A_2$ entonces

$$(z, 1) = (1, 1) * (z-1, 1) \in \mathcal{I} * A_2,$$

cuando $z \neq 1$, pues si $z = 1$ entonces $(z-1, 1) = (0, 1) \notin A_2$. Por lo tanto, $A_2 \setminus \{(1, 1)\} \subseteq \mathcal{I} * A_2$, luego

$$A_2 \setminus \{(1, 1)\} = (A_2 \setminus \{(1, 1)\}) \cap A_2 \subseteq (\mathcal{I} * A_2) \cap A_2 \subseteq A_2.$$

Además, $(1, 1) \notin \mathcal{I} * A_2$, pues si pasa lo contrario se tiene que $(1, 1) = (x + z, x \cdot 1)$, para algún $x \in \mathbb{Z}_p^*$ y algún $z \in \mathbb{Z}_p^*$, esto implica que $x = 1$ y $z = 0$, lo cual es una contradicción. De esta manera, se sigue el resultado.

(j.) $(\mathcal{I} * \mathcal{I}) \cap A_2 = \{(z, 1) \in \mathbb{Z}_p \times \mathbb{Z}_p^*; z \neq 0, z = y + y^{-1}, \exists y \in \mathbb{Z}_p^*\}$.

En efecto, un elemento de $(\mathcal{I} * \mathcal{I}) \cap A_2$ satisface

$$(x + y, xy) = (z, 1),$$

entonces $x + y = z$ y $xy = 1$. Como $x \neq 0$ entonces $x = y^{-1}$. Y dado que $(\mathcal{I} * \mathcal{I}) \cap A_2 \subseteq A_2$ entonces se obtiene el resultado.

4.1.3. Propiedades del conjunto $\mathcal{I}_a$.

El conjunto $\mathcal{I}_a = \{(x - a, x) : x \neq a, x \in \mathbb{Z}_p^*\} \subseteq (\mathbb{Z}_p^*, \cdot) \times (\mathbb{Z}_p^*, \cdot)$ satisface las siguientes propiedades. Denotamos por $\mathcal{I}_a \ominus \mathcal{I}_a$ al conjunto

$$\{(x - a, x)(y - a, y)^{-1} : x, y \in \mathbb{Z}_p, x \neq a \neq y, (x - a, x) \neq (y - a, y)\}.$$

$$(a.) \mathcal{I}_a \ominus \mathcal{I}_a = \mathbb{Z}_p^* \times \mathbb{Z}_p^* \setminus (A \cup B \cup C), \text{ donde } A = \{(1, z) : z \in \mathbb{Z}_p^*\}, \\ B = \{(z, 1) : z \in \mathbb{Z}_p^*\} \text{ y } C = \{(z, z) : z \in \mathbb{Z}_p^*\}.$$

En efecto, tenemos por definición que

$$\mathcal{I}_a \ominus \mathcal{I}_a = \{(x - a, x)(y - a, y)^{-1} : x, y \in \mathbb{Z}_p, x \neq a \neq y, (x - a, x) \neq (y - a, y)\}.$$

Como $(x - a, x)(y - a, y)^{-1} = ((x - a)(y - a)^{-1}, xy^{-1})$, $x \neq y$ y $y \neq 0$ entonces $xy^{-1} \neq 1$, además como $x - a \neq y - a$ y $y - a \neq 0$ entonces $(x - a)(y - a)^{-1} \neq 1$, así los elementos de la forma $(1, z)$ y $(z, 1)$, con $z \in \mathbb{Z}_p^*$, no pertenecen a $\mathcal{I}_a \ominus \mathcal{I}_a$.

Otro tipo de elementos que no pertenece al conjunto dado, son aquellos de la forma (z, z) , con $z \in \mathbb{Z}_p^*$. Pues si suponemos que

$$((x - a)(y - a)^{-1}, xy^{-1}) = (z, z),$$

para algún $z \in \mathbb{Z}_p$, entonces

$$(x - a)(y - a)^{-1} = z \quad y \quad (4.15)$$

$$xy^{-1} = z. \quad (4.16)$$

De (4.15) se sigue que

$$x - a = yz - az, \quad (4.17)$$

y de (4.16) se sigue que

$$x = yz, \quad (4.18)$$

luego reemplazando (4.18) en (4.17) obtenemos que $z = 1$, lo cual es una contradicción pues $x \neq y$ y así $xy^{-1} \neq 1$.

Además, $|\mathbb{Z}_p^* \times \mathbb{Z}_p^*| = (p - 1)^2$, $|A| = |B| = |C| = p - 1$ y como $A \cap B = A \cap C = B \cap C = A \cap B \cap C = \{(1, 1)\}$, entonces

$|A \cup B \cup C| = 3(p-1) - 2$. Y como $|\mathcal{I}_a| = p-2$ entonces

$$\begin{aligned} |\mathcal{I}_a \ominus \mathcal{I}_a| &= 2 \binom{p-2}{2} \\ &= (p-2)(p-3) \\ &= p^2 - 5p + 6 \\ &= p^2 - 2p + 1 - 3p + 3 + 2 \\ &= (p-1)^2 - (3(p-1) - 2), \end{aligned}$$

de esto se sigue el resultado.

(b.) $\mathcal{I}_a \cdot \mathcal{I}_a = \{(u, v) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^* : [a + a^{-1}(v-u)]^2 - 4v \in \mathcal{RC}(p)\}$. En efecto, sea $\mathcal{I}_a \cdot \mathcal{I} = \{((x-a)(y-a), xy) : x, y \in \mathbb{Z}_p^*, x \neq a \neq y, a \neq 0\}$ y como $\mathcal{I} \cdot \mathcal{I} \subseteq \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ entonces existen $u \in \mathbb{Z}_p^*, v \in \mathbb{Z}_p^*$ tales que $((x-a)(y-a), xy) = (u, v)$. Luego,

$$(x-a)(y-a) = u, \quad (4.19)$$

$$xy = v. \quad (4.20)$$

Como $x \in \mathbb{Z}_p^*$, podemos despejar y de (4.20) y luego reemplazarlo en (4.19), de esta manera obtenemos la ecuación

$$x^2 - (a + a^{-1}(v-u))x + v = 0, \quad (4.21)$$

la cual tiene solución en $\mathbb{Z}_p$ si y sólo si el discriminante de la ecuación cuadrática $(a + a^{-1}(v-u))^2 - 4v$ es un cuadrado. De esto se sigue el resultado.

Algunas propiedades que verificamos computacionalmente, de los conjuntos descritos arriba, son las siguientes:

- Si $p \geq 5$ es un número primo, entonces $\mathcal{C}$ es base de orden 3 para el grupo $(\mathbb{Z}_p \times \mathbb{Z}_p, +)$.
- Si $p \geq 11$ es un número primo, entonces $\mathcal{I}$ es base de orden 3 para el grupo $(\mathbb{Z}_p, +) \times (\mathbb{Z}_p^*, \cdot)$.

- Si $p \geq 13$ es un número primo, entonces $\mathcal{I}_a$ es base de orden 3 para el grupo $(\mathbb{Z}_p^* \times \mathbb{Z}_p^*, \cdot)$.

Cabe aclarar que la verificación de éstos resultados se realizó para $p < 10^4$, en cada caso.

4.1.4. Propiedades del conjunto $\mathcal{I}_{ext}$.

Sean $\mathcal{I}_{ext} = \{(u_1x + h_1, u_2x + h_2) : x \in \mathbb{Z}_p^*\} \subseteq (\mathbb{Z}_p, +) \times (\mathbb{Z}_p^*, \cdot)$, $\mathcal{I} = \{(x, x) : x \in \mathbb{Z}_p^*\} \subseteq (\mathbb{Z}_p, +) \times (\mathbb{Z}_p^*, \cdot)$, donde $u_1, u_2 \in \mathbb{Z}_p^*$ y $h_1, h_2 \in \mathbb{Z}_p$. Definimos los conjuntos

$$(u_1, u_2)\mathcal{I} := \{(u_1x, u_2x) : x \in \mathbb{Z}_p^*\},$$

$$\mathcal{I} + (h_1, h_2) := \{(x + h_1, x + h_2) : x \in \mathbb{Z}_p^*\}.$$

- i. Dadas las unidades u_1, u_2, v_1, v_2 en el campo finito $\mathbb{Z}_p$, se cumple que $(u_1, u_2) \cdot \mathcal{I} = (v_1, v_2) \cdot \mathcal{I}$ si y sólo si $u_1v_2 = v_1u_2$.
- ii. La relación dada en el anterior item es una relación de equivalencia.
- iii. Fijando u_1 y haciendo recorrer u_2 sobre todas las unidades de $\mathbb{Z}_p$ entonces

$$\mathbb{Z}_p^* \times \mathbb{Z}_p^* = \bigcup_{u_2 \in \mathbb{Z}_p^*} (u_1, u_2) \cdot \mathcal{I},$$

donde $(u_1, u_2) \cdot \mathcal{I} \cap (u_1, u'_2) \cdot \mathcal{I} = \emptyset$, para $u_2 \neq u'_2$; es decir, tenemos una partición el conjunto $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$.

Verifiquemos que se satisfacen las anteriores propiedades.

- i. Sea θ un elemento primitivo de $\mathbb{Z}_p$ entonces el conjunto $\mathcal{I}$ lo podemos ver como

$$\mathcal{I} = \{(\theta^k, \theta^k) : 1 \leq k \leq p-1\}.$$

Además, existen $1 \leq m, n, r, s \leq p-1$ tales que $u_1 = \theta^r$, $u_2 = \theta^s$, $v_1 = \theta^m$ y $v_2 = \theta^n$, luego para cada $X \in (u_1, u_2) \cdot \mathcal{I}$ existe $1 \leq k \leq p-1$ que depende de X tal que

$$\begin{aligned} X &= (u_1, u_2) \cdot (\theta^k, \theta^k) \\ &= (\theta^r, \theta^s) \cdot (\theta^k, \theta^k) \\ &= (\theta^r \theta^k, \theta^s \theta^k) \\ &= (\theta^{m+r+k-m}, \theta^{n+s+k-n}) \\ &= (\theta^m \theta^{r+k-m}, \theta^n \theta^{s+k-n}) \\ &= (\theta^m, \theta^n) \cdot (\theta^{r+k-m}, \theta^{s+k-n}), \end{aligned}$$

Luego, $(\theta^{r+k-m}, \theta^{s+k-n}) \in \mathcal{I} \Leftrightarrow r+k-m \equiv s+k-n \pmod{p-1} \Leftrightarrow r-s \equiv m-n \pmod{p-1} \Leftrightarrow \theta^{r+n} = \theta^{s+m} \Leftrightarrow \theta^r \theta^n = \theta^s \theta^m$ lo que es equivalente a $u_1 v_2 = u_2 v_1$.

- ii. No es difícil verificar que la anterior relación es reflexiva y simétrica. Sólo vamos a verificar que es transitiva; sean u_i, v_i, w_i , $i = 1, 2$, unidades de $\mathbb{Z}_p$ tales que $(u_1, u_2) \cdot \mathcal{I} = (v_1, v_2) \cdot \mathcal{I}$ y $(v_1, v_2) \cdot \mathcal{I} = (w_1, w_2) \cdot \mathcal{I}$, esto implica que

$$u_1 v_2 = u_2 v_1 \tag{4.22}$$

$$v_1 w_2 = v_2 w_1, \tag{4.23}$$

luego si multiplicamos por u_2 la igualdad (4.23) obtenemos $u_2 v_1 w_2 = u_2 v_2 w_1$ y usando (4.22) tenemos que $u_1 v_2 w_2 = u_2 v_2 w_1$, como v_2 es una unidad entonces $u_1 w_2 = u_2 w_1$, así $(u_1, u_2) \cdot \mathcal{I} = (w_1, w_2) \cdot \mathcal{I}$.

- iii. Tenemos que para r fijo y cualesquier $1 \leq i < j \leq p-1$ con $i \neq j$, el conjunto

$$(\theta^r, \theta^i) \cdot \mathcal{I} \cap (\theta^r, \theta^j) \cdot \mathcal{I} = \emptyset.$$

En efecto, supongamos que existe

$$X \in (\theta^r, \theta^i) \cdot \mathcal{I} \cap (\theta^r, \theta^j) \cdot \mathcal{I},$$

entonces existen $1 \leq k, l \leq p-1$ tales que

$$X = (\theta^r, \theta^i) \cdot (\theta^k, \theta^k) = (\theta^r, \theta^j) \cdot (\theta^l, \theta^l),$$

esto implica que $r + k \equiv r + l \pmod{p-1}$ y $i + k \equiv j + l \pmod{p-1}$, luego $i = j$, en contradicción. Además, para $1 \leq r \leq p-1$ fijo, se cumple

$$\mathbb{Z}_p^* \times \mathbb{Z}_p^* = \bigcup_{i=1}^{p-1} (\theta^r, \theta^i) \cdot \mathcal{I}, \quad (4.24)$$

puesto que $|(\theta^r, \theta^i) \cdot \mathcal{I}| = p-1$ y la unión es disjunta.

4.2. Función Sidon, Secuencias Sonar y Arreglos Costas.

Ahora, tenemos que algunos conjuntos de Sidon en dimensión dos se pueden definir en términos de funciones; en particular, las secuencias sonar y los arreglos Costas que son un tipo especial de conjuntos de Sidon en dimensión dos. Para dar la definición formal de estos conceptos, vamos a definir primero lo que es una función Sidon. En lo que sigue, consideremos G_1 y G_2 dos grupos conmutativos finitos, $A \subseteq G_1$, $B \subseteq G_2$, $f : A \rightarrow B$ una función. Definimos el grafo de f por

$$\mathcal{G}_f := \{(a, f(a)) : a \in A\}.$$

Definición 4.2.1. Una función $f : A \rightarrow B$, se denomina función Sidon si $\mathcal{G}_f$ es un conjunto de Sidon en $G_1 \times G_2$.

Definición 4.2.2. Una secuencia sonar de orden $m \times n$, es una función Sidon $f : A \rightarrow B$, donde $|A| = n$ y $|B| = m$.

Debido a que las secuencias sonar tienen diversas aplicaciones, también presentamos la definición clásica de secuencia sonar [33]. Para ello primero definimos las siguientes funciones.

Definición 4.2.3. Sean $n, m \in \mathbb{N}$ y $f : [1, n] \rightarrow [1, m]$ una función. Se dice que f tiene la propiedad de diferencias distintas si para todo i, j, k tales que $1 \leq k \leq n-1$, $1 \leq i, j \leq n-k$, se cumple que:

$$f(i+k) - f(i) = f(j+k) - f(j) \Rightarrow i = j.$$

Equivalentemente, se tiene el siguiente resultado, el cual no es difícil de verificar.

Proposición 4.2.4. *Una función $f : [1, n] \rightarrow [1, m]$ tiene la propiedad de diferencias distintas si y sólo si el grafo de f , $G_f := \{(x, f(x)) : x \in [1, n]\}$, es un conjunto de Sidon en el grupo aditivo $\mathbb{Z} \times \mathbb{Z}$.*

Demostración. ($\Rightarrow$) Sean $x, y, z, w \in [1, n]$ tales que

$$(x, f(x)) - (y, f(y)) = (z, f(z)) - (w, f(w)),$$

esto implica que

$$x - y = z - w, \quad (4.25)$$

$$f(x) - f(y) = f(z) - f(w). \quad (4.26)$$

Entonces sin pérdida de generalidad podemos considerar $x - y = z - w > 0$, pues el caso negativo se analiza de manera similar, así tenemos que $x > y$, $z > w$, luego existen enteros positivos a, b tales que $x = y + a$, $z = w + b$, luego como $x - y = z - w$ entonces $a = b$, por lo tanto reemplazando $x = y + a$ y $z = w + b$ en (4.26) tenemos

$$f(y + a) - f(y) = f(w + a) - f(w),$$

y como por hipótesis f satisface la propiedad de diferencias distintas entonces $y = w$ y en consecuencia $x = z$.

$$\text{Así, } \{(x, f(x)), (y, f(y))\} = \{(z, f(z)), (w, f(w))\}.$$

($\Leftarrow$) Supongamos que G_f es un conjunto de Sidon entonces para todo $x, y, z, w \in [1, n]$, si $(x, f(x)) - (y, f(y)) = (z, f(z)) - (w, f(w))$, implica que $\{x, y\} = \{z, w\}$. Luego si consideramos $1 \leq h \leq n - 1$ y $1 \leq i, j \leq n - h$ entonces $i + h$ y $j + h$ son elementos de $[1, n]$, luego por la hipótesis que G_f es un conjunto de Sidon, tenemos que

$$(i + h, f(i + h)) - (i, f(i)) = (j + h, f(j + h)) - (j, f(j)),$$

lo que implica que $\{i + h, i\} = \{j + h, j\}$. Por lo tanto, $i = j$ o $h = 0$.

En consecuencia, para $1 \leq h \leq n-1$ y $1 \leq i, j \leq n-h$ tales que

$$f(i+h) - f(i) = f(j+h) - f(j),$$

implica que $i = j$.

Así, f satisface la propiedad de diferencias distintas.

□

En el caso cuando se cambia $[1, n]$ por $\mathbb{Z}_m$ se dice que la función f satisface la propiedad de diferencias distintas modulares, esto es:

Definición 4.2.5. *Una función Sidon modular, es una función $f : [1, n] \rightarrow \mathbb{Z}_m$ tal que tiene la propiedad de diferencias modulares distintas; esto es, si para todo h, i, j con $1 \leq h \leq n-1$ y $1 \leq i, j \leq n-h$, se cumple que:*

$$f(i+h) - f(i) \equiv f(j+h) - f(j) \pmod{m} \Rightarrow i = j.$$

Definición 4.2.6. *Una secuencia sonar de orden $m \times n$ es una función $f : [1, n] \rightarrow [1, m]$ que tiene la propiedad de diferencias distintas.*

Definición 4.2.7. *Una secuencia sonar modular $m \times n$ es una función $f : [1, n] \rightarrow \mathbb{Z}_m$ con la propiedad de diferencias modulares distintas.*

El problema principal en el caso entero de las secuencias sonar es el siguiente: dado m fijo, encontrar

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

y para el caso modular el problema es determinar si existen secuencias sonar modular para todo m con m elementos.

Definición 4.2.8. *Un arreglo Costas de orden n , es una función Sidon biyectiva $f : A \rightarrow B$, donde $|A| = |B| = n$.*

De manera equivalente, un arreglo Costas lo podemos definir en términos de función que satisface la propiedad de diferencias distintas, así:

Definición 4.2.9. *Un arreglo Costas de orden n es una biyección $f : [1, n] \rightarrow [1, n]$ que tiene la propiedad de diferencias distintas.*

Si $\mathcal{C}(n)$ cuenta el número de arreglos Costas de orden n , entonces el problema principal de estudio en los enteros para el caso de los arreglos Costas es determinar si $\mathcal{C}(n) > 0$, para todo n ; es decir se busca determinar si existen arreglos costas para todo n , el primer n para el cual no se conoce si existen es $n = 32$. Cabe destacar que $\mathcal{C}(n)$ es una sucesión que aparece registrada en la OEIS como la sucesión A008404.

Ahora vamos a describir algunas construcciones conocidas de secuencias sonar y arreglos Costas [33]. Sean p un número primo, r un entero positivo, $q = p^r$, y $\mathbb{F}_q$ el campo finito con q elementos.

Teorema 4.2.10 (Construcción cuadrática). *Sean p un primo impar, y a, b, c enteros tales que $a \not\equiv 0 \pmod{p}$. La función $f : [1, p+1] \rightarrow \mathbb{Z}_p$ definida por $f(i) = ai^2 + bi + c$ es una secuencia sonar modular $p \times (p+1)$.*

Teorema 4.2.11 (Construcción Shift). *Sean $q = p^r$ una potencia prima, α un elemento primitivo de $\mathbb{F}_{q^2}$ y β un elemento primitivo de $\mathbb{F}_q$. La función $f : [1, q] \rightarrow \mathbb{Z}_{q-1}$ definida por $f(i) = \log_{\beta}(\alpha^{iq} + \alpha^i)$ es una secuencia sonar modular $(q-1) \times q$.*

Teorema 4.2.12 (Construcción Welch Exponencial Extendida). *Sean α un elemento primitivo modulo p y s un entero. La función $f : [0, p-1] \rightarrow \mathbb{Z}_p$ definida por $f(i) = \alpha^{i+s}$ es una secuencia sonar modular $p \times p$. Si $s = 0$, la función $f : [1, p-1] \rightarrow \mathbb{Z}_p$ definida por $f(i) = \alpha^i$ es una secuencia sonar modular $p \times (p-1)$.*

Teorema 4.2.13 (Construcción Welch Logarítmica). *Sea α un elemento primitivo modulo p . La función $f : [1, p-1] \rightarrow \mathbb{Z}_{p-1}$ definida por $f(i) = \log_{\alpha} i$ es una secuencia sonar modular $(p-1) \times (p-1)$.*

Teorema 4.2.14 (Construcción Golomb-Lempel). *Sea q una potencia prima mayor que 2, y sean α, β elementos primitivos de $\mathbb{F}_q$. La función $f : [1, q-2] \rightarrow \mathbb{Z}_{q-1}$ definida por $f(i) = j$ si y sólo si $\alpha^i + \beta^j = 1$ es una secuencia sonar modular $(q-1) \times (q-2)$. Si $\alpha = \beta$ esta construcción se conoce con el nombre de construcción Lempel.*

4.3. Nuevas Construcciones de Secuencias Sonar.

En Febrero de 2014 publicamos el artículo *New Constructions of Sonar Sequences*, en la revista *IJBAS: International Journal of Basic & Applied Sciences* [37], en el que por primera vez se usan conjuntos de Sidon en dimensión uno para obtener secuencias sonar; es decir, presentamos en este artículo nuevas construcciones de secuencias sonar que provienen del análisis de ciertas propiedades que satisfacen los conjuntos de Sidon tipo Bose y tipo Ruzsa descritas en el Capítulo 3.

Teorema 4.3.1. *Sean $m, b \in \mathbb{N}$ y $\mathcal{A} = \{a_1, \dots, a_n\}$ un conjunto de Sidon en el grupo aditivo $\mathbb{Z}_{mb}$. Si $\mathcal{A}(\text{mód } b) := \{a(\text{mód } b) : a \in \mathcal{A}\} = [1, n]$, entonces la función $f : [1, n] \rightarrow \mathbb{Z}_m$ definida por $f(i) = \lfloor \frac{a_i}{b} \rfloor$, es una secuencia sonar modular $m \times n$, donde a_i es el único elemento en $\mathcal{A}$ tal que $a_i \equiv i(\text{mód } b)$.*

Demostración. Veamos que f es una función que cumple la propiedad de diferencias modulares distintas. Sean i, j, h en $[1, n]$ tales que $1 \leq h \leq n-1$, $1 \leq i, j \leq n-h$. Supongamos que

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

esto es

$$\left\lfloor \frac{a_{i+h}}{b} \right\rfloor - \left\lfloor \frac{a_i}{b} \right\rfloor \equiv \left\lfloor \frac{a_{j+h}}{b} \right\rfloor - \left\lfloor \frac{a_j}{b} \right\rfloor (\text{mód } m),$$

así, existe $t \in \mathbb{Z}$ tal que

$$\left\lfloor \frac{a_{i+h}}{b} \right\rfloor - \left\lfloor \frac{a_i}{b} \right\rfloor = \left\lfloor \frac{a_{j+h}}{b} \right\rfloor - \left\lfloor \frac{a_j}{b} \right\rfloor + tm,$$

Multiplicamos por b y tenemos

$$b \left\lfloor \frac{a_{i+h}}{b} \right\rfloor - b \left\lfloor \frac{a_i}{b} \right\rfloor = b \left\lfloor \frac{a_{j+h}}{b} \right\rfloor - b \left\lfloor \frac{a_j}{b} \right\rfloor + tmb,$$

luego dado que cada $a_k \in \mathcal{A}$ satisface $a_k = b \left\lfloor \frac{a_k}{b} \right\rfloor + k$, se sigue que

$$\begin{aligned} [a_{i+h} - (i+h)] - [a_i - i] &= [a_{j+h} - (j+h)] - [a_j - j] + tmb, \\ a_{i+h} - a_i &= a_{j+h} - a_j + tmb. \end{aligned}$$

Ahora si miramos módulo por mb obtenemos

$$a_{i+h} + a_j \equiv a_{j+h} + a_i \pmod{mb},$$

y como $a_k \in \mathcal{A}$, para $k = i, j, i+h, j+h$ y $\mathcal{A}$ es un conjunto de Sidon en el grupo aditivo $\mathbb{Z}_{mb}$, tenemos que $\{i+h, j\} = \{j+h, i\}$ y como $h \neq 0$ esto implica que $i = j$. Así, f es una función con la propiedad de diferencias modulares distintas y por lo tanto es una secuencia sonar módulo m de tamaño $n = |\mathcal{A}|$. $\square$

En los siguientes corolarios utilizamos las construcciones de conjuntos de Sidon tipo Bose y Ruzsa para obtener nuevas secuencias sonar.

Corolario 4.3.2. Sean q una potencia prima, θ un elemento primitivo del cuerpo finito $\mathbb{F}_q$ y $B(q, \theta)$ un conjunto de Sidon tipo Bose en el grupo aditivo $\mathbb{Z}_{q^2-1}$. La función $f : [1, q] \rightarrow \mathbb{Z}_{q-1}$ definida por

$$f(i) := \left\lfloor \frac{b_i}{q+1} \right\rfloor,$$

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

Demostración. Tomemos $b = q+1$ y $m = q-1$. Por la propiedad (B4) de la Proposición 3.1.3 sabemos que $\mathcal{B}(q, \theta) \pmod{q+1} = [1, q]$, luego para cada $i \in [1, q]$ existe un único $b_i \in \mathcal{B}$ tal que $b_i \equiv i \pmod{q+1}$, de esta manera es posible escribir $b_i = \left\lfloor \frac{b_i}{q+1} \right\rfloor (q+1) + i$, para todo $i = 1, 2, \dots, q$. Así, podemos definir la función $f : [1, q] \rightarrow \mathbb{Z}_{q-1}$ como en el Teorema 4.3.1, la cual define una secuencia sonar módulo $q-1$ con q elementos. $\square$

Corolario 4.3.3. Sean p un número primo, θ un elemento primitivo del campo finito $\mathbb{F}_p$ y $R(p, \theta)$ un conjunto de Sidon tipo Ruzsa en el grupo aditivo $\mathbb{Z}_{p^2-p}$. La función $f : [1, p-1] \rightarrow \mathbb{Z}_{p-1}$ definida por

$$f(i) := \left\lfloor \frac{r_i}{p} \right\rfloor,$$

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

Demostración. Tomemos $m = p - 1$ y $b = p$. Por las propiedad (R5) de la Proposición 3.3.3 tenemos que $R(p, \theta) \pmod{p} = [1, p - 1]$, luego para cada $i \in [1, p - 1]$ existe un único $r_i \in R(p, \theta)$ tal que $r_i \equiv i \pmod{p}$, de esta manera es posible escribir $r_i = \left\lfloor \frac{r_i}{p} \right\rfloor p + i$, para todo $i = 1, 2, \dots, p - 1$. Así, podemos definir la función $f : [1, p - 1] \rightarrow \mathbb{Z}_{p-1}$ como en el Teorema 4.3.1, la cual define una secuencia sonar módulo $p - 1$ con $p - 1$ elementos. $\square$

Corolario 4.3.4. Sean p un número primo, θ un elemento primitivo del campo finito $\mathbb{F}_p$ y $R(p, \theta)$ un conjunto de Sidon tipo Ruzsa en el grupo aditivo $\mathbb{Z}_{p^2-p}$. La función $f : [0, p - 2] \rightarrow \mathbb{Z}_p$ definida por

$$f(i) := \left\lfloor \frac{r_i}{p-1} \right\rfloor,$$

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

Demostración. Tomamos $m = p$ y $b = p - 1$. Por la propiedad (R6) de la Proposición 3.3.3 tenemos que $R(p, \theta) \pmod{p - 1} = [0, p - 2]$, luego para cada $i \in [0, p - 2]$ existe un único $r_i \in R(p, \theta)$ tal que $r_i \equiv i \pmod{p - 1}$.

De esta manera es posible escribir $r_i = \left\lfloor \frac{r_i}{(p-1)} \right\rfloor (p - 1) + i$, para cada $i = 0, 1, \dots, p - 2$. Así, podemos definir la función $f : [0, p - 2] \rightarrow \mathbb{Z}_p$ como en el Teorema 4.3.1, la cual define una secuencia sonar módulo p con $p - 1$ elementos. $\square$

Los siguientes ejemplos ilustran el Teorema 4.3.1, en particular las consecuencias que provienen de los conjuntos de Sidon en una dimensión tipo Bose y Ruzsa.

Ejemplo 7. Sean $q = 9$, $q^2 - 1 = 80 = 10 * 8$. Un conjunto de Sidon de tipo Bose con 9 elementos es

$$\mathcal{B}(9, \theta) = \{1, 4, 37, 38, 49, 53, 55, 62, 76\}.$$

Usando la función $f : [1, 9] \rightarrow \mathbb{Z}_8$, definida por $f(i) = \lfloor b_i/10 \rfloor$, donde $b_i \in \mathcal{B}(9, \theta)$, del Corolario 4.3.2 tenemos una secuencia sonar modular 8×9 dada por

$$\{(1, 0), (2, 6), (3, 5), (4, 0), (5, 5), (6, 7), (7, 3), (8, 3), (9, 4)\}.$$

Ejemplo 8. Sean $p = 7$, $p^2 - p = 42 = 6 * 7$. Un conjunto de Sidon de tipo Ruzsa con 6 elementos es

$$\mathcal{R}_1 = \{2, 4, 5, 27, 31, 36\}.$$

Usando la función $f : [1, 6] \rightarrow \mathbb{Z}_6$, definida por $f(i) = \lfloor r_i/7 \rfloor$, donde $r_i \in \mathcal{R}_1$, del Corolario 4.3.3 tenemos una secuencia sonar modular 6×6 dada por

$$\{(1, 5), (2, 0), (3, 4), (4, 0), (5, 0), (6, 3)\}.$$

Ejemplo 9. Sean $p = 13$, $p^2 - p = 156 = 13 * 12$. Un conjunto de Sidon de tipo Ruzsa con 12 elementos es

$$\mathcal{R}_2 = \{10, 16, 57, 59, 90, 99, 115, 134, 144, 145, 149, 152\}.$$

Usando la función $f : [0, 11] \rightarrow \mathbb{Z}_{13}$, definida por $f(i) = \lfloor r_i/12 \rfloor$, donde $r_i \in \mathcal{R}_2$, del Corolario 4.3.4 tenemos una secuencia sonar modular 13×12 dada por

$$\{(0, 12), (1, 12), (2, 11), (3, 8), (4, 1), (5, 12), (6, 7), (7, 9), (8, 12), (9, 4), (10, 0), (11, 4)\}.$$

Algunas aplicaciones de los arreglos Costas y las secuencias Sonar son las siguientes:

- J. Costas [11] y Golomb-Taylor [22] introducen los arreglos Costas y las secuencias Sonar, respectivamente, para responder al siguiente problema:

“Un objeto se está moviendo a cierta distancia de un observador, y él quiere saber efectivamente la distancia del objeto y su velocidad”.

La solución de este problema se obtiene usando el efecto Doppler, el cual dice lo siguiente: si el observador envía una señal hacia un blanco en movimiento, el cambio entre la frecuencia original y la frecuencia que retorna, permite calcular la velocidad del blanco y cuánto tiempo gasta en ir y volver la señal para así determinar la distancia.

Sin embargo, como el mundo es ruidoso, una señal que es enviada puede no retornar. Por tal razón, se envían n señales consecutivamente, cada

una con una frecuencia en un intervalo de 1 hasta m en rangos de tiempo que varían desde 1 hasta n .

Una vez el modelo de señales se ha recuperado, se pueden determinar la velocidad y la distancia del objeto. Pero si alguna señal no regresa, aparecerán algunas ambigüedades en la interpretación de lo que era el modelo total.

Los arreglos Costas y las secuencias Sonar son aquellos modelos para los cuales se envía exactamente una señal en cada intervalo de tiempo, y con la propiedad especial que aún si sólo dos señales se recuperan se puede reconstruir el modelo entero [34].

- Otra aplicación que tienen estos conjuntos es en comunicaciones. La modulación por posición de pulso PPM (Pulse Position Modulation) se usa en sistemas de comunicaciones con propósitos especiales, en particular en los sistemas militares. Existen otras técnicas de modulación, pero la PPM es más insensible al ruido.

Un pulso se ubica en uno de m intervalos de tiempos consecutivos para representar un m -ésimo símbolo. Los mensajes se envían mediante una secuencia de dichos símbolos. El receptor decodifica el mensaje, generalmente mediante la integración de un símbolo en cada intervalo y selecciona el máximo valor de integración de estos símbolos para la toma de decisiones.

Para lograr esta decodificación se requiere tanto del intervalo de tiempo (para fijar los intervalos de integración) como de los bloques de intervalos (para enumerar correctamente los segmentos de tiempo para la identificación de estos símbolos). Lo anterior se consigue fijando intervalos de tiempo en los cuales ocurren las pulsaciones.

La sincronización de estos bloques se consigue después de establecer los intervalos de tiempo y generalmente se efectúa transmitiendo algo conocido como una secuencia PPM y usando un método de correlación de salto para la reconstrucción del mensaje.

Una secuencia PPM se define como una secuencia en la cual cada bloque contiene exactamente un punto. Y la correlación de salto, con una versión alternada de sí misma, se define como el número de bloques con los cuales coinciden cuando ambas secuencias son sobrepuestas.

La ventaja de las secuencias PPM es que con todos los valores de correlación de salto, el máximo de coincidencias es una, es decir, la versión desplazada, de todos los “saltos” posibles (diferentes de la posición original) coinciden con el modelo original en a lo más un punto.

Las secuencias PPM se pueden representar como casos particulares de arreglos Costas o secuencias Sonar [19].

Capítulo 5

Construcciones de conjuntos B_h en d dimensiones

Otra generalización de los conjuntos de Sidon enteros es cuando, en lugar de sumar dos elementos, se suman h y todas las sumas son distintas, salvo permutación de los sumandos. A estos conjuntos se les conoce con el nombre de conjuntos B_h enteros. Además, en lugar de considerar conjuntos de enteros también se pueden estudiar los conjuntos B_h en cualquier grupo e incluso en d dimensiones; es decir, conjuntos de Sidon contenidos en el producto cartesiano de d grupos. Formalmente:

Definición 5.0.5. *Sea d un entero positivo arbitrario y sean $(G_i, *_{i})$, $i = 1, \dots, d$ grupos arbitrarios, decimos que A es un conjunto B_h en d dimensiones si $A \subseteq G_1 \times \dots \times G_d$ y para todo $x \in G_1 \times \dots \times G_d$, se cumple que la ecuación $x = a_1 * \dots * a_h$ tiene a lo más una solución en A , donde $*$ representa la operación del grupo producto $(G_1, *_{1}) \times \dots \times (G_d, *_{d})$.*

En este capítulo presentamos algunas construcciones de conjuntos B_h en d dimensiones, cuyos elementos se consideran en un campo arbitrario y alguna extensión adecuada del campo.

5.1. Construcción de conjunto B_h tipo Bose y Chowla.

Presentamos la construcción de conjuntos B_h tipo Bose y Chowla usando un campo general. Denotamos, en las secciones que siguen, por σ_k la k -ésima función simétrica elemental en las variables $x_1, x_2, \dots, x_t$ esto es:

$$\begin{aligned}\sigma_1(x_1, \dots, x_t) &= \sum_{i=1}^t x_i \\ \sigma_2(x_1, \dots, x_t) &= \sum_{1 \leq j_1 < j_2 \leq t} x_{j_1} x_{j_2} \\ &\vdots \\ \sigma_k(x_1, \dots, x_t) &= \sum_{1 \leq j_1 < \dots < j_k \leq t} x_{j_1} \cdots x_{j_k} \\ &\vdots \\ \sigma_t(x_1, \dots, x_t) &= x_1 \cdots x_t\end{aligned}$$

Teorema 5.1.1. *Sea $(F, +, \cdot)$ un campo, E una extensión algebraica de grado $h \geq 2$ sobre F con elemento algebraico α y θ un elemento primitivo del campo E . Entonces el conjunto $A(\alpha) = \alpha + F := \{\alpha + a : a \in F\}$. es un conjunto B_h en el grupo multiplicativo de unidades de E .*

Demostración. Supongamos que existen $a_{i_1}, \dots, a_{i_h}, b_{j_1}, \dots, b_{j_h}$ en F tales que

$$\prod_{k=1}^h (\alpha + a_{i_k}) = \prod_{k=1}^h (\alpha + b_{j_k}),$$

esto es equivalente

$$\alpha^h + \sum_{k=1}^h \sigma_k(a_{i_1}, \dots, a_{i_h}) \alpha^{h-k} = \alpha^h + \sum_{k=1}^h \sigma_k(b_{j_1}, \dots, b_{j_h}) \alpha^{h-k},$$

donde σ_k representan las funciones simétricas elementales en las correspondientes variables.

Así, vemos que α satisface el siguiente polinomio en la variable x con coeficientes en F :

$$P(x) = \sum_{k=1}^h (\sigma_k(a_{i_1}, \dots, a_{i_h}) - \sigma_k(b_{j_1}, \dots, b_{j_h})) x^{h-k},$$

pero el grado del polinomio P es menor que h y como α es algebraico de grado h sobre F entonces $P(x)$ debe ser el polinomio nulo. De esto se sigue que

$$\sigma_k(a_{i_1}, \dots, a_{i_h}) = \sigma_k(b_{j_1}, \dots, b_{j_h}),$$

para todo $k \in \{1, \dots, h\}$.

Pero estas funciones simétricas son los coeficientes del polinomio

$$Q(y) = y^h - \sigma_1 y^{h-1} + \dots + (-1)^{h-1} \sigma_{h-1} y + (-1)^h \sigma_h,$$

donde $\sigma_k = \sigma_k(a_{i_1}, \dots, a_{i_h}) = \sigma_k(b_{j_1}, \dots, b_{j_h})$, para todo $k \in \{1, \dots, h\}$.

Así, $Q(y) = (y - a_{i_1}) \cdots (y - a_{i_h}) = (y - b_{j_1}) \cdots (y - b_{j_h})$, por lo tanto,

$$\{a_{i_1}, \dots, a_{i_h}\} = \{b_{j_1}, \dots, b_{j_h}\}.$$

En consecuencia, $\{\alpha + a_{i_1}, \dots, \alpha + a_{i_h}\} = \{\alpha + b_{j_1}, \dots, \alpha + b_{j_h}\}$.

□

Ahora, si F es el campo finito $\mathbb{F}_q$, con q una potencia de un primo, podemos considerar el isomorfismo del logaritmo discreto en la base θ , $\log_\theta$, entre los grupos $(\mathbb{F}_{q^h}^*, \cdot)$ y $(\mathbb{Z}_{q^h-1}, +)$. De esta manera obtenemos la construcción del conjunto B_h tipo Bose-Chowla en el grupo $(\mathbb{Z}_{q^h-1}, +)$, con q elementos.

Teorema 5.1.2. *Sea $q = p^n$, con p primo, $n \in \mathbb{Z}^+$, existe un conjunto B_h en el grupo aditivo $\mathbb{Z}_{q^h-1}$, con q elementos.*

Demostración. Por el Teorema 5.1.1 sabemos que $A(\alpha)$ es un conjunto B_h en $(\mathbb{F}_{q^h}^*, \cdot)$, donde $\alpha \in \mathbb{F}_{q^h}$ es un elemento de orden h sobre $\mathbb{F}_q$. Sean θ un elemento primitivo de $\mathbb{F}_{q^h}$ y $\varphi : (\mathbb{F}_{q^h}^*, \cdot) \longrightarrow (\mathbb{Z}_{q^h-1}, +)$ el isomorfismo del

logaritmo discreto definido por $\varphi(a) = \log_\theta a = k$, donde $a = \theta^k$, para algún $1 \leq k \leq q^h - 1$. Entonces por el Lema 1.0.7 el conjunto imagen de $A(\alpha)$ a través de φ definido por $\varphi(A(\alpha)) := \{\log_\theta(\alpha + a) : a \in \mathbb{F}_q\}$ es un conjunto B_h en $(\mathbb{Z}_{q^h-1}, +)$. $\square$

Ejemplo 10. Sea $p = 7$, θ un elemento primitivo de $\mathbb{F}_{7^2}$ con polinomio minimal sobre $\mathbb{F}_7$, $\min_{\mathbb{F}_7}(\theta) = 2x^2 + x + 3$ y tomemos $\alpha = \theta$ de grado 2 sobre $\mathbb{F}_7$. El conjunto

$$\begin{aligned} A(\theta) &= \{\theta, \theta + 1, \theta + 2, \theta + 3, \theta + 4, \theta + 5, \theta + 6\} \\ &= \{\theta, \theta^{46}, \theta^{36}, \theta^{10}, \theta^{31}, \theta^{35}, \theta^{29}\}, \end{aligned}$$

es un conjunto B_2 en el grupo multiplicativo $\mathbb{F}_{49}^*$. Usando el isomorfismo del logaritmo discreto en la base θ , tenemos que el conjunto

$$A = \{1, 10, 29, 31, 35, 36, 46\}$$

es un conjunto B_2 en el grupo aditivo $\mathbb{Z}_{48}$.

5.2. Construcción de conjunto B_h tipo Singer generalizada.

Aunque en principio la construcción de Singer apareció primero que la de Bose y Chowla, en este caso presentamos la construcción de Singer como una consecuencia de la construcción de Bose y Chowla.

Primero construimos un conjunto B_{h+1} en el grupo aditivo $\mathbb{Z}_{q^{h+1}-1}$ tipo Bose-Chowla con q elementos, luego reducimos este conjunto módulo $q^h + q^{h-1} + \dots + q + 1$, el conjunto resultante es un conjunto B_h en el grupo aditivo $\mathbb{Z}_{q^h+q^{h-1}+\dots+q+1}$ que preserva el número de elementos, por último agregamos un elemento adecuado al último conjunto para así obtener un conjunto B_h tipo Singer generalizado con $q + 1$ elementos en el grupo aditivo $\mathbb{Z}_{q^h+q^{h-1}+\dots+q+1}$.

Sea q una potencia de un primo, $h \geq 2$ un entero, consideremos el campo $\mathbb{F}_{q^{h+1}}$ con elemento primitivo θ y sea $\alpha \in \mathbb{F}_{q^{h+1}}^*$ un elemento de grado $h + 1$

sobre $\mathbb{F}_q$. Construimos un conjunto tipo Bose-Chowla como en la sección anterior, digamos

$$\mathcal{A} = \log_\theta(\alpha + \mathbb{F}_q) \subseteq \mathbb{Z}_{q^{h+1}-1}.$$

Denotamos $n_q := q^h + q^{h-1} + \dots + q + 1 = \frac{q^{h+1}-1}{q-1}$; de esta manera, el conjunto $\mathcal{A}$ es un conjunto B_{h+1} en el grupo aditivo $\mathbb{Z}_{q^{h+1}-1}$ con q elementos. Recordemos que este conjunto proviene del conjunto $A(\alpha) = \alpha + \mathbb{F}_q$ que es un conjunto B_{h+1} en el grupo multiplicativo $\mathbb{F}_{q^{h+1}}^*$.

Ahora bien, demostramos el Teorema de Singer generalizado.

Teorema 5.2.1. *Sean $q = p^n$, con p primo, $n \in \mathbb{N}$ y $h \geq 2$ entero, existe un conjunto B_h en el grupo aditivo $\mathbb{Z}_{q^h+q^{h-1}+\dots+q+1}$, con $q+1$ elementos.*

Demostración. Con la notación anterior consideremos el conjunto $\mathcal{A} = \log_\theta(\alpha + \mathbb{F}_q) \subseteq \mathbb{Z}_{q^{h+1}-1}$ y lo modulamos (mód n_q), obtenemos un nuevo conjunto $S = \mathcal{A} \pmod{n_q}$; verifiquemos que S es un conjunto B_h en el grupo aditivo $\mathbb{Z}_{n_q}$. Supongamos que existe un elemento en $(\mathbb{Z}_{n_q}, +)$ que tiene dos representaciones como suma de h elementos del conjunto S ; es decir, existen $a_{i_1}, \dots, a_{i_h}, a'_{j_1}, \dots, a'_{j_h}$ en S tales que

$$a_{i_1} + \dots + a_{i_h} \equiv a'_{j_1} + \dots + a'_{j_h} \pmod{n_q}$$

entonces

$$a_{i_1} + \dots + a_{i_h} = a'_{j_1} + \dots + a'_{j_h} + rn_q,$$

para algún $r \in \mathbb{Z}$, luego como θ es un elemento primitivo de $\mathbb{F}_{q^{h+1}}$ tenemos

$$\theta^{a_{i_1}+\dots+a_{i_h}} = \theta^{a'_{j_1}+\dots+a'_{j_h}} \theta^{rn_q}$$

y como $\theta^{rn_q} \in \mathbb{F}_q^* = \langle \theta^{n_q} \rangle$ entonces

$$\theta^{a_{i_1}+\dots+a_{i_h}} = v \theta^{a'_{j_1}+\dots+a'_{j_h}},$$

donde $v = \theta^{rn_q}$. Esto equivale a

$$\theta^{a_{i_1}} \dots \theta^{a_{i_h}} = v \theta^{a'_{j_1}} \dots \theta^{a'_{j_h}}.$$

Como para cada elemento $\alpha + u_i \in A(\alpha)$ existe un único elemento $a_i \in \mathcal{A}$ tal que $\log_\theta(\alpha + u_i) = a_i$, esto implica que

$$(\alpha + u_{i_1}) \dots (\alpha + u_{i_h}) = v(\alpha + u'_{j_1}) \dots (\alpha + u'_{j_h}),$$

desarrollando los productos, notamos que α satisface un polinomio de grado h con coeficientes en $\mathbb{F}_q^*$:

$$P(x) = (1 - v)x^h + (\sigma_1 - v\delta_1)x^{h-1} + \cdots + (\sigma_{h-1} - v\delta_{h-1})x + (\sigma_h - v\delta_h),$$

donde $\sigma_k = \sigma_k(u_{i_1}, \dots, u_{i_h})$, $\delta_k = \delta_k(u'_{j_1}, \dots, u'_{j_h})$, para $k = 1, \dots, h$, son las funciones simétricas elementales, luego como α es de grado $h + 1$ sobre $\mathbb{F}_q$ el polinomio $P(x)$ debe ser el polinomio nulo y así tenemos que

$$v = 1 \text{ y } \sigma_k = v\delta_k,$$

para $k = 1, \dots, h$. Así, $v = 1$ y $\{u_{i_1}, \dots, u_{i_h}\} = \{u'_{j_1}, \dots, u'_{j_h}\}$.

En consecuencia,

$$\{a_{i_1}, \dots, a_{i_h}\} = \{a'_{j_1}, \dots, a'_{j_h}\}.$$

Así, S es un conjunto B_h en $\mathbb{Z}_{n_q}$. Además, S tiene q elementos; en efecto, supongamos que existen dos elementos en S que son iguales, digamos

$$a_i \equiv a_j \pmod{n_q},$$

con $i \neq j$. Así, existe $w \in \mathbb{Z}$ tal que

$$a_i = a_j + wn_q,$$

esto implica que en $\mathbb{F}_{q^{h+1}}$ tenemos

$$\theta^{a_i} = \theta^{a_j} \theta^{wn_q}$$

y como $\theta^{wn_q} \in \mathbb{F}_q^* = \langle \theta^{n_q} \rangle$ entonces

$$\theta^{a_i} = x \theta^{a_j}$$

donde $x = \theta^{wn_q}$.

Como para cada elemento $\alpha + u_i \in A(\alpha)$ existe un único elemento $a_i \in \mathcal{A}$ tal que $\log_\theta(\alpha + u_k) = a_k$, esto implica que

$$(\alpha + u_i) = x(\alpha + u_j).$$

Así, α satisface un polinomio de grado uno con coeficientes en $\mathbb{F}_q$, lo que implica que $x = 1$ y $u_i = u_j$ y así $i = j$, lo cual es una contradicción. Por lo tanto, todos los elementos de S son distintos.

Ahora, si tomamos el conjunto $S_0 := S \cup \{0\}$ tenemos un conjunto B_h en $\mathbb{Z}_{n_q}$ con $q+1$ elementos. En efecto, recordemos que para n un entero positivo, nP representa el conjunto suma $P + \dots + P$ (n veces), así tenemos que

$$\begin{aligned} hS_0 &= (hS) \cup ((h-1)S + \{0\}) \cup \dots \cup (S + (h-1)\{0\}) \cup (h\{0\}) \\ &= \bigcup_{i=0}^h [(h-i)S + i\{0\}]. \end{aligned}$$

Por lo tanto,

$$|hS_0| = \sum_{k=0}^h (-1)^k \sum_{|I|=k+1, I \subseteq [0, h]} \left| \bigcap_{i \in I} [(h-i)S + i\{0\}] \right|.$$

Sin embargo, para cada $|I| = k+1$, $I \subseteq [0, h]$, con $1 \leq k \leq h-1$, tenemos que

$$\bigcap_{i \in I} [(h-i)S + i\{0\}] = \emptyset. \quad (5.1)$$

Verifiquemos que se cumple (5.1), aunque esta afirmación es suficiente demostrarla para el caso de la intersección de dos conjuntos de este tipo.

En efecto, supongamos que $x \in [(h-i)S + i\{0\}] \cap [(h-j)S + j\{0\}]$, donde $i, j \in I$, $i \neq j$, $I \subseteq [0, h]$ y $|I| = k+1$ y $1 \leq k \leq h-1$. Así,

$$x = s_1 + s_2 + \dots + s_{h-i} + i0 = s_1 + s_2 + \dots + s_{h-i},$$

$$x = s'_1 + s'_2 + \dots + s'_{h-j} + j0 = s'_1 + s'_2 + \dots + s'_{h-j}.$$

Luego,

$$s_1 + s_2 + \dots + s_{h-i} \equiv s'_1 + s'_2 + \dots + s'_{h-j} \pmod{n_q}$$

Recordemos que $\mathcal{A} = \log_\theta(\alpha + \mathbb{F}_q)$ y $S = \mathcal{A} \pmod{n_q}$, de esta manera lo anterior implica que

$$\theta^{s_1} \theta^{s_2} \dots \theta^{s_{h-i}} = w \theta^{s'_1} \theta^{s'_2} \dots \theta^{s'_{h-j}},$$

donde θ es un elemento primitivo de $\mathbb{F}_{q^{h+1}}$ y $w = \theta^{mn_q} \in \langle \theta^{n_q} \rangle = \mathbb{F}_q^*$, para algún $m \in \mathbb{Z}$. Como para cada $\alpha + u_t \in \alpha + \mathbb{F}_q$ existe un único elemento $s_t \in \mathcal{A}$ talque $\log_\theta(\alpha + u_t) = s_t$ entonces

$$(\alpha + u_1)(\alpha + u_2) \cdots (\alpha + u_{h-i}) = w(\alpha + u'_1)(\alpha + u'_2) \cdots (\alpha + u'_{h-j})$$

Supongamos que $i < j$ entonces α satisface un polinomio con coeficientes en $\mathbb{F}_q$ de grado $h - i < h + 1$, pero α es un elemento algebraico de grado $h + 1$ y además $h - j < h - i$, entonces el polinomio debe ser el polinomio nulo, así desarrollando los polinomios obtenemos que $1 = 0$ lo cual es una contradicción.

En consecuencia, $[(h - i)S + i\{0\}] \cap [(h - j)S + j\{0\}] = \emptyset$.

En consecuencia,

$$\begin{aligned} |hS_0| &= \sum_{i=0}^h |(h - i)S + i\{0\}| \\ &= |hS| + |(h - 1)S + \{0\}| + \cdots + |S + (h - 1)\{0\}| + |h\{0\}| \\ &= |hS| + |(h - 1)S| + \cdots + |S| + |\{0\}| \end{aligned}$$

Además, dado que S es un conjunto B_h en el grupo aditivo $\mathbb{Z}_{n_q}$ con $|S| = q$ tenemos que

$$\begin{aligned} |hS_0| &= |hS| + |(h - 1)S| + \cdots + |S| + |\{0\}| \\ &= \binom{q + h - 1}{h} + \binom{q + h - 2}{h - 1} + \cdots + \binom{q}{1} + \binom{q - 1}{0} \\ &= \binom{q + h}{h} \\ &= \binom{(q + 1) + h - 1}{h} \\ &= \binom{|S_0| + h - 1}{h}. \end{aligned}$$

□

5.3. Construcción de conjunto B_{h+1} en dimensión dos.

Gómez y Trujillo en [23] obtuvieron una nueva construcción de conjuntos B_{h+1} , donde realizan el proceso contrario a la construcción de Singer generalizada, ellos a partir de un conjunto B_h obtienen un conjunto B_{h+1} usando las ideas de la construcción de Ruzsa.

En esta sección presentamos una construcción de conjuntos B_{h+1} en dimensión dos en un campo F arbitrario, usamos las ideas de la construcción dada por Gómez y Trujillo [23], considerando un conjunto B_h tipo Bose-Chowla.

Teorema 5.3.1. *Sea $(F, +, \cdot)$ un campo, α un elemento algebraico de grado h sobre F en alguna extensión E de F , $E = F(\alpha)$ y $E^* = E \setminus \{0\}$ el grupo de unidades de E . El conjunto*

$$A := \{(a, \alpha + a) : a \in F\}$$

es un conjunto B_{h+1} en $(F, +) \times (E^, \cdot)$.*

Demostración. Representamos por $\star$ la operación del grupo producto $(F, +) \times (E^*, \cdot)$. Supongamos que existe un elemento en $(F, +) \times (E^*, \cdot)$ que tiene dos representaciones como el producto de $h + 1$ elementos del conjunto A bajo la operación $\star$, es decir, existen $a_i, b_i \in F$, para $i = 1, \dots, h + 1$, tales que

$$(a_1, \alpha + a_1) \star \dots \star (a_{h+1}, \alpha + a_{h+1}) = (b_1, \alpha + b_1) \star \dots \star (b_{h+1}, \alpha + b_{h+1}).$$

Esta igualdad implica

$$\sum_{i=1}^{h+1} a_i = \sum_{i=1}^{h+1} b_i \tag{5.2}$$

$$\prod_{i=1}^{h+1} (\alpha + a_i) = \prod_{i=1}^{h+1} (\alpha + b_i) \tag{5.3}$$

Si llamamos $a := \{a_1, \dots, a_{h+2}\}$ y $b := \{b_1, \dots, b_{h+2}\}$, tenemos en (5.3) que

$$\begin{aligned} \alpha^{h+1} + \sigma_1(a)\alpha^h + \dots + \sigma_h(a)\alpha + \sigma_{h+1}(a) = \\ \alpha^{h+1} + \sigma_1(b)\alpha^h + \dots + \sigma_h(b)\alpha + \sigma_{h+1}(b), \end{aligned} \quad (5.4)$$

donde σ_k representan las funciones simétricas elementales en las variables correspondientes.

Usando (5.2) y simplificando términos iguales en (5.4) obtenemos

$$\sigma_2(a)\alpha^{h-1} + \dots + \sigma_{h+1}(a) = \sigma_2(b)\alpha^{h-1} + \dots + \sigma_{h+1}(b), \quad (5.5)$$

Así, α satisface un polinomio de grado $h - 1$ y como α es algebraico de grado h sobre F entonces el polinomio debe ser el polinomio nulo, de esta manera tenemos

$$\begin{aligned} \sigma_2(a) &= \sigma_2(b) \\ &\vdots \\ \sigma_{h+1}(a) &= \sigma_{h+1}(b). \end{aligned}$$

Las anteriores igualdades junto con (5.2) son las funciones simétricas elementales en las variables a y b , luego $a = b$, es decir

$$\{a_i : i = 1, \dots, h+1\} = \{b_i : i = 1, \dots, h+1\},$$

en consecuencia

$$\{(a_i, \alpha + a_i) : i = 1, \dots, h+1\} = \{(b_i, \alpha + b_i) : i = 1, \dots, h+1\}.$$

□

Si consideramos el campo finito $F = \mathbb{F}_p$ con p elementos, entonces $E = \mathbb{F}_{p^h}$ y $(\mathbb{F}_p, +) \times (\mathbb{F}_{p^h}^*, \cdot) \cong (\mathbb{Z}_p \times \mathbb{Z}_{p^h-1}, +)$. Además, como p y $p^h - 1$ son primos relativos entonces por el isomorfismo del Teorema Chino del Residuo sabemos que $\mathbb{Z}_p \times \mathbb{Z}_{p^h-1} \cong \mathbb{Z}_{p(p^h-1)}$. Luego usando el Lema 1.0.7 obtenemos la construcción de Gómez y Trujillo [23] de un conjuntos B_{h+1} dado por

$$\mathcal{G} = \{p^h \log_\theta(\alpha + a) - (p^h - 1)a : a \in \mathbb{Z}_p\} \subseteq \mathbb{Z}_{p(p^h-1)}$$

a partir de un conjunto B_h . Aquí, θ es un elemento primitivo de $\mathbb{F}_{p^h}$.

Ejemplo 11. Del Ejemplo 10 tenemos que el conjunto

$$A(\theta) = \{\theta, \theta + 1, \theta + 2, \theta + 3, \theta + 4, \theta + 5, \theta + 6\}$$

es un conjunto B_2 en el grupo multiplicativo $\mathbb{F}_{49}^*$. Luego el conjunto

$$B = \{(0, \theta), (1, \theta + 1), (2, \theta + 2), (3, \theta + 3), (4, \theta + 4), (5, \theta + 5), (6, \theta + 6)\},$$

es un conjunto B_3 en el grupo $(\mathbb{F}_7, +) \times (\mathbb{F}_{49}^*, \cdot)$.

Además, usando el Teorema Chino del Residuo o la construcción de Gómez y Trujillo obtenemos que el conjunto

$$C = \{10, 49, 125, 131, 190, 319, 324\},$$

es un conjunto B_3 en el grupo aditivo $\mathbb{Z}_{336}$.

También, es posible obtener otra construcción de un conjunto B_{h+1} en dimensión dos en un grupo multiplicativo, usando la construcción tipo Bose-Chowla de conjuntos B_h ; sin embargo en esta construcción se pierde un elemento cuando el campo es finito. Presentamos a continuación la construcción general.

Teorema 5.3.2. *Sea $(F, +, \cdot)$ un campo, α un elemento algebraico de grado h sobre F en alguna extensión E de F , $E = F(\alpha)$. El conjunto*

$$A := \{(a, \alpha + a) : a \in F^*\}$$

es un conjunto B_{h+1} en $(F^, \cdot) \times (E^*, \cdot)$.*

La demostración de este resultado es análoga a la del Teorema 5.3.1. En el caso cuando el campo $F = \mathbb{F}_p$ el conjunto del teorema anterior tiene $p - 1$ elementos, en cambio la construcción de Gómez y Trujillo el conjunto tiene p elementos.

5.4. Construcción de conjunto B_{h+2} en dimensión tres.

Ahora presentamos la construcción de un conjunto B_{h+2} en dimensión tres usando como componentes los elementos de dos conjuntos conocidos, el

conjunto de Sidon $\mathcal{I}$ en dos dimensiones y el conjunto B_h tipo Bose-Chowla.

Teorema 5.4.1. *Sea $(F, +, \cdot)$ un campo, α un elemento algebraico de grado h sobre F en alguna extensión E de F , $E = F(\alpha)$. El conjunto*

$$A := \{(a, a, \alpha + a) : a \in F^*\}$$

es un conjunto B_{h+2} en $(F, +) \times (F^, \cdot) \times (E^*, \cdot)$.*

Demostración. Representamos por $\bullet$ la operación del grupo producto $(F, +) \times (F^*, \cdot) \times (E^*, \cdot)$. Supongamos que existe un elemento en $(F, +) \times (F^*, \cdot) \times (E^*, \cdot)$ que tiene dos representaciones como producto de $h+2$ elementos del conjunto A bajo la operación $\bullet$; es decir, existen $a_i, b_i \in F^*$ para $i = 1, \dots, h+2$ tales que

$$\begin{aligned} (a_1, a_1, \alpha + a_1) \bullet \cdots \bullet (a_{h+2}, a_{h+2}, \alpha + a_{h+2}) = \\ (b_1, b_1, \alpha + b_1) \bullet \cdots \bullet (b_{h+2}, b_{h+2}, \alpha + b_{h+2}). \end{aligned}$$

Esta igualdad implica

$$\sum_{i=1}^{h+2} a_i = \sum_{i=1}^{h+2} b_i \tag{5.6}$$

$$\prod_{i=1}^{h+2} a_i = \prod_{i=1}^{h+2} b_i \tag{5.7}$$

$$\prod_{i=1}^{h+2} (\alpha + a_i) = \prod_{i=1}^{h+2} (\alpha + b_i) \tag{5.8}$$

Si llamamos $a := \{a_1, \dots, a_{h+2}\}$ y $b := \{b_1, \dots, b_{h+2}\}$, tenemos en (5.8) que

$$\begin{aligned} \alpha^{h+2} + \sigma_1(a)\alpha^{h+1} + \cdots + \sigma_{h+1}(a)\alpha + \sigma_{h+2}(a) = \\ \alpha^{h+2} + \sigma_1(b)\alpha^{h+1} + \cdots + \sigma_{h+1}(b)\alpha + \sigma_{h+2}(b), \end{aligned} \tag{5.9}$$

donde σ_k representan las funciones simétricas elementales en las variables correspondientes.

Simplificamos términos iguales en (5.9) usando (5.6) y (5.7), obtenemos

$$\sigma_2(a)\alpha^h + \cdots + \sigma_{h+1}(a)\alpha = \sigma_2(b)\alpha^h + \cdots + \sigma_{h+1}(b)\alpha, \tag{5.10}$$

y como $\alpha \neq 0$ entonces

$$\sigma_2(a)\alpha^{h-1} + \cdots + \sigma_{h+1}(a) = \sigma_2(b)\alpha^{h-1} + \cdots + \sigma_{h+1}(b), \quad (5.11)$$

Así, α satisface un polinomio de grado $h-1$, pero α es algebraico de grado h sobre F entonces el polinomio debe ser el polinomio nulo, de esta manera

$$\begin{aligned} \sigma_2(a) &= \sigma_2(b) \\ &\vdots \\ \sigma_{h+1}(a) &= \sigma_{h+1}(b) \end{aligned}$$

las anteriores igualdades junto con (5.6) y (5.7) son las funciones simétricas elementales en las variables a y b , luego $a = b$, es decir

$$\{a_i : i = 1, \dots, h+2\} = \{b_j : j = 1, \dots, h+2\}.$$

En consecuencia

$$\{(a_i, a_i, \alpha + a_i) : i = 1, \dots, h+2\} = \{(b_j, b_j, \alpha + b_j) : j = 1, \dots, h+2\}.$$

□

En el caso cuando consideramos el campo finito $F = \mathbb{F}_p$, con p elementos y p primo, entonces $|A| = p-1$. Luego usando el Lema 1.0.7 tenemos que si $A = \{(a, a, \alpha + a) : a \in \mathbb{F}_p^*\}$ es un conjunto B_{h+2} en $(\mathbb{F}_p, +) \times (\mathbb{F}_p^*, \cdot) \times (\mathbb{F}_{p^h}^*, \cdot)$, entonces el conjunto

$$B = \{(a, \log_{\theta_1} a, \log_{\theta_2}(\alpha + a)) : a \in \mathbb{F}_p^*\}$$

es un conjunto B_{h+2} en $(\mathbb{Z}_p, +) \times (\mathbb{Z}_{p-1}, +) \times (\mathbb{Z}_{p^h-1}, +)$, donde θ_1 y θ_2 son elementos primitivos de $\mathbb{F}_p$ y $\mathbb{F}_{p^h}$, respectivamente.

Además, como p y $p^h - 1$ son primos relativos, por el isomorfismo del Teorema Chino del Residuo el conjunto

$$C = \{(\log_{\theta_1} a, p^h \log_{\theta_2}(\alpha + a) - (p^h - 1)a) : a \in \mathbb{Z}_p^*\}$$

es un conjunto B_{h+2} en $(\mathbb{Z}_{p-1} \times \mathbb{Z}_{p(p^h-1)}, +)$.

Ejemplo 12. Del Ejemplo 10 tenemos que el conjunto

$$A(\theta) = \{\theta, \theta + 1, \theta + 2, \theta + 3, \theta + 4, \theta + 5, \theta + 6\}$$

es un conjunto B_2 en el grupo multiplicativo $\mathbb{F}_{49}^*$. Además el conjunto

$$B = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), \}$$

es un conjunto B_2 en $(\mathbb{F}_7, +) \times (\mathbb{F}_7^*, \cdot)$.

Luego el conjunto

$$C = \{(1, 1, \theta+1), (2, 2, \theta+2), (3, 3, \theta+3), (4, 4, \theta+4), (5, 5, \theta+5), (6, 6, \theta+6), \}$$

es un conjunto B_4 en el grupo $(\mathbb{F}_7, +) \times (\mathbb{F}_7^*, \cdot) \times (\mathbb{F}_{49}^*, \cdot)$.

Además, usando el Teorema Chino del Residuo tenemos que el conjunto

$$D = \{(1, 190), (2, 342), (3, 10), (4, 319), (5, 131), (6, 125)\}$$

es un conjunto B_4 en el grupo producto $\mathbb{Z}_7^* \times \mathbb{Z}_{336}$.

Como $\mathbb{Z}_7^* = \langle 3 \rangle$ entonces el conjunto

$$E = \{(0, 190), (2, 342), (1, 10), (4, 319), (5, 131), (3, 125)\}$$

es un conjunto B_4 en el grupo aditivo $\mathbb{Z}_6 \times \mathbb{Z}_{336}$.

5.5. Construcción de conjunto B_{h+2} en $h + 1$ dimensiones

Dado el conjunto $A_h = \{(x, x^2, \dots, x^h) : x \in F\}$, en [36] se demuestra que A_h es un conjunto B_h en el grupo producto $(F^h, +)$, usando la construcción de Bose de un conjunto B_2 multiplicativo es posible construir un conjunto B_{h+2} en $h+1$ dimensiones. Presentamos dos casos particulares y luego damos la generalización.

Teorema 5.5.1. Sean F un campo, $\text{char}(F) \neq 2$, α un elemento algebraico de grado 2 sobre F en alguna extensión E de F . Entonces el conjunto

$$\mathcal{A} = \{(x, x^2, \alpha + x) : x \in F\}$$

es un conjunto B_4 en el grupo producto $(F, +) \times (F, +) \times (E^*, \cdot)$.

Demostración. Denotemos por $*$ la operación del grupo producto $(F, +) \times (F, +) \times (E^*, \cdot)$. Sean $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in F$ tales que

$$\begin{aligned} & (x_1, x_1^2, \alpha + x_1) * (x_2, x_2^2, \alpha + x_2) * (x_3, x_3^2, \alpha + x_3) * (x_4, x_4^2, \alpha + x_4) = \\ & (y_1, y_1^2, \alpha + y_1) * (y_2, y_2^2, \alpha + y_2) * (y_3, y_3^2, \alpha + y_3) * (y_4, y_4^2, \alpha + y_4) \end{aligned}$$

de esto se sigue que

$$x_1 + x_2 + x_3 + x_4 = y_1 + y_2 + y_3 + y_4 \quad (5.12)$$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = y_1^2 + y_2^2 + y_3^2 + y_4^2 \quad (5.13)$$

$$\begin{aligned} & (\alpha + x_1)(\alpha + x_2)(\alpha + x_3)(\alpha + x_4) = \\ & (\alpha + y_1)(\alpha + y_2)(\alpha + y_3)(\alpha + y_4) \end{aligned} \quad (5.14)$$

Si llamamos $x = \{x_1, x_2, x_3, x_4\}$ y $y = \{y_1, y_2, y_3, y_4\}$, podemos notar que (5.12) es equivalente a

$$\sigma_1(x) = \sigma_1(y).$$

Ahora bien, si elevamos al cuadrado (5.12) obtenemos que

$$\begin{aligned} & x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2(x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4) = \\ & y_1^2 + y_2^2 + y_3^2 + y_4^2 + 2(y_1y_2 + y_1y_3 + y_1y_4 + y_2y_3 + y_2y_4 + y_3y_4), \end{aligned}$$

luego usando la igualdad (5.13) y simplificando obtenemos

$$\begin{aligned} & x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = \\ & y_1y_2 + y_1y_3 + y_1y_4 + y_2y_3 + y_2y_4 + y_3y_4. \end{aligned} \quad (5.15)$$

De forma similar, notemos que (5.15) es equivalente a

$$\sigma_2(x) = \sigma_2(y).$$

Si desarrollemos ahora el producto de (5.14), tenemos

$$\alpha^4 + \sigma_1(x)\alpha^3 + \sigma_2(x)\alpha^2 + \sigma_3(x)\alpha + \sigma_4(x) =$$

$$\alpha^4 + \sigma_1(y)\alpha^3 + \sigma_2(y)\alpha^2 + \sigma_3(y)\alpha + \sigma_4(y), \quad (5.16)$$

luego, si usamos (5.12) y (5.15), al simplificar (5.16) obtenemos

$$\sigma_3(x)\alpha + \sigma_4(x) = \sigma_3(y)\alpha + \sigma_4(y),$$

lo que significa que α satisface el polinomio en la variable z de grado 1 con coeficientes en F

$$P(z) = [\sigma_3(x) - \sigma_3(y)]z + \sigma_4(x) - \sigma_4(y),$$

pero por hipótesis α es algebraico de grado 2 sobre F , entonces P debe ser el polinomio nulo, luego

$$\sigma_3(x) = \sigma_3(y) \quad (5.17)$$

$$\sigma_4(x) = \sigma_4(y). \quad (5.18)$$

En consecuencia, por las ecuaciones (5.12),(5.15),(5.17),(5.18) obtenemos que

$$\{x_1, x_2, x_3, x_4\} = \{y_1, y_2, y_3, y_4\}.$$

□

Teorema 5.5.2. Sean F un campo, $\text{char}(F) \neq 2, 3$, α un elemento algebraico de grado 2 sobre F en alguna extensión E de F . Entonces el conjunto

$$\mathcal{A} = \{(x, x^2, x^3, \alpha + x) : x \in F\}$$

es un conjunto B_5 en el grupo producto $(F, +) \times (F, +) \times (F, +) \times (E^*, \cdot)$.

Demostración. Denotemos por $*$ la operación del grupo producto $(F, +) \times (F, +) \times (E^*, \cdot)$. Sean $x_1, x_2, x_3, x_4, x_5, y_1, y_2, y_3, y_4, y_5 \in F$ tales que

$$\begin{aligned} (x_1, x_1^2, x_1^3, \alpha + x_1) * \cdots * (x_5, x_5^2, x_5^3, \alpha + x_5) = \\ (y_1, y_1^2, y_1^3, \alpha + y_1) * \cdots * (y_5, y_5^2, y_5^3, \alpha + y_5), \end{aligned}$$

de esto se sigue que

$$x_1 + x_2 + x_3 + x_4 + x_5 = y_1 + y_2 + y_3 + y_4 + y_5 \quad (5.19)$$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 = y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 \quad (5.20)$$

$$x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 = y_1^3 + y_2^3 + y_3^3 + y_4^3 + y_5^3 \quad (5.21)$$

$$\begin{aligned} (\alpha + x_1)(\alpha + x_2)(\alpha + x_3)(\alpha + x_4)(\alpha + x_5) = \\ (\alpha + y_1)(\alpha + y_2)(\alpha + y_3)(\alpha + y_4)(\alpha + y_5) \end{aligned} \quad (5.22)$$

Si llamamos $x = \{x_1, x_2, x_3, x_4, x_5\}$ y $y = \{y_1, y_2, y_3, y_4, y_5\}$, podemos notar que (5.19) es equivalente a

$$\sigma_1(x) = \sigma_1(y).$$

Si elevamos al cuadrado (5.19) obtenemos que

$$\sum_{i=1}^5 x_i^2 + 2\sigma_2(x) = \sum_{i=1}^5 y_i^2 + 2\sigma_2(y),$$

luego usando la igualdad (5.20) y simplificando obtenemos

$$\sigma_2(x) = \sigma_2(y). \quad (5.23)$$

Si elevamos al cubo (5.19) obtenemos que

$$\begin{aligned} \sum_{i=1}^5 x_i^3 + 3\sigma_1(x) \left(\sum_{i=1}^5 x_i^2 \right) + 6\sigma_3(x) - 3 \left(\sum_{i=1}^5 x_i^3 \right) = \\ \sum_{i=1}^5 y_i^3 + 3\sigma_1(y) \left(\sum_{i=1}^5 y_i^2 \right) + 6\sigma_3(y) - 3 \left(\sum_{i=1}^5 y_i^3 \right), \end{aligned}$$

y usando (5.19), (5.20), (5.21) obtenemos

$$\sigma_3(x) = \sigma_3(y). \quad (5.24)$$

Ahora, si hacemos la expansión del producto (5.22) obtenemos

$$\alpha^5 + \sum_{i=1}^5 \sigma_i(x) \alpha^{5-i} = \alpha^5 + \sum_{i=1}^5 \sigma_i(y) \alpha^{5-i}, \quad (5.25)$$

luego, si usamos (5.19), (5.23) y (5.24), al simplificar (5.25) obtenemos

$$\sigma_4(x)\alpha + \sigma_5(x) = \sigma_4(y)\alpha + \sigma_5(y),$$

lo que significa que α satisface el polinomio en la variable z de grado 1 con coeficientes en F

$$P(z) = [\sigma_4(x) - \sigma_4(y)]z + \sigma_5(x) - \sigma_5(y),$$

pero por hipótesis α es algebraico de grado 2 sobre F , entonces P debe ser el polinomio nulo, luego

$$\sigma_4(x) = \sigma_4(y) \tag{5.26}$$

$$\sigma_5(x) = \sigma_5(y). \tag{5.27}$$

En consecuencia, por las ecuaciones (5.19),(5.23),(5.24),(5.26) y (5.27) obtenemos que

$$\{x_1, x_2, x_3, x_4, x_5\} = \{y_1, y_2, y_3, y_4, y_5\}.$$

□

Ahora presentamos el caso general de un conjunto B_{h+2} que se obtiene a partir de un conjunto B_h formado por las potencias de un elemento x en un campo F y un conjunto B_2 tipo Bose multiplicativo.

Teorema 5.5.3. *Sean F un campo, $\text{char}(F) \neq 2, 3, \dots, h-2$, α un elemento algebraico de grado 2 sobre F en alguna extensión E de F y $h \geq 1$ un entero. Entonces el conjunto*

$$\mathcal{A} = \{(x, x^2, \dots, x^h, \alpha + x) : x \in F\}$$

es un conjunto B_{h+2} en el grupo producto $(F^h, +) \times (E^, \cdot)$.*

Aquí, $(F^h, +)$ significa el grupo producto de h copias del grupo $(F, +)$.

Demostración. Llamemos $*$ la operación del grupo producto $(F^h, +) \times (E^*, \cdot)$. Sean $x = \{x_1, \dots, x_{h+2}\}$, $y = \{y_1, \dots, y_{h+2}\}$ subconjuntos de F tales que

$$\begin{aligned} (x_1, x_1^2, \dots, x_1^h, \alpha + x_1) * \dots * (x_{h+2}, x_{h+2}^2, \dots, x_{h+2}^h, \alpha + x_{h+2}) = \\ (y_1, y_1^2, \dots, y_1^h, \alpha + y_1) * \dots * (y_{h+2}, y_{h+2}^2, \dots, y_{h+2}^h, \alpha + y_{h+2}) \end{aligned}$$

Esto implica que

$$x_1 + x_2 + \cdots + x_{h+2} = y_1 + y_2 + \cdots + y_{h+2} \quad (5.28)$$

$$x_1^2 + x_2^2 + \cdots + x_{h+2}^2 = y_1^2 + y_2^2 + \cdots + y_{h+2}^2 \quad (5.29)$$

$\vdots$

$$x_1^h + x_2^h + \cdots + x_{h+2}^h = y_1^h + y_2^h + \cdots + y_{h+2}^h \quad (5.30)$$

$$(\alpha + x_1)(\alpha + x_2) \cdots (\alpha + x_{h+2}) = (\alpha + y_1)(\alpha + y_2) \cdots (\alpha + y_{h+2}) \quad (5.31)$$

Las primeras h igualdades, por las identidades de Newton-Girard, implican la igualdad de las funciones simétricas elementales

$$\sigma_k(x_1, x_2, \dots, x_{h+2}) = \sigma_k(y_1, y_2, \dots, y_{h+2}), \quad (5.32)$$

para $1 \leq k \leq h$.

Ahora, si desarrollamos los productos de (5.31) obtenemos

$$\alpha^{h+2} + \sum_{i=1}^{h+2} \sigma_i(x) \alpha^{h+2-i} = \alpha^{h+2} + \sum_{i=1}^{h+2} \sigma_i(y) \alpha^{h+2-i}, \quad (5.33)$$

luego usando las igualdades de (5.32) para $1 \leq k \leq h$ y simplificando obtenemos que α satisface un polinomio de grado 1, pero como α es algebraico de grado 2 sobre F entonces el polinomio debe ser el polinomio nulo, esto implica que

$$\sigma_k(x_1, x_2, \dots, x_{h+2}) = \sigma_k(y_1, y_2, \dots, y_{h+2}), \quad (5.34)$$

para $h+1 \leq k \leq h+2$. En consecuencia, $\{x_1, \dots, x_{h+2}\} = \{y_1, \dots, y_{h+2}\}$ y por lo tanto

$$\begin{aligned} \{(x_i, x_i^2, \dots, x_i^h, \alpha + x_i) : i = 1 \dots, h+2\} = \\ \{(y_i, y_i^2, \dots, y_i^h, \alpha + y_i) : i = 1 \dots, h+2\}. \end{aligned}$$

□

Ejemplo 13. Del Ejemplo 10 tenemos que el conjunto

$$A(\theta) = \{\theta, \theta + 1, \theta + 2, \theta + 3, \theta + 4, \theta + 5, \theta + 6\}$$

es un conjunto B_2 en el grupo multiplicativo $\mathbb{F}_{49}^*$.

Así el conjunto

$$B = \{(0, 0, 0, 0, \theta), (1, 1, 1, 1, \theta + 1), (2, 4, 1, 2, \theta + 2), (3, 2, 6, 4, \theta + 3), \\ (4, 2, 1, 4, \theta + 4), (5, 4, 6, 2, \theta + 5), (6, 1, 6, 1, \theta + 6)\}$$

es un conjunto B_6 en $(\mathbb{F}_7^4, +) \times (\mathbb{F}_{49}^*, \cdot)$ con 7 elementos.

5.6. Consecuencias de las construcciones para la función f_h .

Los conjuntos B_h son más difíciles de manipular ya que no se pueden expresar en términos de diferencias como sí se hace en los conjuntos de Sidon. Por tal razón, hasta el momento, se desconoce el comportamiento asintótico de la función $F_h(n)$, para $h \geq 3$ incluso para el caso de la función $f_h(G)$, donde G un grupo abeliano finito arbitrario.

Las cotas superiores triviales para las funciones $F_h(n)$ y $f_h(G)$ son las siguientes:

$$F_h(n) \leq (h \cdot h!)^{1/h} n^{1/h}, \quad (5.35)$$

$$f_h(G) \leq (h!)^{1/h} |G|^{1/h}. \quad (5.36)$$

Algunos investigadores han logrado mejorar estas cotas, tanto en casos generales como en casos particulares para ciertos valores de h , por ejemplo:

- Lindström [29] demuestra que $F_4(n) \leq (8n)^{1/4}(1 + o(1))$.
- Ben Green [25] demuestra que $F_4(n) \leq (7n)^{1/4}(1 + o(1))$, mejorando el resultado Lindström.

- Para $h = 2r$ ($r \geq 1$) Jia [27] demostró que

$$F_{2r}(n) \leq (r \cdot r!^2 n)^{1/(2r)}(1 + o(1)).$$

Para $h = 2r - 1$ ($r \geq 1$), Chen [12] y Graham [24] demostraron (independientemente) que

$$F_{2r-1}(n) \leq (r!^2 n)^{1/(2r-1)}(1 + o(1)).$$

- Bravo-Ruiz-Trujillo [5] demuestran para G un grupo conmutativo finito:

$$\begin{aligned} f_3(G) &\leq \sqrt[3]{2|G|} + \frac{1}{3}, \\ f_4(G) &\leq \sqrt{2} \sqrt[4]{|G| - 1} + 1, \\ f_{2s}(G) &\leq (s!)^{1/s} |G|^{1/2s} + 2s - 1, \\ f_{2s-1}(G) &\leq (s!(s-1)!)^{1/(2s-1)} |G|^{1/(2s-1)} + 2s - 2. \end{aligned}$$

Por otro lado, como consecuencia de las construcciones conocidas y mencionadas en las secciones anteriores de este capítulo se tiene que

- Bose-Chowla: $f_h(\mathbb{Z}_{q^h-1}) \geq q$.
- Singer Generalizada: $f_h(\mathbb{Z}_{q^h+\dots+q+1}) \geq q + 1$.
- Gómez-Trujillo: $f_{h+1}((\mathbb{F}_q, +) \times (\mathbb{F}_{q^h}^*, \cdot)) \geq q$.

Nuestras construcciones, proporcionan las siguientes cotas inferiores:

- Si $|F|$ es finito, para α un elemento algebraico de grado h sobre F en alguna extensión E de F se tiene

$$f_{h+1}((F^*, \cdot) \times (E^*, \cdot)) \geq |F| - 1.$$

- Si $|F|$ es finito, para α un elemento algebraico de grado h sobre F en alguna extensión E de F se tiene

$$f_{h+2}((F, +) \times (F^*, \cdot) \times (E^*, \cdot)) \geq |F| - 1.$$

- Si $|F|$ es finito de característica diferente de $2, 3, \dots, h-2$, para α un elemento algebraico de grado 2 sobre F en alguna extensión E de F se tiene

$$f_{h+2}((F^h, +) \times (E^*, \cdot)) \geq |F|.$$

Destacamos que la última construcción que obtuvimos nos permite obtener familias de conjuntos B_h que son óptimamente densos cuando $|G|$ tiende a infinito; es decir, si A es un conjunto B_{h+2} en $G = (F^h, +) \times (E^*, \cdot)$ obtenemos que

$$|A| = |F| \gg (|F|^h(|F|^2 - 1))^{h+2} = |G|^{h+2}.$$

Capítulo 6

Resultados obtenidos y trabajos futuros

En este trabajo realizamos un amplio recorrido por un tema importante de Teoría de Números Aditiva, conocido como conjuntos de Sidon. Aunque el principal problema de estudio sobre conjuntos de Sidon es cuando se consideran subconjuntos de los enteros, el tema fundamental de este trabajo son los conjuntos de Sidon en dos dimensiones, donde no necesariamente los elementos son números enteros. Además la definición de conjunto de Sidon es posible generalizarla a conjuntos $B_h[g]$ sobre cualquier grupo abeliano, tema que también abordamos en este trabajo para el caso $g = 1$.

Los aportes de nuestro trabajo son los siguientes:

- Utilizamos la Energía Aditiva y sus propiedades para obtener buenas cotas de funciones extremas relacionadas con problemas de características aditivas y combinatorias, estos problemas han sido objeto de trabajo en varios proyectos de investigación del grupo ALTENUA. Para efectos de completitud del trabajo incluimos algunos ejemplos del uso de energía aditiva en problemas relacionados con conjuntos $B_2^-[g]$ y secuencias sonar; sin embargo nuestro aporte en esta sección es en el caso de conjuntos de Sidon d -dimensionales, $d > 1$, Lindström [10, 30] obtiene una cota superior para la función $F_2^d(n)$ pero no explícitamente, nosotros con el uso de la energía aditiva

logramos obtener las constantes explícitas de dicha cota, para d entero par (Teorema 2.5.1). Para conjuntos de Sidon en dos dimensiones, $d = 2$, con un cambio en el parámetro logramos obtener mejores constantes explícitas (Desigualdad 2.25) que las del Teorema 2.5.1. Obtener las constantes explícitas es importante, porque si las constantes son pequeñas es posible acercarse más rápido al valor exacto de la función dada, y esto tiene mucho valor sobre todo en aplicaciones a otros campos; la cota de Lindström garantiza la existencia de una constante pero al no ser explícita puede tener un tamaño muy grande.

- Presentamos tres construcciones de conjuntos de Sidon en dos dimensiones, $\mathcal{C}$, $\mathcal{I}$, $\mathcal{I}_a$, donde los grupos ambiente de cada conjunto son el producto directo de los grupos provenientes de un campo $(F, +, \cdot)$, cabe destacar que estas construcciones son generales y válidas para un campo arbitrario; como caso particular, por medio de un isomorfismo, se obtienen las construcciones de secuencias sonar: cuadrática, Welch y Golomb-Lempel. Además, analizamos las propiedades que satisfacen los conjuntos $\mathcal{C}$, $\mathcal{I}$, $\mathcal{I}_a$ y encontramos algunas propiedades que no se conocían, por ejemplo, la caracterización de los conjuntos suma y diferencia, también identificamos que al unirle un conjunto adecuado a $\mathcal{C}$ o $\mathcal{I}$, éstos forman bases de orden dos para su grupo ambiente respectivo (Sección 4.1). Estos resultados aún no están publicados, pero ya tenemos un preprint [8].
- Otro aporte en este trabajo, es el Teorema 4.3.1 que permite construir secuencias sonar a partir de conjuntos de Sidon en una dimensión, resultado publicado en [37], como casos particulares se obtienen las construcciones de secuencias Sonar de tamaños específicos (Corolarios 4.3.2, 4.3.3, 4.3.4) a partir de las propiedades que satisfacen los conjuntos de Sidon tipo Bose y Ruzsa, las cuales las estudiamos en detalle en el Capítulo 3.
- Igualmente, el estudio en detalle de las construcciones conocidas de conjuntos de Sidon en una dimensión nos permitió obtener nuevas construcciones de conjuntos B_h en d dimensiones, usando un campo arbitrario $(F, +, \cdot)$; por ejemplo las construcciones de conjuntos B_{h+1} en los grupos $(F, +) \times (E^*, \cdot)$, $(F^*, \cdot) \times (E^*, \cdot)$, y las construcciones de conjuntos B_{h+2} en los grupos $(F, +) \times (F^*, \cdot) \times (E^*, \cdot)$ y $(F^h, +) \times (E^*, \cdot)$ (Teoremas 5.3.1, 5.3.2, 5.4.1, 5.5.3).

Cabe destacar que la última construcción (Teorema 5.5.3) de un conjunto B_{h+2} es una construcción óptimamente densa. Estos resultados tampoco están publicados, pero ya tenemos un preprint [9].

Teniendo como base los logros alcanzados en esta tesis, como trabajos futuros queremos:

- Hacer un estudio más amplio de la energía aditiva, sus generalizaciones y aplicaciones a otros problemas.
- Como en el caso de conjuntos de Sidon en dos dimensiones logramos hacer una caracterización del conjunto suma, queremos estudiar la caracterización del conjunto suma de las construcciones tipo Singer, Bose y Ruzsa en una dimensión.
- Estudiar bases aditivas y conjuntos de Sidon.
- Hacer un estudio de las secuencias sonar y sus propiedades para así comparar las nuevas secuencias sonar con las existentes y determinar si estas construcciones generan secuencias sonar distintas, ya que algunas coinciden en sus tamaños.
- Estudiar de manera más amplia las aplicaciones que tienen las secuencias sonar en otros campos; este aspecto será el objetivo de nuestro proyecto de investigación aprobado en la convocatoria para Ciencias Básicas # 712 de 2015 por Colciencias, titulado: *Aplicaciones a Teoría de la Información y Comunicaciones de los conjuntos de Sidon y sus generalizaciones*, con código 50560.

Bibliografía

- [1] M. D. Atkinson, N. Santoro and J. Urrutia (1986). *Integer sets with distinct sums and differences and carrier frequency assignments for nonlinear repeaters*. IEEE Transactions on Communications, Vol.COM-34, 614-617.
- [2] W.C Babcock (1953). *Intermodulation interference in radio systems*, Bell Systems Technical Journal, vol 31, 63-73.
- [3] R. C. Bose (1942). *An affine analogue of Singer's theorem*, J. Indian Math. Soc. (N.S.) 6 , 1-15.
- [4] R. C. Bose and S. Chowla (1962/1963). *Theorems in the additive theory of numbers*, Comment. Math. Helv. 37, 141-147.
- [5] J. J. Bravo, D. Ruíz and C. A. Trujillo (2012), *Cardinality of sets associated to B_3 and B_4 sets*, Revista Colombiana de Matemáticas, Volumen 46 -1, 27-37.
- [6] Y. Caicedo, J. Gómez and C. A. Trujillo (2015). *$B_h[g]$ modular sets from B_h modular sets*. JP Journal of Algebra, Number Theory and Applications. Vol. 37 Number 1. 1-19.
- [7] Y. Caicedo, C. A. Martos and C. A. Trujillo (2015). *g -Golomb Rulers*. Revista Integración, Escuela de Matemáticas, Universidad Industrial de Santander, Vol. 33, N° 2, 161-172.
- [8] Y. Caicedo, C. A. Gómez y C.A. Trujillo. *Conjuntos de Sidon obtenidos a partir de los grupos de un campo*. Preprint.

BIBLIOGRAFÍA

- [9] Y. Caicedo, C. A. Gómez y C. A. Trujillo. *Construcción de conjuntos B_h en varias dimensiones*. Preprint.
- [10] J. Cilleruelo (2010). *Sidon sets in $\mathbb{N}^d$* . Journal of Combinatorial Theory Series A, Vol. 117, Issue 7, 857-871.
- [11] J. P. Costas (1984). *A study of a class of detection waveforms having nearly ideal range-doppler ambiguity properties*, Proceedings of the IEEE, Vol. 72, No. 8, 996-1009.
- [12] S. Chen (1994), *On the size of finite Sidon sequences*, Proc. Amer. Math. Soc. 121, N° 2, 353-356.
- [13] A. Dimitromanolakis (2002). *Analysis of the Golomb Ruler and the Sidon Set Problems, and Determination of Large, Near-Optimal Golomb Rulers*. Diploma thesis, Department of Electronic and Computer Engineering, Technical University of Crete.
- [14] Distributed.net. Project statistics. Accessed August 2009. URL <http://stats.distributed.net/>
- [15] K. Drakakis (2006). *A review of Costas arrays*, Journal of Applied Mathematics, Volume 2006.
- [16] P. Erdős, R. I. Graham, I. Ruzsa and H. Taylor (1992). *Bounds for arrays of dots with distinct slopes or lengths*, Combinatorica, Volume 12, Issue 1, 39-44.
- [17] P. Erdős and P. Turán (1941). *On a problem of Sidon in additive number theory and on some related problems*, Journal of the London Mathematical Society, Volume s1-16 Issue 4, 857-871.
- [18] P. Fernández (1997). *La convergencia de las series de Fourier y su conexión con la cristalografía*. Tesis Doctoral, Universidad Autónoma de Madrid.
- [19] R.M. Gagliardi, J. Robbins and H. Taylor (1987), *Acquisition Sequences in PPM Communications*, IEEE Transactions on Information Theory, Volume 33, Issue 5, 738 - 744.
- [20] S. W. Golomb (1984). *Algebraic constructions for Costas arrays*, Journal of Combinatorial Theory, Series A, Volume 37, Issue 1, 13-21.

BIBLIOGRAFÍA

- [21] S. W. Golomb and H. Taylor (1984). *Constructions and properties of Costas arrays*, Proceedings of the IEEE, vol. 72, No. 9, 1143-1163.
- [22] S. Golomb and H. Taylor (1982). *Two-dimensional synchronization patterns for minimum ambiguity*, IEEE Trans. on Information Theory, vol IT-28, Issue 4, 600-604.
- [23] C. A. Gómez y C. A. Trujillo (2011). *Una nueva construcción de Conjuntos B_h modulares*. Matemáticas Enseñanza Universitaria (ERM), Vol. XIX, N° 1, 53-62.
- [24] S. W. Graham (1996), *Bh Sequences*, Analytic Number Theory, 1 (Allerton Park, IL, 1995), 431-449. Progress in Mathematics 138, Birkhäuser, Boston MA.
- [25] B. Green (2001), *The number of squares and $B_h[g]$ sets*, Acta Arith. 100, 365-390.
- [26] S. Haykin (2009). *Communication Systems*, 5th ed. New York, Wiley, 440 p.
- [27] X. D. Jia (1993), *On finite Sidon sequences*, Journal Number Theory 44, 84-92.
- [28] B. Lindström (1969). *An inequality for B_2 -sequences*, Journal of Combinatorial Theory Volume 6, Issue 2, 211-212.
- [29] B. Lindström (1969), *A remark on B_4 -sequences*, Journal Combinatorial Theory 7, 276-277.
- [30] B. Lindström (1972). *On B_2 -sequences of vectors*, Journal of Number Theory, Volume 4, Issue 3, 261-265.
- [31] C. Martos (2015). *Reglas g -Golomb*, Tesis Maestría en Ciencias Matemáticas, Universidad del Cauca, 83 p.
- [32] A. M. Mian and S. D. Chowla (1944). *On the B_2 -Sequences of Sidon*, Proc. Nat. Acad. Sci. India Sect. A. 14, 3-4.
- [33] O. Moreno, R. A. Games and H. Taylor (1993). *Sonar Sequences from Costas Arrays and the Best Know Sonar Sequences with up to 100 Symbols*, IEEE Transactions on Information Theory, Vol 39, N° 6.

BIBLIOGRAFÍA

- [34] O. Moreno, D. Bollman and L.Yuchun (2003), *Exhaustive search for Costas-type sequences for multi-target recognition*, Proceedings of the The Ninth IEEE Workshop on Future Trends of Distributed Computing Systems (FTDCS'03), 354 - 358.
- [35] J. P. Robinson (1985). *Golomb Rectangles*, IEEE Transactions on Information Theory, IT-31, 781-787.
- [36] D. Ruiz and C. Trujillo (2013). *Construction of $B_h[g]$ sets in product of groups*. arXiv:1302.0071v1 [math.NT] 1.
- [37] D. Ruiz, C. Trujillo and Y. Caicedo (2014). *New Constructions of Sonar Sequences*. IJBAS: International Journal of Basic & Applied Sciences. Vol. 14 Issue 01, 12-16.
- [38] I. Ruzsa (1993). *Solving a linear equation in a set of integers I*. Acta Arithmetica. Vol. LXV, N° 3, 259-282.
- [39] J. Singer (1938). *A theorem infinite projective geometry and some applications to number theory*, Transactions of the American Mathematical Society, Vol. 43, N° 3, 377-385.
- [40] T. Tao and V.H. Vu (2006). *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics 105, Cambridge University Press, Cambridge.
- [41] C. A. Trujillo, G. García y J. M. Velásquez (2004). $B_2^-[g]$ *Finite Sets*, JP Journal of Algebra, Number Theory and Applications, Vol. 4, No. 3, 593-604.
- [42] C. A. Trujillo (1998). *Sucesiones de Sidon*, Tesis Doctoral, Universidad Politécnica de Madrid, 92 p.
- [43] C. A. Trujillo, D. Ruiz, J. Osorio y C. Urbano (2014). *Secuencias Sonar y conjuntos de Sidon*. Revista de Ciencias. Universidad del Valle, 33-42.

Anexo

Este trabajo de tesis doctoral está adscrito al proyecto de investigación aprobado por Colciencias y titulado *Construcción de conjuntos $B_h[g]$, propiedad de Midy y algunas aplicaciones*, con código 110356935047, del grupo de investigación ALTENUA.

Mencionamos a continuación las ponencias, los artículos publicados y próximos a publicar, realizados durante el desarrollo de este trabajo de investigación.

PONENCIAS:

- XX Congreso Colombiano de Matemáticas. Universidad Nacional de Colombia sede Manizales. Manizales (Caldas) 21-24 de Julio de 2015. Ponencias presentadas:
 - Conjuntos de Sidon obtenidos a partir de los grupos de un campo finito. Autores: Yadira Caicedo y Carlos A. Trujillo.
 - Construcción de conjuntos $B_h[g]$ modulares a partir de conjuntos B_h modulares vía homomorfismos. Autores: Yadira Caicedo, Jhonny Gómez y Carlos A. Trujillo.
- V Encuentro Nacional de Matemáticas y Estadística. Universidad del Tolima. Ibagué (Tolima), 6-8 de Mayo de 2015. Ponencia presentada: Conjuntos $B_h[g]$ modulares a partir de conjuntos B_h modulares. Autores: Yadira Caicedo y Carlos A. Trujillo.
- II Seminario Regional de Teoría de Números- ALTENUA. Universidad del Cauca. Popayán (Cauca), 25-29 de marzo de 2015. Trabajos presentados:

-
- Curso de Construcción de conjuntos $B_h[g]$. Autores: Yadira Caicedo y Carlos A. Trujillo.
 - Ponencia: Conjuntos de Sidon en dimensión dos. Autor: Yadira Caicedo
 - VI Encuentro de Álgebra, Teoría de Números, Combinatoria y Aplicaciones (ALTENCOA 6-2014). Universidad de Nariño. Pasto (Nariño), 11- 15 de Agosto de 2014. Trabajo presentado: Nuevas construcciones de secuencias sonar y sus propiedades. Autores: Yadira Caicedo y Carlos A. Trujillo.
 - International Conference on Applied Mathematics and Informatics. San Andrés Islas, 24-29 de Noviembre de 2013. Trabajo presentado: New Constructions of Sonar Sequences. Autores: Yadira Caicedo y Carlos A. Trujillo.
 - XIX Congreso Colombiano de Matemáticas. Universidad del Norte. Barranquilla (Atlántico), 15-19 de Julio de 2013. Trabajos presentados:
 - Energía Aditiva y Conjuntos $B_2^-[g]$. Autores: Yadira Caicedo y Carlos A. Trujillo.
 - Cota Inferior para la longitud de una regla Golomb. Autores: Yadira Caicedo, Carlos Martos y Carlos A. Trujillo.