CONJUNTOS DE SIDON Y REGLAS GOLOMB

EDUAR BOLIVAR ANACONA OBANDO

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
DEPARTAMENTO DE MATEMÁTICAS
POPAYÁN

2006

CONJUNTOS DE SIDON Y REGLAS GOLOMB

EDUAR BOLIVAR ANACONA OBANDO

TRABAJO DE GRADO

En la modalidad de seminario de grado presentado como requisito parcial para optar al título de Matemático

Director

Dr. CARLOS ALBERTO TRUJILLO

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN

DEPARTAMENTO DE MATEMÁTICAS

POPAYÁN

2006

CONJUNTOS DE SIDON Y REGLAS GOLOMB

EDUAR BOLIVAR ANACONA OBANDO

DOCUMENTO DEL SEMINARIO DE GRADO, REALIZADO CON EL GRUPO DE INVESTIGACIÓN "ÁLGEBRA, TEORÍA DE NÚMEROS Y APLICACIONES"DE LA ESCUELA REGIONAL DE MATEMÁTICAS E.R.M

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
DEPARTAMENTO DE MATEMÁTICAS
POPAYÁN
2006

Nota de aceptación

Director

Doctor Carlos Alberto Trujillo Solarte

Comité evaluador

Profesor Freddy William Bustos

Magister Julian Garces Arango.

Fecha de sustentación: Popayán, Enero 20 de 2006

Este triunfo a Dios, a la Universidad mis mas sinceros agradecimientos, a mis compañeros y amigos, mis mas grandes recuerdos; a mis hermanas que han confiado en mi, mi gratitud sincera; a mi madre ofrezco mi amor, por su entrega, colaboración y sacrificio, sin los cuales no hubiera sido posible este gran triunfo. Al profesor Carlos Alberto Trujillo, mi gratitud, por su paciencia y grandes enseñanzas.

Índice general

Índice de figuras

Índice de cuadros

Resumen

Este documento contiene el informe del Trabajo de Grado en modalidad seminario, titulado "Conjuntos de Sidon y reglas Golomb "realizado dentro del grupo de Fundamentos Matemáticos en la línea de Teoría de Números Aditiva.

Sea $A \subseteq \mathbb{Z}$, A es un conjunto de Sidon si todas las sumas de la forma $a + a'$, con $a, a' \in A$, son distintas.

$A \subseteq \mathbb{Z}$ es una regla Golomb si todas las diferencias de la forma $a - a'$, con $a, a' \in A$ y $a \neq a'$, son distintas.

En el primer y segundo capítulo se presenta un análisis de algunas de las propiedades más importantes de los conjuntos de Sidon y reglas Golomb. Se prosigue en el tercer capítulo con el estudio de las construcciones conocidas para conjuntos de Sidon y reglas Golomb y algunas de sus implicaciones en estos dos campos. El estudio de tales construcciones se ha complementado con ejemplos para una mayor facilidad en su comprensión.

Luego de estudiar las propiedades y las construcciones conocidas para conjuntos de Sidon y reglas Golomb, en el capítulo 4 se hace un estudio de las funciones extremas que se pueden definir en estas dos áreas, la función $F_2(N)$ y la función $G(k)$, que informalmente se pueden describir como sigue:

$F_2(N)$: Máximo número de elementos que pueden seleccionarse de los primeros N enteros positivos de tal forma que constituyan un conjunto de Sidon.

$G(k)$: Mínima longitud ($\text{máx}A - \text{mín}A$) tal que A es una regla Golomb, con $|A| = K$.

Se destacan en este estudio las relaciones que existen entre la función $F_2(N)$ y la función $G(k)$.

Por último en el capítulo 5 se enuncian algunos campos en los cuales las reglas Golomb y los conjuntos de Sidon tienen aplicación.

INTRODUCCIÓN

Sea $A \subseteq \mathbb{Z}$, A es un conjunto de Sidon si todas las sumas de la forma $a + a'$, con $a, a' \in A$, son distintas. Por otra parte si las diferencias de la forma $a - a'$, con $a, a' \in A$ y $a \neq a'$, son todas distintas, se dice que A es una regla Golomb.

Los problemas que tienen que ver con conjuntos de Sidon y reglas Golomb, han sido estudiados desde 1930 y 1960 respectivamente, destacándose por sus trabajos en este campo: Simon Sidon, Salomon Golomb, Paúl Erdös, Paúl Turán, R. Bose, S. Chowla, Imre Ruzsa, Javier Cilleruelo, Carlos Alberto Trujillo entre otros.

Simon Sidon fue el primer investigador que consideró el problema de los conjuntos que hoy llevan su nombre, en relación con su trabajo en Análisis de Fourier. Paúl Erdös y Paúl Turán fueron los primeros investigadores en realizar un estudio sistemático de los conjuntos de Sidon, de hecho fueron ellos quienes en 1940 publicaron un primer artículo sobre este tópico.

Las reglas Golomb fueron primero estudiadas por Babcock en 1953, en relación con su trabajo en problemas sobre interferencia entre canales de comunicación. Salomon Golomb fue el primer investigador que estudió sistemáticamente estas reglas en 1960, y desde entonces su nombre es asociado con estas construcciones.

La relación entre los dos problemas es hoy bien clara puesto que:

"A es un conjunto de Sidon si y solo si A es una regla Golomb".

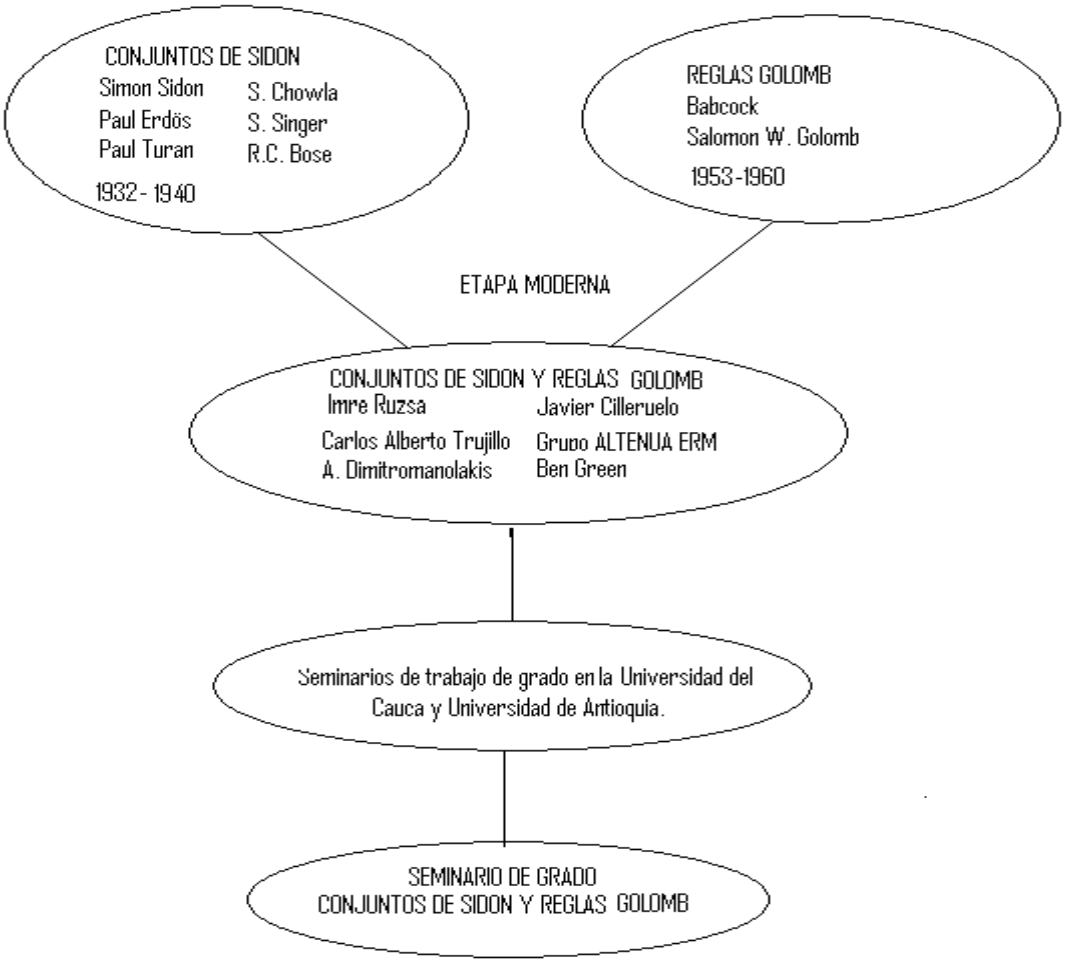
Actualmente, en la Universidad del Cauca el grupo de investigación ALTENUA, "Álgebra, Teoría de Números y Aplicaciones, "de la Escuela Regional de Matemáticas, "ERM", tiene a su cargo dos proyectos de investigación relacionados con estos dos problemas.

Los proyectos de investigación del grupo son:

- "Sucesiones de Sidon y Conjuntos $B_h[g]$". Código COLCIENCIAS $1103-05-11450$.
- "Las Funciones de Graham & Sloane: Problemas de Empaquetamiento y Cubrimiento". Código COLCIENCIAS $1103-05-16865$.

Los resultados obtenidos por el grupo ALTENUA han sido fundamentales en el desarrollo de este trabajo.

El siguiente cuadro resume esta introducción y ubica este trabajo con referencia a la evolución de los problemas que son objeto de estudio.



Capítulo 1

CONJUNTOS DE SIDON

En este capítulo estudiamos un problema de teoría de números aditiva, los conjuntos de Sidon o también llamados conjuntos B_2 por algunos autores. Se presenta un estudio de las principales propiedades de estos conjuntos, así mismo se definen la función F_2 y la función f_2, funciones extremas de las cuales en el presente trabajo interesa estudiar su comportamiento asintótico considerando cotas superiores y cotas inferiores para cada una de ellas.

1.1. Historia del problema

Los conjuntos de Sidon son llamados así después de Simón Sidon, quien fue el primer investigador en proponer este problema en 1932, [1]. Sidon consideró el problema cuando investigaba cuestiones relacionadas con Análisis de Fourier.

Paul Erdös, un matemático destacado del siglo XX, conoció el problema a través de Sidon quedando fascinado por éste, pues estaba estrechamente relacionado con Teoría de Números y Combinatoria, los dos campos en los cuales había trabajado la mayor parte del tiempo. Él le llamo a este problema "Conjuntos de Sidon" y con Paul Turán, publicaron un documento clásico de 1940 *"Un problema de Sidon en Teoría de Números Aditiva"* [10]. Este documento fue el primer tratado sistemático del problema.

Desde entonces, numerosos autores han mejorado los resultados de Erdös y Turán. No obstante, los esfuerzos han sido limitados pues no hay una solución general del problema.

1.2. Conjuntos de Sidon

Un conjunto de Sidon es un conjunto A de enteros, el cual tiene la propiedad de que para cada dos elementos a, a' del conjunto A no necesariamente distintos, todas las sumas de la forma $a + a'$ son diferentes.

1.2.1. Definición de conjunto de Sidon

Una definición formal de Conjunto de Sidon se dará a continuación, pero primero se definirá la función de representación para cada entero s; es una función de conteo que hace refierencia al número de maneras en que el entero s se puede representar como suma de dos elementos de un conjunto.

Definición 1. ***(Función de representación)*** *Sea $A \subseteq \mathbb{Z}$, mediante $\sigma_A(s)$ denotamos el número de formas en que el entero s puede ser representado como suma de dos elementos de A no necesariamente distintos. Es decir:*

$$\sigma_A(s) = |\{(a, a') \in A \times \ A : a \leq a', s = a + a'\}|,$$

en donde $|x|$ representa el cardinal del conjunto x. $\sigma_A(s)$ es la función de representación aditiva asociada con A.

Definición 2. ***(Conjunto de Sidon)*** *A se llama un conjunto $B_2[g]$ si $\sigma_A(s) \leq g$ para todo $s \in \mathbb{Z}$. Cuando $g = 1$ los conjuntos $B_2[1]$ se llaman conjuntos de Sidon o conjuntos B_2. De esta manera: $A \subseteq \mathbb{Z}$ es un conjunto de Sidon si las sumas de la forma $a + a'$, con a, a' en A, son todas distintas.*

NOTACIÓN

Mediante $[1, N]$, B_2,$B_2(N)$ y $A + A$, se representan los siguientes conjuntos

$$[1, N] = \{1, 2, ..., N\}$$
$$B_2 = \{A \subseteq \mathbb{Z} : \text{A es un conjunto de Sidon}\}$$
$$B_2(N) = \{A \subseteq [1, N] : A \in B_2\}$$
$$A + A = \{a + a' : a, a' \in A\}$$

OBSERVACIONES

1. Puesto que las sumas en un conjunto de Sidon A, son todas distintas debe darse que:

   A es un conjunto de Sidon si y sólo si

   $$|A + A| = \binom{k+1}{2} = \frac{k(k+1)}{2},$$

   en donde $|A| = k$

2. Para demostrar que un conjunto $A \subseteq \mathbb{Z}$ es un conjunto de Sidon debemos probar que:

   $$a + a' = b + b' \Rightarrow ((a = b \quad y \quad a' = b') \quad \text{o} \quad (a = b' \quad y \quad a' = b))$$

   Para todos $a, a', b, b' \in A$.

Veamos algunos ejemplos de conjuntos de Sidon:

Ejemplo 1.

Sea $A = \{1, 4, 6\}$; las sumas de los elementos de A se muestran en la siguiente tabla

+	1	4	6
	2	5	7
		8	10
			12

Como todas son distintas, A es un conjunto de Sidon.

Ejemplo 2. ***Un conjunto de Sidon infinito:***

Sea $\theta \geq 2$ en $\mathbb{Z}$, el conjunto:

$$A = \left\{\theta^a : a \in \mathbb{Z}^+ \cup \{0\}\right\}$$

es un conjunto de Sidon infinito. En otras palabras el conjunto de las potencias no negativas de un entero $\theta \geq 2$, es un conjunto de Sidon infinito.

En efecto; sean a, b, c, d, enteros no negativos, tales que:

$$\theta^a + \theta^b = \theta^c + \theta^d$$

con $a \leq b$ y $c \leq d$. Basta probar que:

$$(a = c \quad y \quad b = d)$$

Supongase que $a < c$, por lo cual tenemos:

$$1 + \theta^{b-a} = \theta^{c-a} + \theta^{d-a}$$

Lo cual implica que:

$$1 = \theta K, \quad \text{en donde} \quad K = \theta^{c-a-1} + \theta^{d-a-1} - \theta^{b-a-1}$$

que no es posible, puesto que $\theta \geq 2$.

De la misma forma se prueba que $c < a$ no puede darse y por lo tanto $a = c$. Se sigue entonces que $b = d$. por lo tanto

$$\left(\theta^a = \theta^c \quad y \quad \theta^b = \theta^d\right).$$

En consecuencia, el conjunto A de las potencias no negativas de θ es un conjunto de Sidon.

Ejemplo 3.

Sea $A = \{1, 2, 3, 4, \}$ su tabla de sumas es:

$+$	1	2	3	4
	2	3	4	5
		4	5	6
			6	7
				8

En esta tabla se puede ver por ejemplo que $4 = 2 + 2$ y $4 = 3 + 1$, por lo tanto A no es un conjunto de Sidon.

Ejemplo 4.

En un conjunto de Sidon no puede haber tres enteros en progresión aritmética. Puesto que si A es un conjunto de Sidon tal que $a, a + b, a + 2b \in A$ entonces

$$a + (a + 2b) = (a + b) + (a + b).$$

1.2.2. Propiedades de los conjuntos de Sidon

Cuando conocemos que un conjunto A dado es un conjunto de Sidon podemos a partir de él encontrar nuevos conjuntos de Sidon, pues existen transformaciones bajo las cuales la propiedad de ser conjunto de Sidon permanece invariante, este hecho se puede apreciar en la siguiente proposición.

Proposición 1. *Sea $A \subseteq \mathbb{Z}$ un conjunto de Sidon, entonces*

1. *Para cada entero x el conjunto $x + A = \{a + x : a \in A\}$ es un conjunto de Sidon.*
2. *Para cada entero $x \neq 0$, el conjunto $xA = \{ax : a \in A\}$ es un conjunto de Sidon.*
3. *Para cada entero x el conjunto $x - A = \{x - a : a \in A\}$ es un conjunto de Sidon.*

Prueba.

Se probará solamente la parte (1), ya que para la prueba de las partes (2) y (3) se procede de forma analóga.

Para ello designemos cada elemento de $x + A$ por $x_a = x + a$, con a en A y sean $x_a, x_{a'}, x_b, x_{b'}$, en $x + A$ tales que:

$$x_a + x_{a'} = x_b + x_{b'}$$

Por definición de $x + A$, tenemos:

$$(a + x) + (a' + x) = (b + x) + (b' + x)$$

De lo cual se tiene que:

$$a + a' = b + b'$$

Entonces, puesto que A es un conjunto de Sidon,

$$(a = b \quad y \quad a' = b') \quad \text{o} \quad (a = b' \quad y \quad a' = b)$$

por lo tanto

$$(a + x = b + x \quad y \quad a' + x = b' + x) \quad \text{o} \quad (a + x = b' + x \quad y \quad a' + x = b + x)$$

así, se tiene que

$$(x_a = x_b \quad y \quad x_{a'} = x_{b'}) \quad \text{o} \quad (x_a = x_{b'} \quad y \quad x_{a'} = x_b)\,,$$

Como consecuencia se concluye que el conjunto $x + A$ es un conjunto de Sidon. □

NOTA: Las afirmaciones 1 y 2 de la proposición anterior reciben el nombre de propiedad de traslación y propiedad de multiplicación, respectivamente, de los conjuntos de Sidon.

1.3. Conjuntos de Sidon modulares

El concepto de conjunto de Sidon puede considerarse en los enteros módulo n.

Definición 3. ***(Conjunto de Sidon modular)*** *Decimos que $A \subseteq \mathbb{Z}$ es un conjunto de sidon módulo n o un conjunto $B_2(mód\ n)$, si todas las sumas de la forma $a + a'$, son incongruentes módulo n.*

Ejemplo 5.

En $\mathbb{Z}_7$ el conjunto $A = \{1, 2, 6\}$ es un conjunto de Sidon módulo 7,

$+$	1	2	6
	2	3	0
		4	1
			5

Las sumas de sus elementos son todas incongruentes módulo 7.

Teorema 1. *Todo conjunto de Sidon modular es un conjunto de Sidon.*

Prueba.

Sea $n \geq 2$ un entero, $A \subseteq \mathbb{Z}$ un conjunto de Sidon módulo n y $a, a', b, b' \in A$, tales que:

$$a + a' = b + b'$$

Entonces,

$$a + a' \equiv b + b' \,(\text{mód } n)$$

Como A es conjunto de Sidon módulo n, tenemos:

$$(a = b \quad y \quad a' = b') \quad \text{o} \quad (a = b' \quad y \quad a' = b)$$

Y por lo tanto A es un conjunto de Sidon. □

Proposición 2. ***(Propiedades de los conjuntos de Sidon modulares)*** *Sean $n \geq 2$ y $A \subseteq \mathbb{Z}$ un conjunto de Sidon módulo n, entonces*

1. *Para cada entero x, el conjunto $x + A = \{a + x : a \in A\}$ es un conjunto de Sidon módulo n.*

2. *Para cada entero x, tal que $mcd\,(x, n) = 1$, el conjunto $xA = \{ax : a \in A\}$ es un conjunto de Sidon módulo n.*

3. *Para cada entero x, el conjunto $x - A = \{x - a : a \in A\}$ es un conjunto de Sidon módulo n.*

Prueba.

Se probará solamente la parte (2), ya que para la prueba de la partes (1) y (3) se procede de forma analóga.
Para ello designemos cada elemento de xA por $x_a = ax$, con a en A y sean $x_a, x_{a'}, x_b, x_{b'}$, en xA tales que:

$$x_a + x_{a'} \equiv x_b + x_{b'} \,(\text{mód } n)$$

Por definición de xA, tenemos:

$$(ax) + (a'x) \equiv (bx) + (b'x) \,(\text{mód } n)\,,$$

puesto que $mcd(x, n) = 1$:

$$a + a' \equiv b + b' \,(\text{mód } n)\,,$$

entonces, como A es un conjunto de Sidon módulo n,

$$(a = b \quad y \quad a' = b') \quad \text{o} \quad (a = b' \quad y \quad a' = b)\,,$$

por lo tanto

$$(ax = bx \quad y \quad a'x = b'x) \quad \text{o} \quad (ax = b'x \quad y \quad a'x = bx)\,.$$

así, se tiene que

$$(x_a = x_b \quad y \quad x_{a'} = x_{b'}) \quad \text{o} \quad (x_a = x_{b'} \quad y \quad x_{a'} = x_b)\,,$$

En consecuencia xA es un conjunto de Sidon módulo n. □

1.4. La función $F_2(N)$ y la función $f_2(N)$

Para todo $N \geq 3$, puesto que no todos los elementos de $[1, N] = \{1, 2, 3, .., N\}$ pueden ser seleccionados para formar un conjunto de Sidon, existe un máximo número de elementos que puede ser seleccionado, este número se denota por $F_2(N)$, de manera analóga en

el caso modular se busca encontrar el máximo cardinal de un conjunto de Sidon módulo N contenido en $\mathbb{Z}_N$, este cardinal para cualquier N se denota por $f_2(N)$.

Definición 4. ***(Función*** F_2***)*** *Definimos* $F_2(N)$ *como el máximo tamaño de un conjunto de Sidon contenido en* $[1, N] = \{1, 2, 3, .., N\}$ *es decir:*

$$F_2(N) = \max\{|A| : A \in B_2(N)\}$$

OBSERVACIONES

1. De la definición de $F_2(N)$, se puede ver que $F_2(N)$ es una función no decreciente:

$$N \geq M \Rightarrow F_2(N) \geq F_2(M)$$

2. Se puede calcular una cota superior sencilla para $F_2(N)$.

   Sea $A \in B_2(N)$ y $|A| = k$, por lo tanto, como A es un conjunto de Sidon y $A + A \subseteq [2, 2N]$ se tiene que:

$$|A + A| = \binom{k+1}{2} = \frac{k(k+1)}{2} \leq 2N - 1$$

   De lo cual:

$$k(k+1) \leq 4N - 2$$

   Y completando cuadrados

$$\left(k + \frac{1}{2}\right)^2 \leq 4N - \frac{7}{4}$$

   En consecuencia;

$$k \leq \sqrt{4N - \frac{7}{4}} - \frac{1}{2}$$

   En particular;

$$F_2(N) \leq \sqrt{4N - \frac{7}{4}} - \frac{1}{2} \tag{1.1}$$

Definición 5. ***(Función*** f_2***)*** *Definimos* $f_2(N)$ *como el máximo cardinal de un Conjunto de Sidon módulo* N *es decir:*

$$f_2(N) = \max\{|A| : A \in B_2(\textit{mód } N)\}.$$

Puesto que todo conjunto de Sidon modular es un conjunto de Sidon,

$$B_2\left(\text{mód } N\right) \subseteq B_2\left(N\right),$$

lo cual permite afirmar que

$$f_2\left(N\right) \leq F_2\left(N\right),$$

y por este hecho, toda cota inferior de $f_2\left(N\right)$ es cota inferior de $F_2\left(N\right)$, también toda cota superior de $F_2\left(N\right)$ es cota superior para $f_2\left(N\right)$; como una consecuencia de (1.1); se obitiene:

$$f_2\left(N\right) \leq \sqrt{4N - \frac{7}{4}} - \frac{1}{2}.$$

Uno de los problemas centrales en conjuntos de Sidon modulares es determinar el comportamiento asintótico de $f_2(N)$, más especificamente se busca determinar si:

$$\lim_{N\to\infty} \frac{f_2(N)}{\sqrt{N}} \quad \text{existe,} \tag{1.2}$$

pues para conjuntos de Sidon, (vease [2]), se conoce que:

$$\lim_{N\to\infty} \frac{F_2(N)}{\sqrt{N}} = 1.$$

Por lo tanto se busca determinar cual es el valor exacto del limite en (1.2), esto nos lleva a estudiar la exitencia de:

$$\liminf_{N\to\infty} \frac{f_2(N)}{\sqrt{N}}$$

y

$$\limsup_{N\to\infty} \frac{f_2(N)}{\sqrt{N}}$$

Una forma de atacar estos problemas es estudiar las mejores construcciones conocidas para conjuntos de Sidon modulares para mejorar las cotas inferiores que se puedan obtener para $f_2(N)$ y contar de la mejor manera posible para mejorar las cotas superiores que se puedan obtener para $f_2(N)$.

Capítulo 2

REGLAS GOLOMB

En este capítulo se estudia un problema que apareció en teoría de comunicaciones cuya relación con los conjuntos de Sidon es uno de los principales intereses de este Trabajo de Grado: las reglas Golomb o conjuntos de diferencias distintas.

2.1. Historia del problema

Babcock [13] fue el primer investigador en hacer uso de las reglas Golomb bajo un nombre diferente, en su trabajo sobre asignación de radiofrecuencias para evitar ciertos tipos de interferencia en intermodulación ("tercer orden" y "quinto orden") causadas por un amplificador potencial común no lineal.

El mismo Babcock observó que si las radiofrecuencias de los canales de comunicación para el proceso de intermodulación se asignan en proporción a las marcas de una regla Golomb, entonces el tercer orden de interferencia entre los canales de comunicación es eliminado.

Aunque Babcock fue el primero en estudiar las reglas Golomb, éstas son nombradas así despues de Salomón W. Golomb, profesor de ingeniería y matemáticas de la Universidad de Southern California, quien fue el primer investigador en realizar el primer tratamiento sistemático del problema.

Construcciones similares han sido estudiadas por otros autores bajo diferentes nombres como por ejemplo DDS (distinct difference sets), entre estos autores cabe destacar a Fang y Sandrin, según M. D. Atkinson,[14], quienes formularon el problema como un problema de diferencias distintas y aplicaron algunos resultados de la teoría de grafos y de la teoría de códigos.

El nombre del profesor Golomb es comúnmente asociado con tales construcciones, desde entonces las reglas Golomb han tenido diversas aplicaciones, iniciando desde la teoría de códigos hasta radioastronomía.

2.2. Las reglas Golomb

El concepto de regla Golomb surge a partir del siguiente problema formulado por Babcock:

Para todo n dado, encontrar un conjunto de enteros $A = \{0 \leq a_1 < ... < a_n\}$ *tales que ninguna igualdad no trivial* $a_r - a_t = a_u - a_s$ *sea valida*

Este problema surgió de sus trabajos en asignación de radiofrecuencias para evitar interferencias entre canales de comunicación, en este caso los enteros a_i, para $i = 1, ..., n$, son llamados radiofrecuencias.

2.2.1. Definición formal

Una regla Golomb consiste de un conjunto de enteros que pueden ser pensados como marcas (con localizaciones enteras) de manera análoga a las reglas comunes, de modo que las distancias entre elementos distintos del conjunto son todas diferentes.

Definición 6. ***(Regla Golomb)*** *Un conjunto A de enteros con k elementos, se llama una regla Golomb con k marcas, si las diferencias de la forma:* $a - a'$, *con* $a' \neq a$ *y* $a, a' \in A$, *son todas distintas. En términos de ecuaciones decimos que el conjunto A forma una regla Golomb, si para todo entero* $x \neq 0$ *existe a lo más una solución de la ecuación:*

$$x = a - a' \ con \ a \neq a' \ y \ a, a' \ en \ A$$

NOTACIÓN

Denotaremos por GOL al conjunto de todas las reglas Golomb, y por $GOL\,(k)$ al conjunto dado por:

$$GOL\,(k) = \{A \in GOL : |A| = k\}$$

Por $A - A$, al conjunto siguiente:

$$A - A = \{a - a' : a, a' \in A \quad y \quad a \neq a'\}$$

OBSERVACIONES

1. Puesto que las diferencias positivas en una regla Golomb A, son todas distintas debe darse que,

   A es una regla Golomb si y sólo si

   $$|A - A| = \binom{k}{2} = \frac{k\,(k-1)}{2},$$

   donde $|A| = k$.

2. Para demostrar que un conjunto $A \subseteq \mathbb{Z}$ es una regla Golomb basta probar que:

   $$(a - a' = b - b') \Rightarrow (a = b \quad y \quad a' = b')$$

   Para todo $a, a', b, b' \in A$, con $a' \neq a$ y $b' \neq b$.

3. Una regla Golomb no necesariamente inicia en la posición cero, esta puede iniciar en algún entero positivo o incluso negativo.

4. La diferencia entre el elemento máximo y el elemento mínimo de una regla Golomb se conoce como la longitud de dicha regla, ésta se denota por $L\,(A)$, en otras palabras

   $$L\,(A) = \text{máx}\,(A) - \text{mín}\,(A)\,.$$

   Es de interés encontrar reglas Golomb A con $L\,(A)$ tan pequeña como sea posible, es decir, reglas Golomb óptimas, o al menos en reglas cuya longitud esté cercana a la longitud de una regla óptima, es decir, reglas Golomb casi-óptimas.

5. Una regla Golomb puede pensarse como un caso especial de una regla común (en una regla común las marcas o localizaciones siempre están ubicadas a igual distancia y de forma consecutiva), en donde las distancias entre dos puntos (o marcas) de la regla deben ser todas distintas.

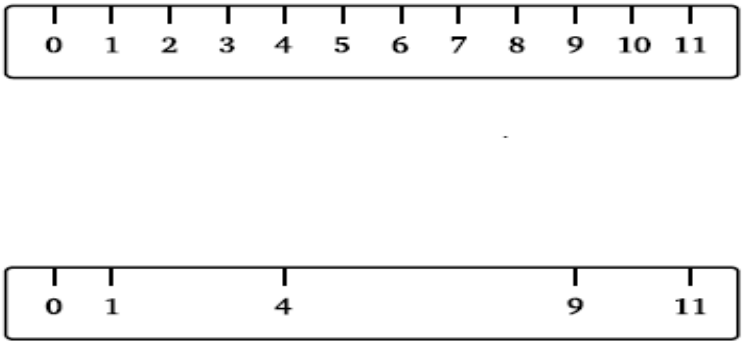


Figura 2.1: Una regla común y una regla Golomb.

2.2.2. Propiedades de las reglas Golomb

Del capítulo anterior sabemos que la propiedad de ser conjunto de Sidon no se ve afectada bajo traslaciones o bajo el producto de sus elementos por una cantidad constante distinta de cero. De la misma manera si conocemos que un conjunto A dado constituye una regla Golomb, podemos a partir de él encontrar nuevas reglas Golomb, pues en este caso también la propiedad de ser regla Golomb permanece invariante bajo traslaciones o bajo el producto de sus elementos por un entero distinto de cero, hecho que se puede apreciar en la siguiente proposición.

Proposición 3. *Sea $A \subseteq \mathbb{Z}$ una regla Golomb, las siguientes afirmaciones son válidas:*

1. *Para cada entero x el conjunto $x + A = \{a + x : a \in A\}$ es una regla Golomb.*

2. *Para cada entero x el conjunto $x - A = \{x - a : a \in A\}$ es una regla Golomb.*

3. *Para cada entero $x \neq 0$, el conjunto $xA = \{ax : a \in A\}$ es una regla Golomb.*

OBSERVACIONES:

1. La parte 1 del teorema anterior es la propiedad de traslación para reglas Golomb, Usando esta propiedad una regla Golomb puede ser traslasdada de tal manera que $\text{Mín}\,(A) = 0$, lo que permite asumir que una regla Golomb siempre inicia en la posición cero. Esta regla Golomb con su punto inicial en el origen es llamada la forma canónica de una regla Golomb. De esta manera se puede denotar por $GOL_0\,(k)$, al conjunto:

$$GOL_0\,(k) = \{A \in GOL\,(k) : \text{Mín}\,(A) = 0\}$$

   Es decir; $GOL_0\,(k)$ denota al conjunto de todas las reglas Golomb con k marcas cuya primera marca es 0 y en adelante en el transcurso de este trabajo todas las reglas Golomb se consideraran en $GOL_0\,(k)$.

2. Cuando $x = \text{máx}\,(A)$ en la parte 2 de la proposición anterior se obtiene a partir del conjunto A una nueva regla Golomb conocida como la imagen espejo de la regla Golomb A y se caracteriza porque tiene misma longitud de la regla Golomb original A.

Figura 2.2: Una regla Golomb y su imagen espejo.

Proposición 4. *A es una regla Golomb si y solo si A es un conjunto de Sidon.*

Prueba.

Supóngase $A \subseteq \mathbb{Z}$ es una regla Golomb y probemos que A es un conjunto de Sidon.

Sean $a, a', b, b' \in A$ tales que:

$$a + a' = b + b'. \tag{2.1}$$

Por lo tanto

$$a - b = b' - a'$$

Sin perdida de generalidad se puede suponer que $a - b \geq 0$.

Si $a - b > 0$, puesto que A forma una regla Golomb se tiene

$$(a = b' \quad y \quad a' = b)$$

Si $a - b = 0$ se tiene que

$$(a = b \quad y \quad a' = b')\,.$$

Por lo tanto (2.1) implica que

$$(a = b' \quad y \quad a' = b) \quad \text{o} \quad (a = b \quad y \quad a' = b')\,.$$

Reciprocamente, Supóngase $A \subseteq \mathbb{Z}$ es un conjunto de Sidon y probemos que A es una regla Golomb.

Sean a, a' y b, b' en A tales que:

$$a - a' = b - b' \quad \text{con} \quad a \neq a', b \neq b' \tag{2.2}$$

luego

$$a + b' = b + a',$$

como A es un conjunto de Sidon

$$(a = b \quad y \quad a' = b') \quad \text{o} \quad (a = a' \quad y \quad b = b'),$$

puesto que $a \neq a'$ y $b \neq b'$, (2.2) implica que

$$a = b \quad y \quad a' = b'.$$

En consecuencia A es una regla Golomb. □

El resultado anterior es importante pues permite poder estudiar a los conjuntos de Sidon y a las reglas Golomb de manera paralela, es decir que las construcciones para conjuntos de Sidon y reglas Golomb serán las mismas y aunque las funciones extremas que se pueden definir sobre conjuntos de Sidon y reglas Golomb son distintas podremos encontrar relaciones entre éstas.

2.3. Reglas Golomb modulares

El concepto de regla Golomb puede considerarse en el conjunto de los enteros módulo el entero $m \geq 2$.

Definición 7. *Un conjunto A de enteros con k elementos, se llama una regla Golomb módulo m con k marcas, si las diferencias de la forma: $a - a'$, con $a \neq a'$ y $a, a' \in A$, son incongruentes módulo m. En términos de ecuaciones decimos que el conjunto A forma una regla Golomb módulo m, si para todo entero $x \neq 0$ existe a lo más una solución de la congruencia:*

$$x \equiv (a - a') \,(mód\ m) \quad con \quad a, a' \quad en \quad A$$

NOTACIÓN

Denotaremos por $GOL\,(\text{mód } m)$ al conjunto de todas las reglas Golomb módulo m y por $GOL\,(\text{mód } m, k)$, al conjunto:

$$GOL\,(\text{mód } m, k) = \{A \in GOL\,(\text{mód } m) : |A| = k\}$$

OBSERVACIÓN

1. Puesto que las diferencias en una regla Golomb A módulo m, son todas distintas debe darse que,

   A es una regla Golomb módulo m si y sólo si

   $$|A - A| = 2\binom{k}{2} = k\,(k-1)\,,$$

   donde $|A| = k$.

Proposición 5. ***Propiedades de las reglas Golomb modulares***

Sea $A \subseteq \mathbb{Z}$ una regla Golomb módulo m, las siguientes afirmaciones son validas:

1. *Para cada entero x el conjunto $x+A = \{a + x : a \in A\}$ es una regla Golomb módulo m.*

2. *Para cada entero x el conjunto $x-A = \{x - a : a \in A\}$ es una regla Golomb módulo m.*

3. *Para cada entero $x \neq 0$, talque: $m.c.d(x, m) = 1$, el conjunto $xA = \{ax : a \in A\}$ es una regla Golomb módulo m.*

Teorema 2. *Sea $A \subseteq \mathbb{Z}$, si A es una regla Golomb módulo m, entonces A es una regla Golomb.*

OBSERVACIÓN:

Este teorema permite afirmar que:

$$GOL\,(\text{mód } m) \subseteq GOL$$

En particular:

$$GOL\,(\text{mód } m, k) \subseteq GOL\,(k)$$

Proposición 6. *Sea $A \subseteq \mathbb{Z}$; A es una regla Golomb módulo m si y sólo si A es un conjunto de Sidon módulo m.*

2.4. La función $G\,(k)$

Consideraremos a continuación la función $G\,(k)$, la cual es importante en este trabajo, puesto que interesa estudiar su comportamiento asintótico, sin embargo en esta sección solo se hace una antesala al estudio de esta función.

Definición 8. *Definimos $G\,(k)$ como la longitud más pequeña de una regla Golomb que se puede construir con k marcas. Debido a la propiedad de traslación de las reglas Golomb, proposición (3); se puede considerar que una regla Golomb A tiene su primera marca en*

el origen $(\text{mín}(A) = 0)$ *y por lo tanto se puede escribir a* $G(k)$*, como sigue:*

$$G(k) = \text{mín}\{\text{máx}\, A : A \in GOL_0(k)\}$$

Sea $A \in GOL_0(k)$, se puede calcular de manera sencilla una cota inferior para $G(k)$, puesto que el número de diferencias positivas de elementos de A esta dado por:

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

Y como las diferencias son todas distintas se tiene que:

$$\frac{k(k-1)}{2} \leq \text{máx}(A)$$

En particular:

$$\frac{k(k-1)}{2} \leq G(k) = \text{mín}\{\text{máx}\, A : A \in GOL_0(k)\}$$

Es decir;

$$G(k) \geq \frac{k(k-1)}{2}$$

OBSERVACIONES

1. De la definición 8, se desprende que la función $G(k)$ es una aplicación estrictamente creciente.

$$l < k \Rightarrow G(l) < G(k)$$

2. En el siguiente cuadro se muestran valores de $G(k)$ para $k \leq 24$, [1], sin embargo, hasta el momento no se conocen reglas Golomb óptimas para $k > 24$.

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$G(k)$	0	1	3	6	11	17	25	34	44	55	72	85	106	127

k	15	16	17	18	19	20	21	22	23	24
$G(k)$	151	177	199	216	246	283	333	356	372	425

Cuadro 2.1: Valores conocidos para $G(k)$.

Conocer las mejores cotas para $G(k)$, es uno de los intereses principales de este trabajo; puesto que lo que se busca es acercarse a responder el siguiente interrogante:

$$¿\lim_{k\to\infty} \frac{G(k)}{k^2} = 1?$$

Capítulo 3

CONSTRUCCIONES

Las construcciones que se conocen para conjuntos de Sidon y reglas Golomb corresponden a versiones modulares, para valores apropiados del módulo, en este caso cuando el módulo es un número primo o potencia de un número primo. En este capítulo se presentan estas construcciones, las cuales se deben a Singer, Bose y Ruzsa.

3.1. Resultados preliminares

Las diferentes construcciones para conjuntos de Sidon y reglas Golomb, se fundamentan en los siguientes resultados básicos de la teoría de números y de la teoría de campos finitos.

1. Sea θ una raíz primitiva módulo p, con p primo y sean $i, j \in \mathbb{N}$. Entonces; $\theta^i \equiv \theta^j (\text{mód } p)$ si y sólo si, $i \equiv j (\text{mód } p-1)$.

2. Para cada primo p y cada natural r existe un único (salvo isomorfismos) campo finito con p^r elementos. Este campo se denota por $\text{GF}(p^r)$.

3. Si d es un divisor de r entonces el campo $\text{GF}(p^d)$ es un subcampo de $\text{GF}(p^r)$.

4. El grupo multiplicativo $GF^*(p^r)$ es ciclico de orden $p^r - 1$.

5. Sea d un divisor de r y θ un generador de $GF^*(p^r)$. Entonces los elementos θ^a y θ^b de $GF^*(p^r)$ son linealmente dependientes sobre GF(p^d) si y sólo si

$$a \equiv b(\text{mód } q) \quad Donde \quad q = \frac{p^r - 1}{p^d - 1}$$

6. El generador θ es algebraico de grado r/d sobre GF(p^d) y θ^q es un generador de $GF^*(p^d)$

7. Sea p un número primo, k un entero positivo y θ un generador de $GF^*(p^{2k})$, entonces para todo par de enteros a y b, se tiene:

   a) $\theta^a = \theta^b$ si y sólo si $a \equiv b(\text{mód } p^{2k} - 1)$

   b) $\theta^a \in GF(p^k)$ si y sólo si $a \equiv 0(\text{mód } p^k + 1)$

Para un estudio más detallado de estos resultados cualquier lector puede consultar [4] y [5]

3.2. Construcción de Ruzsa

En 1993, Ruzsa [3] diseña una forma de construir conjuntos de Sidon y reglas Golomb, haciendo uso de raíces primitivas módulo un número primo.
Para dar una ilustración de la construcción de Ruzsa, Sean p un número primo y θ una raíz primitiva módulo p, Ruzsa define el conjunto siguiente:

$$R(\theta, p) = \{a_1, a_2, ..., a_{p-1}\}$$

Donde a_i es la única solución módulo $p(p-1)$ del sistema de congruencias:

$$X \equiv i \,(\text{mód } p - 1)$$

$$X \equiv \theta^i \,(\text{mód } p)$$

Con $i = 1, 2, ..., p-1$. Las soluciones de este sistema de congruencias estan garantizadas por el teorema chino de los residuos.

La idea central de la construcción de Ruzsa consiste en probar que $R(\theta, p)$ da lugar a un conjunto de Sidon y una regla Golomb, con módulo $p(p-1)$ y con $p-1$ elementos; además $R(\theta, p) \subseteq [1, p^2 - p]$. De manera más precisa tenemos el siguiente teorema:

Teorema 3. ***(Ruzsa** 1993**)*** *Para todo primo p existe un conjunto de Sidon y una regla Golomb módulo $p(p-1)$, con $p-1$ elementos, contenido en $[1, p(p-1)]$.*

La prueba de este teorema es consecuencia de un resultado más general correspondiente a la generalización de la construcción de Ruzsa que se prueba en la próxima sección.

Ejemplo 6.

Veamos un caso particular de la construccion de Ruzsa, sea $p = 11$ y $\theta = 2$ una raíz primitiva módulo 11, para $i = 1, 2, ..., 10$ se toma a_i como la única solución del sistema de congruencias:

$$X \equiv i \,(\text{mód } 10) \qquad X \equiv 2^i \,(\text{mód } 11)$$

Donde $1 \leq X \leq 10 \times 11$. El teorema chino de los residuos permite establecer que el sistema de congruencias tiene solución única; al solucionar los 10 sistemas de congruencias resultantes se obtiene:

i	1	2	3	4	5	6	7	8	9	10
$2^i = (mód\ 11)$	2	4	8	5	10	9	7	3	6	1
$a_i = (mód\ 110)$	101	92	63	104	65	86	7	58	39	100

Cuadro 3.1: Ejemplo 6 Construcción de Ruzsa.

Por lo tanto el conjunto que se obtiene es:

$$A = \{a_i : i = 1, 2, ..., 10\} = \{7, 39, 58, 63, 65, 86, 92, 100, 101, 104\}$$

A es un conjunto de Sidon y una regla Golomb módulo $10 \times 11 = 110$. En las tablas de sumas y diferencias módulo 110, respectivamente; se puede verficar esta afirmación.

Tabla de sumas módulo 110

7	39	58	63	65	86	92	100	101	104
14	46	65	70	72	93	99	107	108	1
	78	97	102	104	15	21	29	30	33
		6	11	13	34	40	48	49	52
			16	18	39	45	53	54	57
				20	41	47	55	56	59
					62	68	76	77	80
						74	82	83	86
							90	91	94
								92	95
									98

Tabla de diferencias módulo 110

7	39	58	63	65	86	92	100	101	104
0	32	51	56	58	79	85	93	94	97
78	0	21	24	26	47	53	61	62	65
59	91	0	5	7	28	34	42	43	46
54	86	105	0	2	23	29	37	38	41
52	84	103	108	0	21	27	35	36	39
29	63	82	87	89	0	6	14	15	18
25	57	76	81	83	104	0	8	9	12
17	49	68	73	75	96	102	0	1	4
16	48	67	72	74	95	101	109	0	3

Corolario 1. *(**ruzsa**) Para todo primo p, se tiene:*

1. $F_2(p\,(p-1)) \geq p-1$
2. $G(p-1) \leq p\,(p-1)$
3. $f_2(p\,(p-1)) = p-1$

Prueba.

1. Por el teorema 3 de Ruzsa, existe un conjunto de sidon A, con $p-1$ elementos, módulo $p\,(p-1)$ y $A \subseteq [1, p(p-1)]$, como todo conjunto de Sidon módular forma un conjunto de Sidon, se tiene que:

$$F_2(p\,(p-1)) \geq p-1$$

2. Por el teorema 3 de Ruzsa, existe un conjunto de sidon A, con $p-1$ elementos, módulo $p\,(p-1)$ y $A \subseteq [1, p(p-1)]$, por la proposición 6, A forma una regla Golomb , con $p-1$ elementos, módulo $p\,(p-1)$, como toda regla Golomb módular forma una regla Goomb, entonces A forma una regla Golomb con máx$(A) \leq p\,(p-1)$; así se puede decir que,

$$G(p-1) \leq p\,(p-1)$$

3. Por otro lado, $f_2(p\,(p-1))$ representa el máximo cardinal de un conjunto de sidon contenido en $\mathbb{Z}_{(p(p-1))}$, por lo cual se puede afirmar que:

$$f_2(p\,(p-1)) \geq p-1$$

Veamos que no se puede dar que

$$f_2(p\,(p-1)) > p-1$$

Supongase que existe un conjunto de Sidon B módulo $p\,(p-1)$, talque:

$$|B| = f_2(p\,(p-1)) \geq p$$

Por la proposición 6, B forma una regla Golomb módulo $p\,(p-1)$, por lo tanto:

$$|B-B| \geq 2\binom{p}{2} = p\,(p-1)$$

Lo cual contradice que B forma una regla Golomb módulo $p\,(p-1)$ y por ende contradice que B sea conjunto de Sidon módulo $p\,(p-1)$, en consecuencia debe tenerse que:

$$f_2(p\,(p-1)) = p-1$$

□

3.3. Generalización de la construcción de Ruzsa

La construcción de Ruzsa puede generalizarse como sigue:

Sea p un primo y θ una raíz primitiva módulo p. Para cada $u \in \mathbb{Z}_p$ y $f \in \mathbb{Z}_p^*$ y m.c.d$(f, p-1) = 1$, para f fijo, definamos el conjunto $R\,(\theta, p, u, f)$,

$$R\,(\theta, p, u, f) = \left\{a_{u_1}, a_{u_2}, ..., a_{u_{(p-1)}}\right\}$$

Donde a_{u_i} es la única solución módulo $p(p-1)$ del sistema de congruencias:

$$X \equiv fi\,(\text{mód } p-1)$$

$$X \equiv \theta^i u\,(\text{mód } p)$$

Con $i = 1, 2, ..., p-1,$. La solución de este sistema de congruencias esta garantizada por el teorema chino de los residuos y esta dada por:

$$X = a_{u_i} \equiv pfi - u(p-1)\theta^i\,(\text{mód } p\,(p-1))$$

Teorema 4. *Para todo primo p y toda raíz primitiva θ módulo p y $u, f \in \mathbb{Z}_p$, con m.c.d$(f, p-1) = 1$, f fijo y $u \neq 0$; el conjunto $R\,(\theta, p, u, f)$ forma un conjunto de Sidon y una regla Golomb módulo $p\,(p-1)$.*

Prueba.

Probemos que $R(\theta, p, u, f)$, para $u \neq 0$; forma un conjunto de Sidon y una regla Golomb módulo $p(p-1)$, por la proposición 6 es suficiente probar que $R(\theta, p, u, f)$ forma un conjunto de Sidon módulo $p(p-1)$.

Sean $i, j, s, t \in [1, p-1]$ y $a_{u_i}, a_{u_j}, a_{u_s}, a_{u_t} \in R(\theta, p, u, f)$, tales que:

$$a_{u_i} + a_{u_j} \equiv a_{u_s} + a_{u_t} \,(\text{mód } p(p-1))$$

Como p y $p-1$ son primos relativos, la congruencia anterior es equivalente al sistema:

$$a_{u_i} + a_{u_j} \equiv a_{u_s} + a_{u_t} \,(\text{mód } p-1)$$

$$a_{u_i} + a_{u_j} \equiv a_{u_s} + a_{u_t} \,(\text{mód } p)$$

Entonces, por definición de $R(\theta, p, u, f)$, se ve que:

$$f(i+j) \equiv f(s+t) \,(\text{mód } p-1) \tag{3.1}$$

$$u\left(\theta^i + \theta^j\right) \equiv u\left(\theta^s + \theta^t\right) (\text{mód } p) \tag{3.2}$$

Debido a que θ es una raíz primitiva módulo p y a que m.c.d$(f, p) = 1$ y m.c.d.$(u, p) = 1$, (3.1) y (3.2) implican que:

$$\theta^i + \theta^j \equiv \theta^s + \theta^t \,(\text{mód } p) \quad \text{y} \quad \theta^i\theta^j \equiv \theta^s\theta^t \,(\text{mód } p) \tag{3.3}$$

Dado que $\mathbb{Z}_p$ es el campo de los residuos módulo p, de (3.3) obtenemos:

$$(\theta^i \equiv \theta^s \,(\text{mód } p) \quad \text{y} \quad \theta^j \equiv \theta^t \,(\text{mód } p)) \quad \text{o} \quad (\theta^i \equiv \theta^t \,(\text{mód } p) \quad \text{y} \quad \theta^j \equiv \theta^s \,(\text{mód } p))$$

Supongase que:

$$\theta^i \equiv \theta^s \,(\text{mód } p) \quad \text{y} \quad \theta^j \equiv \theta^t \,(\text{mód } p)$$

Entonces, nuevamente como θ es una raíz primitiva módulo p, tenemos:

$$i \equiv s \,(\text{mód } p-1) \quad \text{y} \quad j \equiv t \,(\text{mód } p-1)$$

pero, $1 \leq i, j, s, t \leq p-1$, por tanto:

$$i = s \qquad y \qquad j = t$$

De manera analóga, si se supone que:

$$\theta^i \equiv \theta^t \,(\text{mód } p) \quad \text{y} \quad \theta^j \equiv \theta^s \,(\text{mód } p)$$

se llega a:

$$i = t \qquad \text{y} \qquad j = s$$

Por lo tanto se puede concluir que:

$$\left(a_{u_i} = a_{u_s} \quad \text{y} \quad a_{u_j} = a_{u_t}\right) \qquad \text{o} \qquad \left(a_{u_i} = a_{u_t} \quad \text{y} \quad a_{u_j} = a_{u_s}\right)$$

Por todo lo anterior $R(\theta, p, u, f)$ es un conjunto de Sidon módulo $p(p-1)$. □

Teorema 5. *Para todo primo p y toda raíz primitiva θ módulo p y $u, f \in \mathbb{Z}_p$, con $m.c.d(f, p-1) = 1$ y f fijo; la colección*

$$\{R(\theta, p, u, f) : u \in \mathbb{Z}_p\}$$

es una partición del intervalo $[1, p^2 - p]$, en p clases,

$$R(\theta, p, 0, f), R(\theta, p, 1, f), R(\theta, p, 2, f), ..., R(\theta, p, p-1, f),$$

tales que:

1. $|R(\theta, p, u, f)| = p - 1$
2. $R(\theta, p, 0, f) = \{p, 2p, 3p, ..., p(p-1)\}$

Prueba.

1. probemos que el cardinal de $R(\theta, p, u, f)$ es $p-1$. y sean $i, j \in [1, p-1]$ y $a_{u_i}, a_{u_j} \in R(\theta, p, u, f)$, tales que:

$$a_{u_i} = a_{u_j}$$

Por lo tanto, por la forma como se ha definido $R(\theta, p, u, f)$, se tiene que:

$$a_{u_i} \equiv i \,(\text{mód } p-1) \qquad y \qquad a_{u_j} \equiv j \,(\text{mód } p-1)$$

Lo cual implica que:

$$i \equiv j \,(\text{mód } p-1)$$

y puesto que

$$1 \leq i, j \leq p-1$$

Entonces:

$$i = j$$

Por lo tanto:

$$|R(\theta, p, u, f)| = p-1$$

2. El conjunto $R(\theta, p, 0, f)$ esta formado por todos los múltiplos de p que estan en el intervalo $[1, p^2-p]$

$$R(\theta, p, 0, f) = \{p, 2p, 3p, ..., p(p-1)\}$$

De la definición de $R(\theta, p, 0, f)$, es claro que para todo $x \in R(\theta, p, 0, f)$, se cumple que:

$$X \equiv fi \,(\text{mód } p-1) \qquad X \equiv 0 \,(\text{mód } p) \tag{3.4}$$

y

$$1 \leq X \leq p(p-1) \tag{3.5}$$

Las ecuaciones (3.4) y (3.5), implican que: X es un múltiplo de p que esta en el intervalo $[1, p^2-p]$

Por ultimo debemos probar que la colección $\{R(\theta, p, u, f) : u \in \mathbb{Z}_p\}$, da lugar a una partición de $[1, p(p-1)]$, probemos que los elementos de esta colección son dos a dos a disjuntos; sean x, u, v, tales que:

$$x \in R(\theta, p, u, f) \cap R(\theta, p, v, f)$$

Por definición existen $i, j \in [1, p-1]$,$f, u, v \in \mathbb{Z}_p$ y una raíz primitiva θ módulo p, tales que:

$$X \equiv fi \,(\text{mód } p-1) \qquad X \equiv \theta^i u \,(\text{mód } p) \quad (*)$$

$$X \equiv fj \,(\text{mód } p-1) \qquad X \equiv \theta^j v \,(\text{mód } p) \quad (**)$$

De (*) y (**)

$$fi \equiv fj \,(\text{mód } p-1)$$

Puesto que:

$$m.c.d\,(f, p-1) = 1$$

Se tiene que:

$$i \equiv j \,(\text{mód } p-1)$$

Como $i, j \in [1, p-1]$, entonces

$$i = j$$

Por lo tanto:

$$\theta^i v \equiv \theta^i u \,(\text{mód } p)$$

como $m.c.d\,(\theta, p) = 1$, se deduce que:

$$v \equiv u \,(\text{mód } p)$$

Además, dado que: $u, v \in \mathbb{Z}_p$, se concluye que:

$$u = v$$

En consecuencia los elementos de la colección $\{R(\theta, p, u, f) : u \in \mathbb{Z}_p\}$ son disjuntos dos a dos.

Probemos que:

$$\cup_{u=0}^{p-1} R(\theta, p, u, f) = [1, p(p-1)]$$

Calculemos

$$\left|\cup_{u=0}^{p-1} R(\theta, p, u, f)\right|$$

Puesto que los $R(\theta, p, u, f)$ son dos a dos disjuntos, se tiene que:

$$\left|\cup_{u=0}^{p-1} R(\theta, p, u, f)\right| = \sum_{u=0}^{p-1} |R(\theta, p, u, f)|$$

como $|R(\theta, p, u, f)| = p - 1$,

$$\left|\cup_{u=0}^{p-1} R(\theta, p, u, f)\right| = \sum_{u=0}^{p-1} p - 1 = p(p-1) = |[1, p(p-1)]|$$

Por tanto:

$$\cup_{u=0}^{p-1} R(\theta, p, u, f) = [1, p(p-1)]$$

□

Ejemplo 7.

Sea $u \in \mathbb{Z}_{11}$, $\theta = 2$ y sea $f = 1$, se define

$$R(2, 11, u, 1) = \{a_{u_1}, a_{u_2}, ..., a_{u_{10}}\}$$

De tal manera que a_{u_i}, para $i = 1, 2, ..., 10$; se escoje como la única solución módulo 110 del sistema de congruencias

$$X \equiv i \,(\text{mód } 10)$$

$$X \equiv u2^i \,(\text{mód } 11)$$

La solución esta garantizada por el teorema chino de residuos y esta dada por:

$$X = a_{u_i} = 11i - 10u2^i$$

Para $u = 0$, tenemos

$$a_{0_i} = 11i$$

para $i = 1, 2, ..., 10$, se obtiene el conjunto

$$R\,(2, 11, 0, 1) = \{11, 22, 33, 44, 55, 66, 77, 88, 99, 110\}$$

Para $u = 1$, tenemos

$$a_{1_i} = 11i - (10)2^i$$

para $i = 1, 2, ..., 10$, se obtiene el conjunto

$$R\,(2, 11, 1, 1) = \{7, 39, 58, 63, 65, 86, 92, 100, 101, 104\}$$

Para $u = 2$, tenemos

$$a_{2_i} = 11i - 2(10)2^i$$

para $i = 1, 2, ..., 10$, se obtiene el conjunto

$$R\,(2, 11, 2, 1) = \{28, 47, 52, 54, 75, 81, 89, 90, 93, 106\}$$

Para $u = 3$, tenemos

$$a_{3_i} = 11i - 3(10)2^i$$

para $i = 1, 2, ..., 10$, se obtiene el conjunto

$$R\,(2, 11, 3, 1) = \{4, 12, 13, 16, 29, 61, 80, 85, 87, 108\}$$

Para $u = 4$, tenemos

$$a_{4_i} = 11i - 4(10)2^i$$

para $i = 1, 2, ..., 10$, se obtiene el conjunto

$$R\,(2, 11, 4, 1) = \{17, 36, 41, 43, 64, 70, 78, 79, 82, 95\}$$

Para $u = 5$, tenemos

$$a_{5_i} = 11i - 5(10)2^i$$

para $i = 1, 2, ..., 10$, se obtiene el conjunto

$$R\,(2, 11, 5, 1) = \{14, 19, 21, 42, 48, 56, 57, 60, 73, 105\}$$

Para $u = 6$, tenemos

$$a_{6_i} = 11i - 6(10)2^i$$

para $i = 1, 2, ..., 10$, se obtiene el conjunto

$$R\,(2, 11, 6, 1) = \{1, 2, 5, 18, 50, 69, 74, 76, 97, 103\}$$

Para $u = 7$, tenemos

$$a_{7_i} = 11i - 7(10)2^i$$

para $i = 1, 2, ..., 10$, se obtiene el conjunto

$$R\,(2, 11, 7, 1) = \{9, 15, 23, 24, 27, 40, 72, 91, 96, 98\}$$

Para $u = 8$, tenemos

$$a_{8_i} = 11i - 8(10)2^i$$

para $i = 1, 2, ..., 10$, se obtiene el conjunto

$$R\,(2, 11, 8, 1) = \{6, 25, 30, 32, 53, 59, 67, 68, 71, 84\}$$

Para $u = 9$, tenemos

$$a_{9_i} = 11i - 9(10)2^i$$

para $i = 1, 2, ..., 10$, se obtiene el conjunto

$$R\,(2, 11, 9, 1) = \{20, 26, 34, 35, 38, 51, 83, 102, 107, 109\}$$

Para $u = 10$, tenemos

$$a_{10_i} = 11i - 10(10)2^i$$

para $i = 1, 2, ..., 10$, se obtiene el conjunto

$$R\,(2, 11, 10, 1) = \{3, 8, 10, 31, 37, 45, 46, 49, 62, 94\}$$

Por los teoremas 4 y 5, los conjuntos obtenidos en este ejemplo forman conjuntos de Sidon(y reglas Golomb) módulo 110, para $u \neq 0$; y $R\,(2, 11, 0, 1)$ consta de los múltiplos de 11 en el intervalo $[1, 110]$, y todos estos conjuntos dan lugar a una partición del intervalo $[1, 110]$.

3.4. Construcción de Bose

En 1942, Bose [7], realiza construcciones de conjuntos de Sidon y reglas Golomb, la construcción de Bose será tratada en esta sección, su forma general e implicaciones serán tratadas más adelante.
Sean p un número primo, k un entero positivo, y θ un generador de $GF^*(p^{2k})$, Bose define un conjunto con parámetros p y θ, de la siguiente manera:

$$B(p,\theta) = \left\{a \in \left[1, p^{2k}-1\right] : \theta^a - \theta \in GF(p^k)\right\}$$

El siguiente teorema y su demostración ilustran la construcción de Bose.

Teorema 6. ***(Bose*** 1.942***)*** *Para toda potecia prima p^k existe un conjunto de Sidon y una regla Golomb módulo $p^{2k}-1$, con p^k elementos, contenido en $\left[1, p^{2k}-1\right]$.*

Prueba.

La prueba de este resultado consiste en demostrar que el conjunto $B(p,\theta)$ definido anteriormente satisface las condiciones este teorema, iniciemos probando que el cardinal de $B(p,\theta)$ es p^k. Para ello definamos la función L como sigue:

$$L : B(p,\theta) \to GF(p^k)$$

$$a \to L(a) = \theta^a - \theta$$

probemos que L es una función inyectiva, en efecto; sean a,b en $B(p,\theta)$, tales que:

$$L(a) = L(b)$$

Por definición de L se tiene que

$$\theta^a - \theta = \theta^b - \theta$$

Osea que

$$\theta^a = \theta^b$$

Por el resultado preliminar 7, parte (a); esto se da si y sólo si:

$$a \equiv b (\text{mód } p^{2k}-1)$$

Y puesto que por definición de $B(p,\theta)$, se sabe que $a, b \in \left[1, p^{2k}-1\right]$, entonces $a = b$. Probemos que L es una función sobreyectiva, sea $c \in GF(p^k)$, dado que $\theta \notin GF(p^k)$, se puede decir que $\theta + c \neq 0$, por lo tanto existe a en $\left[1, p^{2k}-1\right]$, tal que:

$$\theta + c = \theta^a$$

Es decir para cada $c \in GF(p^k)$, existe a, para el cual, $L(a) = c$, Como L es inyectiva y sobreyectiva, podemos establecer que:

$$|B(p,\theta)| = p^k$$

Probemos ahora que $B(p,\theta)$ forma un conjunto de Sidon y una regla Golomb módulo $p^{2k}-1$, es suficiente probar que $B(p,\theta)$ forma un conjunto de Sidon módulo $p^{2k}-1$ (proposición 6), en este caso sean $a, b, c, d \in B(p,\theta)$, tales que:

$$a + b \equiv c + d \left(\text{mód } p^{2k}-1\right)$$

Por el resultado preliminar 7, parte (a)

$$\theta^{a+b} = \theta^{c+d}$$

$$\theta^a\theta^b = \theta^c\theta^d \tag{3.6}$$

Entonces, por definición de $B(p,\theta)$ y de la función L, existen $L(a), L(b), L(c)$ y $L(d)$, que satisfacen:

$$L(a) = \theta^a - \theta, L(b) = \theta^b - \theta, L(c) = \theta^c - \theta \quad y \quad L(d) = \theta^d - \theta$$

Y por lo tanto (3.6) se puede expresar como:

$$\left(L(a) + \theta\right)\left(L(b) + \theta\right) = \left(L(c) + \theta\right)\left(L(d) + \theta\right)$$

Luego,

$$\left(L(a) + L(b)\right)\theta + L(a)L(b) = \left(L(c) + L(d)\right)\theta + L(c)L(d) \tag{3.7}$$

(3.7), implica que θ satisface un polinomio de grado 1, pero como por el resultado preliminar 6, θ es álgebraico de grado 2 sobre $GF(p^k)$, entonces se tiene que:

$$L(a) + L(b) = L(c) + L(d) \quad \text{y} \quad L(a)L(b) = L(c)L(d)$$

Como $GF(p^k)$ forma un campo, entonces:

$$(L(a) = L(c) \quad \text{y} \quad L(b) = L(d)) \quad \text{o} \quad (L(a) = L(d) \quad \text{y} \quad L(b) = L(c)) \tag{3.8}$$

La inyectividad de L y (3.8), implican que:

$$(a = c \quad \text{y} \quad b = d) \quad \text{o} \quad (a = d \quad \text{y} \quad b = c)$$

Por todo lo anterior $B(p, \theta)$ es un conjunto de Sidon módulo $p^{2k} - 1$. □

Ejemplo 8.

sea θ una raíz del polinomio $f(x) = x^2 + 3x + 3$ sobre $GF(5) = \mathbb{Z}_5$. θ es un generador de $GF^*(25)$, lo cual se puede apreciar en el siguiente cuadro:
Como θ una raíz del polinomio $f(x) = x^2 + 3x + 3$, entonces $\theta^2 = 2\theta + 2$

$B(\theta, 5)$	θ^a	$\theta^a - \theta$
1	θ	0
2	$2\theta + 2$	$\theta + 2$
3	$\theta + 4$	4
4	$\theta + 2$	2
5	$4\theta + 2$	$3\theta + 2$
6	3	$3 - \theta$
7	3θ	2θ
8	$\theta + 1$	1
9	$3\theta + 2$	$2\theta + 2$
10	$3\theta + 1$	$2\theta + 1$
11	$2\theta + 1$	$\theta + 1$
12	4	$4 - \theta$
13	4θ	3θ
14	$3\theta + 3$	$2\theta + 3$
15	$4\theta + 1$	$3\theta + 1$
16	$4\theta + 3$	$3\theta + 3$
17	$\theta + 3$	3
18	2	$2 - \theta$
19	2θ	θ
20	$4\theta + 4$	$3\theta + 4$
21	$2\theta + 3$	$\theta + 3$
22	$2\theta + 4$	$\theta + 4$
23	$3\theta + 4$	$2\theta + 4$
24	1	$1 - \theta$

Cuadro 3.2: Ejemplo 8 Construcción de Bose.

Por lo tanto el conjunto:

$$B(5,\theta) = \left\{a \in \left[1, 5^2 - 1\right] : \theta^a - \theta \in GF(p^5)\right\} = \{1, 3, 4, 8, 17\}$$

Forma un conjunto de Sidon y una regla Golomb módulo 24, las tablas de sumas y diferencias de este conjunto se presentan a continuación.

Tabla de sumas módulo 24

1	3	4	8	17
2	4	5	9	18
	6	7	11	20
		8	12	21
			16	1
				10

Tabla de diferencias módulo 24

1	3	4	8	17
0	2	3	7	16
22	0	1	5	14
21	23	0	4	13
17	19	20	0	9

Corolario 2. *(**Bose**) Sea p un número primo y k un entero positivo, para toda potencia prima p^k, se tiene:*

1. $F_2(p^{2k} - 1) \geq p^k$
2. $G(p^k) \leq p^{2k} - 1$
3. $f_2(p^{2k} - 1) = p^k$

Prueba.

1. Por el teorema 6 de Bose, existe un conjunto de sidon $A \subseteq [1, p^{2k}-1]$, con p^k elementos, módulo $p^{2k}-1$, dado que todo conjunto de Sidon módular forma un conjunto de Sidon, es claro que:

$$F_2(p^{2k}-1) \geq p^k$$

2. Por el teorema 6 de Bose, existe un conjunto de sidon $A \subseteq [1, p^{2k}-1]$, con p^k elementos, módulo $p^{2k}-1$, por la proposición 6, A forma una regla Golomb , con p^k elementos, módulo $p^{2k}-1$, como toda regla Golomb módular forma una regla Goomb, entonces A forma una regla Golomb, con máx$(A) \leq p^{2k}-1$; de donde se deduce que,

$$G(p^k) \leq p^{2k}-1$$

3. Por otra parte, $f_2(p^{2k}-1)$ representa el máximo cardinal de un conjunto de sidon contenido en $\mathbb{Z}_{\left(p^{2k}-1\right)}$, por lo tanto se puede afirmar que:

$$f_2(p^{2k}-1) \geq p^k$$

Veamos que no se puede dar que

$$f_2(p^{2k}-1) > p^k$$

Supongase que existe un conjunto de Sidon A módulo $p^{2k}-1$, talque:

$$|A| = f_2(p^{2k}-1) \geq p^k + 1$$

Por la proposición 6, A forma una regla Golomb módulo $p^{2k}-1$, por lo tanto:

$$|A-A| \geq 2\binom{p^k+1}{2} = p^k\left(p^k+1\right) > p^{2k}-1$$

Lo cual contradice que A forma una regla Golomb módulo $p^{2k}-1$ y por ende contradice que A sea conjunto de Sidon módulo $p^{2k}-1$, en consecuencia debe tenerse que:

$$f_2(p^{2k}-1) = p^k$$

□

3.5. Generalización de la construcción de Bose

La construcción de Bose puede generalizarse como sigue:

Sean p un primo, k un entero positivo y θ un generador de $GF^*(p^{2k})$, para cada $i \in GF(p^k)$, se define el conjunto

$$B(\theta, p, i) = \left\{a \in \left[1, p^{2k} - 1\right] : \theta^a - i\theta \in GF(p^k)\right\} \tag{3.9}$$

Los teoremas que se presentan a continuación muestran la forma general de la construcción de Bose.

Teorema 7. *Sean p un primo, k un entero positivo y θ un generador de $GF^*(p^{2k})$. Para toda potencia prima p^k; el conjunto $B(\theta, p, i)$, con $i \neq 0$; forma un conjunto de Sidon y una regla Golomb módulo $p^{2k} - 1$*

La prueba de que $B(\theta, p, i)$, con $i \neq 0$; forma un conjunto de Sidon y una regla Golomb módulo $p^{2k} - 1$ es en esencia la misma que la realizada en el teorema 6.

Teorema 8. *Sean p un primo, k un entero positivo y θ un generador de $GF^*(p^{2k})$. Para toda potencia prima p^k; la colección*

$$\left\{B(\theta, p, i) : i \in GF(p^k)\right\}$$

Da lugar a una partición del intervalo $\left[1, p^{2k} - 1\right]$, en p^k clases, tales que:

1. $|B(\theta, p, i)| = p^k$, *donde;* $i \in GF^*(p^k)$
2. $B(\theta, p, 0) = \left\{p^k + 1, 2(p^k + 1), 3(p^k + 1), \ldots, (p^k - 1)(p^k + 1)\right\}$

Prueba.

La prueba de que $|B(\theta, p, i)| = p^k$ es analóga a la prueba realizada en el teorema 6.

Probemos que

$$B(\theta, p, 0) = \left\{p^k + 1, 2(p^k + 1), 3(p^k + 1), \ldots, (p^k - 1)(p^k + 1)\right\}$$

Sea $a \in B(\theta, p, 0)$, por (3.9); se tiene que $a \in \left[1, p^{2k}-1\right]$ y que $\theta^a \in GF(p^k)$, pero por el resultado preliminar 7, parte (b); $\theta^a \in GF(p^k)$ si y sólo si

$$a \in \left[1, p^{2k}-1\right] \quad \text{y} \quad a \equiv 0(\text{mód } p^k+1).$$

Lo cual equivale a decir, $a \in \left[1, p^{2k}-1\right]$ y a es múltiplo de p^k+1.
Luego,

$$B(\theta, p, 0) = \left\{p^k+1, 2(p^k+1), 3(p^k+1), \ldots, (p^k-1)(p^k+1)\right\}$$

Este resultado permite establecer también que $|B(\theta, p, 0)| = p^k - 1$.
Por último probemos que la colección $\left\{B(\theta, p, i) : i \in GF(p^k)\right\}$, da lugar a una partición del intervalo $\left[1, p^{2k}-1\right]$.

Mostremos que los elementos de la colección $\left\{B(\theta, p, i) : i \in GF(p^k)\right\}$ son disjuntos por pares.
Sean $i, j \in GF(p^k)$ y $a \in \left[1, p^{2k}-1\right]$, tales que,

$$a \in B(\theta, p, i) \cap B(\theta, p, j)$$

por definición de $B(\theta, p, i)$ y $B(\theta, p, j)$, existe $x, y \in GF(p^k)$, para los cuales,

$$x = \theta^a - i\theta \quad e \quad y = \theta^a - j\theta$$

restando estas dos ecuaciones, se obtiene:

$$\theta(i-j) + x - y = 0$$

como por el resultado preliminar 6, θ es algebraico de grado 2 sobre $GF(p^k)$, entonces,

$$i = j \quad y \quad x = y$$

por lo tanto,

$$B(\theta, p, i) = B(\theta, p, j).$$

Probemos que

$$\bigcup_{i \in GF(p^k)} B(\theta, p, i) = \left[1, p^{2k}-1\right]$$

basta ver que,

$$\left| \bigcup_{i \in GF(p^k)} B(\theta, p, i) \right| = \left| \left[1, p^{2k} - 1\right] \right|$$

Puesto que los $B(\theta, p, i)$ son dos a dos disjuntos, se tiene que:

$$\left| \bigcup_{i \in GF(p^k)} B(\theta, p, i) \right| = \sum_{i \in GF(p^k)} |B(\theta, p, i)| = |B(\theta, p, 0)| + \sum_{i \in GF(p^k)} |B(\theta, p, i)|$$

como $|B(\theta, p, i)| = p^k$ y $|B(\theta, p, 0)| = p^k - 1$,

$$\left| \bigcup_{i \in GF(p^k)} B(\theta, p, i) \right| = (p^k - 1) + \sum_{i \in GF(p^k)} p^k$$

$$\left| \bigcup_{i \in GF(p^k)} B(\theta, p, i) \right| = (p^k - 1) + (p^k - 1)p^k = p^{2k} - 1 = \left| \left[1, p^{2k} - 1\right] \right|$$

Por tanto:

$$\bigcup_{i \in GF(p^k)} B(\theta, p, i) = \left[1, p^{2k} - 1\right]$$

□

NOTA:

Una consecuencia directa del teorema 8, es que si agregamos el cero tanto al intervalo $\left[1, p^{2k} - 1\right]$ como a $B(\theta, p, 0)$, se obtiene que los elementos de la colección,

$$\left\{ B(\theta, p, i) : i \in GF(p^k) \right\};$$

dan lugar a una partición del intervalo $\left[0, p^{2k} - 1\right]$.

Ejemplo 9.

sea θ una raíz del polinomio $f(x) = x^2 + 3x + 3$ sobre $GF(5)$. θ es un generador de $GF^*(25)$, vease cuadro 3.2.

Como θ una raíz del polinomio $f(x) = x^2 + 3x + 3$, entonces

$$\theta^2 = 2\theta + 2$$

para $i = 0, 1, \ldots, 4$, considerese el siguiente conjunto,

$$B(\theta, 5, i) = \left\{ a \in \left[1, 5^2 - 1\right] : \theta^a - i\theta \in GF(5) \right\}$$

para $i = 0, 1, \ldots, 4$, calculamos los posibles valores de $\theta^a - i\theta$, los cuales se muestran en el cuadro 3.3.

a	$i = 0 \backslash \theta^a$	$i = 1 \backslash \theta^a - \theta$	$i = 2 \backslash \theta^a - 2\theta$	$i = 3 \backslash \theta^a - 3\theta$	$i = 4 \backslash \theta^a - 4\theta$
1	θ	0	θ	3θ	2θ
2	$2\theta + 2$	$\theta + 2$	2	$2 - \theta$	$2 - 2\theta$
3	$\theta + 4$	4	$4 - \theta$	$4 - 2\theta$	$4 - 3\theta$
4	$\theta + 2$	2	$2 - \theta$	$2 - 2\theta$	$2 - 3\theta$
5	$4\theta + 2$	$3\theta + 2$	$2\theta + 2$	$\theta + 2$	2
6	3	$3 - \theta$	$3 - 2\theta$	$3 - 3\theta$	$3 - 4\theta$
7	3θ	2θ	θ	0	4θ
8	$\theta + 1$	1	$1 - \theta$	$1 - 2\theta$	$1 - 3\theta$
9	$3\theta + 2$	$2\theta + 2$	$\theta + 2$	2	$2 - \theta$
10	$3\theta + 1$	$2\theta + 1$	$\theta + 1$	1	$1 - \theta$
11	$2\theta + 1$	$\theta + 1$	1	$1 - \theta$	$1 - 2\theta$
12	4	$4 - \theta$	$4 - 2\theta$	$4 - 3\theta$	$4 - 4\theta$
13	4θ	3θ	2θ	θ	0
14	$3\theta + 3$	$2\theta + 3$	$\theta + 3$	3	$3 - \theta$
15	$4\theta + 1$	$3\theta + 1$	$2\theta + 1$	$\theta + 1$	1
16	$4\theta + 3$	$3\theta + 3$	$2\theta + 3$	$\theta + 3$	3
17	$\theta + 3$	3	$3 - \theta$	$3 - 2\theta$	$3 - 3\theta$
18	2	$2 - \theta$	$2 - 2\theta$	$2 - 3\theta$	$2 - 4\theta$
19	2θ	θ	0	4θ	3θ
20	$4\theta + 4$	$3\theta + 4$	$2\theta + 4$	$\theta + 4$	4
21	$2\theta + 3$	$\theta + 3$	3	$3 - \theta$	$3 - 2\theta$
22	$2\theta + 4$	$\theta + 4$	4	$4 - \theta$	$4 - 2\theta$
23	$3\theta + 4$	$2\theta + 4$	$\theta + 4$	4	$4 - \theta$
24	1	$1 - \theta$	$1 - 2\theta$	$1 - 3\theta$	$1 - 4\theta$

Cuadro 3.3: Ejemplo 9 Generalización de la construcción de Bose.

Por lo tanto los conjuntos que dan lugar a la partición de $[1, 24]$, que se obtienen en generalización de la construcción de Bose son:

$$\text{Para} \quad i = 0 \rightarrow B(\theta, 5, 0) = \{6, 12, 18, 24\},$$

$$\text{Para} \quad i = 1 \rightarrow B(\theta, 5, 1) = \{1, 3, 4, 8, 17\},$$

$$\text{Para} \quad i = 2 \rightarrow B(\theta, 5, 2) = \{2, 11, 19, 21, 22\},$$

$$\text{Para} \quad i = 3 \rightarrow B(\theta, 5, 3) = \{7, 9, 10, 14, 23\},$$

$$\text{Para} \quad i = 4 \rightarrow B(\theta, 5, 4) = \{5, 13, 15, 16, 20\}.$$

Si agregamos el cero tanto a $[1, 24]$ como a $B(\theta, 5, 0)$, los conjuntos descritos anteriormente forman una partición de $[0, 24]$, los conjuntos $B(\theta, 5, i)$, para $i = 1, 2, 3, 4$; forman conjuntos de Sidon y reglas Golomb módulo 24, y $B(\theta, 5, 0) \cup \{0\}$ consta de los múltiplos de 6 que pertenecen a $[0, 24]$.

3.6. Construcción de Singer

En 1938, Singer [8], construye conjuntos de Sidon y reglas Golomb, fundamentandose al igual que Bose en los resultados sobre campos finitos presentados en la sección (3.1).

Sean p un número primo, k un entero positivo, y θ un generador de $GF^*(p^{3k})$, Singer define el conjunto $S(p, \theta)$, como sigue,

$$S(p, \theta) = \left\{ a \in \left[1, p^{3k} - 1\right] : \theta^a - \theta \in GF(p^k) \right\}. \tag{3.10}$$

El siguiente teorema da una ilustración de la construcción de Singer.

Teorema 9. ***(Singer*** 1.938***)*** *Para toda potecia prima p^k existe un conjunto de Sidon y una regla Golomb módulo $p^{2k} + p^k + 1$, con p^k elementos, contenido en $\left[1, p^{3k} - 1\right]$.*

Prueba.

Probemos que el conjunto $S(p,\theta)$ definido en (3.10), tiene p^k elementos y forma un conjunto de Sidon y una regla Golomb módulo $p^{2k}+p^k+1$.
La prueba de que el cardinal de $S(p,\theta)$ es p^k, se hace definiendo la función L, como sigue:

$$L : S(p,\theta) \to GF(p^k)$$

$$a \to L(a) = \theta^a - \theta$$

Y probando que L es una biyección entre $S(p,\theta)$ y $GF(p^k)$, esta prueba se hace de manera analóga a la prueba realizada en el teorema 6 y por lo tanto se omite.

Probemos, entonces; que $S(p,\theta)$ forma un conjunto de Sidon y una regla Golomb módulo $p^{2k}+p^k+1$, por la proposición 6, sólo basta probar que $S(p,\theta)$ forma un conjunto de Sidon módulo $p^{2k}+p^k+1$, sean $a,b,c,d \in S(p,\theta)$, tales que:

$$a+b \equiv c+d \left(\text{mód } p^{2k}+p^k+1\right) \tag{3.11}$$

Por el resultado preliminar 5, (3.11); se da si y sólo si θ^{a+b} y θ^{c+d}, son linealmente dependientes sobre $GF(p^k)$, por tanto existe $\alpha \in GF^*(p^k)$, talque,

$$\theta^{a+b} = \alpha\theta^{c+d}$$

$$\theta^a\theta^b = \alpha\theta^c\theta^d \tag{3.12}$$

por definición de $S(p,\theta)$ y de la función L, existen $L(a), L(b), L(c)$ y $L(d)$, que satisfacen:
$L(a) = \theta^a - \theta, L(b) = \theta^b - \theta, L(c) = \theta^c - \theta \quad \text{y} \quad L(d) = \theta^d - \theta$

de manera que (3.12) se puede expresar como:

$$(L(a)+\theta)(L(b)+\theta) = \alpha(L(c)+\theta)(L(d)+\theta)$$

Luego de varios cálculos se llega a,

$$(1-\alpha)\theta^2 + [(L(a)+L(b)) - \alpha(L(c)+L(d))]\theta + L(a)L(b) - \alpha L(c)L(d) = 0 \tag{3.13}$$

de (3.13), se ve que θ satisface un polinomio de grado 2, pero el resultado preliminar 6, permite establecer que θ es álgebraico de grado 3, sobre $GF(p^k)$, así que,

$$\alpha = 1,$$

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

Y

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

Como $GF(p^k)$ forma un campo, entonces:

$$(L(a) = L(c) \quad y \quad L(b) = L(d)) \quad \text{o} \quad (L(a) = L(d) \quad y \quad L(b) = L(c)) \tag{3.14}$$

La inyectividad de L y (3.14), implican que:

$$(a = c \quad y \quad b = d) \quad \text{o} \quad (a = d \quad y \quad b = c)$$

En consecuencia, $S(p, \theta)$ forma un conjunto de Sidon y una regla Golomb módulo $p^{2k} + p^k + 1$. □

Veamos un ejemplo que se puede apreciar la construcción de Singer.

Ejemplo 10.

sea θ una raíz del polinomio $f(x) = x^3 + 3x + 2$ sobre $GF(p^5) = \mathbb{Z}_5$, es decir;

$$\theta^3 = 2\theta + 3$$

θ es un generador de $GF^*(p^{5^3})$, lo cual se puede apreciar en el cuadro (3.4) y se obtiene el conjunto:

$$S(5, \theta) = \left\{a \in \left[1, 5^3 - 1\right] : \theta^a - \theta \in GF(p^5)\right\} = \{1, 14, 34, 103, 119\}$$

Reduciendo módulo $5^2 + 5 + 1 = 31$; se obtiene el conjunto,

$$S(5, \theta) = \{1, 3, 10, 14, 26\}$$

el cual por el teorema 9, forma un conjunto de Sidon y una regla Golomb módulo 31.

α	θ^{α}	α	θ^{α}	α	θ^{α}	α	θ^{α}	α	θ^{α}
1	θ	26	$3\theta + 1$	51	$2\theta^2 + 4\theta + 2$	76	$4\theta + 2$	101	$4\theta^2 + 2\theta + 2$
2	θ^2	27	$3\theta^2 + \theta$	52	$4\theta^2 + \theta + 1$	77	$4\theta^2 + 2\theta$	102	$2\theta^2 + 2$
3	$2\theta + 3$	28	$\theta^2 + \theta + 4$	53	$4\theta^2 + 4\theta + 2$	78	$2\theta^2 + 3\theta + 2$	103	$\theta + 1$
4	$2\theta^2 + 3\theta$	29	$\theta^2 + \theta + 3$	54	$4\theta^2 + 4\theta + 3$	79	$3\theta^2 + \theta + 1$	104	$\theta^2 + \theta$
5	$3\theta^2 + 4\theta + 1$	30	$\theta^2 + 3$	55	$4\theta^2 + \theta + 2$	80	$\theta^2 + 2\theta + 4$	105	$\theta^2 + 2\theta + 3$
6	$4\theta^2 + 2\theta + 4$	31	3	56	$\theta^2 + 2$	81	$2\theta^2 + \theta + 3$	106	$2\theta^2 + 3$
7	$2\theta^2 + 2\theta + 2$	32	3θ	57	$4\theta + 3$	82	$\theta^2 + 2\theta + 1$	107	$2\theta + 1$
8	$2\theta^2 + \theta + 1$	33	$3\theta^2$	58	$4\theta^2 + 3\theta$	83	$2\theta^2 + 3\theta + 3$	108	$2\theta^2 + \theta$
9	$\theta^2 + 1$	34	$\theta + 4$	59	$3\theta^2 + 3\theta + 2$	84	$3\theta^2 + 2\theta + 1$	109	$\theta^2 + 4\theta + 1$
10	$3\theta + 3$	35	$\theta^2 + 4\theta$	60	$3\theta^2 + 3\theta + 4$	85	$2\theta^2 + 2\theta + 4$	110	$4\theta^2 + 3\theta + 3$
11	$\theta^2 + 3\theta$	36	$4\theta^2 + 2\theta + 3$	61	$3\theta^2 + 4$	86	$2\theta^2 + 3\theta + 1$	111	$3\theta^2 + \theta + 2$
12	$3\theta^2 + \theta + 4$	37	$2\theta^2 + \theta + 2$	62	4	87	$3\theta^2 + 1$	112	$\theta^2 + 3\theta + 4$
13	$\theta^2 + 4$	38	$\theta^2 + \theta + 1$	63	4θ	88	$2\theta + 4$	113	$3\theta^2 + \theta + 3$
14	$\theta + 3$	39	$\theta^2 + 3\theta + 3$	64	$4\theta^2$	89	$2\theta^2 + 4\theta$	114	$\theta^2 + 4\theta + 4$
15	$\theta^2 + 3\theta$	40	$3\theta^2 + 3$	65	$3\theta + 2$	90	$4\theta^2 + 4\theta + 1$	115	$4\theta^2 + \theta + 3$
16	$3\theta^2 + 2\theta + 3$	41	$4\theta + 4$	66	$3\theta^2 + 2\theta$	91	$4\theta^2 + 4\theta + 2$	116	$\theta^2 + \theta + 2$
17	$2\theta^2 + 4\theta + 4$	42	$4\theta^2 + 4\theta$	67	$2\theta^2 + \theta + 4$	92	$4\theta^2 + 2$	117	$\theta^2 + 4\theta + 3$
18	$4\theta^2 + 3\theta + 1$	43	$4\theta^2 + 3\theta + 2$	68	$\theta^2 + 3\theta + 1$	93	2	118	$4\theta^2 + 3$
19	$3\theta^2 + 4\theta + 2$	44	$3\theta^2 + 2$	69	$3\theta^2 + 3\theta + 3$	94	2θ	119	$\theta + 2$
20	$4\theta^2 + 3\theta + 4$	45	$3\theta + 4$	70	$3\theta^2 + 4\theta + 4$	95	$2\theta^2$	120	$\theta^2 + 2\theta$
21	$3\theta^2 + 3\theta + 1$	46	$3\theta^2 + 4\theta$	71	$4\theta^2 + 4$	96	$4\theta + 1$	121	$\theta^2 + 2\theta + 3$
22	$2\theta^2 + 3\theta + 4$	47	$4\theta^2 + \theta + 4$	72	$2\theta + 2$	97	$4\theta^2 + \theta$	122	$\theta^2 + 2\theta + 1$
23	$3\theta^2 + 3\theta + 1$	48	$\theta^2 + 2\theta + 2$	73	$2\theta^2 + 2\theta$	98	$\theta^2 + 3\theta + 2$	123	$2\theta^2 + 1$
24	$3\theta^2 + 2\theta + 4$	49	$2\theta^2 + 4\theta + 3$	74	$2\theta^2 + 4\theta + 1$	99	$3\theta^2 + 4\theta + 3$	124	1
25	$2\theta^2 + 4$	50	$4\theta^2 + 2\theta + 1$	75	$4\theta^2 + 1$	100	$4\theta^2 + 4\theta + 4$	–	–

Cuadro 3.4: Ejemplo 10 Construcción de Singer.

Las tablas de sumas y diferencias distintas para este conjunto se presentan a continuación.

Tabla de sumas módulo 31

1	3	10	14	26
2	4	11	15	27
	6	13	17	29
		20	24	5
			28	9
				21

Tabla de diferencias módulo 31

1	3	10	14	26
0	2	9	13	25
29	0	7	11	23
22	24	0	4	16
18	20	27	0	12

Sea $q = \frac{p^{3k}-1}{p^k-1} = p^{2k} + p^k + 1$, tenemos el siguiente lema que permite carecterizar los elementos del conjunto $S(p, \theta)$ definido en (3.10).

Lema 1. *Los elementos de $S(p, \theta)$ satisfecen que,*

1. *No existe a en $S(p, \theta)$ talque,*

$$a \equiv 0 \, (mód \; q)$$

2. *Elementos de $S(p, \theta)$ distintos son incongruentes módulo q.*

3. *No existen a,b en $S(p, \theta)$, tales que,*

$$a + b \equiv 0 \, (mód \; q)$$

4. *No existen a,b,c, en $S(p, \theta)$, tales que,*

$$a + b \equiv c \, (mód \; q)$$

Prueba.

Prueba de 1, supongase que existe a en $S(p,\theta)$, talque,

$$a \equiv 0 \,(\text{mód } q)$$

entonces existe t en $\mathbb{Z}$, para el cual, $a = tq$; pero como $a \in S(p,\theta)$, entonces; existe x en $GF(p^k)$, con la propiedad de que,

$$x = \theta^a - \theta = \theta^{tq} - \theta,$$

de donde resulta que,

$$\theta = \theta^{tq} - x = (\theta^q)^t - x \tag{3.15}$$

por otro lado del resultado preliminar 6, se conoce que θ^q, genera a $GF^*(p^k)$, por tanto de (3.15) se tiene que $\theta \in GF(p^k)$, que es imposible, puesto que θ genera a $GF(p^{3k})$.

Prueba de 2, supongase que existen a, b en $S(p,\theta)$, tales que,

$$a \equiv b \,(\text{mód } q)\,, \tag{3.16}$$

por el resultado preliminar 5, (3.16); se da si y sólo si θ^a y θ^b, son linealmente dependientes sobre $GF(p^k)$, por tanto existe $\alpha \in GF^*(p^k)$, talque,

$$\theta^a = \alpha\theta^b \tag{3.17}$$

por definición de $S(p,\theta)$ y de la función L definida en el teorema 9, existen $L(a) = \theta^a - \theta$ y $L(b) = \theta^b - \theta$, que junto con (3.17), implican que,

$$(1-\alpha)\,\theta + (L(a) - \alpha L(b)) = 0 \tag{3.18}$$

de (3.18), se ve que θ satisface un polinomio de grado 1, pero por el resultado preliminar 6, θ es álgebraico de grado 3, sobre $GF(p^k)$, así que,

$$\alpha = 1,$$

$$L(a) = L(b)$$

como L es inyectiva se concluye que, $a = b$.

Prueba de 3, supongase que existen a, b en $S(p, \theta)$, tales que,

$$a + b \equiv 0 \,(\text{mód } q)\,, \tag{3.19}$$

por el resultado preliminar 5, (3.19); se da si y sólo si θ^a y θ^{-b}, son linealmente dependientes sobre $GF(p^k)$, por tanto existe $\alpha \in GF^*(p^k)$, talque,

$$\theta^a = \alpha\theta^{-b}$$

$$\theta^a\theta^b = \alpha \tag{3.20}$$

por definición de $S(p, \theta)$ y de la función L definida en el teorema 9, existen $L(a) = \theta^a - \theta$ y $L(b) = \theta^b - \theta$, que junto con (3.20), implican que,

$$\theta^2 + (L(a) + L(b))\,\theta + L(a)L(b) - \alpha = 0 \tag{3.21}$$

de (3.21), θ satisface un polinomio de grado 2, que no es posible, ya que; por el resultado preliminar 6, θ es álgebraico de grado 3, sobre $GF(p^k)$.

Prueba de 4, supongase que existen a, b, c en $S(p, \theta)$, tales que,

$$a + b \equiv c \,(\text{mód } q)\,, \tag{3.22}$$

por el resultado preliminar 5, (3.22); se da si y sólo si θ^{a+b} y θ^c, son linealmente dependientes sobre $GF(p^k)$, por tanto existe $\alpha \in GF^*(p^k)$, talque,

$$\theta^{a+b} = \alpha\theta^c \tag{3.23}$$

por definición de $S(p, \theta)$ y de la función L definida en el teorema 9, existen $L(a) = \theta^a - \theta$, $L(b) = \theta^b - \theta$ y $L(c) = \theta^c - \theta$, que junto con (3.23), implican que,

$$\theta^2 + (L(a) + L(b) - \alpha)\,\theta + L(a)L(b) - \alpha L(c) = 0 \tag{3.24}$$

de (3.24), θ satisface un polinomio de grado 2, que no es posible, ya que; por el resultado preliminar 6, θ es álgebraico de grado 3, sobre $GF(p^k)$.

□

Teorema 10. *Existe un conjunto de Sidon A módulo q, contenido en* $[1, q]$ *con* $p^k + 1$ *elementos.*

Prueba.

Definamos A, como sigue;

$$A = \{x \in [1, q] : x \equiv a \,(\text{mód } q)\,, a \in S(p, \theta)\} \cup \{q\}$$

Por las partes 1 y 2 del lema 1,

$$|A| = p^k + 1.$$

Por el teorema 9 y las partes 3 y 4, del lema 1, se tiene que A forma un conjunto de Sidon módulo $q = p^{2k} + p^k + 1$, contenido en $[1, q]$.

Corolario 3. ***(Singer)*** *Sea p un número primo y k un entero positivo,para toda potencia prima* p^k*, se tiene:*

1. $F_2(p^{2k} + p^k + 1) \geq p^k + 1$
2. $G(p^k + 1) \leq p^{2k} + p^k + 1$
3. $f_2(p^{2k} + p^k + 1) = p^k + 1$

Prueba.

1. Por el teorema 10, existe un conjunto de Sidon A, con $p^k + 1$ elementos, módulo $p^{2k} + p^k + 1$ y $A \subseteq [1, p^{2k} + p^k + 1]$, dado que todo conjunto de Sidon módular forma un conjunto de Sidon, entonces; es claro que:

$$F_2(p^{2k} + p^k + 1) \geq p^k + 1$$

2. Por la proposición 6, el conjunto de Sidon A del teorema 10 forma una regla Golomb módulo $p^{2k}+p^k+1$, con p^k+1 elementos, y $A \subseteq [1, p^{2k}+p^k+1]$, por la propiedad de traslación para reglas Golomb módulares y puesto que toda regla Golomb módular forma una regla Golomb, es inmediato que,

$$G(p^k+1) \leq p^{2k}+p^k+1$$

3. Por otra parte, $f_2(p^{2k}+p^k+1)$ representa el máximo cardinal de un conjunto de Sidon contenido en $\mathbb{Z}_{\left(p^{2k}+p^k+1\right)}$, por lo tanto se puede afirmar que:

$$f_2(p^{2k}+p^k+1) \geq p^k+1$$

Veamos que no se puede dar que

$$f_2(p^{2k}+p^k+1) > p^k+1.$$

Supongase que existe un conjunto de Sidon A módulo $p^{2k}+p^k+1$, talque:

$$|A| = f_2(p^{2k}+p^k+1) \geq p^k+2$$

Por la proposición 6, A forma una regla Golomb módulo $p^{2k}+p^k+1$, por lo tanto:

$$|A-A| \geq 2\binom{p^k+2}{2} = \left(p^k+1\right)\left(p^k+2\right) = p^{2k}+3p^k+2 > p^{2k}+p^k+1$$

Lo cual contradice que A forma una regla Golomb módulo $p^{2k}+p^k+1$ y por ende contradice que A sea conjunto de Sidon módulo $p^{2k}+p^k+1$, en consecuencia debe tenerse que:

$$f_2(p^{2k}+p^k+1) = p^k+1.$$

□

3.7. Algunas implicaciones de las construcciones de Ruzsa y Bose

Como consecuencia de la generalización de las construcciones de Ruzsa y Bose, se tienen las siguientes implicaciones tanto para reglas Golomb como para conjuntos de Sidon.

3.7.1. Acerca del conjunto de diferencias de una regla Golomb

Si denotamos por $A = R(p, \theta, f, u),$ con $u \neq 0$; a cualquiera de los conjuntos obtenidos en la generalización de la construcción de Ruzsa y dado que para $u \neq 0$ estos conjuntos forman reglas Golomb, interesa dar una determinación completa del conjunto de diferencias de A, lo cual se puede apreciar en el siguiente corolario.

Corolario 4. *Si $A = R(p, \theta, f, u),$ con $u \neq 0$, es uno de los conjuntos obtenidos en la forma general de la construcción de Ruzsa, entonces*

$$A - A = \mathbb{Z}_N \setminus R(\theta, p, 0, f) \cup M_{p-1}$$

Donde:

$$N = p(p-1)$$

$$M_{p-1} = \{p-1, 2(p-1), ..., p(p-1)\}$$

Prueba.

Sabemos que $A = R(p, \theta, f, u),$ con $u \neq 0$ es una regla Golomb módulo $p(p-1)$, con p primo, y $|A| = p-1$, entonces se debe probar que el conjunto $A - A$ no esta conformado por multiplos de p y $p-1$, primero probemos que no hay multiplos de p en $A - A$, para ello supongase que existen i, j en $[1, p-1]$ distintos, tales que:

$$a_i - a_j \equiv 0(\text{mód } p) \quad \text{donde} \quad a_i, a_j \in A$$

Entonces,

$$a_i \equiv a_j(\text{mód } p) \tag{3.25}$$

Sea θ la raíz primitiva módulo p asociada con A, por la forma como se han definido los elementos del conjunto A, se tiene que:

$$a_i \equiv i(\text{mód } p-1) \quad y \quad a_i \equiv \theta^i(\text{mód } p)$$

$$a_j \equiv j(\text{mód } p-1) \quad y \quad a_j \equiv \theta^j(\text{mód } p)$$

De (3.25), tenemos:

$$\theta^i \equiv \theta^j(\text{mód } p)$$

Por el resultado preliminar 1, se tiene que:

$$i \equiv j(\text{mód } p-1)$$

y como i, j estan en $[1, p-1]$, entonces se concluye que $i = j$, lo que contradice el supuesto de que j e i son distintos, por lo tanto en el conjunto $A - A$ no hay múltiplos de p.

De manera analóga se prueba que en el conjunto $A - A$ no hay múltiplos de $p-1$. □

Sea p un número primo, k un entero positivo y θ un generador de $GF^*(p^{2k})$, si denotamos por $A = B(p, \theta, i)$, con $i \neq 0$; a cualquiera de los conjuntos obtenidos en la generalización de la construcción de Bose y dado que para $i \neq 0$ estos conjuntos forman reglas Golomb, al igual que en el corolario 4 interesa dar una determinación completa del conjunto de diferencias de A, lo cual se puede apreciar en el siguiente corolario.

Corolario 5. *Si $A = B(p, \theta, i)$, con $i \neq 0$, entonces,*

$$A - A = \mathbb{Z}_{p^{2k}-1} \setminus B(\theta, p, 0)$$

Prueba.

puesto que $B(\theta, p, 0) = \left\{p^k + 1, 2(p^k + 1), \ldots, p^{2k} - 1\right\}$, se debe probar que el conjunto $A - A$ no esta conformado por múltiplos de $p^k + 1$, para ello supongase que existen $a, b \in A$ distintos, tales que

$$a - b \equiv 0(\text{mód } p^k + 1)$$

Entonces, por el resultado preliminar 7,parte (b); se deduce que,

$$\theta^{a-b} \in GF(p^k)$$

es decir, que existe z en $GF(p^k)$, para el cual, $\theta^{a-b} = z$.
Por la forma como se han definido los elementos del conjunto A, existen x, y, i, j en $GF(p^k)$, con la propiedad de que,

$$\theta^a - i\theta = x \quad y \quad \theta^b - j\theta = y$$

luego de algunos calculos se obtiene,

$$\theta^{a-b} = z = \frac{x + i\theta}{y + j\theta}$$

de donde,

$$\theta(i - jz) + x - yz = 0 \tag{3.26}$$

pero (3.26), es imposible, pues θ es álgebraico de grado 2 sobre $GF(p^k)$,(resultado preliminar 6).
En consecuencia,

$$A - A = \mathbb{Z}_{p^{2k}-1} \setminus B\,(\theta, p, 0)$$

□

3.7.2. Sobre el máximo elemento de una regla Golomb

Como consecuencia de la generalización de la construcción de Ruzsa, se puede calcular una cota superior para el máximo elemento de una regla Golomb módulo $p(p-1)$, lo que permite entonces encontrar una cota superior para la función $G(k)$, que mejora la cota encontrada para esta función en el corolario 1.

Corolario 6. *Para todo primo p, se tiene*

$$G(p-1) \leq p^2 - 2p$$

Prueba.

Consideremos las reglas Golomb módulares que se obtienen en la generalización de la construcción de Ruzsa (teoremas 4 y 5), con sus elementos ordenados de menor a mayor:

$$R(\theta, p, 0, f) = \{p < 2p < \ldots < (p-1)\, p\}$$

$$R(\theta, p, 1, f) = \left\{a_{1_1} < a_{1_2} < \ldots < a_{1_{(p-1)}}\right\} \Rightarrow a_{1_{(p-1)}} \leq (p-1)\, p - 1$$

$$R(\theta, p, 2, f) = \left\{a_{2_1} < a_{2_2} < \ldots < a_{2_{(p-1)}}\right\} \Rightarrow a_{2_{(p-1)}} \leq (p-1)\, p - 2$$

$$\vdots$$

$$R(\theta, p, p-1, f) = \left\{a_{(p-1)_1} < a_{(p-1)_2} < \ldots < a_{(p-1)_{(p-1)}}\right\} \Rightarrow a_{(p-1)_{(p-1)}} \leq (p-1)\, p - (p-1)$$

Y puesto que toda regla Golomb módular forma una regla Golomb, existe $A \in GOL_0(p-1)$, con la propiedad de que:

$$\text{máx}(A) \leq (p-1)^2 - 1 = p^2 - 2p$$

Así, se puede concluir que:

$$G(p-1) \leq p^2 - 2p$$

□

Como consecuencia de la generalización de la construcción de Bose, se puede cálcular una cota superior para el máximo elemento de una regla Golomb módulo $p^{2k} - 1$, lo que permite entonces encontrar una cota superior para la función $G(k)$, que mejora la cota encontrada para esta función en en corolario 2.

Corolario 7. *Sea p un número primo y k un entero positivo, para toda potencia prima p^k, se tiene*

$$G(p^k) \leq p^{2k} - p^k - 1$$

Prueba.

Consideremos las reglas Golomb módulares que se obtienen en la generalización de la construcción de Bose, con sus elementos ordenados de menor a mayor:

$$B(\theta, p, 0) = \left\{p^k + 1 < 2(p^k + 1) < \ldots < p^{2k} - 1\right\}$$

$$B(\theta, p, 1) = \left\{a_{1_1} < a_{1_2} < \ldots < a_{1_{p^k}}\right\} \Rightarrow a_{1_{p^k}} \leq p^{2k} - 2$$

$$B(\theta, p, 2) = \left\{a_{2_1} < a_{2_2} < \ldots < a_{2_{p^k}}\right\} \Rightarrow a_{2_{p^k}} \leq p^{2k} - 3$$

$$\vdots$$

$$B\left(\theta, p, p^k - 1\right) = \left\{a_{\left(p^k-1\right)_1} < a_{\left(p^k-1\right)_2} < \ldots < a_{\left(p^k-1\right)_{\left(p^k\right)}}\right\} \Rightarrow a_{\left(p^k-1\right)_{p^k}} \leq p^{2k} - p^k$$

Puesto que toda regla Golomb módular forma una regla Golomb, existe $A \in GOL_0(p^k)$, con p^k elementos, con la propiedad de que:

$$\text{máx}(A) \leq p^{2k} - p^k - 1$$

Así, se puede concluir que:

$$G(p^k) \leq p^{2k} - p^k - 1$$

□

3.7.3. Número de conjuntos de Sidon

Denotemos por $Sd(N)$ el número total de conjuntos de Sidon módulo N. Con respecto a este número, Erdös y Cameron [6] preguntan si es cierto que:

$$\frac{Sd(N)}{2^{f_2(N)}} \to \infty \quad \text{cuando} \quad N \to \infty$$

Relación entre la generalización de la construcción de Ruzsa y la conjetura de Erdös-Cameron

La partición correspondiente al teorema 5 permite obtener una cota inferior para $Sd(p(p-1))$.

En fecto; sea $A = R(p, \theta, f, u),$ con $u \neq 0$, el número de subcojuntos de Sidon contenidos en A es 2^{p-1}.

Puesto que el conjunto vacio ϕ es también un conjunto de Sidon, no es necesario contar a ϕ en los $p-2$ conjuntos restantes, es decir; si $B = R(p, \theta, f, v)$, con $v \neq u \neq 0$; el número total de subconjuntos de Sidon contenidos en B es $2^{p-1} - 1$ y como los elementos de $R(p, \theta, f, 0)$ vistos como conjuntos unitarios forman también reglas Golomb módulo $p(p-1)$, se tiene que el número total de conjuntos de Sidon módulo $(p(p-1))$, esta dado por:

$$Sd(p(p-1)) = 2^{p-1} + (p-2)\left(2^{p-1} - 1\right) + p - 1$$

Luego de algunas manipulaciones encontramos que:

$$Sd(p(p-1)) = 2^{p-1}(p-1) + 1 > 2^{p-1}(p-1) \tag{3.27}$$

y la mejor cota inferior para $Sd(p(p-1))$, esta dada por:

$$Sd(p(p-1)) = 2^{p-1}(p-1) + 1 > (p-1)$$

Usando (3.27), probamos que:

$$\frac{Sd(p(p-1)}{2^{f_2(p(p-1))}} = \frac{Sd(p(p-1)}{2^{(p-1)}} \to \infty \quad \text{cuando} \quad p \to \infty$$

Por lo cual se puede afirmar que la generalización de la construcción de Ruzsa permite demostrar que la conjetura de Erdös y Cameron [6], es válida para todo N de la forma $p(p-1)$.

Relación entre la generalización de la construcción de Bose y la conjetura de Erdös-Cameron

La partición correspondiente al teorema 7 permite obtener una cota inferior para $Sd(p^{2k}-1)$.

En fecto; sea $A = B(p,\theta,i),$ con $i \neq 0$, el número de subcojuntos de Sidon contenidos en A es 2^{p^k}.

Puesto que el conjunto vacio ϕ es también un conjunto de Sidon, no es necesario contar a ϕ en los $p^k - 2$ conjuntos restantes, es decir; si $A' = B(p,\theta,j)$, con $i \neq j \neq 0$; el número total de subconjuntos de Sidon contenidos en A' es $2^{p^k} - 1$, tambien cada elemento de $B(p,\theta,0)$ visto como un conjunto unitario forma un conjunto de Sidon con módulo $p^{2k}-1$, por lo tanto el número total de conjuntos de Sidon módulo $p^{2k} - 1$, esta dado por:

$$Sd(p^{2k}-1) = 2^{p^k} + \left(p^k - 2\right)\left(2^{p^k} - 1\right) + p^k - 1$$

Luego de algunas manipulaciones se obtiene,

$$Sd(p^{2k}-1) = 2^{p^k}(p^k - 1) + 1 > 2^{p^k}\left(p^k - 1\right) \tag{3.28}$$

y la mejor cota inferior para $Sd(p^{2k}-1)$, esta dada por,

$$Sd(p^{2k}-1) = 2^{p^k}(p^k - 1) + 1 > p^k - 1$$

Usando (3.28), probamos que:

$$\frac{Sd(p^{2k}-1)}{2^{f_2(p^{2k}-1)}} = \frac{Sd(p^{2k}-1)}{2^{p^k}} \to \infty \quad \text{cuando} \quad p \to \infty$$

Por lo anterior se puede decir que la generalización de la construcción de Bose permite demostrar que la conjetura de Erdös y Cameron [6], es también válida para todo N de la forma $p^{2k} - 1$.

Capítulo 4

FUNCIONES EXTREMAS

En este capítulo se realiza un analísis de las funciones F_2 y f_2, definidas sobre conjuntos de Sidon y conjuntos de Sidon módulares, así mismo se estudia la función G definida sobre reglas Golomb.

4.1. Comportamiento asintótico de la función F_2

De la definición de $F_2(N)$, se sabe que ésta representa el máximo número de elementos que pueden seleccionarse de $[1, N] = \{1, 2, \ldots, N\}$, de tal manera que formen un conjunto de Sidon. En esta sección se estudia el comportamiento asintótico de la función $F_2(N)$, iniciando con la estimación de las cotas inferiores de esta función proporcionadas por las construcciones estudiadas en el capítulo anterior y posteriormente se estimarán las cotas superiores para $F_2(N)$.

4.1.1. Cotas inferiores

Sean p un número primo, k un entero positivo; para todo primo p y toda potencia prima p^k, a partir de las construcciones debidas a Ruzsa, Bose,Singer y sus respectivos corolarios se obtienen las siguientes cotas inferiores de $F_2(N)$.

a) Corolario 1 (Ruzsa) $\Rightarrow F_2(p\,(p-1)) \geq p-1$

b) Corolario 2 (Bose) $\Rightarrow F_2(p^{2k}-1) \geq p^k$

c) Corolario 3 (Singer) $\Rightarrow F_2(p^{2k}+p^k+1) \geq p^k+1$

Estos resultados permiten enunciar y probar los siguientes teoremas.

Teorema 11. *Para infinitos valores de N,*

$$F_2(N) \geq \sqrt{N}$$

Prueba.

Por el corolario 2 de Bose se sabe que para toda potencia prima p^k, se da que,

$$F_2(p^{2k}-1) \geq p^k,$$

además como F_2 es por definición no decreciente, tenemos;

$$F_2(p^{2k}-1) \leq F_2(p^{2k}),$$

por lo tanto, se puede tomar $N = p^{2k}$, como el conjunto de los números primos es infinito, entonces el resultado se satisface para infinitos valores de N. □

Teorema 12. *Para todo $N \geq 4$,*

$$\liminf_{N\to\infty} \frac{F_2(N)}{\sqrt{N}} \geq 1$$

Prueba.

Sea $N \geq 4$. Existen primos consecutivos p y q tales que,

$$p < \sqrt{N} < q,$$

además por el corolario 2 de Bose, para todo primo p, se tiene;

$$F_2(p^2) \geq p$$

entonces,

$$\frac{F_2(N)}{\sqrt{N}} \geq \frac{F_2(p^2)}{q} \geq \frac{p}{q}$$

como el cociente entre primos consecutivos tiende a 1, ver [6], se tiene,

$$\liminf_{N\to\infty} \frac{F_2(N)}{\sqrt{N}} \geq 1$$

□

4.1.2. Cotas superiores

Sea $A \in B_2(N)$ y $|A| = k$, en la sección 1.4, se probo que,

$$F_2(N) \leq \sqrt{4N - \frac{7}{4}} - \frac{1}{2}$$

Esta cota puede mejorarse puesto que como $A \in B_2(N)$, la proposición 4 permite establecer que $A \in GOL(k)$, en otras palabras; A forma una regla Golomb con k marcas, además de la definición de regla Golomb sabemos que,

$$|A - A| = \binom{k}{2} = \frac{k(k-1)}{2},$$

todas las diferencias estan en $[1, N-1]$. Entonces,

$$\frac{k(k-1)}{2} \leq N - 1$$

luego,

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

Por tanto,

$$k \leq \sqrt{2(N-1)} + 1$$

en particular cuando $k = F_2(N)$, tenemos;

$$F_2(N) \leq \sqrt{2(N-1)} + 1$$

Erdös y Turán, fueron los primeros en mejorar esta cota en 1941. Ellos probaron en [10] que,

$$F_2(N) \leq \sqrt{N} + O(N^{\frac{1}{4}})$$

Esta cota fue después mejorada por Lindström [11] y esta nueva cota es la mejor cota conocida para $F_2(N)$. El resultado que se enuncia a continuación se demuestra de tres maneras diferentes en [2], sin embargo; con el fin de realizar un estudio más completo del comportamiento asintótico de la función $F_2(N)$ también en este trabajo se presenta una demostración de dicho resultado debida a Lindström.

Teorema 13.

$$F_2(N) \leq N^{\frac{1}{2}} + N^{\frac{1}{4}} + 1$$

Prueba.

Sea $A = \{a_1 < a_2 < ... < a_k\} \in B_2(N)$, un conjunto de Sidon con cardinalidad máximal. Por la proposición 4, las diferencias de la forma $a_j - a_i, 1 \leq i < j \leq k$ deben ser todas diferentes. Llamemos al número $j - i$ el orden de la diferencia $a_j - a_i$.
La suma de las diferencias de orden r, con valor fijo r, está dada por:

$$S_r = \sum_{i=1}^{k-r} (a_{i+r} - a_i) \,. \tag{4.1}$$

Para cada m, con $1 \leq m \leq k$, se define $S_A(m)$ como la suma de todas las diferencias de orden r con $r \leq m$.
Entonces,

$$S_A(m) = \sum_{r=1}^{m} S_r = \sum_{r=1}^{m} \sum_{i=1}^{k-r} (a_{i+r} - a_i)$$

Llamando **s** al número de estas diferencias, se tiene

$$s = \sum_{r=1}^{m} (k - r) = \sum_{r=1}^{m} k + \sum_{r=1}^{m} r = km - \frac{m(m+1)}{2}$$

y por tanto,

$$s = km - \binom{m+1}{2} \tag{4.2}$$

Puesto que A es un conjunto de Sidon, por la proposición 4, todas las s diferencias en consideración son distintas y lo menos que puede ocurrir es que sean las más pequeñas: $1, 2, 3, ..., s$.
Entonces,

$$S_A(m) \geq \sum_{i=1}^{s} i = \frac{1}{2} s(s+1) \tag{4.3}$$

Por otra parte, desarrollando la suma S_r de (4.1) se tiene

$S_1 = \sum_{i=1}^{k-1} (a_{i+1} - a_i) = a_k - a_1$

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

$S_2 = (a_{k-2} - a_2) + (a_{k-1} - a_1)$

$$\vdots$$

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

$S_r = (a_k - a_r) + (a_{k-1} - a_{r-1}) + \ldots + (a_{k-r+1} - a_1)$

$$\vdots$$

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

$S_m = (a_k - a_m) + (a_{k-1} - a_{m-1}) + \ldots + (a_{k-m+1} - a_1)$

Luego $S_A(m)$ consta de

$$t = \sum_{r=1}^{m} r = \binom{m+1}{2} \tag{4.4}$$

sumandos que son diferencias. Todas estas diferencias son menores que N pues $A \subseteq [1, N]$. Por lo tanto,

$$S_A(m) < tN. \tag{4.5}$$

De (4.3) y (4.5), se tiene

$$\frac{1}{2}s^2 < \frac{1}{2}s(s+1) \leq S_A(m) < tN.$$

Esto, junto con (4.2) y (4.4)

$$[km - \frac{1}{2}m(m+1)]^2 < Nm(m+1)$$

Dividiendo ambos miembros de esta deisgualdad por m^2,

$$[k - \frac{1}{2}(m+1)]^2 < (1 + \frac{1}{m})N.$$

Como $\frac{1}{2}(m+1) < k$, entonces

$$k < \left(\sqrt{1 + \frac{1}{m}}\right)\sqrt{N} + \frac{1}{2}(m+1) = \left(\sqrt{\left(1 + \frac{1}{2m}\right)^2 - \frac{1}{4m^2}}\right)\sqrt{N} + \frac{1}{2}(m+1),$$

luego,

$$k < \left(1 + \frac{1}{2m}\right)\sqrt{N} + \frac{1}{2}(m+1),$$

Tomando $m = \left\lfloor N^{\frac{1}{4}} \right\rfloor + 1$, se tiene

$$N^{\frac{1}{4}} < m \leq N^{\frac{1}{4}} + 1$$

Y

$$k < \sqrt{N} + \frac{\sqrt{N}}{2N^{\frac{1}{4}}} + \frac{1}{2}(N^{\frac{1}{4}} + 1) + \frac{1}{2},$$

en consecuencia

$$k \leq N^{\frac{1}{2}} + N^{\frac{1}{4}} + 1$$

es decir;

$$F_2(N) \leq N^{\frac{1}{2}} + N^{\frac{1}{4}} + 1$$

□

Teorema 14.

$$\lim_{N\to\infty} \frac{F_2(N)}{\sqrt{N}} = 1$$

Prueba.

Del teorema 12 y del teorema anterior, se tiene que

$$1 \leq \liminf_{N\to\infty} \frac{F_2(N)}{\sqrt{N}} \leq \lim_{N\to\infty} \frac{F_2(N)}{\sqrt{N}} \leq \limsup_{N\to\infty} \frac{F_2(N)}{\sqrt{N}} \leq 1$$

De lo cual se sigue el resultado. □

4.2. La función $f_2(N)$

Por definición de $f_2(N)$, se sabe que ésta representa el máximo número de elementos que pueden seleccionarse de $\mathbb{Z}_N$, de tal manera que formen un conjunto de Sidon módulo N. En esta sección se realiza un estudio de la función $f_2(N)$, en lo que tiene que ver con las cotas superiores e inferiores de ésta función.

4.2.1. Cotas inferiores

Sean p un número primo, k un entero positivo; para todo primo p y toda potencia prima p^k, las construcciones debidas a Ruzsa, Bose y Singer; permiten obtener las siguientes cotas inferiores de $f_2(N)$.

a) Ruzsa $\Rightarrow f_2(p\,(p-1)) \geq p-1$

b) Bose $\Rightarrow f_2(p^{2k}-1) \geq p^k$

c) Singer $\Rightarrow f_2(p^{2k}+p^k+1) \geq p^k+1$

Sin embargo haciendo uso de la proposición 6, al contar el número de diferencias distintas de un conjunto de Sidon módular en los corolarios $1, 2$, y 3, de Ruzsa, Bose y Singer, respectivamente; se probo que,

a) Corolario 1(Ruzsa) $\Rightarrow f_2(p\,(p-1)) = p-1$

b) Corolario 2 (Bose) $\Rightarrow f_2(p^{2k}-1) = p^k$

c) Corolario 3 (Singer) $\Rightarrow f_2(p^{2k}+p^k+1) = p^k+1$

4.2.2. Cotas superiores

Sea $A \in B_2(\text{mód}N)$ y $|A| = k$, en el teorema 1, se probo que todo conjunto de Sidon módular es un conjunto de Sidon, lo cual implicó que $B_2(\text{mód}N) \subseteq B_2(N)$ y por lo tanto también se tenía que $f_2(N) \leq F_2(N)$, de este modo toda cota inferior de $f_2(N)$ es cota inferior para $F_2(N)$ y toda cota superior de $F_2(N)$ es cota superior de $f_2(N)$. Como $F_2(N) \leq \sqrt{2(N-1)}+1$, entonces;

$$f_2(N) \leq \sqrt{2(N-1)}+1.$$

Esta cota puede mejorarse puesto que como $A \in B_2(\text{mód}N)$, la proposición 6 permite afirmar que $A \in GOL(k, \text{mód}N)$, en otras palabras; A forma una regla Golomb módulo

N con k marcas, además de la definición de regla Golomb modular se tiene que,

$$|A - A| = 2\binom{k}{2} = k(k-1),$$

como todas las diferencias estan en $[1, N-1]$, entonces,

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

luego,

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

Por tanto,

$$k \leq \sqrt{(N-1)} + 1$$

en particular cuando $k = f_2(N)$, tenemos;

$$f_2(N) \leq \sqrt{(N-1)} + 1$$

por lo tanto,

$$\limsup_{N\to\infty} \frac{f_2(N)}{\sqrt{N}} \leq 1$$

Sin embargo, no se tiene una afirmación analóga para el limite inferior, es decir que no se ha podido establecer si,

$$\liminf_{N\to\infty} \frac{f_2(N)}{\sqrt{N}} \geq 1$$

por lo tanto, no se tienen las herramientas necesarias para determinar el comportamiento asintótico de $f_2(N)$.

4.3. Relaciones entre $F_2(N)$ y $G(k)$

Como consecuencia de la proposición 4, hablar de conjuntos de Sidon y de reglas Golomb es lo mismo, sin embargo; aunque las funciones extremas consideradas sobre estos dos conjuntos se han definido de manera distinta, se pueden encontrar relaciones entre dichas funciones.

Sean $n, k \in \mathbb{N}$

Lema 2. *1.* $F_2(N) = k \Leftrightarrow G(k) \leq N - 1 < G(k+1)$

2. $G(k) = N \Leftrightarrow F_2(N) = k - 1 \quad y \quad F_2(N+1) = k$

Prueba.

1. Supongase que $F_2(N) = k$, entonces existe un conjunto de Sidon con cardinal máximal k contenido en $[1, N]$, sea este,

$$A = \{a_1, a_2, \ldots, a_k\},$$

sin perdida de generalidad sea $a_1 = \text{mín}\, A$, por la propiedad de traslación de conjuntos de Sidon $A' = A - \text{mín}\, A$ forma unconjunto de Sidon contenido en $[0, N-1]$ y por la proposición 4, el conjunto $A' = A - \text{mín}\, A$ forma una regla Golomb que esta en $GOL_0(K)$ y contenida en $[0, N-1]$, con $\text{máx}\, A' \leq N - 1$, esto es; $G(k) \leq N - 1$. Como el cardinal de A es k máximal, entonces el cardinal de A' es también k máximal, es decir que A' es la regla Golomb más grande que se puede construir dentro del intervalo $[0, N-1]$, por lo tanto; $G(k+1) > N - 1$.

Reciprocamente; supongase que $G(k) \leq N - 1 < G(k+1)$, esto implica que existe una regla Golomb A en $GOL_0(K)$ contenida en $[0, N-1]$, con a lo más k elementos, por la proposición 4, A forma un conjunto de Sidon contenido en $[0, N-1]$ con a lo más k elementos y por la propiedad de traslación para conjuntos de Sidon el conjunto $A' = A + \text{máx}\, A$ es de Sidon y esta contenido en $[1, N]$, con cardinal máximal k, por lo tanto, $F_2(N) = k$

2. Supongase que $G(k) = N$, por lo tanto existe A en $GOL_0(K)$ y $A \subseteq [0, N]$, tal que $\text{máx}\, A = G(k) = N$ y como $|A| = k$, ningun conjunto contenido en $[0, N]$ con más de k elementos puede formar una regla Golomb, es decir k es máximal, por la propiedad de traslación para reglas Golomb y por la proposición 4, el conjunto $A + 1$ forma un conjunto de Sidon contenido en $[1, N+1]$ y $|A + 1| = k$, como k es

máximal, entonces $F_2(N+1) = k$.

Por otra parte, es claro que todo subconjunto de un conjunto de Sidon forma un conjunto de Sidon, por lo tanto el conjunto $A' = (A+1) \setminus \{N\}$ forma un conjunto de Sidon contenido en $[1, N]$ y $|A'| = k-1$, como k es máximal, entonces; $k-1$ es también máximal, en consecuencia $F_2(N) = k-1$.

Reciprocamente; asumamos que $F_2(N) = k-1 \quad y \quad F_2(N+1) = k$, por la parte 1 de este lema se tiene que,

$$G(k-1) \leq N-1 < G(k) \text{ y } G(k) \leq N < G(k+1),$$

por lo tanto de lo anterior se tiene,

$$N \leq G(k) \text{ y } G(k) \leq N,$$

entonces,

$$G(k) = N$$

□

Lema 3. *1.* $F_2(N) > k \Rightarrow G(k) < N-1$

2. $F_2(N) < k \Rightarrow G(k) > N-1$

Prueba.

1. Asumamos que $F_2(N) = k' > k$, como $F_2(N) = k'$ por la parte 1 del lema 2, se tiene que,

$$G(k') \leq N-1 < G(k'+1),$$

puesto que G es una función estrictamente creciente y $k < k'$, entonces, $G(k) < G(k')$, y por lo tanto,

$$G(k) < N-1$$

2. Supongase que $F_2(N) = k' < k$, puesto que $F_2(N) = k'$ por la parte 1 del lema 2, se tiene que,

$$G(k') \leq N - 1 < G(k' + 1),$$

Como G es una función estrictamente creciente y $k' < k' + 1 \leq k$, entonces, $G(k') < G(k' + 1) \leq G(k)$ y se puede entonces concluir que,

$$G(k) > N - 1.$$

□

Haciendo uso del lema 3 podemos demostrar el siguiente teorema que permite a partir de cotas inferiores y superiores de la función $F_2(N)$, obtener cotas inferiores y superiores para la función $G(k)$.

Teorema 15. *Sean $I(x)$ y $S(x)$, funciones inyectivas tales que:*

$$I(N) < F_2(N) < S(N) \quad \textit{para cada} \quad N \in \mathbb{N}$$

Entonces,

$$S^{-1}(k) < G(k) + 1 < I^{-1}(k)$$

Prueba.

Supongamos que $I(x)$ y $S(x)$, son funciones inyectivas tales que,

$$I(N) < F_2(N) < S(N) \quad \text{para cada} \quad N \in \mathbb{N},$$

en primera instancia sabemos que, $F_2(N) < S(N)$ y sea $S(N) = k$, entonces; por la parte 2 del lema 3,

$$G(k) > N - 1,$$

puesto que, $S(X)$ es inyectiva la función inversa $S^{-1}(X)$ existe, por tanto se tiene que,

$$G(k) > S^{-1}(k) - 1, \tag{4.6}$$

de manera analóga se prueba que,

$$G(k) < I^{-1}(k) - 1 \tag{4.7}$$

(4.6) y (4.7), implican que,

$$S^{-1}(k) < G(k) + 1 < I^{-1}(k).$$

□

Lema 4. *1.* $G(k) > N \Rightarrow F_2(N) \leq k$

2. $G(k) < N \Rightarrow F_2(N) \geq k$

Prueba.

La prueba de este resultado es inmediata a partir de la parte 2 del lema 2. □

De la misma manera que el teorema 15, el teorema que sigue permite a partir de cotas inferiores y superiores de la función $G(k)$, encontrar tanto cotas inferiores como cotas superiores para la función $F_2(N)$.

Teorema 16. *Sean* $I(x)$ *y* $S(x)$*, funciones inyectivas tales que:*

$$I(k) < G(k) < S(k) \quad \textit{para cada} \quad k \in \mathbb{N}$$

Entonces,

$$S^{-1}(N) \leq F_2(N) \leq I^{-1}(N)$$

4.4. Comportamiento asintótico de la función $G(k)$

En la sección 2.4, se definió la función $G(k)$ como la mínima longitud de una regla Golomb con k marcas, sin embargo; debido a la propiedad de traslación para reglas Golomb se puede considerar que una regla Golomb A tiene su primera marca en el origen (Mín$(A) = 0$) y por lo tanto se puede escribir a $G\,(k)$, como sigue:

$$G\,(k) = \text{Mín}\,\{\text{MáxA} : A \in GOL_0\,(k)\}$$

En esta sección se estudia el comportamiento asintótico de esta función.

4.4.1. Cotas inferiores para $G(k)$

También en la sección 2.4, se encontró una cota inferior sencilla para $G\,(k)$ mediante el conteo del número total de las diferencias distintas de una regla Golomb, de manera más precisa se probo que,

$$G\,(k) \geq \frac{k\,(k-1)}{2}.$$

Sin embargo, esta cota puede mejorarse a partir de la relación descrita en el teorema 15 y de la cota superior encontrada para $F_2(N)$ en el teorema 13.

Teorema 17. *Para todo $k \in \mathbb{N}$,*

$$G(k) > k^2 - 2k\sqrt{k} + \sqrt{k} - 2$$

Prueba.

Por el teorema 13, se sabe que,

$$F_2(N) \leq N^{\frac{1}{2}} + N^{\frac{1}{4}} + 1,$$

con el fin de aplicar el teorema 15, sea

$$S(x) = x^{\frac{1}{2}} + x^{\frac{1}{4}} + 1,$$

es claro que $S(x)$ es una fución inyectiva y que $F_2(N) \leq S(N)$ para cada $N \in \mathbb{N}$, puesto que $S(x)$ es una función inyectiva $S^{-1}(x)$ existe, veamos quien es $S^{-1}(x)$.
Para esto sea $t = x^{\frac{1}{4}}$, entonces; $x = t^4$, y luego de algunos calculos se encuentra que,

$$t = \sqrt{x - \frac{3}{4}} - \frac{1}{2}$$

y consecuentemente,

$$S^{-1}(x) = \left(\sqrt{x - \frac{3}{4}} - \frac{1}{2}\right)^4$$

$$S^{-1}(x) = x^2 - 2x\sqrt{x - \frac{3}{4}} + \sqrt{x - \frac{3}{4}} - \frac{1}{2}$$

luego,

$$S^{-1}(k) = k^2 - 2k\sqrt{k - \frac{3}{4}} + \sqrt{k - \frac{3}{4}} - \frac{1}{2} \tag{4.8}$$

puesto que,

$$F_2(N) \leq S(N),$$

por el teorema 15 y (4.8), se tiene,

$$G(k) > S^{-1}(k) = k^2 - 2k\sqrt{k - \frac{3}{4}} + \sqrt{k - \frac{3}{4}} - \frac{3}{2} > k^2 - 2k\sqrt{k} + \sqrt{k - \frac{3}{4}} - \frac{3}{2}$$

como,

$$\sqrt{k - \frac{3}{4}} \geq \sqrt{k} - \frac{1}{2}, \quad \text{para todo} \quad k \geq 1,$$

se puede concluir que,

$$G(k) > k^2 - 2k\sqrt{k} + \sqrt{k} - 2.$$

□

NOTA: Como consecuencia del resultado anterior, se puede afirmar que,

$$\liminf_{k\to\infty} \frac{G(k)}{k^2} \geq 1 \tag{4.9}$$

4.4.2. Cotas superiores para $G(k)$

Con base en el estudio de las construcciones conocidas para conjuntos de Sidon y reglas Golomb, los corolarios consecuencia de éstas, han proporcionado las siguientes cotas superiores para la función $G(k)$.

Sean p un número primo, k un entero positivo; para todo primo p y toda potencia prima p^k, se tiene,

a) corolario 1, (Ruzsa) $\Rightarrow G(p-1) \leq p\,(p-1)$

b) Corolario 2, (Bose) $\Rightarrow G(p^k) \leq p^{2k} - 1$

c) Corolario 3, (Singer) $\Rightarrow G(p^k + 1) \leq p^{2k} + p^k + 1$

Sin embargo las cotas superiores proporcionadas por el corolario 1 y el corolario 2, de Ruzsa y Bose, respectivamente, son mejoradas en los corolarios 6 y 7, como consecuencia de la generalización de las construcciones de Ruzsa y Bose, respectivamente, mas especificamente se tiene:
Dados un número primo p, un entero positivo k; para todo primo p y toda potencia prima p^k, las cotas que mejoran las cotas encontradas en los corolarios 1 y 2, respectivamente; son,

a) corolario 6 $\Rightarrow G(p-1) \leq p^2 - 2p$

b) Corolario 7 $\Rightarrow G(p^k) \leq p^{2k} - p^k - 1$

Estos resultados permiten enunciar y probar los siguientes teoremas.

Teorema 18. *Para infinitos valores de k,*

$$G(k) < k^2$$

Prueba.

Por el corolario 2 de Bose se sabe que para toda potencia prima p^t, se da que,

$$G(p^t) \leq p^{2t} - 1 < p^{2t},$$

por lo tanto, se puede tomar $k = p^t$, como el conjunto de los números primos es infinito, entonces el resultado se satisface para infinitos valores de k. □

Teorema 19. *Para todo $k \geq 4$,*

$$\limsup_{k\to\infty} \frac{G(k)}{k^2} \leq 1$$

Prueba.

Sea $k \geq 4$. Existen primos consecutivos p y q tales que,

$$p < \sqrt{k} < q$$

y

$$p^2 < k < q^2,$$

puesto que G es estrictamente creciente se tiene,

$$G(p^2) < G(k) < G(q^2),$$

además el corolario 2 de Bose, implica que para toda potencia prima p^t,

$$G(p^t) < p^{2t},$$

en particular para el primo q,

$$G(k) < G(q^2) < q^4$$

entonces,

$$\frac{G(k)}{k^2} < \frac{G(q^2)}{p^4} < \frac{q^4}{p^4},$$

debido a que,

$$p^4 < k^2 < q^4.$$

Por otra parte se puede usar el siguiente hecho,

$$\text{si} \quad k \to \infty, \quad \text{entonces;} \quad \frac{q^4}{p^4} \to 1,$$

pues el cociente entre primos consecutivos grandes tiende a 1, ver [6], por tanto,

$$\limsup_{k\to\infty} \frac{G(k)}{k^2} \leq 1$$

□

Teorema 20.

$$\lim_{k\to\infty} \frac{G(k)}{k^2} = 1$$

Prueba.

El teorema 19 y (4.9), implican que,

$$1 \leq \liminf_{k\to\infty} \frac{G(k)}{k^2} \leq \lim_{k\to\infty} \frac{G(k)}{k^2} \leq \limsup_{k\to\infty} \frac{G(k)}{k^2} \leq 1,$$

y el resultado se sigue. □

Por lo tanto se ha probado que $G(k)$ se comporta asintóticamente como k^2.

Capítulo 5

APLICACIONES DE C.S. y R.G.

En los capítulos anteriores han sido establecidas las principales características de los conjuntos de Sidon y reglas Golomb, pero no han sido indicados los propósitos por los cuales muchos investigadores hayan trabajado tan arduamente en estos dos campos y la gran mayoría de manera independiente, razón por la cual en este capítulo se da una muestra de algunos de los campos en los cuales las reglas Golomb y los conjuntos de Sidon juegan un papel importante, en las aplicaciones a considerar solo se hara mención de las reglas Golomb.

5.1. Radiocomunicaciones

Radiocomunicación es el método que debe seguirse para el establecimiento de las comunicaciones por medio de la radio telefonía. Así nos podemos comunicar desde una aeronave a la torre o a otra aeronave operando los equipos para ello dispuesto.

5.1.1. Historia

Para establecer el origen de la radiocomunicación se debe distinguir entre la física y la ingeniería, donde la primera precede a la segunda en un siglo. El desarrollo de las comunicaciones ha venido ligado inexorablemente al de la electrónica, de forma que antes de que se explotase el fenómeno electromagnético en las radiotelecomunicaciones haría falta un

avance decisivo en este campo: el **cohesor**. Este dispositivo era un tubo de cristal relleno de partículas metálicas que presenta una resistencia baja en presencia de una descarga electrica cercana, Si ésta es ocasionada por la presencia de una onda electromagnética y el cohesor está convenientemente alimentado y conectado a una lampara o timbre, se puede detectar la precensia o no de una transmisión. Este es uno de los primeros diseños de receptores, propuesto por el francés Edouard Branly en 1891, y que propició en 1894 que Popov y Marconi pasaran de la física a la ingeniería realizando las primeras transmisiones de mensajes, nace la radiocomunicación.

Más adelante entre 1934 y 1940 nace y se inicia la comercialización de la transmisión fm, así con el inicio de la radiodifusión se daría pie al nacimiento de las comunicaciones via satélite. Para el desarrollo de los sistemas de comunicaciones móviles hubo que esperar hasta finales del siglo pasado, pues en 1979 las principales compañias inician el emplazamiento de redes de radio celular, apareciendo las redes públicas de radio móvil terrestre. En la decada de los 90 se avanza hacia una nueva etapa al implantarse las redes celulares digitales y los sistemas de telecomunicación inalámbricos.

5.1.2. Algunos elementos del proceso de radiocomunicación

El proceso de radiocomunicación consta de las siguientes partes,

El canal de comunicación

El cual es el medio por el que se trasmite el mensaje. Éste puede ser una conversación, un medio escrito, electrónico, etc. No todos los canales poseen la misma capacidad para trasmitir información.

Los canales de comunicación pueden ser *formales o informales*. En la vida organizacional, los **canales formales** son aquellos como cartas, correos electrónicos, etc, en donde se transmite información sobre aspectos laborales. Los **canales informales**, por su parte, son las redes de comunicación que se llevan a cabo a través de interacción social, con preguntas, comentarios, etc.

La interferencia

Se produce cuando un mensaje es recibido con cualquier tipo de cosa añadida después de que la fuente lo origina o por cualquier cosa que dificulte la buena recepción del mensaje o señal emitida originalmente. Existen así la interferencia técnica o de ingeniería y la interferencia semántica, distorsión de los significados que influye en la buena recepción del mensaje emitido.

Modular

Es el proceso que consiste en Variar el valor de la amplitud, frecuencia o fase de una onda portadora en función de una señal.

Ancho de banda

Es el rango de frecuencias determinado por una transmisión.

Es importante conocer en buena parte algunas de las razones de porque se módula en el proceso de la radiocomunicación.

¿Por qué se módula?

Existen varias razones para modular, entre ellas:

- Facilita la propagación de la señal de información por cable o por el aire.
- Ordena el radioespectro, distribuyendo canales a cada información distinta.
- Disminuye dimensiones de antenas.
- Optimiza el ancho de banda de cada canal
- Protege a la Información de las degradaciones por ruido.
- Define la calidad de la información trasmitida.

5.1.3. Distorsión de intermodulación

La distorsión de intermodulación es un fenómeno no lineal el cual ocurre cuando N canales de multiples frecuencias pasan através de un dispositivo nolineal, como por jemplo un amplifiacador potencial. La caracteristica nolineal de tal mecanismo genera varios cruces de modulación no deseados en términos de frecuencias, conocidas como producto de intermodulación, entre las cuales cabe destacar,
$2f_i - f_j$, producto de intermodulación de segundo orden,
$f_i + f_j - f_k$, producto de intermodulación de tercer orden,
$f_i + f_j + f_k - f_r - f_s$ producto de intermodulación de quinto orden.

Estos productos de intermodulación pueden caer sobre los canales de frecuencias deseados, deteriorando el conductor de la proporción de ruido (CNR), alterando el rendimiento de enlace de radio en los sistemas de radiocomunicación.

Los productos de intermodulación en sus diferentes ordenes producen interferencias, lo que lleva al surgimiento del problema de asignación de canales buscando eliminar los productos de intermodulación o por lo menos reducirlos sustancialmente, para que las interferancias causadas por estos productos sean también reducidas o eliminadas.

5.1.4. Relación con las reglas Golomb

Una de las primeras referencias acerca de reglas Golomb, aunque bajo un nombre diferente; fue el articulo de 1.953 dado por Babcock [13], quien al observar el tercer y quinto orden de interferencia entre canales consecutivos de comunicación en el proceso de distorción de íntermodulación, propone los siguientes problemas,

1. *Para todo n dado, encontrar un conjunto de enteros* $A = \{0 \leq a_1 < ... < a_n\}$ *tales que ninguna igualdad no trivial* $a_r + a_s - a_t = a_u$ *sea válida,*

2. *Para todo n dado, encontrar un conjunto de enteros* $A = \{0 \leq a_1 < ... < a_n\}$ *tales que ninguna igualdad no trivial* $a_r + a_s + a_t - a_u - a_v = a_w$ *sea válida.*
   En estos problemas los enteros son radiofrecuencias.

El primer problema hace referncia a los productos de intermodulación de segundo orden y es el que mótiva a la definición de las reglas Golomb estudiadas en el capítulo 2, el segundo problema hace referencia a los productos de intermodulación de quinto orden.

Luego de revisar varios métodos algebraicos y de distribución aleatoria de canales, Babcock propone que la ubicación de cada canal de comunicación sea dentro de un espectro de frecuencia en intervalos correspondientes a las marcas de una regla Golomb óptima, con lo cual se consigue que el tercer orden de interferencia entre los canales de comunicación sea eliminado y el quinto orden de interferencia sea sustancialmente reducido.

5.2. Radioastronomía

Radioastronomía, rama de la astronomía que estudia los objetos celestes y los fenómenos astrofísicos midiendo su emisión de radiación electromagnética en la región de radio del espectro.

5.2.1. Historia

A finales del siglo XIX se llevaron a cabo intentos infructuosos para detectar la radioemisión celeste. El ingeniero estadounidense Karl G. Jansky, mientras trabajaba en Bell Laboratories en 1932, fue el primero en detectar ruidos provenientes de la región cercana al centro de nuestra galaxia, la Vía Láctea, durante un experimento para localizar fuentes lejanas de interferencias de radio terrestres. La distribución de esta radioemisión galáctica fue cartografiada por el ingeniero estadounidense Grote Reber, utilizando un paraboloide de $9,5m$ que construyó en su patio de Wheaton, Illinois. En 1943 Reber también descubrió la largamente codiciada radioemisión del Sol. La radioemisión solar había sido detectada pocos años antes, cuando fuertes estallidos solares produjeron interferencias en los sistemas de radar británicos, estadounidenses y alemanes, diseñados para detectar aviones.

Como resultado de los grandes progresos realizados durante la II Guerra Mundial en

antenas de radio y receptores sensibles, la radioastronomía floreció en la década de 1950. Los científicos adaptaron las técnicas de radar de tiempo de guerra para construir diversos radiotelescopios en Australia, Gran Bretaña, Países Bajos, Estados Unidos y la Unión de Repúblicas Socialistas Soviéticas, y muy pronto se despertó el interés de los astrónomos profesionales.

Fuentes de radioemisión discretas fueron catalogadas en número creciente y, desde la década de 1950, fueron identificadas muchas radiofuentes como distantes galaxias visibles. En 1963, la continua investigación de radiofuentes muy pequeñas llevó al descubrimiento de radiofuentes casi estelares llamadas quásares que, debido a que presentaban desplazamientos hacia el rojo de una magnitud sin precedentes, parecían encontrarse a distancias enormes de la Tierra. Poco después, en 1965, los radioastrónomos estadounidenses Arno Penzias y Robert W. Wilson anunciaron el descubrimiento de la radiación de fondo de microondas cósmica de $3K(-270°C)$, que tiene muchas implicaciones para las teorías del origen del Universo y su evolución. En 1968 se descubrió un tipo nuevo de radiofuente, el púlsar, identificado rápidamente como una estrella de neutrones que gira a gran velocidad.

Durante muchos años, los astrónomos se concentraron en el estudio de longitudes de onda relativamente largas, para las que era fácil construir grandes estructuras de antenas y receptores sensibles. Al desarrollarse las técnicas para construir estructuras más grandes y más precisas, y perfeccionarse los equipos de recepción de onda corta, las bandas de longitud de onda de hasta $1mm$ cobraron especial importancia. Al mismo tiempo, el desarrollo de la tecnología espacial permitió realizar observaciones de longitudes de onda muy largas por encima de la ionosfera.

5.2.2. Radiotelescopios

Instrumento que se utiliza en la investigación astronómica para detectar y medir la potencia, en radio frecuencias, proveniente de varias direcciones en el cielo.Consta de tres partes que se complementan: la gran superficie colectora, donde se recoge y enfoca la radiación incidente; el receptor electrónico, con el cual se amplifican y detectan las señales cósmicas de radio, y un dispoditivo para desplegar datos.

El principio fundamental del funcionamiento de un radio telescopio es idéntico al de un telescopio reflector. Las ondas incidentes (de radio u ópticas) se interceptan mediante un espejo preciso y se reflejan a un punto focal común. la forma de la superficie reflectora o plato es muy importante: las radioondas deben llegar en fase al punto focal, despues de reflejarse en el plato, esto es, la longitud de paso a partir del punto de reflexión hasta el foco debe ser la misma para todos los puntos sobre el plato. Esta restricción puede satisfacerse si la forma de la superficie reflectora es parabólica; en consecuenia, los más modernos radiotelescopios tienen esta forma.

Cuando las ondas de radio se colectan y conducen al punto focal del telescopio, las señales son, en general, débiles en extremo. Las señales de radiofrecuencias (rf)incidentes se amplifican por primera vez de 10 a 100 veces en el foco y se convierten a una frecuencia más baja; la frecuencia intermedia (f-i) puede transmitirse con facilidad medianta cables, desde el punto focal hasta el edificio en donde se controla el telescopio. Allí la f-i se amplifiaca aún más y la señal se detecta y se despliega en la forma más adecuada para su análisis por los astrónomos en su investigación particular.

Los tipos de objetos astronómicos que emiten radiofrecuencias y, por lo tanto, que los astrónomos pueden estudiar son de naturaleza tan diversa que se necesita una gran variedad de radiotelescopios y equipo receptor en los modernos radioobservatorios. Dos consideraciones astronómicas generales determinan la clase de instrumentos necesarios: primero, los radio telescopios deberán tener la mayor resolución angular posible, de tal manera que puedan estudiarse los detalles de pequeña escala en las fuentes de radio; segundo, el radio receptor deberá ser en extremo sensible a las señales débiles emitidas por las fuentes cósmicas de radio.

5.2.3. Relación con las reglas Golomb

Uno de los mayores problemas que presentan los radiotelescopios a la hora de realizar las observaciones es su baja resolución angular. Esto les impide poder apreciar detalles pequeños. Para solucionar este problema se utilizan los interferómetros.

La interferometría se basa en el uso de varios radiotelescopios que observan la misma

fuente de manera simultánea. La radiación recibida por los radiotelescopios se hace interferir por parejas. El resultado de la interferencia de dos ondas es una serie de franjas, de mayor o menor brillo. Midiendo el contraste de brillo de estas franjas de interferencia, se puede reconstruir la imagen del objeto observado con una resolución equivalente a la que tendría un telescopio cuyo diámetro fuese igual a la máxima separación entre los radiotelescopios del interferómetro.

En radioastronomía, los astrónomos acostumbran a menudo a usar una serie de telescopios en línea para tomar medidas diferentes de la luz o radiación electromagnética emitida por un objeto celeste lejano. Para realizar estas mediciones en el proceso de interferometría se hace uso grandes radiotelescopios distribuidos por toda la Tierra ubicados en posiciones determinadas por las marcas de una regla Golomb, todos estos radiotelescopios observan simultáneamente el mismo objeto celeste. De este modo los radiotelescopios quedan ubicados a diferentes distancias y sean analizan las diferencias de las medidas tomadas por dos radiotelescopios al mismo tiempo comparando las diferncias mas pequeñas con las más grandes, de esta manera se obtiene información más precisa de la que se pueda obtener al analizar la información proporcionada por un solo radiotelescopio.

Cabe destacar que la ubicación de radiotelescipios en posiciones determinadas por las marcas de una regla Golomb ofrece grandes ventajas entre las cuales se pueden considerar:

- El uso de las reglas Golomb óptimas o casi-óptimas, permite que la ubicación de radiotelescopios no sea realizada de manera arbitraria si no en las posiciones determinadas por esta clase de reglas.
- Disminuye dimensiones de radiotelescopios.
- El ordenar los radiotelescopios en las posiciones determinadas por las marcas de una regla Golomb permite simular un radiotelescopio cuyo diametro sea equivalente al diametro de la Tierra.
- En los nuevos proyectos de radio astronomia se busca simular radiotelescopios cuyo diametro sea mayor que el diametro de la tierra, buscando una extensión de las reglas Golomb para ubicar radio telescopios tanto en la Tierra como en el espacio.

Apéndice

Problemas relacionados

En el presente capítulo se presentan algunos problemas que se relacionan con los conjuntos de Sidon y reglas Golomb, y cuyo estudio se deja propuesto para posteriores trabajos.

Bases aditivas para $\mathbb{Z}_N$

Sea $\mathbb{Z}_N = \{0, 1, ..., N-1\}$ el grupo aditivo de los enteros módulo N y A un subconjunto de $\mathbb{Z}_N$.

De la misma manera que para conjuntos de Sidon denotemos por $A + A$ y por $\sigma_A(x)$, a cada una de las siguientes expresiones,

$$A + A = \{a + a' : a, a' \in A\}$$

$$\sigma_A(x) = |\{(a, a') \in A \times A : a \leq a', x = a + a'\}|$$

Definición 9. *Si $A + A = \mathbb{Z}_N$, decimos que A es una base aditiva para $\mathbb{Z}_N$, o de manera equivalente A es una base aditiva para $\mathbb{Z}_N$ si y sólo si $\sigma_A(x) \geq 1$ para todo $x \in \mathbb{Z}_N$.*

Definición 10. *Se define la función $B(N)$, como sigue;*

$$B(N) \min \{|A| : A \in BAS(N)\},$$

donde, $Bas(N)$ es la clase de todas las bases aditivas para $\mathbb{Z}_N$.

Uno de los problemas fundamentales en el caso de las bases aditivas es determinar el comportamiento asintótico de la función $B(N)$, mas precisamente se debe determinar si el limite,

$$\lim_{N\to\infty} \frac{B(N)}{\sqrt{N}}$$

existe y si este es el caso determinar su valor.

Teorema 21. *La función $B(N)$ satisface la siguiente relación*

$$\sqrt{2} \leq \liminf_{N\to\infty} \frac{B(N)}{\sqrt{N}} \leq \limsup_{N\to\infty} \frac{B(N)}{\sqrt{N}} \leq 2$$

Relación con los C.S & R.G

A partir de las construcciones conocidas para conjuntos de Sidon y reglas Golomb modulares es posible obtener buenas construcciones de bases para $\mathbb{Z}_N$, para valores apropiados de N. El siguiente teorema permite ilustrar una de tales construcciones.

Teorema 22. *Para todo primo p y toda raíz primitiva θ módulo p, el conjunto $A = R(p,\theta,u) \cup M_p \subseteq \mathbb{Z}_{p(p-1)}$ donde*

$R(p,\theta,u) = \{x \equiv (pi - u(p-1)\theta^i)\ mód p(p-1) : i = 1,2,...,p-1\}$ *con $u \neq 0$; es uno de los conjuntos de Sidon obtenidos en la forma general de la construcción de Ruzsa*

$M_p = \{0, p, ..., (p-2)p\}$

es una base aditiva para $\mathbb{Z}_{p(p-1)}$ con $2(p-1)$ elementos y es talque $\sigma_A(x) \leq \frac{p+1}{2}$ para todo $x \in \mathbb{Z}_{p(p-1)}$

Las funciones de Graham y Sloane

Las funciones de Graham y Sloane a considerar en esta sección tienen que ver con problemas de empaquetar.

Se denota por $A\hat{+}A$, al conjunto dado por

$$A\hat{+}A = \{a + a' : a, a' \in A, a \neq a'\}$$

Definición 11. *Definimos $v_\alpha(k)$ como el mínimo número v talque existe un conjunto A de enteros con k elementos*

$$A = \{0 = a_1 < a_2 < \ldots < a_k\}$$

Con la propiedad de que las sumas $a_i + a_j$, con $i < j$; estan en $[0, v]$ y representan cada elemento de $[0, v]$ a lo sumo una vez

Definición 12. *Definimos $v_\beta(k)$ como el mínimo número v talque existe un conjunto A de Sidon con k elementos*

$$A = \{0 = a_1 < a_2 < \ldots < a_k\}$$

Con la propiedad de que las sumas $a_i + a_j$, con $i \leq j$; estan en $[0, v]$, es decir; que las sumasrepresentan cada elemento de $[0, v]$ a lo sumo una vez

Definición 13. *Definimos $v_\gamma(k)$ como el mínimo número v talque existe un conjunto A de enteros con k elementos*

$$A = \{0 = a_1 < a_2 < \ldots < a_k\}$$

Con la propiedad de que las sumas $a_i + a_j$, con $i < j$; estan en $\mathbb{Z}_v$ y representan cada elemento de $\mathbb{Z}_v$ a lo sumo una vez.

Definición 14. *Definimos $v_\delta(k)$ como el mínimo número v talque existe un conjunto A de Sidon con k elementos*

$$A = \{0 = a_1 < a_2 < \ldots < a_k\}$$

Con la propiedad de que las sumas $a_i + a_j$, con $i \leq j$; estan en $\mathbb{Z}_v$ y representan cada elemento de $\mathbb{Z}_v$ a lo sumo una vez.

Un argumento de conteo simple permite establecer que:

$$\left|A\hat{+}A\right| = \binom{k}{2} \leq v$$
$$|A + A| = \binom{k+1}{2} \leq v + 1$$

De lo cual:

$$\frac{k(k-1)}{2} \leq v_\alpha(k)$$
$$\frac{k(k+1)}{2} \leq v_\beta(k)$$

Por tanto:

$$v_\alpha(k) \leq v_\beta(k)$$

De la misma manera se puede probar que,

$$v_\gamma(k) \leq v_\delta(k)$$

El problema central en este campo en los trabajos hasta ahora realizados ha sido determinar las mejores cotas conocidas para cada una de las funciones definidas previamente, determinar su comportamiento asintótico y las relaciones que se puedan encontrar entre éstas. Para un estudio más detallado de las funciones de Graham y Sloane cualquier lector puede consultar [20].

Es claro que los problemas de las bases aditivas para $\mathbb{Z}_N$ y las funciones de Graham y Sloane estan estrechamente relacionados con los conjuntos de Sidon y reglas Golomb, problemas que en este documento no se han estudiado en detalle pues no hacen parte de los objetivos de este trabajo, sin embargo; se dan a conocer pues como se habia mencionado previamente se busca proponerlos para futuros trabajos.

Bibliografía

Bibliografía

[1] DIMITROMANOLAKIS Apostolos. *Analysis of the Golomb ruler and the Sidon set problems, and determination of large, near-optimal Golomb rulers.* Department of electronic and computer engineering, Technical University of Crete, junio de 2002.

[2] CAMPO M. Liliana M; GÓMEZ C. Sandra L; PISO M. Patricia M; MUTIS C. Wilson F. *Conjuntos de Sidon en dimension uno.* Facultad de Ciencias, Naturales, Exactas y de la Educación, Departamento de Matemáticas, Universidad del Cauca, Popayán 23 – 03/2001.

[3] RUZSA Imre. *Solving a linear equation in a set integer I, Acta Arithmetica LXV.*3(1993), 259 – 282.

[4] SARKÖZY A. and SÓS,V.T. *On additive representation functions. En: R.L. Graham, J. Nesetril. Algorithms and combinatorics.* N° 13, New York: Springer-Verlag, 1966. p. 129 – 150.

[5] JIMÉNEZ B. Luis R. GORDILLO A, JOrge E. RUBIANO O, Gustavo N. *Teoría de números para principiantes.* 2ª Edición. Universidad Nacional de Colombia, sede Bogotá. Facultad de Ciencias, 2004. p.172 – 193.

[6] R. K. Guy. *Unsolved Problems in Number Theory.* Springer-Verlag, New York, 1994.

[7] BOSE, R.C. *An affine analogue of singer's theorem,* journal of the Indian Mathematical Society 6 (1942), 1 – 15.

[8] SINGER, J. *A theorem in finite projective geometry and some applications to number theory, Transactions of the American Mathematical Society* 43 (1938), 377 − 385.

[9] CHOWLA, S. *Solution of a problem of Erdös in and Turán in additive number theory, proceedings of the national Academy of de Sciences*, India 14 (1944), 1 − 2.

[10] ERDÖS, P and TURAN, P. *On a problem of Sidon in additive number theory and some related problems, journal*. Of the London Mathematical Society 16 (1941), 212− 215, Addendum (by p. Erdös), (1944).

[11] LINDSTRÖM, Bern.*An inequality for b_2-sequences, Journal of combinatorial Theory* 6 (1969),211 − 212.

[12] KLAZAR, Martin. *Note on the maximum size of a Sidon set*, unpublished.

[13] W.C. BABCOCK.*Intermodulation Interference in Radio Systems*. Bell Systems technical Journal, pages 63 − 73, January 1953

[14] M. D. Atkinson, N. Santoro, and J. Urrutia. *Integer Sets with Distinct Sums and Differences and Carrier Frequency Assignments for Nonlinear Repeaters*. IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. COM−34, No. 6, JUNE 1986, pp. 614 − 617.

[15] MURILLO F, Juan j. *Radiación y radiocomunicación. Ingeniería de telecomunicación*, Escuela técnica superior de ingenieros industriales, Universidad de Sevilla. Enero 13 de 2005

[16] ——.*Proyecto académico con el radio telescopio de Nasa en Robledo, Curso de iniciación a la radioastronomía*

[17] VRIZLYNN L.L. Thing, M.K.Rao,P. Shum. *Fractional optimal Golomb ruler based WDM channel allocation*. Nanyang Technological University, School of Electrical & Electronic Engineering. Vol. 23, Supplement 631, October 2003.

[18] ASTUDILLO, Pilar; BUSTOS, Freddy et all. *Conjuntos de Sidon sobre* $\mathbb{Z}_N$. XI encuentro de la Escuela Regional de Matemáticas, Universidad del valle, Cali Junio 27-Julio 1 de 2005.

[19] ASTUDILLO, Pilar; BUSTOS, Freddy et all. *Bases aditivas para* $\mathbb{Z}_N$. XI encuentro de la Escuela Regional de Matemáticas, Universidad del valle, Cali Junio 27-Julio 1 de 2005.

[20] GUTIERREZ BECERRA, Elida Lucia. *El problema de los recubrimientos modulares, grafos armoniosos etiquetados.* Universidad de Antioquia, Facultad de Ciencias Exactas y Naturales.