CONJUNTOS DE SIDON FINITOS

Jairo Humberto Villamil Hernández

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga
2016

CONJUNTOS DE SIDON FINITOS

Autor
Jairo Humberto Villamil Hernández

Trabajo de grado como requisito parcial para optar el título de
Licenciado en Matemáticas

Director
Carlos Arturo Rodriguez Palma
Matemático, MSc

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga
2016

Agradecimientos

- Agradezco a Dios por darme la fuerza para sobrellevar cada dificultad y permitirme culminar mis estudios universitarios satisfactoriamente (*¡Sé fuerte y valiente! No temas ni te acobardes, porque el SEÑOR tu Dios estará contigo dondequiera que vayas*, Josué 1:9).

- Agradezco sinceramente al profesor Carlos Arturo Rodriguez Palma por haber aceptado ser mi director de proyecto. Por su dedicación, su paciencia y esfuerzo en la realización de este trabajo.

- Sin duda alguna agradezco a mi madre Alba Yaneth por ser mi apoyo incondicional, por su infinito amor y cariño y por ser mi guia a lo largo de mi vida, Dios te bendiga grandemente madre hermosa.

- Agradezco a bienestar universitario, especialmente a Don Jaime Almeyda y a las señoras de comedores con las cuales compartí momentos muy especiales.

- Agradezco a todas las personas con las cuales compartí durante mi carrera, se que de estas personas obtuve experiencias buenas como también malas experiencias, pero de estas experiencias aprendí mucho, a todas aquellas personas Dios las bendiga, siempre las recordaré. (*no es quien seas en el interior tus actos son los que te definen*).

Índice General

Índice de Cuadros

Índice de Figuras

RESUMEN

TITULO: CONJUNTOS DE SIDON FINITOS*

AUTOR: JAIRO HUMBERTO VILLAMIL HERNÁNDEZ**

PALABRAS CLAVE: Conjuntos de Sidon, Teoría de Números Aditiva, Secuencias Sonar.

DESCRIPCIÓN:

Un conjunto de enteros A es llamado un Conjunto de Sidon si todas las sumas $a+a'$, con $a \leq a', a, a' \in A$ son diferentes; de manera similar un conjunto A es un Conjunto de Sidon si todas la diferencias $a-a'$ con $a \neq a'$, $a, a' \in A$ son diferentes. Un problema interesante relacionado con estos conjuntos es el siguiente: ¿Cual es el mayor cardinal que un conjunto de Sidon puede tener en el intervalo $[1,n]$? Para darle respuesta esta pregunta definimos la siguiente función: $F_2(n) = \text{máx}\{|A| : A \subset [1,n], A \text{ es de Sidon}\}$.

De esta manera, la función $F_2(n)$ se define como el máximo número de elementos que pueden seleccionarse de $[1,n]$ de tal forma que constituyan un Conjunto de Sidon. En ese sentido se estudiaremos el comportamiento de esta función mediante dos tipos de Conjuntos de Sidon, en dimensión uno y dimensión dos. Los Conjuntos de Sidon en dimensión uno junto con algunas técnicas de conteo, nos proporcionaran las mejores cotas superiores para esta función, por otro lado mediante la construcción de Conjuntos de Sidon en dimensión dos encontraremos una cota inferior óptima para dicha función.

A demás observaremos el papel que tiene los Conjuntos de Sidon en dimensión dos para el modelamiento de algunas aplicaciones en el área de las telecomunicaciones, particularmente las secuencias Sonar. El objetivo de este trabajo es dar a conocer algunas definiciones y propiedades básicas de los Conjuntos de Sidon Finitos permitirán resolver y comprender los problemas ya antes mencionados.

*Tesis.

**Facultad de Ciencias. Escuela de Matemáticas. Director: Carlos Arturo Rodriguez Palma. MSc. en Matemáticas.

ABSTRACT

TITLE: SIDON'S FINITE SETS*

AUTHOR: JAIRO HUMBERTO VILLAMIL HERNÁNDEZ**

KEYWORDS: Sidon's finite sets, Additive number theory, Sonar sequences.

DESCRIPTION:

A set A of integers is called a Sidon's set if all sums $a+a'$, with $a \leq a', a, a' \in A$ are different; similarly a set A of integers is called a Sidon's set if all differences $a-a'$, with $a \neq a', a, a' \in A$ are distinct. An interesting problem regarding these sets is as follows: What is the greatest cardinal a set of Sidon may have in the range $[1,n]$? To give you answer this question we define the following function: $F_2(n) = \max\{|A| : A \subset [1,n], A \text{es de Sidon}\}$.

Thus, the $F_2(n)$ function is defined as the maximum number of elements that can be selected from $[1,n]$ so as to constitute a Sidon's set. In this sense the behavior of this function study using two types of Sidon's sets in dimension one and two dimensions. Sidon's sets in dimension one along with some counting techniques, provide us with the best upper bounds for this function. on the other hand by building Sidon's sets in two dimensions find an optimal lower bound for the function.

Observe the role that Sidon's sets in dimension two for the modeling of some applications in the area of telecommunications, particularly Sonar sequences. Precisely the aim of this work is aimed at knowing some definitions and basic properties Sidon's finite sets that will allow us to solve and understand the problems already mentioned above.

*Thesis.

**Science Faculty. School of Mathematics. Director: Carlos Arturo Rodriguez Palma. MSc. in mathematics.

INTRODUCCIÓN

El interés del hombre por los números es tan remoto como la misma civilización, son varios los pueblos de la antigüedad que se motivaron por los números, ya sea bien por razones prácticas inmediatas o por su relación con la astronomía y el cómputo del tiempo. La primera orientación científica al estudio de los números enteros, es decir, el origen de la Teoría de números, se atribuye a los griegos, precisamente fueron ellos los primeros en desarrollar una teoría basada en números, tal es el caso de Diofanto de Alejandría que en el siglo III d.c. escribió trece libros (siete de los cuales se han perdido) dedicados a la resolución de ecuaciones algebraicas y en los cuales se intentaba dar métodos para encontrar sus soluciones enteras o racionales. Después de Diofanto no hubo muchos progresos en Teoría de números hasta el siglo XVII, periodo en el cual esta teoria renace gracias en gran parte a los trabajos hechos por Pierre de Fermat. Poco tiempo después de Fermat, los nombres de Euler (1707-1783), Lagrange (1763-1813), Legendre (1752-1833), Gauss (1777-1855) y Dirichlet (1805-1859) fueron muy importantes en el posterior desarrollo de la Teoría números [1]. Así pues desde los tiempos de Gauss, ha existido un desarrollo enorme de esta área de las matemáticas en varias direcciones, enfocándose especialmente en el estudio de las propiedades y relaciones de los números enteros, o de subconjuntos de ellos que satisfacen ciertas propiedades especiales.

Según los problemas que se intentan resolver y los métodos empleados para ello, la teoría de números se subdivide en diversas ramas: Teoría analítica de números, teoría algebraica de números, teoría combinatoria de números y teoría de números aditiva; esta última de nuestro interés particular. La teoría de números aditiva estudia subconjuntos de números enteros y su comportamiento bajo la adición, mediante dos tipos de problemas: *Problemas directos* y *problemas inversos*. Un problema directo en teoría aditiva de números es aquel en el que se trata de determinar la estructura y propiedades del conjunto hA, es decir, el conjunto de todas las sumas de elementos de un conjunto dado A. El segundo

tipo de problema es aquel en el que se intenta deducir propiedades del conjunto A a partir de algunas propiedades que se derivan del conjunto suma hA. De esta manera, bajo la perspectiva de la teoría de números aditiva consideremos el siguiente problema: Dado el conjunto $X = \{1,\ 2, \ldots,\ 50\}$, se quiere construir un subconjunto $A \subseteq X$ con la propiedad de que las diferencias de cada par de elementos distintos de A sean distintas. Por ejemplo, el siguiente conjunto $A = \{1,\ 2,\ 4,\ 8\}$ cumple con dicha propiedad. Esto se puede evidenciar en la siguiente tabla de diferencias de A.

-	1	2	4	8
1	0	-1	-3	-7
2	1	0	-2	-6
4	3	2	0	-4
8	7	6	4	0

Observe que aparecen varias preguntas alrededor de este problema: ¿El conjunto $A \subseteq X$ es el de mayor tamaño que satisface la propiedad? Es fácil ver que no es así, pues el conjunto $B = \{1,\ 2,\ 5,\ 10,\ 16,\ 23,\ 33,\ 35\} \subseteq X$ cumple también la propiedad antes mencionada, esto se puede ver en la siguiente tabla de la diferencias para el conjunto B.

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

Note que construir este tipo de conjuntos no presenta mayor dificultad si se hace con unos pocos elementos, pero quizá si se quiere ir añadiendo más elementos a la colección lo más probable es que nos encontremos con mayor dificultad para hacerlo, en ese sentido surge de manera natural la siguiente pregunta ¿Cuál es el conjunto de mayor tamaño contenido en $X = \{1,\ 2, \ldots,\ 50\}$ con la propiedad de que todas las diferencias de dos elementos distintos del conjunto sean distintas? más aún,

si generalizamos este problema la pregunta seria ¿Cuál es el conjunto de mayor tamaño contenido en el intervalo $[1,\ n]$ [1] o en un grupo aditivo finito dado, en el que todas las diferencias de dos elementos distintos del conjunto sean distintas? Esta última pregunta fue planteada por Simón Sidon a Paul Erdős en el año 1932, aunque el interés de Sidon por estos conjuntos debían a razones del análisis de Furier, el problema llamó la atención de Erdös por su vertiente aritmética y combinatoria. Fue el propio Erdös quien bautizó a estos conjuntos con el nombre de *Conjuntos de Sidon.*

Desde el mismo año en que se planteó el problema se le han dado respuestas parciales gracias a los trabajos realizados por varios expertos en matemáticas, algunas de estas se deben a Ruzsa, Bose, Lidnström, Erdős y Turan, entre otros [13], los cuales encontraron cotas superiores óptimas para estos conjuntos, en ese sentido algunas de estas respuestas serán el punto central del desarrollo de esta monografía.

El documento está organizado en tres capítulos. En el primer estarán aquellos conceptos básicos que se tuvieron en cuenta para el desarrollo y la comprensión de este trabajo. En el capítulo 2, estudiaremos los conjuntos de Sidon en dimensión uno, en particular mostraremos algunos argumentos de conteo que nos permitirán obtener las mejores cotas superiores conocidas para estos conjuntos. En el capitulo 3 estudiaremos algunas construcciones de Conjuntos de Sidon en dimensión dos las cuales proveen de una cota inferior para los conjuntos de Sidon en dimensión uno; a demás, se presentaran algunas aplicaciones que tienen los Conjuntos de Sidon en dimensión dos en el área de las telecomunicaciones y por ultimo veremos las conclusiones obtenidas de este trabajo.

[1] *A lo largo de este trabajo el intervalo* $[1,n]$ *representa el conjunto* $\{1,\ldots,n\}$.

Capítulo 1

PRELIMINARES

Esta sección estará dedicada a definir algunos conceptos necesarios para la correcta comprensión de este trabajo. Dichos resultados están relacionados con la teoría de números, grupos, campos finitos y acotamiento asintótico. Los siguientes resultados fueron tomados de [1] y [10] allí se podrá observar con detalle sus respectivas demostraciones.

1.1. TEORÍA DE NÚMEROS

Teorema 1.1. *Dados enteros a y b, con* $b > 0$*, existen enteros únicos q y r tales que*

$$a = bq + r \qquad 0 \leq r < b$$

Los enteros q y r se llaman, respectivamente, el cociente y el residuo en la división de a por b.

- *Sean a, b números enteros con a diferente de cero. Decimos que a divide a b si existe un entero c tal que* $b = ac$*. En tal caso escribimos* $a|b$*. Decimos también que a es un divisor de b o que b es un múltiplo de a.*

- *Un entero positivo* $p > 1$ *se denomina un* ***número primo*** *si tiene exactamente dos divisores positivos a saber,* 1 *y p. Un entero positivo mayor que* 1 *que no es primo se denomina* ***compuesto****.*

- Si $n = \prod_{i=1}^{k} p_i^{n_i}$ es la representación canónica de un entero positivo n, entonces

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

donde $\phi(n)$ indica el numero de ***primos relativos*** menores e iguales que n.

- *Sea n un entero fijo. Dos enteros a y b se dice que son* ***congruentes módulo*** *n, denotado por*

$$a \equiv b \,(mod n)$$

si n divide a $a-b$; es decir si existe un entero k tal que $a-b=nk$. Podemos comprobar que la relación de congruencia modulo n es una relación de equivalencia, (es decir es reflexiva, simétrica y transitiva). Esta relación induce una partición $\mathbb{Z}$ en clases de equivalencia $[a]$ (donde para $a \in \mathbb{Z}$ fijo, $[a] = \{x \in \mathbb{Z} : x \equiv a \,(mod\, n)\}$). El conjunto de todas las clases de equivalencia bajo esta relación de congruencia lo denotamos por $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$.

- Sean $m_1, m_2, \ldots, m_r$ enteros positivos primos relativos dos a dos, y sean $a_1, a_2, \ldots, a_r$ enteros arbitrarios. Entonces el sistema de congruencias lineales

$$\begin{aligned} x &\equiv a_1 \,(\text{mód}\, m_1) \\ x &\equiv a_2 \,(\text{mod}\, m_2) \\ &\vdots \\ x &\equiv a_r \,(\text{mod}\, m_r) \end{aligned}$$

tiene solución única modulo $m = \prod_{i=1}^{r} m_i$.

Una de las aplicaciones importantes de la teoría de congruencias consiste en encontrar criterios especiales bajo los cuales un entero dado es divisible por otro.

Dado un entero $b > 1$, cualquier entero positivo N se puede escribir en forma única en términos de b como:

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0,$$

donde $0 \leq a_k \leq b-1$.

Con esta escritura, el entero N esta completamente determinado por los coeficientes en la representación. Así, el número

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0,$$

se puede representar por:

$$N = (a_m a_{m-1} \cdots a_2 a_1 a_0)_b.$$

A esta representación se le denomina ; ***la notación en base*** b ***de*** N. El caso más simple se tiene cuando $b = 2$, el sistema de numeración resultante se denomina *sistema binario*. Así cuando un número se escribe en el sistema binario, únicamente los enteros 0 y 1 aparecen en tal representación; es decir, todo entero positivo se representa en forma única como una suma de potencias diferentes de 2. Por ejemplo 105 se puede representar como $105 = (1101001)_2$.

1.2. GRUPOS Y CAMPOS

Definición 1.1. Un ***grupo*** es un conjunto no vaco G junto con una operación binaria$*$ sobre G, denotado por $\langle G, * \rangle$, tal que se cumplen las siguientes propiedades:

a. Para todo $a, b, c \in G$, se tiene que $a*(b*c) = (a*b)*c$.

b. Existe un elemento identidad (o neutro) $e \in G$ tal que para todo $a \in G$, $a*e = e*a = a$.

c. Para todo $a \in G$, existe un elemento inverso $a^{-1} \in G$ tal que $a*a^{-1} = a^{-1}*a = e$.

- El elemento identidad $e \in G$ y el elemento inverso $a^{-1} \in G$ de un elemento dado $a \in G$ son únicos.
- Si para todo $a, b \in G$, $a*b = b*a$, diremos que G es un grupo ***abeliano*** (o conmutativo). Generalmente en esta clase de grupos adoptamos una notación aditiva, escribimos $a+b$ en lugar de $a*b$, $-a$ en lugar de a^{-1} y 0 en lugar de e.
- Se dice que un grupo G es un ***grupo finito*** si consta de un número finito de elementos. El número de elementos de G se llama ***orden*** de G y se denota por $|G|$.

- El grupo G se llama ***grupo cíclico*** si existe un elemento $a \in G$ tal que para todo $b \in G$ existe algún entero j con $b = a^j$. Tal elemento a se llama un ***generador*** del grupo cíclico, y escribimos $G = \langle a \rangle$.

- Sean A y B dos grupos. Diremos que una aplicación $f : A \longrightarrow B$ es un **homomorfismo de grupos** si $f(ab) = f(a) f(b)$ para todo $a, b \in A$. A demás un homomorfismo sea biyectivo se le denominará **isomorfismo.**

  Ejemplo 1.1. La aplicación f definida de la siguiente manera:

$$\begin{array}{rccc} f: & \mathbb{Z}_{p-1} \times \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_{p(p-1)} \\ & (a, b) & \longrightarrow & [x] \end{array}$$

  donde $x \equiv a \pmod{p-1}$ y $x \equiv b \pmod{p}$ es un isomorfismo.

  Demostración. Probemos que la función f es inyectiva es decir, supongamos $f((a, b)) = [x]$ y $f((c, d)) = [y]$ con $(a, b), (c, d) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_p$ donde

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

  así

$$[x] = [y]$$

  de donde sabemos que las clases residuales son disjuntas o iguales por lo tanto

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

  Note que $\forall\, [x] \in \mathbb{Z}_{p(p-1)}$ existe $(a, b) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_p$ tal que $f((a, b)) = [x]$, por lo cual f es sobre. Para probar que f es isomorfismo sabemos que la operación $+$ en clase residuales se define como $[x] + [y] = [x + y]$, así pues

$$f((a, b)) + f((c, d)) = [x] + [y] = [x + y] = f((a, b) + (c, d)).$$

  □

El estudio de los campos ha tenido un gran desarrollo en los últimos años, debido principalmente a problemas surgidos de sus aplicaciones, tales como la criptografía, teoría de códigos, combinatoria entre otros.

Definición 1.2. *Un campo o cuerpo* $\mathbb{F}$ *es un conjunto con dos operaciones binarias denotadas* $+$ *y* $\cdot$ *tales que:*

a. $\langle \mathbb{F}, + \rangle$ es un grupo abeliano.

b. Para todo $a, b, c \in \mathbb{F}$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

c. Existe un elemento identidad multiplicativa $1 \in G$ tal que para todo $a \in G$, $a \cdot 1 = 1 \cdot a = a$.

d. Para todo$a \in G$ con $a \neq 0$, existe un elemento a^{-1} tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

e. Si para todo $a, b \in \mathbb{F}$, $a \cdot b = b \cdot a$.

f. Para todo $a, b, c \in \mathbb{F}$ se tiene $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a$.

Ejemplo 1.2. Sea p un número primo. El conjunto $\mathbb{Z}_p = \{[0], [1], \ldots, [p-1]\}$ es un campo, con las operaciones suma $+$ y producto $\cdot$ definidas respectivamente por:

$$[a] + [b] = [a + b] \text{ y } [a] \cdot [b] = [a \cdot b].$$

- La característica de cualquier cuerpo es cero o un número primo. (la característica se define como el número entero positivo más pequeño n tal que $n \cdot 1 = 0$, o cero si no existe tal n; aquí $n \cdot 1$ significa n sumandos $1 + 1 + 1 + \ldots + 1$.)

- Si $q > 1$ es una potencia de un número primo, entonces existe (salvo isomorfismo) exactamente un cuerpo finito con q elementos. Además, estos son los únicos cuerpos finitos posibles.

- El conjunto de elementos diferentes de cero de un cuerpo $\mathbb{F}$ (denotado por $\mathbb{F}^*$) es un grupo abeliano bajo multiplicación. Cada subgrupo finito de $\mathbb{F}^*$es cíclico.

- Un elemento $\alpha \in \mathbb{F}_q$ de orden $q - 1$, es decir, un generador de $\mathbb{F}_q^*$, se llama ***elemento primitivo*** del campo $\mathbb{F}_q$.

- Una **extensión de cuerpos** es un par $[K, \mathbb{F}]$ donde $\mathbb{F}$ es un cuerpo y K un subcuerpo de $\mathbb{F}$; una extension de cuerpos se denota como $\mathbb{F}/K$.

- Sea una extensión de cuerpos $\mathbb{F}_{q^m}/\mathbb{F}_q$ y sea $\alpha \in \mathbb{F}_{q^m}$. A los elementos $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ se les denomina **conjugados** α sobre $\mathbb{F}_q$.

- Para cada $\alpha \in \mathbb{F}_{q^m}$ se define la **traza** de α sobre $\mathbb{F}_q$ y se denotará $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ como:

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}$$

  Es decir, la traza de α sobre $\mathbb{F}_q$ es la suma de los conjugados de α.

1.3. NOTACIÓN ASINTÓTICA

A lo largo de este trabajo se observó también la notación $O(g(x))$, esta representación llamada *Landau* $O(g(x))$ o comúnmente notación O grande, es un conjunto de funciones las cuales sirve como cota superior de otra función cuando el argumento tiende a infinito [16]. Formalmente se define así:

Definición 1.3. *Sea $g : \mathbb{N}_0 \to \mathbb{R}^+$ una función . Entonces, $O(g)$ es el conjunto de funciones $f : \mathbb{N}_0 \to \mathbb{R}^+$ tal que para alguna constante real $c > 0$ y alguna constante entera no negativa n_0, $f(n) \leq cg(n)$ para toda $n \geq n_0$.*

Con frecuencia es útil pensar en g como alguna función dada, y en f como la función que estamos analizando. Observe que una función f podría estar en $O(g)$ aunque $f(n) > g(n)$ para toda n. Lo importante es que f esté acotada por arriba por algún múltiplo constante de g. Además, no se considera la relación entre f y g para valores pequeños de n [16].

- Una función $f \in O(g)$ si $\lim_{n\to\infty} \dfrac{f(n)}{g(n)} = c < \infty$.

Es decir, si el límite del cociente de f entre g existe y no es ∞, entonces f no crecerá más rápidamente que g. Si el límite es ∞, entonces f sí crece más rápidamente que g.

Ejemplo 1.3. Sea $f(n) = n^{1/4} + 1$ y $g(n) = n^{1/4}$ demostremos que $f \in O(g)$. Aplicando la definición anterior tenemos:

$$\lim_{x\to\infty} \frac{n^{1/4}+1}{n^{1/4}} = 1$$

así se prueba de que este limite existe y por tanto $n^{1/4}+1 \in O\left(n^{1/4}\right)$.

Observación 1.1. Algunas veces se utiliza también las notaciones $f(x) \ll g(x)$ o $g(x) \gg f(x)$ para indicar lo mismo. Estas ultimas se utilizan sobre todo cuando del termino principal solo nos interesa el orden de magnitud.

Capítulo 2

CONJUNTOS DE SIDON EN DIMENSIÓN UNO

En este capitulo abordaremos los Conjuntos de Sidon en dimensión uno, principalmente estudiaremos con detalle algunas técnicas de conteo que permiten obtener cotas superiores para estos conjuntos.

Definición 2.1. *Un conjunto de enteros positivos A es un* ***Conjunto de Sidon en dimensión uno*** *si todas las sumas de la forma*

$$a+a', \;\; a,a' \in A \quad a \leq a'$$

son distintas.

Observe que $a+b=c+d$ si y solo si $a-c=d-b$, por lo tanto los conjuntos Sidon también se definen indistintamente, como aquellos con la propiedad de que todas las diferencias no nulas de cada par de elementos en el conjunto sean distintas, es decir, A es un conjunto de Sidon si todas las diferencias de la forma

$$a-a', \;\; a,a' \in A \quad a \neq a'$$

son distintas.

Ejemplo 2.1. El conjunto $A=\{1,\ 2,\ 5,\ 10,\ 16,\ 23,\ 33,\ 35\}$, es un ejemplo clásico de conjunto de Sidon en dimensión uno el cual podemos verlo en [4]. Para verificar que A es efectivamente un Conjunto

de Sidon podemos hacer la construcción de un triangulo de diferencias positivas, el cual se construye así: En la primera fila aparece los elementos del conjunto y en las filas inferiores todas las diferencias positivas de cada par de elementos distintos del conjunto A, como se muestra a continuación:

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

De hecho, se puede demostrar que el intervalo$[1, 35]$ no contiene ningún conjunto de Sidon con más de 8 elementos; es decir A es un conjunto de Sidon de tamaño maximal.

Una pregunta que surge de manera natural es: ¿Cual es el mayor número de elementos que puede tener un conjunto de Sidon contenido en el intervalo $[1,\ n]$? Esta pregunta ha sido resuelta parcialmente por algunos matemáticos tales como Erdös y Turan, B. Lindström, Rusza y Cilleruelo, quienes encontraron respuestas asintóticas al problema. Con el propósito de estudiar las respuestas a dicha pregunta se define la siguiente función contadora:

Definición 2.2. *Sea n un entero positivo. La función contadora $F_2(n)$ se define como el máximo número de elementos que pueden seleccionarse del intervalo $[1, n]$ de tal forma que ellos constituyan un conjunto de Sidon, es decir:*

$$F_2(n) = máx\{|A| : A \subset [1, n]\,; A \text{ es Sidon}\}$$

El estudio de la función $F_2(n)$ lo abordaremos en primera instancia buscando cotas superiores para la misma, esto se realizara a partir de algunas técnicas de conteo y del estudio de Conjuntos de Sidon en grupos abelianos. Por otro lado la obtención de cotas inferiores para la función $F_2(n)$ se realizará mediante la construcción de Conjuntos de Sidon.

2.1. COTAS SUPERIORES PARA LA FUNCIÓN $F_2(n)$

Comenzaremos por obtener una primera cota superior para la función $F_2(n)$.

Teorema 2.1. *Si A es un conjunto de Sidon contenido en el intervalo* $[1, n]$*, entonces:*

$$F_2(n) < \sqrt{2n} + 1/2$$

Demostración. Como todas las diferencias positivas $a - b$ con $a, b \in A$ son distintas y menores que n y hay exactamente $\binom{|A|}{2}$[1] de esas diferencias, se tiene la desigualdad

$$\binom{|A|}{2} \leq n - 1,$$

de donde

$$\binom{|A|}{2} = \frac{|A|!}{2!(|A|-2)!} = \frac{|A|(|A|-1)}{2} \leq n - 1,$$

lo cual es equivalente a tener

$$|A|^2 - |A| \leq 2(n-1),$$

de ahí que

$$|A| < \sqrt{2n} + 1/2,$$

y por lo tanto

$$F_2(n) < \sqrt{2n} + 1/2.$$

□

Observación 2.1. Esta cota superior permite evidenciar que un conjunto de Sidon en el intervalo $[1, 35]$ no puede tener mas de 8 elementos, pues:

$$F_2(35) < \sqrt{70} + 1/2 = 8,866\ldots$$

[1] *El coeficiente binomial* $\binom{n}{k}$ *es el número de subconjuntos de k elementos escogidos de un conjunto con n elementos.*

En particular de este resultado el conjunto A del ejemplo anterior es un **CONJUNTO DE SIDON MAXIMAL**.

La cota del teorema 2.1 no es óptima cuando n toma valores muy grandes, sin embargo se puede mejorar si en lugar de tener en cuenta todas las diferencias $a-b$ con $a,b \in A$ se consideran solo las diferencias pequeñas. Usando este hecho en 1941, Paúl Erdős y Turán, en [5] demostraron:

Teorema 2.2. *Si $A \subset [1, n]$ es un conjunto de Sidon, entonces:*

$$F_2(n) < \sqrt{n} + O\left(n^{1/4}\right)$$

Demostración. Sea $A = \{a_1, a_2, \ldots, a_k\} \subset [1, n]$ un conjunto cualquiera, con $|A| = k$, sean m, $n \in \mathbb{Z}$ tales que $1 \leq m \leq n$ y consideremos los intervalos

$$I_i = [i-m,\, i-1]\,, \text{ con } i = 1, 2, \ldots, m+n.$$

Observe que a medida que aumenta i los intervalos se desplazan una unidad hacia la derecha. Sea A_i el número de elementos de A que hay en I_i, en otras palabras $A_i = |A \cap I_i|$, es claro que si $i = 1$ entonces $A_1 = 0$, ya que $A \subset [1, n]$. Dado que $a \in A$ nos preguntamos lo siguiente ¿En cuantos intervalos aparece a?.

Afirmación 2.1. *Si $a \in A$ entonces a aparece exactamente en m intervalos.*

Note que el primer intervalo donde aparece a ocurre cuando $i = a+1$, es decir; $I_{a+1} = [a+1-m,\, a]$ y el último se tiene cuando $i = a+m$, es decir; $I_{a+m} = [a,\, a+m-1]$. Teniendo en cuenta que i en cada intervalo aumenta una unidad hacia la derecha se tiene entonces que desde el primer intervalo donde aparece a y hasta el último donde aparece, hay exactamente m intervalos, con lo cual la afirmación queda plenamente justificada.

Ahora como cada $a \in A_i$ aparece exactamente en m intervalos, entonces tenemos que:

$$\sum_{i=2}^{n+m} A_i = mk, \tag{2.1}$$

de donde

$$(mk)^2 = \left(\sum_{i=2}^{n+m} A_i\right)^2,$$

y utilizando la desigualdad de Cauchy–Schwarz, se tiene que:

$$(mk)^2 = \left(\sum_{i=2}^{n+m} A_i\right)^2 \leq \left(\sum_{i=2}^{n+m} 1^2\right)\left(\sum_{i=2}^{n+m} A_i^2\right) = (m+n-1)\left(\sum_{i=2}^{n+m} A_i^2\right),$$

es decir

$$\frac{(mk)^2}{m+n-1} \leq \sum_{i=2}^{n+m} A_i^2. \tag{2.2}$$

Por otro lado el número de pares $a, a' \in A$ y que están en el intervalo I_i está dado por:

$$\binom{A_i}{2} = \frac{1}{2} A_i (A_i - 1),$$

así el total de estos pares es:

$$\sum_{i=2}^{m+n} \binom{A_i}{2} = \frac{1}{2} \sum_{i=2}^{n+m} A_i (A_i - 1),$$

luego, usando 2.1 y 2.2 tenemos:

$$\sum_{i=2}^{m+n} \binom{A_i}{2} \geq \frac{1}{2}\left(\frac{m^2k^2}{m+n-1} - mk\right). \tag{2.3}$$

Ahora si $a, a' \in A$ con $a > a'$, se encuentra en el mismo intervalo, es decir, a, $a' \in I_i$ para algún $1 \leq i \leq m+n$, entonces $i - m \leq a$, $a' \leq i - 1$, de ahí que la diferencia $d = a - a' > 0$ cumple:

$$1 \leq d \leq m - 1.$$

Afirmación 2.2. *Si $a, a' \in A$ están en un mismo intervalo y $d = a - a'$ entonces la pareja a, a' se encuentra en exactamente $(m-d)$ intervalos.*

Observe que a' aparece en los siguientes intervalos

$$\left[a'+1-m,a'\right],\left[a'+2-m,a'+1\right],\ldots,\left[a'+d+1-m,a'+d\right],\ldots,\left[a',a'+m-1\right]$$

ya que $a=a'+d$ y $a'+m-1=a'+d+(m-d-1)$ entonces a pertenece a los intervalos

$$\left[a'+d+1-m,a'+d\right],\ldots,\left[a',a'+m-1\right]$$

por lo cual la pareja $a,a'\in A$ se encuentra en $m-d$ intervalos, de esta manera se justifica la afirmación anterior.

Si A es un conjunto de Sidon, se tiene que todas sus diferencias son distintas, de ahí que

$$\sum_{i=2}^{m+n}\binom{A_i}{2}\leq\sum_{d=1}^{m-1}(m-d)=\frac{1}{2}m(m-1). \tag{2.4}$$

Entonces de 2.3 y de 2.4 tenemos:

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

de donde se obtiene

$$k\leq\frac{1}{m}(n+m-1)(k+m-1)$$

Si $m=\left\lfloor n^{3/4}\right\rfloor+1$, y como

$$m-1\leq\quad n^{3/4}\quad\leq m,$$

es decir

$$\frac{1}{m}\quad\leq\quad\frac{1}{n^{3/4}},$$

entonces se tiene que

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

de ahí que

$$k^2-\left(n^{3/4}+1\right)k \leq n+n^{3/4},$$

luego

$$\left[k-\frac{1}{2}\left(n^{1/4}+1\right)\right]^2 \leq \left[\sqrt{n}+\frac{1}{2}\left(n^{1/4}+1\right)\right]^2-\sqrt{n},$$

así

$$\left[k-\frac{1}{2}\left(n^{1/4}+1\right)\right]^2 < \left[\sqrt{n}+\frac{1}{2}\left(n^{1/4}+1\right)\right]^2,$$

y por tanto

$$k < \sqrt{n}+O\left(n^{1/4}\right)$$

□

B. Lindström en 1969, logra obtener (en [11]) mediante argumentos combinatorios una cota más fina para la función$F_2(n)$, él demostró el siguiente resultado:

Teorema 2.3. *Si $A \subset [1,n]$ es un conjunto de Sidon, entonces:*

$$F_2(n) < \sqrt{n}+n^{1/4}+1$$

Demostración. Sea $A \subset [1,n]$ un conjunto de Sidon con $|A| = k$ y ordenemos los elementos de A de forma creciente, es decir.

$$1 \leq a_1 < a_2 < \ldots < a_k \leq n$$

Las diferencias $a_j - a_i$, con $1 \leq i \leq j \leq k$, son distintas. Al entero $j-i$ lo llamaremos el orden de la diferencia $a_j - a_i$.

Ahora para $t > 0$ fijo, la suma de las diferencias de orden t, esta dada por:

$$S_t = \sum_{i=1}^{k-t} (a_{i+t} - a_i). \tag{2.5}$$

Tomemos $m \in \mathbb{Z}$, $1 \leq m \leq k$. simbolicemos con T la suma de diferencias de orden t, para $t \leq m$; es decir,

$$T = \sum_{t=1}^{m} \sum_{i=1}^{k-t} (a_{i+t} - a_i)$$

En T el número de sumandos, cada uno de los cuales representa una diferencia, es:

$$\sum_{t=1}^{m} (k-t) = \sum_{t=1}^{m} k - \sum_{t=1}^{m} t = km - \frac{m(m+1)}{2} = m\left(k - \frac{m+1}{2}\right) = ms$$

Donde ms es el número de estas diferencias.

Como A es un conjunto de Sidon, entonces todas las ms diferencias son distintas y lo mínimo que puede ocurrir es que sean mas pequeñas que $1, 2, 3, 4, \ldots, ms$, es decir

$$T \geq \sum_{i=1}^{ms} i = \frac{ms(ms+1)}{2}. \tag{2.6}$$

Por otro lado, desarrollando los S_t de 2.5 se tiene

$$S_1 = \sum_{i=1}^{k-1} (a_{i+1} - a_i)$$

$$S_1 = (a_k - a_1)$$

$$S_2 = \sum_{i=1}^{k-2} (a_{i+2} - a_i) = \left(\sum_{i=1}^{k-2} (a_{i+2} - a_{i+1})\right) + \left(\sum_{i=1}^{k-2} (a_{i+1} - a_i)\right)$$

$$S_2 = (a_k - a_2) + (a_{k-1} - a_1)$$

$$\vdots$$

$$S_t = \sum_{i=1}^{k-t} (a_{i+t} - a_i) = \left(\sum_{i=1}^{k-t} (a_{i+t} - a_{i+t-1}) \right) + \ldots + \left(\sum_{i=1}^{k-t} (a_{i+1} - a_i) \right)$$
$$S_t = (a_k - a_t) + (a_{k-1} - a_{t-1}) + \ldots + (a_{k-m+1} - a_1)$$
$$\vdots$$
$$S_m = \sum_{i=1}^{k-m} (a_{i+m} - a_i) = \left(\sum_{i=1}^{k-m} (a_{i+m} - a_{i+m-1}) \right) + \ldots + \left(\sum_{i=1}^{k-m} (a_{i+1} - a_i) \right)$$
$$S_m = (a_k - a_m) + (a_{k-1} - a_{m-1}) + \ldots + (a_{k-m+1} - a_1)$$

Luego el número de sumandos (diferencias) en T es:

$$\sum_{t=1}^{m} t = \frac{1}{2} m (m+1).$$

Como todas sus diferencias son menores que n, para $A \subset [1,n]$ se tiene

$$T < \frac{1}{2} m (m+1) n \tag{2.7}$$

De lo cual de 2.6 y 2.7 se llega a

$$\frac{m^2 s^2}{2} < \frac{1}{2} ms (ms+1) \leq T < \frac{1}{2} m (m+1) n,$$

por lo tanto

$$m^2 s^2 < m (m+1) n,$$

donde

$$s < \sqrt{n} \left(\sqrt{1 + \frac{1}{m}} \right), \tag{2.8}$$

Por la desigualdad *MA-MG*[2], se tiene

$$\sqrt{1 + \frac{1}{m}} \leq \frac{1}{2} + \frac{1}{2m} < 1 + \frac{1}{2m}$$

[2] *La desigualdad de las medias aritmética y geométrica establece que para* $x_1, x_2 \in \mathbb{R}^+$ *se cumple* $\frac{x_1 + x_2}{2} \geq \sqrt{x_1 x_2}$.

de ahí que

$$s < \sqrt{n}\left(1+\frac{1}{2m}\right)$$

Observe que $ms = km - \frac{m(m+1)}{2}$ donde $s = k - \frac{(m+1)}{2}$, ahora reemplazando en la desigualdad anterior se llega a

$$k < \sqrt{n}\left(1+\frac{1}{2m}\right) + \frac{(m+1)}{2} \tag{2.9}$$

Sea la escogencia óptima de $m = \left\lfloor n^{1/4} \right\rfloor + 1$ y aplicando esto en 2.9 tenemos

$$k < \frac{1}{2}\left(n^{1/4}+2\right) + n^{1/2}\left(1+\frac{1}{2n^{1/4}}\right),$$

y por lo tanto

$$k < \sqrt{n} + n^{1/4} + 1,$$

esto termina la demostración . □

Ruzsa en [14] proporciona una demostración alternativa del Teorema 2.3, extendiendo el concepto de Conjuntos de Sidon a grupos.

Definición 2.3. *Un conjunto A en un grupo abeliano $\langle G, + \rangle$ es un conjunto de Sidon si todas las diferencias no nulas $a - a'$ con $a, a' \in A$ son distintas.*

Ejemplo 2.2. En el grupo aditivo $\mathbb{Z}_{42}$ el conjunto $A = \{2, 4, 5, 27, 31, 36\}$ es un Conjunto de Sidon, esto se puede ver en la siguiente tabla de diferencias:

$-$	2	4	5	27	31	36
2	0	40	39	17	13	8
4	2	0	41	19	15	10
5	3	1	0	20	16	11
27	25	23	22	0	38	33
31	29	27	26	4	0	37
36	34	32	31	9	5	0

Antes de dar a conocer el resultado dado por Ruzsa vamos a introducir algunas definiciones y notaciones que son habituales en la teoría combinatoria de números, estas definiciones y notaciones se pueden ver en [4].

Si G es un grupo abeliano y $A, B \subset G$, el conjunto suma de A y B entonces:

- El conjunto suma de A y B se define por:

$$A+B = \{a+b,\ a \in A,\ b \in B\},$$

- Para $x \in G$ el numero de representaciones de x como suma de un elemento en A y otro en B esta dado por:

$$r_{A+B}(x) = |\{(a,b) \in A \times B, a+b = x\}|,$$

  Note que habrá elementos $x \in G$ los cuales no poseen una representación como la suma de dos elementos de A y B respectivamente, sin embargo este hecho no afecta el conteo que realiza $r_{A+B}(x)$. Así pues cada elemento x que puede representarse mediante dicha suma pertenece en realidad a $A+B$, de donde para $x \in G$ indistintamente $x \in A+B$.

Consideremos ahora las siguientes identidades las cuales serán utilizadas para la demostración de posteriores resultados.

- La identidad

$$r_{A-A}(0) = |A| \tag{2.10}$$

  se cumple debido a que el número de representaciones de 0 están dadas por todas las diferencias nulas entre pares de elementos de A, las cuales coinciden precisamente con la cantidad de ele-

mentos que tiene el conjunto A. A demás como $r_{A+B}(x)$ cuenta el número parejas $(a,b) \in A \times B$, entonces la suma de todas estas parejas esta dada por:

$$\sum_{x \in G} r_{A+B}(x) = |A|\,|B|\,. \tag{2.11}$$

- El número de soluciones de la ecuación $x = a+b = a'+b'$ con a,$a' \in A$ y b,$b' \in B$, se denomina ***energía aditiva*** entre A y B y esta dado por:

$$E(A,B) = \sum_{x} r^2_{A+B}(x)\,,$$

donde $r^2_{A+B}(x) = r_{A+B}(x)\,r_{A+B}(x) = |\{(a,b,a',b') \in A \times B \times A \times B,\, a+b = a'+b' = x\}|$ que al reorganizar la ecuación tenemos que $x = a-a' = b'-b$, por lo tanto $r^2_{A+B}(x) = r_{A-A}(x)\,r_{B-B}(x) = |\{(a,a',b,b') \in A \times A \times B \times B,\, a-a' = b'-b = x\}|$, esta observación da lugar a la siguiente identidad (ver [15] para una prueba detallada):

$$\sum_{x} r^2_{A+B}(x) = \sum_{x} r_{A-A}(x)\,r_{B-B}(x) \tag{2.12}$$

- Por otro lado para cada pareja b, b' con $b \neq b'$ existe un único par a, a' donde la ecuación $x = a-a' = b'-b$ tiene solución, de ahí que tenemos:

$$\sum_{x \neq 0} r_{B-B}(x) = |B|\,(|B|-1)\,. \tag{2.13}$$

El siguiente resultado, que se prueba con las identidades anteriores, sera clave en la demostración dada por Rusza del Teorema 2.3

Lema 2.1. *Sea A un conjunto de Sidon en un grupo abeliano G y sea B cualquier subconjunto de G. Entonces se tiene:*

$$|A|^2 \leq |A+B| \left(1 + \frac{|A|-1}{|B|}\right)$$

Demostración. De la desigualdad de Cauchy y las identidades 2.11 y 2.12 tenemos:

$$\begin{aligned}(|A|\,|B|)^2 &= \left(\sum_{x\in A+B} r_{A+B}\right)^2 \\ &\leq |A+B|\sum_x r_{A+B}^2(x) \\ &= |A+B|\sum_x r_{A-A}(x)\, r_{B-B}(x)\end{aligned}$$

Como el Conjunto A es de Sidon, entonces $r_{A-A}(x) \leq 1$ para $x \neq 0$ y dadas la identidades 2.10 y 2.13 tenemos que

$$\begin{aligned}\sum_x r_{A-A}(x)\, r_{B-B}(x) &= r_{A-A}(0)\, r_{B-B}(0) + \sum_{x\neq 0} r_{A-A}(x)\, r_{B-B}(x) \\ &\leq r_{A-A}(0)\, r_{B-B}(0) + \sum_{x\neq 0} r_{B-B}(x) \\ &= |A|\,|B| + |B|\,(|B|-1)\end{aligned}$$

lo que nos lleva a la desigualdad

$$(|A|\,|B|)^2 \leq |A+B|\,(|A|\,|B| + |B|\,(|B|-1))$$

de donde

$$|A|^2 \leq |A+B|\left(1 + \frac{|A|-1}{|B|}\right)$$

□

Ahora miraremos una demostración alternativa del Teorema 2.3 dada en este caso por Rusza en [14].

Demostración. Sea $A \subset [1,n]$ un conjunto de Sidon con $|A| = m$, aplicando el lema anterior al conjunto $B = \{1,2,\ldots,k\}$, como $A+B = [2, n+k]$ tenemos:

$$n+k-1 \geq |A+B| \geq \frac{m^2 k}{m+k-1}$$

Esto da una estimación inferior de n que depende de k. El valor óptimo esta alrededor de $m\sqrt{m}-m$. Tomando $k=\lfloor m\sqrt{m}\rfloor - m+1$ obtenemos

$$n \geq \frac{m^2\left(m\sqrt{m}-m\right)}{m\sqrt{m}} - m\sqrt{m}+m = m^2-2m\sqrt{m}+m = \left(m-\sqrt{m}\right)^2$$

Esto genera una desigualdad cuadrática para $\sqrt{m}$, de la que obtenemos

$$m \leq \sqrt{n}+\frac{1}{2}+\sqrt{\sqrt{n}+\frac{1}{4}} < \sqrt{n}+n^{1/4}+1.$$

□

Una pequeña modificación a la técnica usada por Ruzsa le permitió a Cilleruelo, en [4], mejora ligeramente la cota mostrada en el teorema anterior. Este resultado es el siguiente.

Teorema 2.4. *Si $A \subset [1,n]$ es un conjunto de Sidon entonces*

$$|A| < n^{1/2}+n^{1/4}+1/2$$

Demostración. Dado el conjunto $B=[0,t]\cap\mathbb{Z}$, donde $t=\left\lfloor \sqrt{n\left(|A|-1\right)}\right\rfloor$. Entonces $|A+B|\leq n+t$ y $|B|=t+1$, luego del 2.1 se tiene que

$$\begin{aligned} |A|^2 &\leq (n+t)\left(1+\frac{|A|-1}{t+1}\right) \\ &= (n+t)+\frac{n\left(|A|-1\right)}{t+1}+\frac{t\left(|A|-1\right)}{t+1}. \end{aligned}$$

Como $\frac{t}{t+1}<1$ entonces $\frac{t(|A|-1)}{t+1}<|A|-1$, de ahí que

$$|A|^2 < (n+t)+\frac{n\left(|A|-1\right)}{t+1}+|A|-1.$$

Dado que $t\leq\sqrt{n\left(|A|-1\right)}<t+1$ entonces $n\left(|A|-1\right)<(t+1)\sqrt{n\left(|A|-1\right)}$, de donde

$$\frac{n\left(|A|-1\right)}{t+1} < \sqrt{n\left(|A|-1\right)},$$

de ahí que

$$\begin{aligned} |A|^2 &\leq n + 2\sqrt{n(|A|-1)} + |A| - 1 \\ &= \left(\sqrt{n} - \sqrt{|A|-1}\right)^2, \end{aligned}$$

luego

$$|A| < \sqrt{n} - \sqrt{|A|-1},$$

de donde

$$\left(|A| - \sqrt{n}\right)^2 < |A| - 1. \tag{2.14}$$

Haciendo $|A| = n^{1/2} + cn^{1/4} + 1/2$ y reemplazando en 2.14 se tiene:

$$c^2 n^{1/2} + cn^{1/4} + \frac{1}{4} < n^{1/2} + cn^{1/4} - \frac{1}{2},$$

lo cual es una contradicción cuando $c \geq 1$, luego $c > 1$ y así por lo tanto.

$$|A| < n^{1/2} + n^{1/4} + 1/2$$

□

La cota superior

$$F_2(n) < n^{1/2} + n^{1/4} + 1/2$$

parece ser la mejor posible cuando contamos diferencias pequeñas.

Erdős sin embargo había conjeturado que $F_2(n) < \sqrt{n} + O(1)$. Hoy en día nadie ha sido capaz de refutar la conjetura de Erdös, precisamente él termina afirmando, en [5], que la conjetura era demasiado optimista y que la forma correcta de enunciarla debería ser $F_2(n) < \sqrt{n} + O(n^{\varepsilon})$ para $\varepsilon > 0$.

Capítulo 3

CONJUNTOS DE SIDON EN DIMENSIÓN DOS Y ALGUNAS APLICACIONES

En el capítulo anterior estudiamos Conjuntos de Sidon (en dimensión uno), sin embargo resulta interesante estudiar Conjuntos de Sidon en otras dimensiones , tal es el caso de los Conjuntos de Sidon en dimensión dos, los cuales nos permitirán obtener buenas cotas inferiores para la función $F_2(n)$; Además estos Conjuntos de Sidon tiene aplicaciones interesantes en el área de las telecomunicaciones particularmente en problemas relaciones con el SONAR.

Definición 3.1. *Un conjunto $A = \{v_1, v_2, \ldots\} \subseteq \mathbb{Z} \times \mathbb{Z}$ se llama un* ***Conjunto de Sidon en dimensión dos*** *si todas las sumas de la forma*

$$v_i + v_j, \text{ con } i \leq j,$$

son distintas. Es decir:

$$(v_i + v_j = v_k + v_l) \Longrightarrow \{v_i, v_j\} = \{v_k, v_l\}$$

Un aspecto llamativo que tienen los Conjuntos de Sidon en dimensión dos es su interpretación geométrica, es decir, ellos se pueden ver como aquellos conjuntos que tienen la propiedad de que cualesquiera cuatro de sus elementos nunca forman un paralelogramo.

De forma análoga como se observó en el capítulo anterior el conjunto $A = \{v_1, v_2, \ldots\}$ es un Conjunto de Sidon (en dimensión dos) si y sólo si todas las diferencias de la forma

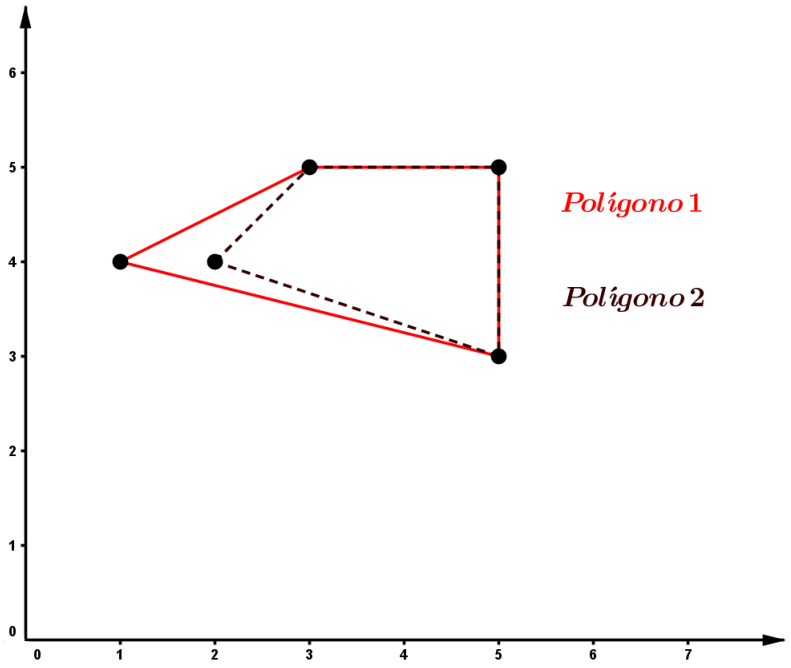
$$v_i - v_j, \quad v_i, v_j \in A, \quad i \neq j, \tag{3.1}$$

son distintas.

Ejemplo 3.1. El conjunto $A = \{(1,4), (2,4), (3,5), (5,3), (5,5)\}$ es un Conjunto de Sidon en dimensión dos, esto se puede evidenciar en la siguiente tabla de sumas para A.

+	$(1,4)$	$(2,4)$	$(3,5)$	$(5,3)$	$(5,5)$
$(1,4)$	$(2,8)$	$(3,8)$	$(4,9)$	$(6,8)$	$(6,9)$
$(2,4)$		$(4,8)$	$(5,9)$	$(7,7)$	$(7,9)$
$(3,5)$			$(6,10)$	$(8,8)$	$(8,10)$
$(5,3)$				$(10,6)$	$(10,8)$
$(5,5)$					$(10,10)$

También podríamos verificar geométricamente que el conjunto A es un Conjunto de Sidon en dimensión dos, pues cualesquiera cuatro de sus elementos nunca forman un paralelogramo, como se observa en la siguiente Figura.



Los siguientes ejemplos nos muestran como construir Conjuntos de Sidon en dimensión dos a partir de Conjuntos de Sidon en dimensión uno.

Ejemplo 3.2. El conjunto $S = \{(1,1),(2,4),(4,9),(8,13)\} \subset \mathbb{Z} \times \mathbb{Z}$ es un Conjunto de Sidon en dimensión dos, esto se puede evidenciar en la siguiente tabla de sumas para S.

$+$	$(1,1)$	$(2,4)$	$(4,9)$	$(8,13)$
$(1,1)$	$(2,2)$	$(3,5)$	$(5,10)$	$(9,14)$
$(2,4)$		$(4,8)$	$(6,13)$	$(10,17)$
$(4,9)$			$(8,18)$	$(12,22)$
$(8,13)$				$(16,26)$

Note que S puede verse como el producto cartesiano $S = A \times B$, donde $A = \{1,2,4,8\}$ y $B = \{1,4,9,13\}$ son Conjuntos de Sidon en dimensión uno. De manera general se puede probar que si A y B son Conjuntos de Sidon en dimensión uno, entonces $A \times B$ es un Conjunto de Sidon en dimensión dos.

Ejemplo 3.3. El conjunto $S = \{(1,1),(2,2),(5,1),(10,2)\}$ es un Conjunto de Sidon en dimensión dos como se puede observar en la tabla de sumas para S.

$+$	$(1,1)$	$(2,2)$	$(5,1)$	$(10,2)$
$(1,1)$	$(2,2)$	$(3,3)$	$(6,2)$	$(11,3)$
$(2,2)$		$(4,4)$	$(7,3)$	$(12,4)$
$(5,1)$			$(10,2)$	$(15,3)$
$(10,2)$				$(20,4)$

Note que cada pareja $(q,r) \in S$, esta formada por el cociente q y el residuo r que se obtienen al dividir por 3 algún $a \in A = \{4,8,16,32\}$, donde A es un Conjunto de Sidon en dimensión uno. De manera general, se puede probar que si A es un Conjunto de Sidon en dimensión uno y $b \in \mathbb{Z}^+$, entonces el conjunto $S = \{(q,r) : a = qb + r, \text{ con } a \in A\}$ es un Conjunto de Sidon en dimensión dos.

Definición 3.2. *Sean $v = (a,b)$, $u = (c,d)$, $n = (n_1,n_2) \in \mathbb{Z}^+ \times \mathbb{Z}^+$. Se dice que v es congruente con u módulo n, lo cual se denota por $v \equiv u\,(mod\, n)$, si*

$$\begin{aligned} a &\equiv c\,(mód\, n_1) \\ b &\equiv d\,(mód\, n_2)\,. \end{aligned}$$

En caso contrario diremos v es incongruente con u módulo n lo cual se denota por $v \not\equiv u\,(mód\ n)$.

Definición 3.3. *Un conjunto* $A = \{v_1, v_2, \ldots\} \subseteq \mathbb{Z} \times \mathbb{Z}$ *se llama conjunto de Sidon módulo n (en dimensión dos) si todas las sumas de la forma*

$$v_i + v_j, \quad v_i, v_j \in A, \quad i \neq j,$$

son incongruentes módulo n, es decir

$$v_i + v_j \equiv v_k + v_l\,(mód n) \Rightarrow \{v_i, v_j\} = \{v_k, v_l\}.$$

Ejemplo 3.4. El conjunto $A = \{(1,3), (2,4), (3,2)\ (4,1)\}$ es un Conjunto de Sidon en dimensión dos modulo $(4, 5)$. Esto se observa fácilmente en la tabla de sumas de A que se muestra a continuación.

+	(1,3)	(2,4)	(3,2)	(4,1)
(1,3)	(2,1)	(3,2)	(0,0)	(1,4)
(2,4)		(0,3)	(1,1)	(2,0)
(3,2)			(2,4)	(3,3)
(4,1)				(0,2)

Definición 3.4. *Si A es un conjunto de Sidon modulo n entonces A es un Conjunto de Sidon.*

Las técnicas de conteo estudiadas en el Capitulo anterior nos permitieron obtener cotas superiores óptimas para la función $F_2(n)$. En la siguiente sección vamos a obtener cotas inferiores para la función $F_2(n)$ a partir de la construcción de conjuntos de Sidon maximales en dimensión dos.

3.1. COTAS INFERIORES PARA LA FUNCIÓN $F_2(n)$

La construcción que veremos a continuación de un conjunto de Sidon se genera sobre el grupo aditivo $G = \mathbb{Z}_{q-1} \times \mathbb{F}_q$, donde q es una potencia prima y $\mathbb{F}_q$ un campo finito con q elementos. Con esta construcción se establecen una cota inferior y una fórmula cerrada para el máximo cardinal de un conjunto de Sidon sobre el grupo aditivo aquí considerado.

Teorema 3.1. *Para todo generador* α *de* $\mathbb{F}_q^*$*, el conjunto*

$$A = \left\{(x, \alpha^x) :\ x \in \mathbb{Z}_{q-1}\right\}$$

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

Demostración. Para probar que A es un conjunto de Sidon, es suficiente probar que si $(a,b) \in \mathbb{Z}_{q-1} \times \mathbb{F}_q$, $(a,b) \neq (0,0)$, entonces en la ecuación

$$(x,\alpha^x) - (y,\alpha^y) = (a,b) \tag{3.2}$$

los valores de x y y están determinados. La igualdad 3.2 se puede escribir de la siguiente manera

$$\begin{cases} x - y \equiv a \,(\text{mód } q-1) \\ \alpha^x - \alpha^y = b \,(\text{en } \mathbb{F}_q) \end{cases} \tag{3.3}$$

donde $x = a + y + (q-1)t$ con $t \in \mathbb{Z}$, luego

$$\alpha^x = \alpha^{a+y+(q-1)t},$$

como $\left|\mathbb{F}_q^*\right| = q-1$,entonces $\alpha^{q-1} = 1$, de ahí que

$$\alpha^x = \alpha^{a+y}$$

De la primera ecuación tenemos

$$\alpha^{a+y} - \alpha^y = b \text{ en } \mathbb{F}_q,$$

luego al sustituir esta en la segunda se obtiene la ecuación $\alpha^y(\alpha^a - 1) = b$ en $\mathbb{F}_q$. Note que si $a = 0$ entonces $b = 0$, lo cual no es posible. Si $a \neq 0$, entonces $\alpha^a - 1 \neq 0$ y como α es generador de $\mathbb{F}_q^*$, entonces el valor de y queda determinado y por lo tanto también el de x. □

Ejemplo 3.5. Sea $p = 7$ un número primo y el grupo multiplicativo $\mathbb{Z}_7^* = \langle 3 \rangle$, entonces por el teorema anterior el conjunto

$$A = \{(1,3),(2,2),(3,6),(4,4),(5,5),(6,1)\}$$

es un conjunto de Sidon en dimensión dos, esto se puede evidenciar en la siguiente tabla de sumas de A.

$+$	$(1,3)$	$(2,2)$	$(3,6)$	$(4,4)$	$(5,5)$	$(6,1)$
$(1,3)$	$(2,6)$	$(3,5)$	$(4,2)$	$(5,0)$	$(0,1)$	$(1,4)$
$(2,2)$		$(4,4)$	$(5,1)$	$(0,6)$	$(1,0)$	$(2,3)$
$(3,6)$			$(0,5)$	$(1,3)$	$(2,4)$	$(3,0)$
$(4,4)$				$(2,1)$	$(3,2)$	$(4,5)$
$(5,5)$					$(4,3)$	$(5,6)$
$(6,1)$						$(6,2)$

En la anterior sección vimos como construir Conjuntos de Sidon en dimensión dos a partir de conjuntos de Sidon en dimensión uno, el siguiente resultado nos permitirá observar el caso contrario, es decir, construir Conjuntos de Sidon en dimensión uno a partir de Conjuntos de Sidon en dimensión dos, esto con el fin de obtener una buena cota inferior para la función $F_2(n)$.

Lema 3.1. *Sea $f:\ G \longrightarrow G'$ un isomorfismo entre los grupos G y G'. Si A es un conjunto de Sidon en G, entonces el conjunto $f(A) = \{f(a):\ a \in A\}$ es un conjunto de Sidon en G'.*

Demostración. Sean a, b, c y d elementos en A, y supongamos que

$$f(a)+f(b) = f(c)+f(d).$$

Como f es un isomorfismo entonces

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

como G' es grupo tenemos que

$$f((a+b)-(c+d)) = 0_{G'},$$

y aplicando otra vez el hecho de que f es isomorfismo

$$(a+b)-(c+d) = 0_G,$$

y como G es grupo

$$a+b=c+d$$

□

Esta última igualdad no es posible pues A es un conjunto de Sidon. Esto implica que $f(A)$ es un Conjunto de Sidon.

Ejemplo 3.6. Dado el primo $p=7$ y el grupo multiplicativo $\mathbb{Z}_7^*=\langle 3\rangle$, entonces del Teorema 3.1 sabemos que

$$A=\{(1,3),(2,2),(3,6),(4,4),(5,5),(6,1)\},$$

es un conjunto de Sidon en dimensión dos. Luego aplicando el resultado anterior con el isomorfismo natural $f(a,b)=[x]$ (ver ejemplo 1.1), donde $[x]$ es un elemento de $\mathbb{Z}_{7\times 6}$ tal que $x\equiv a\,(\mathrm{mod}\,6)$ y $x\equiv b\,(\mathrm{mod}\,7)$, se obtiene el conjunto de Sidon:

$$f(A)=\{2,4,5,27,31,36\}.$$

El ejemplo de anterior se puede generalizar, asi de manera general podemos demostrar este resultado.

Teorema 3.2. *Sea α un generador $\mathbb{Z}_p^*$, entonces el conjunto*

$$\left\{(p-1)\left(i-\alpha^i\right)_p+i:\ 1\leq i\leq p-1\right\}$$

es un Conjunto de Sidon en $\mathbb{Z}_{p(p-1)}$.

Demostración. Como α es un generador de $\mathbb{Z}_p^*$, entonces del Teorema 3.1 tenemos que

$$A=\left\{\left(i,\alpha^i\right):\ i\in\mathbb{Z}_{p-1}\right\},$$

es un Conjunto de Sidon en $\mathbb{Z}_{p-1}\times\mathbb{Z}_p$. Consideremos (ref) el isomorfismo: $f:\mathbb{Z}_{p-1}\times\mathbb{Z}_p\longrightarrow\mathbb{Z}_{p(p-1)}$ dado por $(a,b)=[x]$ donde x es la solución del sistema de congruencias

$$\begin{cases} x\equiv a\,(\mathrm{mod}\ p-1)\\ x\equiv b\,(\mathrm{mod}\ p)\end{cases}.$$

Aplicando f a cada $\left(i, \alpha^i\right) \in A$ entonces tenemos el sistema

$$\begin{cases} x \equiv i \,(\text{mod } p-1) \\ x \equiv \alpha^i \,(\text{mod } p) \end{cases},$$

de donde

$$\begin{cases} x = i + (p-1)t \\ x = \alpha^i + pk \end{cases}$$

para algún $t, k \in \mathbb{Z}$, así

$$(p-1)t = i - \alpha^i + pk$$

como $p-1 \equiv -1 \,(\text{mod } p)$, tenemos que $t \equiv i - \alpha^i \,(\text{mod } p)$. Donde

$$[x] = i + (p-1)\left(i - \alpha^i\right)_p .$$

Así, el conjunto

$$A = \left\{ i + (p-1)\left(i - \alpha^i\right)_p, 1 \leq i \leq p-1 \right\} \subset \mathbb{Z}_{p(p-1)} \tag{3.4}$$

por el Lema 3.1 es un Conjunto de Sidon. □

Dado que un Conjunto de Sidon en $\mathbb{Z}_m$ es también un Conjunto de Sidon en $[1, m]$ y que hay garantía de la existencia de un Conjunto de Sidon en $\mathbb{Z}_m$ con aproximadamente $m^{1/2}$ elementos (Teorema 2.4) , entonces podemos utilizar el Conjunto de Sidon del Teorema 3.2, el cual se le debe a Rusza [14], para hallar un Conjunto de Sidon en $[1, n]$ si encontramos el mayor primo p tal que $p(p-1) \leq n$.

Uno de los problemas interesantes cuando estudiamos de la distribución de los números primos consiste en hallar el menor θ que garantice que todo intervalo $\left(x - x^\theta, x\right)$ contiene algún primo para x suficientemente grande. En este sentido Baker R. C., Harman G., Pintz G. y Pintz J en [2] demuestran el siguiente resultado.

Teorema 3.3. *Para un x suficientemente grande, el intervalo* $\left[x - x^{0,525}, x\right]$*, contiene números primos.*

Este último resultado, junto con la observación hecha anteriormente nos permite obtener una cota inferior óptima para la función $F_2(n)$.

Teorema 3.4. *Sea θ con la propiedad de que para todo x suficientemente grande, el intervalo $\left(x-x^{\theta}, x\right)$ contiene algún primo. Entonces*

$$F_2(n) \geq n^{1/2} + O\left(n^{\theta/2}\right).$$

Demostración. Dado un n suficientemente grande, para $\theta \geq 0,525$, existe un primo $p \in \left(n^{1/2} - n^{\theta/2}, n^{1/2}\right)$, es decir

$$n^{1/2} - n^{\theta/2} < p < n^{1/2},$$

de donde

$$n^{1/2} - n^{\theta/2} - 1 < p - 1 < n^{1/2} - 1.$$

De lo anterior es claro que

$$p(p-1) < n^{1/2}\left(n^{1/1} - 1\right) < n,$$

y así de la observación anterior y el teorema 3.3 el conjunto $A = \left\{(p-1)\left(i-\alpha^i\right)_p + i,\ 1 \leq i \leq p-1\right\}$. Construido en el Teorema 3.2 es un conjunto de Sidon en $[1, n]$, con más de $n^{1/2} - n^{\theta/2}$ elementos. En consecuencia

$$F_2(n) \geq |A| \geq n^{1/2} - n^{\theta/2}.$$

□

Del capítulo anterior observamos que mediante la utilización de técnicas de conteo Erdös y Turán, Lindström, Rusza y Cilleruelo lograron obtener que la función $F_2(n) < \sqrt{n} + n^{1/4} + 1/2$. Así pues de esta manera se puede establecer un limite superior para la función $F_2(n)$, es decir:

Corolario 3.1. *La función $F_2(n)$ satisface la relación*

$$\lim_{n\to\infty} sup \frac{F_2(n)}{\sqrt{n}} \leq 1.$$

Demostración. Sea $\sqrt{n}+n^{1/4}+1/2$ la cota superior para $F_2(n)$, de donde:

$$F_2(n) < \sqrt{n}+n^{1/4}+1/2,$$

así

$$\frac{F_2(n)}{\sqrt{n}} < \frac{\sqrt{n}+n^{1/4}+1/2}{\sqrt{n}},$$

como $\frac{F_2(n)}{\sqrt{n}}$ esta acotado superiormente, entonces existe el supremo[1] para esta función, es decir

$$\sup\frac{F_2(n)}{\sqrt{n}} \leq \frac{\sqrt{n}+n^{1/4}+1/2}{\sqrt{n}}$$

al calcular el limite cuando n tiende al infinito obtenemos

$$\lim_{n\to\infty}\sup\frac{F_2(n)}{\sqrt{n}} \leq \lim_{n\to\infty}\frac{\sqrt{n}+n^{1/4}+1/2}{\sqrt{n}} = 1$$

y por tanto

$$\lim_{n\to\infty}\sup\frac{F_2(n)}{\sqrt{n}} \leq 1.$$

□

Por otro lado observemos que en este capítulo se obtuvo una cota inferior para la función $F_2(n)$, es decir $F_2(n) \geq n^{1/2}+O\left(n^{\theta/2}\right)$, de esta manera también se puede establecer un limite inferior para $F_2(n)$.

Corolario 3.2. *La función $F_2(n)$ satisface la relación*

$$\lim_{n\to\infty} inf\frac{F_2(n)}{\sqrt{n}} \geq 1.$$

Demostración. Note que $n^{1/2}+O\left(n^{\theta/2}\right)$ es la cota inferior para $F_2(n)$ por tanto

$$F_2(n) \geq n^{1/2}+O\left(n^{\theta/2}\right),$$

[1] Sea S un subconjunto de R, si S está acotado superiormente, entonces se dice que una cota superior u es un ***supremo*** o una ***mínima cota superior*** de S si ningún numero menor que u es cota superior de S.

de ahí que

$$\frac{F_2(n)}{\sqrt{n}} \geq \frac{n^{1/2} + O\left(n^{\theta/2}\right)}{\sqrt{n}},$$

como $\frac{F_2(n)}{\sqrt{n}}$ esta acotado interiormente, entonces existe el ínfimo[2] para esta función, es decir:

$$\inf \frac{F_2(n)}{\sqrt{n}} \geq \frac{n^{1/2} + O\left(n^{\theta/2}\right)}{\sqrt{n}},$$

al calcular el limite cuando n tiende al infinito se obtiene

$$\lim_{n\to\infty} \inf \frac{F_2(n)}{\sqrt{n}} \geq \lim \frac{n^{1/2} + O\left(n^{\theta/2}\right)}{\sqrt{n}} = 1$$

□

En consecuencia del Corolario 3.1 y Corolario 3.2 se establece la estimación asintótica para $F_2(n)$.

Teorema 3.5. $F_2(n) \sim \sqrt{n}$.

3.2. APLICACIONES

Algunos Conjuntos de Sidon en dimensión dos se han utilizado para estudiar algunos dispositivos como el Sonar (*"Sound Navigation And Ranging"*), el cual se usa como medio de localización acústica, y el Radar *("Radio Detection And Ranging")* , sistema de localización electromagnética. Estos dispositivos permiten determinar la distancia (rango) desde un objeto a la fuente, y la velocidad (razón de cambio del rango) a la cual el objeto se está acercando. En los dispositivos como el Sonar y el Radar el observador emite una señal a una frecuencia determinada y con base en el tiempo entre su emisión y recepción es posible obtener la distancia, mientras que con la diferencia entre la frecuencia emitida y la frecuencia que regresa al observador se obtiene un estimado de la velocidad relativa del objetivo. En un sistema de Radar o Sonar de salto de frecuencia ("frequency-hopping"), la señal esta formada por una o varias frecuencias escogidas de un conjunto $\{f_1, f_2, \ldots, f_m\}$ de frecuencias disponibles, las cuales son transmitidas durante cada uno de los intervalos de tiempo consecutivos $\{t_1, t_2, \ldots, t_n\}$. Para fines de modelamiento de problemas de aplicación, es sensato considerar $m = n$. La representación de

[2]Sea S subconjunto de R, si S esta acotado inferiormente, entonces se dice que una cota inferior v es un ínfimo o una máxima cota inferior de S si ningún número mayor que v es cota inferior de S.

la señal S_A se realiza a través de una matriz cuadrada $A = (a_{ij})$ de orden n, donde las filas representan las n frecuencias y las columnas los n intervalos de tiempo, así , A es una matriz de ceros y unos con $a_{ij} = 1$ si la frecuencia f_i es transmitida en el intervalo de tiempo t_j y 0 en caso contrario. Por ejemplo, la siguiente matriz A representa una señal S_A para la cual en unos intervalos de tiempo del 1 al 5, se ha emitido una frecuencia particular escogida del conjunto $\{f_1, f_2, f_3, f_4, f_5\}$.

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

En este trabajo se considerara simplemente el conjunto de las coordenadas (i, j) que corresponde a $1's$ en la representación matricial de la señal, de esta manera que el conjunto $A = \{(1,3), (2,1), (3,4), (4,2) (5,5)\}$ esta formado por las coordenadas (i, j) que tienen $1's$ en la matriz del ejemplo anterior.

El mecanismo por el cual el Sonar detecta un objeto, consiste en tomar una señal de salto de frecuencia y enviarla a través de una antena emisora, si la señal se encuentra con un objeto en su camino, esta rebotará dirigiéndose nuevamente hacia la antena pero con variaciones en la longitud de onda y en la frecuencia de cada uno de los impulsos. Estas variaciones están perfectamente explicadas por el efecto Doppler [17]. Según la cantidad de estas variaciones, es posible determinar ambos factores, distancia y velocidad. El observador determina la cantidad de estas variaciones comparando (en ambos factores, en tiempo y frecuencia) de una réplica de la señal enviada con la señal de retorno, y apuntando para cada combinación de cambio de tiempo y cambio de frecuencia la mejor coincidencia. Para llevar el conteo de estas coincidencias se utiliza una función de autocorrelación [7]. Esta función puede entenderse como el conteo de coincidencias de los $1's$ de la matriz de permutación $A = (a_{ij})$ con los $1's$ de en una versión desplazada de la misma matriz A que denotaremos como R, en el que todas las entradas se han desplazado r unidades hacia la derecha o r unidades hacia la izquierda si r es negativo , y s unidades hacia arriba o s unidades hacia abajo si s es negativo. Precisamente el número de tales coincidencias, denotado como $C(r, s)$, se denomina la función de autocorrelación o función de ambigüedad, conocida así en la literatura del Sonar y el Radar y la cual posee las siguientes

propiedades:

- $C_{AR}(0,0) = n$
- $C_{AR}(r,s) = 0$ si $|r| \geq n$ o $|s| \geq n$
- $0 \leq C_{AR}(r,s) < n$ excepto cuando $r = s = 0$

A demás si se sabe que tanto las frecuencias como los intervalos de tiempo están modulados por el ancho de banda y el tiempo de duración de la señal respectivamente, entonces el conjunto que representa la señal de retorno será un desplazamiento modulado del conjunto que representa a la señal enviada. Por ejemplo, Si $A = \{(1,3),(2,1),(3,4),(4,2)\ (5,5)\}$ representa S_A la señal que se enviá, entonces $R = A + (4,2) = \{(5,5),(1,3),(2,1),(3,4),(4,2)\}$ representa la señal S_R que retorna al emisor con un ancho de banda de longitud 5. Este cambio de frecuencias y tiempo se puede representar matricialmente como sigue:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \overset{+(4,2)}{\Longrightarrow} \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Note que $A = \{(1,3),(2,1),(3,4),(4,2)\ (5,5)\}$ y $R = \{(5,5),(1,3),(2,1),(3,4),(4,2)\}$ son iguales lo cual permite decir que $C_{AR}(4,2) = 5$, así pues la señal enviada no sufrió ningún cambio aparentemente. Sin embargo si la señal de retorno es idéntica o muy parecida a la señal de salida, no se podrá realizar un buen análisis de las variaciones, ya que la señal aparenta no tenerlas. De esta manera se necesitan señales de frecuencia de salto S_A tales que si A es el conjunto que las representa y el conjunto R representa el conjunto de las señal de retorno , entonces la función $C_{AR}(r,s)$ debe ser de mínima ambigüedad. En ese sentido se puede construir un modelo original sin ambigüedades, para ello recurrimos a la ***secuencias Sonares***. Estas secuencias fueron sugeridas por Solomon W. Golomb y Herbet Taylor en [6] las cuales son modelos de señales $m \times n$, que presenta a lo más una coincidencia en la función de autocorrelación. Por ejemplo si se dispone de un ancho de banda de longitud 4 y se enviá una señal señal S_A, cuya representación es $A = \{(1,2),(2,4),(3,3),(4,1)\}$, y esta choca contra un objeto produciendo un cambio de 1 en tiempo y 1 en frecuencia, la señal S_R de retorno al

emisor estará representada por $R = \{(2,3),(3,1),(4,4),(1,2)\}$. La representación matricial de los cambios de Frecuencia y tiempo es la siguiente:

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \begin{matrix} \\ +(1\,1) \\ \Longrightarrow \\ \\ \end{matrix} \quad \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Observe que en este caso $C_{AR}(1,1) = 1$, esto significa que a partir de estos datos podremos realizar una análisis de las variaciones de frecuencia y tiempo. Por otro lado podemos ver que el conjunto A es un Conjunto de Sidon en dimensión dos, pues este conjunto es un ejemplo del Teorema 3.1 con $p = 5$ y $\alpha = \langle 2 \rangle = \mathbb{Z}_5^*$, de ahí la importancia de la relación que existe entre los Conjuntos de Sidon en dimensión dos y las Secuencias Sonar.

En lo que sigue se mostrarán las construcciones de Secuencias Sonar que se conocen actualmente, cabe resaltar que estas construcciones requieren de elementos propios de la teoría de campos finitos. Las siguientes construcciones se pueden ver en [12].

3.2.1. Secuencias Sonar

Los conjuntos de Sidon han sido estudiados en diferentes contextos de la matemáticas y las telecomunicaciones, especialmente para representar frecuencias de diferentes tipos de señales.

Dado $n \in \mathbb{N}$, denotaremos el conjunto de enteros $\{1, 2, \cdots, n\}$ por N y por N^* el conjunto $\{0, 1, 2, \cdots, n\}$. De igual forma se denota por, $x \,(\text{mód}\, m)$ al único entero $0 \leq a \leq m-1$ tal que $x \equiv a \,(\text{mód}\, m)$.

Definición 3.5. *Una función $f : N^* \longrightarrow M^*$ tiene la propiedad de **diferencias distintas** si para todo entero i, j y h, con $1 \leq h \leq n-1$ y $1 \leq i,\ j \leq n-h$, se tiene que:*

$$f(i+h) - f(i) = f(j+h) - f(j) \Rightarrow i = j. \tag{3.5}$$

Si M^* se identifica con el conjunto de representantes de los enteros módulo m y la condición 3.5 se cambia por

$$f(i+h) - f(i) = f(j+h) - f(j)\,(mod\, m) \Rightarrow i = j.$$

f tiene la propiedad de ***diferencias modulares distintas*** .

Definición 3.6. *Una función $f: N^* \longrightarrow M^*$ que tiene la propiedad de diferencias modulares distintas, se denomina una* ***Secuencia Sonar modular de orden*** $m \times n$.

Definición 3.7. *Si $f: A \subseteq \mathbb{N} \to \mathbb{N}$ es una función, de define su grafo asociado como:*

$$G_f = \{(x,\ f(x)):\ x \in A\} \subseteq A \times \mathbb{N}.$$

Observación 3.1. Note que de la Definición 3.5 se puede establecer la relación entre conjuntos de Sidon y secuencias sonar, es decir, una función $f: [1,n] \longrightarrow [1,m]$ es una secuencia sonar modular $m \times n$ si y solo si G_f es un conjunto de Sidon en $(\mathbb{Z} \times \mathbb{Z}_m, +)$.

La siguiente construcción Sonar se debe a Welch [8] en el año 1984, la cual se denomina ***construcción de Welch logarítmica***.

Teorema 3.6. *Sea α un elemento primitivo modulo p. La función $f: [p-1] \to [p-1]^*$ definida por $f(i) = log_\alpha i$ es una secuencia sonar módulo $p-1$ con $p-1$ elementos.*

Demostración. Sea p primo y $\langle \alpha \rangle = \mathbb{Z}_p^*$ y h, i, j enteros con $1 \leq h \leq p-2$ y $1 \leq j \leq i \leq p-1-h$. Donde

$$\begin{aligned}
\log_\alpha(i+h) - \log_\alpha(i) &\equiv \log_\alpha(j+h) - \log_\alpha(j) \,(\text{mód}\, p) \\
\log_\alpha(i+h) + \log_\alpha(j) &\equiv \log_\alpha(j+h) + \log_\alpha(i) \,(\text{mód}\, p) \\
\log_\alpha((i+h)\,j) &\equiv \log_\alpha((j+h)\,i) \,(\text{mód}\, p) \\
(i+h)\,j &= (j+h)\,i \\
ij + jh &= ij + ih \\
h(j-i) &= 0.
\end{aligned}$$

Como $1 \leq h \leq p-2$ entonces $i = j$. Por lo tanto la función f es una una secuencia sonar módulo $p-1$ con $p-1$ elementos. □

Ejemplo 3.7. Sea $p = 7$ y $\langle 5 \rangle = \mathbb{Z}_7^*$. La función $f : [6] \to [6]^*$ definida por $f(i) = \log_5 i$, permite la construcción del conjunto

$$A = \{(1,0), (2,4), (3,5), (4,2), (5,1), (6,3)\},$$

el cual es una secuencia sonar modulo 6 y por tanto un conjunto de Sidon en dimensión dos con 6 elementos. Note que si disponemos de un ancho de banda 6 y un tiempo de duración de la señal de 6 segundos, del conjunto A que representa la señal de emisión S_A obtenemos $R = A + (1,4) = \{(2,4), (3,2), (4,3), (5,0), (6,5), (1,1)\}$ que corresponde a la señal S_R de retorno al emisor. La representación matricial de los cambios de Frecuencia y tiempo es la siguiente:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \quad \begin{matrix} \\ \\ +(1,4) \\ \Longrightarrow \\ \\ \\ \end{matrix} \quad \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

La siguiente construcción se debe a Welch [8] en el año 1984, la cual se denomina ***construcción Welch Exponencial Extendida***.

Teorema 3.7. *Sean α un elemento primitivo modulo p y r un entero. La función $f : [p-1]^* \to [p]^*$ definida por $f(i) = \alpha^{i+r}$ es una secuencia sonar módulo p con p elementos.*

Demostración. Sea p un número primo, r entero y $\langle \alpha \rangle = \mathbb{Z}_p^*$ y h, i, j enteros con $1 \leq h \leq p-2$ y $1 \leq j \leq i \leq p-1-h$. Por definición de secuencia sonar modular tenemos:

$$\begin{aligned} \alpha^{i+h+r} - \alpha^{i+r} &\equiv \alpha^{j+h+r} - \alpha^{j+r} \,(\text{mód}\, p) \\ \alpha^i \left(\alpha^{h+r} - \alpha^r\right) &\equiv \alpha^j \left(\alpha^{h+r} - \alpha^r\right) (\text{mód}\, p) \end{aligned}$$

Como $1 \leq h \leq p-2$ entonces $\alpha^{h+r} \not\equiv \alpha^r \,(\text{mód}\, p)$, por lo tanto $\alpha^i \equiv \alpha^j \,(\text{mód}\, p)$, es decir, $\alpha^{i-j} \equiv 1 \,(\text{mód}\, p)$. Ahora como $i - j \leq p-2$, entonces $i = j$, en consecuencia la función f es una secuencia

sonar módulo p con p elementos. □

Ejemplo 3.8. Considere $p = 7$, $r = 2$ y $\langle 3\rangle = \mathbb{Z}_7^*$. La función $f : [6]^* \to [7]$ definida por $f(i) = 3^{i+2} \pmod 7$ proporciona el siguiente conjunto

$$\{(0,2),(1,6),(2,4),(3,5),(4,1),(5,3),(6,2)\},$$

el cual es una secuencia sonar módulo 7 y por tanto un conjunto de Sidon en dimensión dos con 7 elementos. Observe que si disponemos de un ancho de banda 7 y un tiempo de duración de la señal de 7 segundos, del conjunto A que representa la señal de emisión S_A obtenemos $R = A + (1,4) = \{(1,6),(2,3),(3,1),(4,2),(5,5),(6,7),(0,6)\}$ que corresponde a la señal S_R de retorno al emisor. La representación matricial de los cambios de Frecuencia y tiempo es la siguiente:

$$\begin{bmatrix} 0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&1&0&0&0\\ 0&0&0&0&1&0&0\\ 1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&1&0&0&0&0&0 \end{bmatrix} \overset{+(1,4)}{\Longrightarrow} \begin{bmatrix} 0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0\\ 0&0&1&0&0&0&0\\ 1&0&0&0&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1 \end{bmatrix}$$

La siguiente construcción aparece en [12], la cual se denomina ***construcción Cuadrática***.

Teorema 3.8. *Sean p primo impar y a,b,c constantes enteras con $a \not\equiv 0 \,(mod\ p)$. La función $f(i) : [p+1] \to [p]$ definida por $f(i) = ai^2 + bi + c \,(mod\ p)$ es una secuencia sonar modulo p, con $p+1$ elementos.*

Demostración. Consideremos h, i, j enteros tales que $1 \leq h \leq p$, $1 \leq j \leq i \leq p+1-h$. De donde tenemos que:

$$a(i+h)^2 + b(i+h) + c - \left(ai^2 + bi + c\right) \equiv a(j+h)^2 + b(j+h) + c - \left(aj^2 + bj + c\right) \pmod p,$$

desarrollando obtenemos

$$2aih \equiv 2ajh \,(\mathrm{mod}\, p)\,.$$

Como p es primo impar y $a \not\equiv 0 \,(\mathrm{mod}\, p)$ entonces $2a$ es invertible y por tanto tenemos

$$h\,(i-j) \equiv 0 \,(\mathrm{mod}\, p)\,.$$

consideramos los siguientes casos

- Si $h = p$ entonces $i = j = 1$ y por tanto se tendría la prueba.
- Si $h \neq p$ entonces $i - j \equiv 0 \,(\mathrm{mod}\, p)$ y dadas las condiciones tanto de i como de j se tiene que $i - j \leq p - 1$, donde $i = j$

□

Ejemplo 3.9. Sea $p = 7$, $a = 3$, $b = 1$, $c = 2$. Así la función $f : [8] \to [7]$ dada por $f\,(i) = 3i^2 + i + 2 \,(\mathrm{mód}\, 7)$ proporciona el siguiente conjunto

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

el cual es una secuencia sonar módulo 7 y por tanto un conjunto de Sidon en dimensión dos con 8 elementos. Observe que si disponemos de un ancho de banda 7 y un tiempo de duración de la señal de 8 segundos, del conjunto A que representa la señal de emisión S_A, entonces obtenemos $R = A + (1,1) = \{(2,7)\,,(3,3)\,,(4,5)\,,(5,6)\,,(6,6)\,,(7,5)\,,(8,3)\,,(1,7)\}$ que corresponde a la señal S_R de retorno al

emisor. La representación matricial de los cambios de Frecuencia y tiempo es la siguiente:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad \begin{matrix} \\ \\ \\ \\ +(1,1) \\ \Longrightarrow \\ \\ \\ \end{matrix} \quad \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

La siguiente construcción denominada ***Shift*** proviene de [12] y la cual miraremos en detalle a a continuación:

Teorema 3.9. *Sea p un primo, α un elemento primitivo de $\mathbb{F}_{p^{2r}}$ y β un elemento primitivo de $\mathbb{F}_{p^r}$. La función $f : A \longrightarrow [p^r-1]^*$ definida $f(i) = log_\beta\left(\left(\alpha^i\right)^{p^r} + \alpha^i\right)$, donde $A = [p^r]^*$ si $p = 2$ y $A = \{i : -(p^r-1)/2 \leq i \leq (p^r-1)/2\}$ si p es impar, define una secuencia sonar modulo p^r-1 con p^r elementos.*

Demostración. Sea h, i, j enteros con $1 \leq h \leq p^r-1$, $-(p^r-1)/2 \leq i \leq (p^r-1)/2-h$, ademas consideremos la expresión $T(i) = \alpha^{ip^r} + \alpha^i$, que corresponde a la traza de α^i sobre el subcampo $\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^{2r}}$ así:

$$\log_\beta\left(\frac{T(i+h)}{T(i)}\right) = \log_\beta\left(\frac{T(j+h)}{T(j)}\right),$$

esto significa que

$$\frac{\left(\alpha^{i+h}\right)^{p^r} + \alpha^{i+h}}{\left(\alpha^i\right)^{p^r} + \alpha^i} = \frac{\left(\alpha^{j+h}\right)^{p^r} + \alpha^{j+h}}{\left(\alpha^j\right)^{p^r} + \alpha^j},$$

donde

$$\alpha^h\left(\frac{\left(\alpha^{i+h}\right)^{p^r-1}+1}{\left(\alpha^i\right)^{p^r-1}+1}\right) = \alpha^h\left(\frac{\left(\alpha^{j+h}\right)^{p^r-1}+1}{\left(\alpha^j\right)^{p^r-1}+1}\right),$$

esto implica

$$\begin{aligned}\left(\alpha^{i+j+h}\right)^{p^r-1}+\left(\alpha^{i+h}\right)^{p^r-1}+\left(\alpha^{j}\right)^{p^r-1}+1 &= \left(\alpha^{i+j+h}\right)^{p^r-1}+\left(\alpha^{j+h}\right)^{p^r-1}+\left(\alpha^{i}\right)^{p^r-1}+1\\ \left(\alpha^{i}\right)^{p^r-1}\left(\left(\alpha^{h}\right)^{p^r-1}-1\right) &= \left(\alpha^{j}\right)^{p^r-1}\left(\left(\alpha^{h}\right)^{p^r-1}-1\right).\end{aligned}$$

Como $h \leq p^r-1$, y dado que α es un generador tenemos que $\left(\alpha^h\right)^{p^r-1} \neq 1$, así $\left(\alpha^{j-i}\right)^{p^r-1}=1$, de donde $j-i \leq p^r-1$, y por lo tanto debemos tener que $i=j$. □

Ejemplo 3.10. Sea $p=5$, $r=1$, $\langle 3\alpha+2\rangle = \mathbb{F}_{5^2}^*$ y $\langle 2\rangle = \mathbb{F}_5^*$. En este caso $f:\{-2,-1,0,1,2\} \to \{1,2,3,4\}$ que esta definida por $f(i)=\log_2\left((3\alpha+2)^{5i}+(3\alpha+2)^{i}\right)$. Asi de esta manera se construye el conjunto $\{(-2,3),(-1,1),(0,1),(1,2),(2,1)\}$, que al aplicarle la traslación $(3,0)$ obtenemos el conjunto

$$\{(1,3),(2,1),(3,1),(4,2),(5,1)\},$$

que es una secuencia sonar módulo 4 y por lo tanto un conjunto de Sidon en dimensión dos con 5 elementos. Observe que si disponemos de un ancho de banda 5 y un tiempo de duración de la señal de 4 segundos, del conjunto A que representa la señal de emisión S_A obtenemos $R=A+(1,4)=\{(2,3),(3,1),(4,1),(5,2),(1,1)\}$ que corresponde a la señal S_R de retorno al emisor. La representación matricial de los cambios de Frecuencia y tiempo es la siguiente:

$$\begin{bmatrix}0&0&1&0&0\\1&0&0&0&0\\1&0&0&1&0\\0&1&0&0&0\\1&0&0&0&0\end{bmatrix} \xrightarrow[\Longrightarrow]{+(1,4)} \begin{bmatrix}1&0&0&0&0\\0&0&1&0&0\\1&0&0&0&0\\1&0&0&0&0\\0&1&0&0&0\end{bmatrix}$$

En la siguiente construcción si $\alpha \neq \beta$ esta construcción se denomina ***Construcción de Golomb*** o ***construcción Lempel*** si $\alpha=\beta$, (ver [8], [12]).

Teorema 3.10. *Sea $q \geq 2$ una potencia prima, y sean α, β elementos primitivos de $\mathbb{F}_q$. La función $f:[q-2] \to [q-1]$ definida por $f(i)=j$ si y solo si $\alpha^i+\beta^j=1$ es una secuencia sonar modular*

$(q-1)$ *con* $q-2$ *elementos* .

Demostración. Observe que si $\alpha^i+\beta^j=1$, podemos escribir $j=\log_\beta\left(1-\alpha^i\right)$. Ademas se tiene que $1-\alpha^i\neq 0$ ya que $1\leq i\leq q-2$. Ahora sean h, i, j enteros tales que $1\leq h\leq q-3$ y $1\leq j\leq i\leq q-2-h$, de donde:

$$\log_\beta\left(\left(1-\alpha^{i+h}\right)\left(1-\alpha^i\right)\right)\equiv\log_\beta\left(\left(1-\alpha^{j+h}\right)\left(1-\alpha^j\right)\right),$$

y dado que la función logaritmo es inyectiva entonces

$$\begin{aligned}\left(1-\alpha^{i+h}\right)\left(1-\alpha^i\right) &= \left(1-\alpha^{j+h}\right)\left(1-\alpha^j\right)\\ 1-\alpha^{i+h}-\alpha^j+\alpha^{i+j+h} &= 1-\alpha^{j+h}-\alpha^i+\alpha^{i+j+h}\\ \alpha^i-\alpha^{i+h} &= \alpha^j-\alpha^{j+h}\\ \alpha^i\left(1-\alpha^h\right) &= \alpha^j\left(1-\alpha^h\right)\end{aligned}$$

Como $1\leq h\leq q-3$ se tiene que $\alpha^h-1\neq 0$ y por lo tanto $\alpha^i=\alpha^j$ dado que α es generador $\mathbb{F}_q^*$, entonces $i=j$. □

Ejemplo 3.11. Sea $p=2$ y $\langle\alpha\rangle=\left\langle\beta=\alpha^3\right\rangle=\mathbb{F}_{2^3}^*$. La función $f:[6]^*\to[7]^*$ definida por $f(i)=\log_{\alpha^3}\left(1-\alpha^i\right)$ permite construir el conjunto

$$A=\{(1,1),(2,2),(3,5),(4,4),(5,6),(6,3)\},$$

el cual es una secuencia sonar módulo 7 y por tanto un conjunto de Sidon en dimensión dos con 6 elementos. Observe que si disponemos de un ancho de banda 6 y un tiempo de duración de la señal de 6 segundos, del conjunto A que representa la señal de emisión S_A obtenemos $R=A+(1,4)=\{(2,5),(3,6),(4,3),(5,2),(6,4),(1,1)\}$ que corresponde a la señal S_R de retorno al emisor. La

representación matricial de los cambios de Frecuencia y tiempo es la siguiente:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \quad \begin{matrix} \\ \\ +(1,4) \\ \Longrightarrow \\ \\ \\ \end{matrix} \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Capítulo 4

CONCLUSIONES

En el desarrollo de este trabajo se pudo concluir lo siguiente:

1. En el Capitulo 1, se estudiaron los Conjuntos de Sidon en dimensión 1, así como la función $F_2(n)$ para la cual se encontró una cota superior óptima dada por:

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

2. En capitulo 2, construimos conjuntos de Sidon en dimensión dos y se mostraron ejemplos particulares de estos conjuntos mediante a partir de conjuntos de Sidon en dimensión uno.
   Mediante el Lema 3.1 se construyó un Conjunto de Sidon en dimensión uno, a partir de un Conjunto de Sidon en dimensión dos, esto con el fin de establecer una cota inferior para la función $F_2(n)$, esta cota esta dada por:

$$F_2(n) \geq n^{1/2} + O\left(n^{\theta/2}\right).$$

3. A partir de los resultados de los Capítulos 1 y 2 se concluyó que la función $F_2(n)$ es asintóticamente $\sqrt{n}$, es decir, $F_2(n) \sim \sqrt{n}$ o equivalentemente a $\lim_{n\to\infty} \frac{F_2(n)}{\sqrt{n}} = 1$.

4. En la Sección 2.2, del capitulo 2, de este trabajo se pudo ver la importancia que tiene los Conjuntos de Sidon en dimensión dos para el modelamiento de algunas aplicaciones en el área de las telecomunicaciones, específicamente a las Secuencias Sonar.

Bibliografía

[1] APOSTOL, T. Introducción a la Teoría Analítica de Números. Editorial Reverté España, 1980.

[2] BAKER R. C., HARMAN G., PINTZ G. and PINTZ J . The difference between consecutive primes, II. Proceedings of the London Mathematical Society 83 (3): p 532-5-62.

[3] CILLERUELO J., Sidon sets in $\mathbb{N}^d$. J. Combin. Theory Ser. A 117, 2010, no. 7, p 857-871.

[4] CILLERUELO J., Conjuntos de Sidon. Escuela Venezolana de Matemáticas, 2014.

[5] ERDÖS P and TURAN P . On a problem of Sidon in additive number theory, and on some related problems, J. London Math. Soc. 16 (1941), p 212-215.

[6] GOLOMB S. and TAYLOR H., Two-dimensional.synchronization. patterns. for. minimum. ambiguity, IEEE. Trans. Inform. Theory, vol. IT-28, (1982): p 263-272.

[7] GOLOMB S. and TAYLOR H., Constructions and properties of Costas arrays, Proceedings of the IEEE 72 , No. 9, (1984): p 1143-1163.

[8] GOLOMB S. Algebraic constructions for Costas arrays, J. Combin. Theory (A), 37, (1984): p 13-21.

[9] KEN T., SCOTT R. and KONSTANTINOS D. Costas arrays: survey, standardization, and matlab toolbox, ACM Transactions on Mathematical Software , (TOMS) 37 (2011): p 4-41.

[10] LIDL R. and NIEDERREITER H. Introduction to finite fields and their applications. Cambridge University Press. 1986.

[11] LINDSTROM B. An inequality for $B_2 - sequences$, J. Combinatorial Theory 6 (1969): p 211-212.

[12] MORENO O. GAMES R. and TAYLOR H. Sonar sequences from Costas arrays and the best known sonar sequences with up to 100 symbols, Information Theory, IEEE Transactions, 39 (1993), no. 6: p 1985-1987.

[13] O'BRYANT K. A Complete Annotated Bibliography of Work Related to Sidon Sequences, Electronic Journal of Combinatorics, DS11(2004).

[14] RUZSA I. Solving a linear equation in a set of integers. I. Acta Arith. 65 (1993), no. 3: p 259-282.

[15] TERENCE T. & VAN H. Additive combinatorics, Cambridge Studies in Advanced Mathematics, Cambridge University Press, (2006).

[16] VAN GELDER B. Algoritmos computacionales Introducción al análisis y diseño, 3ªed. Mexico, Thomson, 2002.

[17] ZEMANSKY S. and FREEDMAN Y. Fisica Universitaria, Vol. I y II, Pearson, 1999.