CONJUNTOS DE SIDON Y APLICACIONES AL SONAR

RIGO JULIAN OSORIO

CRISTHIAN LEON URBANO

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN

DEPARTAMENTO DE MATEMÁTICAS

POPAYÁN, CAUCA

2013

CONJUNTOS DE SIDON Y APLICACIONES AL SONAR

TRABAJO DE GRADO

En la modalidad de Investigación presentado

como requisito parcial para optar al título de Matemático

RIGO JULIAN OSORIO

CRISTHIAN LEON URBANO

Director:

Mg. DIEGO FERNANDO RUIZ SOLARTE

Codirector:

Dr. CARLOS ALBERTO TRUJILLO SOLARTE

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN

DEPARTAMENTO DE MATEMÁTICAS

POPAYÁN, CAUCA

2013

Nota de aceptación _____

_____

_____

_____

Director:

_____

Mg. Diego Fernando Ruiz Solarte

Codirector:

_____

Dr. Carlos Alberto Trujillo Solarte

Jurados:

_____

Dr. John Hermes Castillo Gómez

_____

Mg. Alfredo Gómez Calvache

Fecha de sustentación: Agosto 23 de 2013

Dedicado a mis padres Gonzalo Alirio Urbano, María Leon y mi hermano Eduar Fabián Urbano.

Dedicado a mi mamá Otilia Angulo, por su infinito apoyo y paciencia.

Agradecimientos

A los profesores Diego Fernando Ruiz y Carlos Alberto Trujillo, por su constante colaboración y apoyo en la realización de este trabajo. Han sido una fuente de gran inspiración, tanto en la parte matemática como en la parte humana al compartir sus conocimientos y experiencias.

A nuestras familias por el apoyo incondicional que siempre nos han brindado durante estos años.

A nuestros amigos, compañeros y a todas aquellas personas que de una u otra forma colaboraron o participaron en nuestra formación y en la realización del presente trabajo.

Resumen

Un conjunto $\mathcal{A}$ es un conjunto de Sidon sobre un grupo G si todo elemento de G, distinto del cero, puede escribirse a lo sumo una vez como diferencia de dos elementos de $\mathcal{A}$. Entre tanto, el sonar, es un sistema que permite detectar y ubicar objetos valiéndose del cambio que presentan las frecuencias de una señal enviada al chocar contra un objeto. Este trabajo se enfoca en presentar fundamentos matemáticos de algunas de las aplicaciones que tiene los conjuntos de Sidon en el área de las telecomunicaciones, más específicamente su aplicación al sonar, junto con los conceptos y principios de la ciencias de la comunicación necesarios para su compresión.

Introducción

Uno de los problemas en teoría aditiva de números que data desde los años 30 y que ha tenido un impacto en el área de las telecomunicaciones es el de los conjuntos de Sidon, los cuales reciben su nombre en honor al analista Simon Sidon quien los introdujo con el objetivo de resolver un problema en análisis armónico [3]. Sidon se preguntaba sobre la existencia de conjuntos de enteros positivos con la propiedad de que todas las sumas entre cualquier par de sus elementos sean distintas. Esta propiedad equivale a encontrar conjuntos de enteros positivos donde todas las diferencias no cero entre cualquier par de elementos del conjunto sean distintas. Los conjuntos que se determinan con ésta última característica tambíen se denominan reglas Golomb y derivan su nombre de Solomon Golomb, quien ha realizado trabajos relevantes en aplicaciones a las comunicaciones y a la teoría de códigos.

En dimensión dos se usan conjuntos de Sidon especiales en aplicaciones a dispositivos como el sonar, denominado así por sus siglas en inglés "Sound Navigation And Ranging" el cual puede usarse como medio de localización acústica, funcionando de forma similar al radar "Radio Detection And Ranging". Estos son sistemas en donde se desea conocer la velocidad de un objeto y la distancia de éste a un observador valiéndose para tal fin del efecto Doppler, el cual es el aparente cambio de frecuencia de una onda producida por el movimiento relativo de la fuente respecto a su observador. Este cambio de frecuencia también puede apreciarse cuando una onda choca contra un objeto y regresa, y es precisamente este fenómeno el que permite a dichos dispositivos realizar cálculos acerca de la distancia de los objetos, su velocidad y su dirección.

Algunos de los conjuntos de Sidon considerados en el sonar, se obtienen a partir de una matriz de permutación y reciben el nombre de arreglos Costas. Dado $N \in \mathbb{Z}^+$, un arreglo Costas es un conjunto de Sidon, que representado gráficamente por una matriz de orden $N \times N$ compuesta de unos y ceros, cumple que en cada fila y cada columna hay exactamente un 1 (es decir, la matriz representa una permutación de los enteros $1, \ldots, N$) [8]. En los dispositivos como el sonar y el

radar, el observador emite una señal a una frecuencia determinada y con base en el tiempo entre su emisión y recepción de vuelta es posible obtener la distancia, mientras que con la diferencia entre la frecuencia emitida y la frecuencia que regresa al observador se obtiene un estimado de la velocidad relativa del objetivo. Esta señal está constituida de varias frecuencias $f_1, \ldots, f_m$ las cuales son transmitidas durante cada uno de los intervalos de tiempo consecutivos $t_1, \ldots, t_n$. Aunque m y n no necesariamente son iguales, en problemas de aplicación se puede considerar la igualdad sin pérdida de generalidad. La representación de la señal se realiza a través de una matriz cuadrada $\mathcal{A} = (a_{ij})$ de orden n, donde las filas representan las n frecuencias y las columnas los n intervalos de tiempo, así, $\mathcal{A}$ es una matriz de ceros y unos, con $a_{ij} = 1$ si la frecuencia f_i es transmitida en el intervalo de tiempo t_j y 0 en caso contrario. Dado que la fuente envía la señal al objetivo y ésta se regresa al primero, a partir del número de coincidencias de 1's entre la matriz enviada y la matriz recibida, es posible determinar la velocidad y la distancia deseada [6, 13].

En la aplicación especifica del sonar, aparece el concepto de "secuencia sonar" el cual es una función $f : \mathcal{C} \subset \mathbb{N} \to \mathbb{N}$ tal que su grafo asociado $G_f := \{(x, f(x)) : x \in \mathcal{C}\} \subseteq \mathcal{C} \times \mathbb{N}$ es un conjunto de Sidon. Para estas secuencias sonar se conocen algunas construcciones como la cuadrática, shift, exponencial y logarítmica de Welch , la construcción exponencial extendida de Welch y la de Golomb [7] además, nuevas construcciones, que si bien no tienen un nombre característico, son propiedad intelectual del profesor Carlos Trujillo y están basadas en las construcciones de conjuntos de Sidon tipo Bose y tipo Ruzsa [11].

A una secuencia sonar se le puede hacer la correspondencia biunívoca con el arreglo $\mathcal{A}$ mencionado anteriormente. Así, el problema fundamental en secuencias sonar consiste en hallar el numero máximo de columnas en el arreglo, dado un número fijo de filas de tal forma que el arreglo represente una secuencia sonar. Para este problema se ha establecido una cota [4], la cual ha sido mejorada en este trabajo mediante el uso de una técnica llamada "Energía Aditiva" [12]. Otras aplicaciones de los conjuntos de Sidon en dimensión dos se encuentran en sistemas de comunicaciones óptimos, en criptografía, en la distribución de claves en redes de celulares, e incluso en el campo militar [13].

Este documento contiene el informe final del trabajo de grado de los estudiantes Cristhian Leonardo Urbano y Rigo Julian Osorio, el cual se encuentra adscrito al proyecto de investigación titulado "Construcción de Conjuntos $B_h[g]$, Propiedad de Midy y Algunas Aplicaciones" con código VRI: 3744 del grupo de investigación ALTENUA y está dividido en tres capítulos y dos

Apéndices como sigue. En el Capítulo I se presenta la aplicación de los conjuntos de Sidon al sonar y conceptos básicos, en el Capítulo II se detallan algunas construcciones conocidas de secuencias sonar y se presentan dos nuevas construcciones, en el Capítulo III se trata el problema fundamental, se hace una revisión de las contribuciones de este trabajo y se da una mirada a trabajos futuros, finalmente en el Apéndice A se hace una comparación de las cotas anteriores con la nueva cota obtenida en este trabajo y en el Apéndice B se muestran los algoritmos implementados en **MuPAD Pro 4.0** usados en este trabajo.

Índice general

Capítulo 1

Aplicación al Sonar y Conceptos Básicos

1.1. Aplicaciones

El sonar es un acrónimo de "Sound Navigation And Ranging" y se refiere al sistema que se utiliza ondas sonoras para detectar la ubicación, velocidad y dirección de diferentes objetos que se encuentran en el océano, esto con el fin de navegar más eficientemente. El sistema sonar requiere para su funcionamiento una serie de elementos como lo son, resonadores, antenas y analizadores de espectro los cuales en conjunto conforman un dispositivo al que también se le denomina sonar [1], este dispositivo es el encargado de enviar, recibir y analizar los datos acústicos especialmente las frecuencias, las cuales tienen como unidad al hercio (Hz) que mide las vibraciones que emite una fuente sonora por unidad de tiempo. El rango en hercios del que se dispone para enviar una señal es conocido como ancho de banda [14] y es el que limita el uso de cualquier frecuencia en el sonar que generalmente varían entre 20 Hz y 20 000 Hz [1].

El sistema sonar utiliza como principio fundamental para su funcionamiento el efecto Doppler, el cual no es mas que el aparente cambio de frecuencia de una onda producida por el movimiento relativo de la fuente respecto a su observador. Este cambio de frecuencia, también puede apreciarse cuando una onda choca contra un objeto y regresa [14].

Para poder aprovechar dichos cambios de frecuencia, el sonar trabaja con una señal de salto de frecuencia de longitud T segundos, la cual es un tren de N impulsos de igual longitud, tales que el k-ésimo pulso se encuentra modulado por una frecuencia f_k con $k \in \{1, 2, 3 \dots N\}$.

Si cada una de estas frecuencias se emite en un tiempo específico secuencialmente, entonces el tren de impulsos está determinado por una sucesión ordenada de enteros $y(k)$, $k \in \{1, 2, 3, ..., N\}$.

Esta sucesión $y(k)$ se denomina operador de ubicación u operador de posición. Dicha señal de salto de frecuencia puede escribirse también como

f_1	f_2	f_3	...	f_{N-1}	f_N

.

Otra representación de uso común para estos impulsos y además muy útil para nuestro trabajo, se hace a través de un arreglo Tiempo-Frecuencia $N \times N$, en donde las N filas corresponden a los N canales de frecuencia y las N columnas a los N intervalos de igual longitud en el orden que es emitido cada pulso, de tal manera que si una marca aparece en la casilla (l, k), es porque la frecuencia f_k ha sido emitida en el intervalo l-ésimo. En la Figura 1.1 se ilustra cómo en unos intervalos de tiempo específicos, denotados del 1 al 5, se ha emitido una frecuencia en particular.

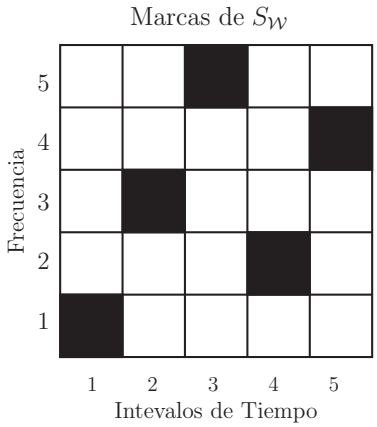

Figura 1.1: Arreglo Tiempo-Frecuencia para una señal particular.

Para una mejor comprensión y análisis de los datos, suele hacerse una correspondencia de este arreglo con una matriz $N \times N$ de $0's$ y $1's$ en donde los unos reemplazan las marcas del arreglo. Así la entrada a_{kl} de la matriz, está dada por:

$$a_{kl} = \begin{cases} 1 & \text{si la frecuencia } f_k \text{ es emitida en el intervalo } l\text{-ésimo,} \\ 0 & \text{en otro caso.} \end{cases}$$

Sin embargo, en este trabajo se considera simplemente el conjunto de las coordenadas (l, k) de las marcas en el arreglo, teniendo en cuenta que la segunda componente corresponde al número de la frecuencia y la primera componente corresponde al número del intervalo de tiempo en el

cual se emite dicha frecuencia. Note que $\mathcal{W} = \{(1,1),(2,3),(3,5),(4,2),(5,4)\}$ es el conjunto de marcas que representa la señal $S_{\mathcal{W}}$ como en la Figura 1.1.

El proceso mediante el cual los dispositivos de detección de objetivos como el sonar realizan su trabajo, es precisamente tomando una señal de salto de frecuencia y enviándola a través de una antena emisora. Si la señal se encuentra con un objeto en su camino, ésta rebotará dirigiéndose nuevamente hacia la antena pero con variaciones en la longitud de onda y en la frecuencia de cada uno de los impulsos. Estas variaciones están perfectamente explicadas por el efecto Doppler [14].

Haciendo una comparación de la señal enviada con la señal retornada, es posible determinar la velocidad y la distancia del objeto

Sabiendo que tanto las frecuencias como los intervalos de tiempo se encuentran modulados por el ancho de banda y el tiempo de duración de la señal respectivamente, entonces el conjunto que representa la señal de retorno será un desplazamiento modulado del conjunto que representa a la señal enviada. Por ejemplo, suponga que dispone de un ancho de banda de longitud 5 y se envía una señal $S_{\mathcal{W}}$ la cual choca contra un objeto y experimenta un desplazamiento de 1 en tiempo y 1 en frecuencia, convirtiéndose en la señal $S_{\mathcal{R}}$ la cual retorna al emisor. Si $\mathcal{W} = \{(1,1),(2,3),(3,5),(4,2),(5,4)\}$ representa a $S_{\mathcal{W}}$, entonces $\mathcal{R} = \{(1,5),(2,2),(3,4),(4,1),(5,3)\}$ representa a $S_{\mathcal{R}}$ y su representaciones en el arreglo Tiempo-Frecuencia son como en la Figura 1.2. Note además que $\mathcal{R} = \mathcal{W} + (1,1)$.

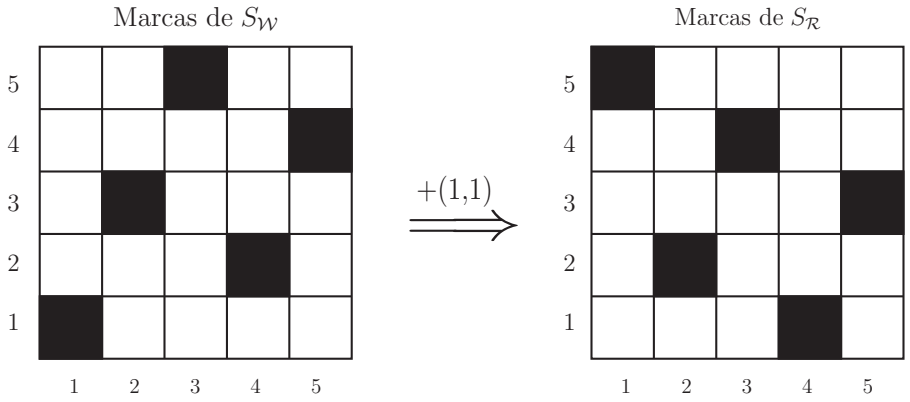

Figura 1.2: Representación de las señales $S_{\mathcal{W}}$ y $S_{\mathcal{R}}$.

Si en el ejemplo anterior, la señal experimenta un cambio de $(1,2)$, es decir una variación de 2 en frecuencia y 1 en tiempo, se obtendrá una representación como en la Figura 1.3. Note ahora

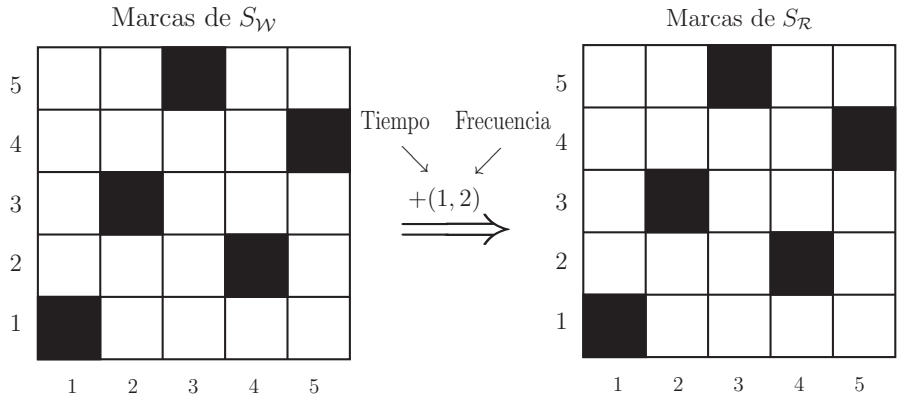

Figura 1.3: Variación $(1, 2)$.

que, tanto $\mathcal{W} = \{(1,1),(2,3),(3,5),(4,2),(5,4)\}$, como $\mathcal{R} = \{(1,1),(2,3),(3,5),(4,2),(5,4)\}$ son iguales. Es claro que si la señal de retorno es idéntica o muy parecida a la señal de salida, no se podrá realizar un buen análisis de las variaciones, ya que la señal aparenta no tenerlas. Así pues se necesitan señales de frecuencia de salto $S_{\mathcal{W}}$ tales que si $\mathcal{W}$ es el conjunto que la representa, entonces $|\mathcal{W} \cap \mathcal{R}|$ sea lo menor posible, para $\mathcal{R}$ cualquier desplazamiento modulado de este, donde $|\mathcal{X}|$ denota el cardinal del conjunto finito $\mathcal{X}$.

1.2. Conceptos Básicos

Sean $(G, +)$ un grupo conmutativo notado aditívamente y $\mathcal{A} \subseteq G$. Se define el conjunto diferencia asociado con $\mathcal{A}$ como

$$\mathcal{A} - \mathcal{A} := \{a - b : \ a, b \in \mathcal{A}\}.$$

Sea $x \in G$. La función representación de x con respecto al conjunto $\mathcal{A} - \mathcal{A}$ se define como

$$R_{\mathcal{A}-\mathcal{A}}(x) := |\{(a,b) \in \mathcal{A} \times \mathcal{A} : \ x = a - b\}| = |\mathcal{A} \cap (\mathcal{A} + x)|\,,$$

donde $\mathcal{A} + x$ es la traslación de $\mathcal{A}$ mediante x, es decir

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

De este modo se dice que $\mathcal{A}$ es un conjunto $B_2^-[g]$ sobre G si $R_{\mathcal{A}-\mathcal{A}}(x) \leq g$ para todo $x \in G \setminus \{0\}$. Si $g = 1$, los conjuntos $B_2^-[1]$ se llaman conjuntos de Sidon sobre G. Los conjuntos $B_2^-[g]$ han sido estudiados en diferentes contextos de la matemática y de las telecomunicaciones, en donde

son relevantes aquellos $\mathcal{A} \in B_2^-[g]$ en donde g es "pequeña", ya que estos son usados para representar frecuencias de diferentes tipos de señales. Dado $n \in \mathbb{N}$, en lo que sigue, mediante $[n]$ se denota al conjunto de enteros $\{0, 1, 2, ..., n\}$ y mediante $[n]^*$ al conjunto $\{1, 2, 3, ..., n\}$. Además $x \pmod m$ denota el único entero a con $0 \leq a \leq m-1$ tal que $x \equiv a \pmod m$.

Definición 1.2.1. *Si $f : \mathcal{A} \subseteq \mathbb{N} \to \mathbb{N}$ es una función, se define su grafo asociado como:*

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

Definición 1.2.2. *Una función $f : [n]^* \to [m]^*$ se denomina una **función Sidon** si para todo entero h, i, j tales que $1 \leq h \leq n-1$, $1 \leq i,\ j \leq n-h$ se tiene que*

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

Note que el grafo asociado a una función Sidon es libre de paralelogramos, esto es; dada cualquier cuádrupla de puntos en G_f, al formar un cuadrilátero con dichos puntos jamas se tendrá un paralelogramo.

Definición 1.2.3. *Considere ahora $[m]^*$, como el conjunto de representantes de los enteros módulo m. Una función $f : [n]^* \to [m]^*$ se denomina una **función Sidon modular** si para todo entero h, i, j tales que $1 \leq h \leq n-1$, $1 \leq i,\ j \leq n-h$ se tiene que*

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

Usando las definiciones anteriores, es posible ahora introducir el concepto de secuencia sonar.

Definición 1.2.4. *Una función $f : [n]^* \to [m]^*$ se denomina una **secuencia sonar** $m \times n$ si es una función Sidon.*

Observación 1.2.1. *Decir que f es una secuencia sonar $m \times n$ es equivalente a decir que f es una secuencia sonar entera con n elementos.*

Definición 1.2.5. *Una función $f : [n]^* \to [m]^*$ se denomina una **secuencia sonar modular** $m \times n$ si es una función Sidon modular.*

Observación 1.2.2. *Decir que f es una secuencia sonar modular $m \times n$ es equivalente a decir que f es una secuencia sonar módulo m con n elementos.*

Con base en lo anterior, si se considera ahora el conjunto de Sidon $\mathcal{B}$ como el conjunto de marcas que representa la señal $S_{\mathcal{B}}$, donde $\mathcal{B} = \{(1,1), (2,3), (3,4), (4,2), (5,5)\}$, entonces $\mathcal{B} + (2,4) = \{(1,3), (3,5), (4,1), (5,2), (6,6)\}$, de donde $|\mathcal{B} \cap (\mathcal{B} + (2,4))| = 0$, y se tiene una representación como se muestra en la Figura 1.4.

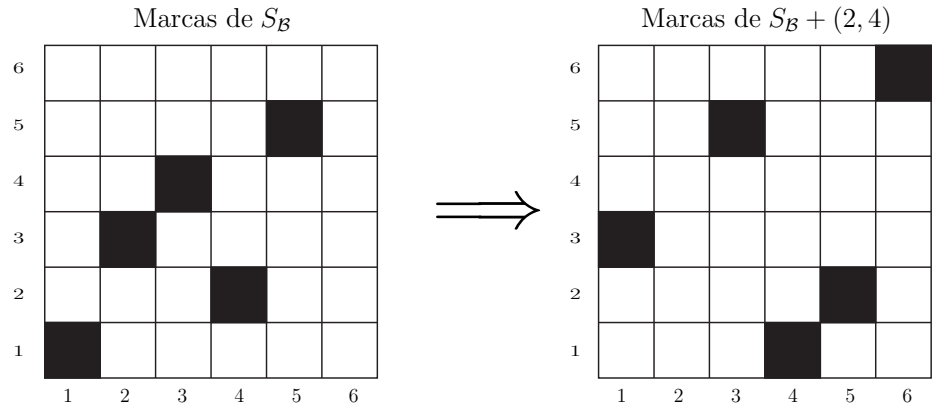

Figura 1.4: Desplazamiento de un conjunto de Sidon.

Así, $R_{\mathcal{B}-\mathcal{B}}((2,4)) = 0$, más aún $R_{\mathcal{B}-\mathcal{B}}((a,b)) \leq 1$ para cualquier $(a,b) \in \mathbb{Z}_6 \times \mathbb{Z}_6$ diferente de $(0,0)$ por ser $\mathcal{B}$ un conjunto de Sidon, con lo que se muestra que la ambigüedad en los datos es mínima y se podrá hacer un buen análisis de las variaciones en tiempo y frecuencia [5].

Capítulo 2

Construcciones de Secuencias Sonar

En este capítulo se exponen construcciones conocidas y construcciones nuevas de secuencias sonar, donde algunas de ellas se basan en la teoría de campos finitos, lo cual quiere decir que se trata de secuencias sonar modulares. Cabe resaltar que hasta el momento no se tiene conocimiento de construcciones de secuencias sonar enteras. Las construcciones que se presentan en las secciones 2.1 a 2.6 se basan en [7].

Nota 2.0.1. *Vale aclarar que las imágenes de las siguientes aplicaciones se deben hacer según el módulo del campo en el que se está trabajando, mientras que el módulo de la respectiva secuencia sonar se debe utilizar una vez se haya construido esta, y se desee comprobar que en efecto lo es.*

2.1. Construcción Cuadrática

Teorema 2.1.1. *Sean p un primo impar y a, b, c enteros constantes con a no congruente con* 0 *módulo p. La función*

$$\begin{aligned} f : [p+1]^* &\longrightarrow [p]^* \\ i &\longmapsto ai^2 + bi + c \pmod{p}, \end{aligned}$$

es una secuencia sonar modular módulo p con $p+1$ elementos.

Demostración. Considere h, i, j enteros tales que $1 \leq h \leq p$ y $1 \leq j \leq i \leq p+1-h$. Se desea comprobar la Definición 1.2.3. Suponga que $f(i+h) - f(i) \equiv f(j+h) - f(j) \pmod{p}$, es decir

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

de donde $2aih \equiv 2ajh \pmod{p}$, esto es, $2ah(i-j) \equiv 0 \pmod{p}$. Como p es impar y a no es congruente con 0 módulo p entonces $2a$ es invertible y por lo tanto se tiene que $h(i-j) \equiv 0 \pmod{p}$. Considere los siguientes casos:

I. Si $h = p$ entonces $i = j = 1$, con lo que se probaría lo deseado.

II. Si $h \neq p$ entonces $(i-j) \equiv 0 \pmod{p}$. Debido a las condiciones de i, j es fácil ver que $i - j \leq p - 1$ luego $i = j$.

Por lo tanto f define una secuencia sonar módulo p con $p+1$ elementos. ■

Ejemplo 2.1.1. *Considere $p = 7$, $a = 2$, $b = 3$, $c = 4$. Así, a través de la función $f : [8]^* \longrightarrow [7]^*$ dada por $f(i) = 2i^2 + 3i + 4 \pmod{7}$ se construye el conjunto*

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

el cual es una secuencia sonar módulo 7 con 8 elementos. En la Figura 2.1 se observa la aplicación de la función f junto con su arreglo rectangular asociado.

i	$f(i) \pmod 7$
1	$2+3+4=2$
2	$2*4+3*2+4=4$
3	$2*9+3*3+4=3$
4	$2*16+3*4+4=6$
5	$2*25+3*5+4=6$
6	$2*36+3*6+4=3$
7	$2*49+3*7+4=4$
8	$2*64+3*8+4=2$

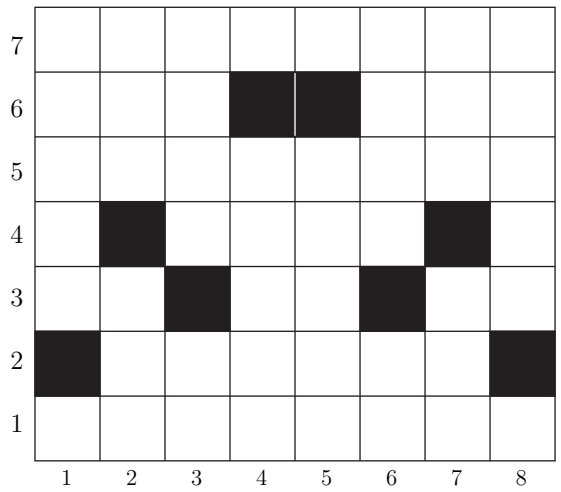

Figura 2.1: Construcción asociada al Teorema 2.1.1 y su respectivo arreglo rectangular.

2.2. Construcción Shift

Teorema 2.2.1. *Sean p un primo, α un elemento primitivo de $\mathbb{F}_{p^{2r}}^*$ y β un elemento primitivo de $\mathbb{F}_{p^r}^*$. La función*

$$\begin{aligned} f : \mathcal{A} &\longrightarrow [p^r - 1]^* \\ i &\longmapsto \log_\beta \left((\alpha^i)^{p^r} + \alpha^i \right) \end{aligned}$$

donde $\mathcal{A} = [p^r]^*$ si $p = 2$, y $\mathcal{A} = \{i : -(p^r - 1)/2 \leq i \leq (p^r - 1)/2\}$ si p es impar, define una secuencia sonar módulo $p^r - 1$ con p^r elementos.

Demostración. Sean $\langle \alpha \rangle = \mathbb{F}_{p^{2r}}^*$ y $\langle \beta \rangle = \mathbb{F}_{p^r}^*$. Note que $T(i) := \left(\alpha^i\right)^{p^r} + \alpha^i$ corresponde a la traza[1] de α^i sobre el subcampo $\mathbb{F}_{p^r}$ de $\mathbb{F}_{p^{2r}}$, por lo tanto $T(i) \in \mathbb{F}_{p^r}$. Se debe ver que $T(i) \neq 0$, y con ello se concluye que f está bien definida. Suponga que $T(i) = 0$. Considere los siguientes casos:

- Si p es impar, entonces

$$\begin{aligned} \left(\alpha^i\right)^{p^r} + \alpha^i = 0 &\iff \left(\alpha^i\right)^{p^r} = -\alpha^i \\ &\iff \left(\alpha^i\right)^{p^r - 1} = -1 \\ &\iff \left(\alpha^i\right)^{p^r - 1} = \alpha^{\frac{p^{2r}-1}{2}} \\ &\iff (p^r - 1)i \equiv \frac{(p^r - 1)(p^r + 1)}{2} \pmod{p^{2r} - 1} \end{aligned}$$

  de donde $i = (p^r + 1)/2$ o $-(p^r + 1)/2$. Así, $-(p^r - 1)/2 \leq i \leq (p^r - 1)/2$ para que $T(i) \neq 0$

- Si p es par, entonces

$$\begin{aligned} \left(\alpha^i\right)^{p^r} + \alpha^i = 0 &\iff \left(\alpha^i\right)^{p^r} = -\alpha^i \\ &\iff \left(\alpha^i\right)^{p^r} = \alpha^i \\ &\iff p^r i \equiv i \pmod{p^{2r} - 1} \\ &\iff (p^r - 1)i \equiv 0 \pmod{p^{2r} - 1} \end{aligned}$$

  con lo que $i = p^r + 1$. Así, $1 \leq i \leq p^r$ para que $T(i) \neq 0$.

[1] Para $\alpha \in F = \mathbb{F}_{q^m}$ y $K = \mathbb{F}_q$, la traza $Tr_{F/K}(\alpha)$ de α sobre K se define mediante $Tr_{F/K}(\alpha) = \sum_{i=0}^{m-1} \alpha^{q^i}$.

Ahora considere h, i, j enteros tales que $1 \leq h \leq p^r - 1$ y $-(p^r-1)/2 \leq i \leq j \leq (p^r-1)/2 - h$. Se desea comprobar la Definición 1.2.3. Suponga que $f(i+h) - f(i) \equiv f(j+h) - f(j) \pmod{p^r - 1}$, esto es

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

lo que implica

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

Ya que $h \leq p^r - 1$, se tiene que $(\alpha^h)^{p^r-1} \neq 1$ y por lo tanto $(\alpha^{j-i})^{p^r-1} = 1$, y dado que $j - i \leq p^r - 1$ entonces $j - i = 0$, así $i = j$. Para p par la prueba es similar.

Por lo tanto f define una secuencia sonar módulo $p^r - 1$ con p^r elementos. ■

Ejemplo 2.2.1. *Considere* $p = 5$, $r = 1$, $\langle 3\theta + 2\rangle = \mathbb{F}_{5^2}^*$ *y* $\langle 2\rangle = \mathbb{F}_5^*$. *En este caso* $f : \{-2, -1, 0, 1, 2\} \longrightarrow \{1, 2, 3, 4\}$ *está definida por* $f(i) = \log_2\left((3\theta + 2)^{5i} + (3\theta + 2)^i\right)$. *Así, se construye el conjunto* $\{(-2, 3), (-1, 1), (0, 1), (1, 2), (2, 1)\}$, *al cual se le aplica la traslación* $(3, 0)$ *para así obtener el conjunto*

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

que es una secuencia sonar módulo 4 *con* 5 *elementos. En la Figura 2.2, se observa la aplicación de la función* f *junto con su arreglo rectangular asociado.*

i	$f(i)$
-2	$\log_2\left((3\theta+2)^{-10}+(3\theta+2)^{-2}\right)=3$
-1	$\log_2\left((3\theta+2)^{-5}+(3\theta+2)^{-1}\right)=1$
0	$\log_2\left((3\theta+2)^{0}+(3\theta+2)^{0}\right)=1$
1	$\log_2\left((3\theta+2)^{5}+(3\theta+2)^{1}\right)=2$
2	$\log_2\left((3\theta+2)^{10}+(3\theta+2)^{2}\right)=1$

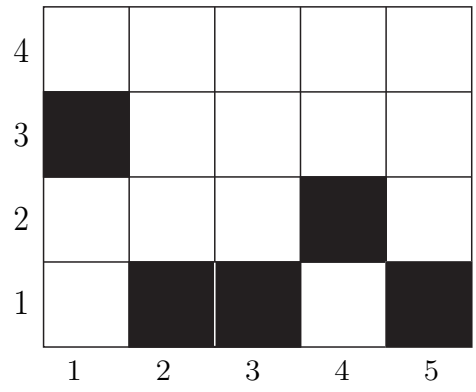

Figura 2.2: Construcción asociada al Teorema 2.2.1 y su respectivo arreglo rectangular.

Ejemplo 2.2.2. *Considere* $p=2$, $r=3$, $\left\langle \theta^4+\theta^3\right\rangle = \mathbb{F}_{2^6}^*$ *y* $\left\langle \theta^4+\theta+1\right\rangle = \mathbb{F}_{2^2}^*$. *En este caso* $f:[8]^* \longrightarrow [7]^*$ *está definida por* $f(i)=\log_{\theta^4+\theta+1}\left((\theta^4+\theta^3)^{8i}+(\theta^4+\theta^3)^{i}\right)$. *Así, se construye el conjunto*

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

el cual es una secuencia sonar módulo 7 *con* 8 *elementos. En la Figura 2.3, se observa la aplicación de la función* f *junto con su arreglo rectangular asociado.*

i	$f(i)$
1	$\log_{\theta^4+\theta+1}\left((\theta^4+\theta^3)^{8}+(\theta^4+\theta^3)\right)=2$
2	$\log_{\theta^4+\theta+1}\left((\theta^4+\theta^3)^{16}+(\theta^4+\theta^3)^{2}\right)=4$
3	$\log_{\theta^4+\theta+1}\left((\theta^4+\theta^3)^{24}+(\theta^4+\theta^3)^{3}\right)=5$
4	$\log_{\theta^4+\theta+1}\left((\theta^4+\theta^3)^{32}+(\theta^4+\theta^3)^{4}\right)=1$
5	$\log_{\theta^4+\theta+1}\left((\theta^4+\theta^3)^{40}+(\theta^4+\theta^3)^{5}\right)=5$
6	$\log_{\theta^4+\theta+1}\left((\theta^4+\theta^3)^{48}+(\theta^4+\theta^3)^{6}\right)=3$
7	$\log_{\theta^4+\theta+1}\left((\theta^4+\theta^3)^{56}+(\theta^4+\theta^3)^{7}\right)=3$
8	$\log_{\theta^4+\theta+1}\left((\theta^4+\theta^3)^{64}+(\theta^4+\theta^3)^{8}\right)=2$

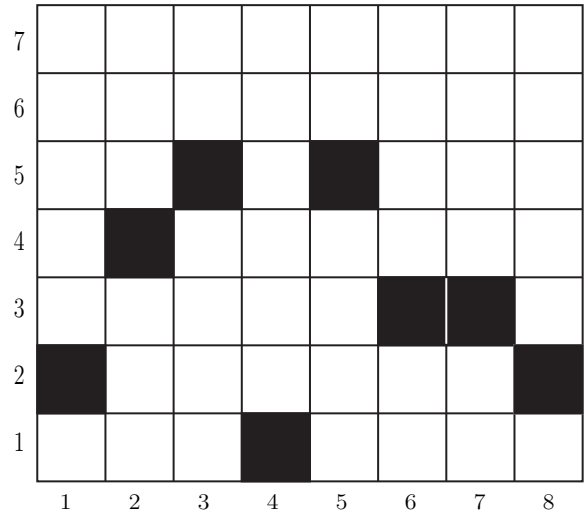

Figura 2.3: Construcción asociada al Teorema 2.2.1 y su respectivo arreglo rectangular.

Las construcciones que se presentan en las secciones 2.3, 2.4 y 2.5 se obtienen a partir de las construcciones de arreglos Costas tipo Welch y tipo Golomb.

2.3. Construcción Exponencial de Welch

Teorema 2.3.1. *Sea α una raíz primitiva de $\mathbb{Z}_p^*$. La función*

$$\begin{aligned} f : [p-1]^* &\longrightarrow [p]^* \\ i &\longmapsto \alpha^i, \end{aligned}$$

es una secuencia sonar módulo p con $p-1$ elementos.

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

$$f(i+h) - f(i) \equiv f(j+h) - f(j) \pmod{p}$$

Aplicando la definición de f se tiene que

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

Como $1 \leq h \leq p-2$ entonces $\alpha^h \not\equiv 1 \pmod{p}$ y así $\alpha^i \equiv \alpha^j \pmod{p}$, es decir $\alpha^{i-j} \equiv 1 \pmod{p}$ y dado que $h \geq 1$ entonces $i - j \leq p-2$. Así $i = j$.

Por lo tanto f define una secuencia sonar módulo p con $p-1$ elementos. ■

Ejemplo 2.3.1. *Considere $p = 7$ y $\langle 3 \rangle = \mathbb{Z}_7^*$. La función $f : [6]^* \longrightarrow [7]^*$ definida por $f(i) = 3^i$ permite construir el conjunto*

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

el cual es una secuencia sonar módulo 7 con 6 elementos. En la Figura 2.4 se observa la aplicación de la función f junto con su arreglo rectangular asociado.

i	$f(i)$ (mód 7)
1	$3^1 = 3$
2	$3^2 = 2$
3	$3^3 = 6$
4	$3^4 = 4$
5	$3^5 = 5$
6	$3^6 = 1$

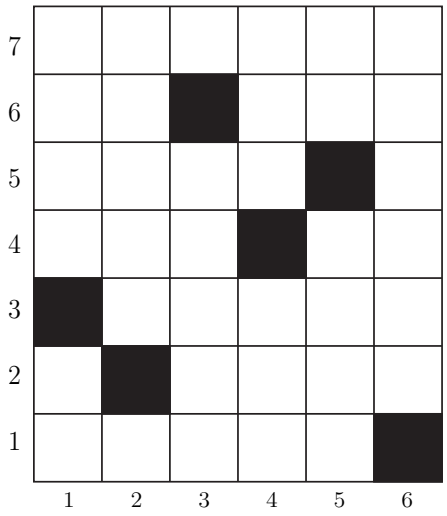

Figura 2.4: Construcción asociada al Teorema 2.3.1 y su respectivo arreglo rectangular.

2.4. Construcción Logarítmica de Welch

Teorema 2.4.1. *Sea α una raíz primitiva en $\mathbb{Z}_p^*$. La función*

$$\begin{aligned} f : [p-1]^* &\longrightarrow [p-1]^* \\ i &\longmapsto \log_\alpha i, \end{aligned}$$

es una secuencia sonar módulo $p-1$ con $p-1$ elementos.

Demostración. Sea p un primo y $\langle \alpha \rangle = \mathbb{Z}_p^*$. Considere h, i, j enteros con $1 \leq h \leq p-2$ y $1 \leq j \leq i \leq p-1-h$ tales que $f(i+h) - f(i) \equiv f(j+h) - f(j) \pmod{p}$, es decir,

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

Dado que $1 \leq h \leq p-2$ entonces $i = j$. Por lo tanto f define una secuencia sonar módulo $p-1$ con $p-1$ elementos. ■

Ejemplo 2.4.1. *Considere* $p = 7$ *y* $\langle 3\rangle = \mathbb{Z}_7^*$. *La función* $f : [6]^* \longrightarrow [6]^*$ *definida por* $f(i) = \log_3 i$, *permite construir el conjunto*

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

el cual es una secuencia sonar módulo 6 *con* 6 *elementos. En la Figura 2.5 se observa la aplicación de la función* f *junto con su arreglo rectangular asociado.*

i	$f(i)$ (mód 7)
1	$\log_3 1 = 0$
2	$\log_3 2 = 2$
3	$\log_3 3 = 1$
4	$\log_3 4 = 4$
5	$\log_3 5 = 5$
6	$\log_3 6 = 3$

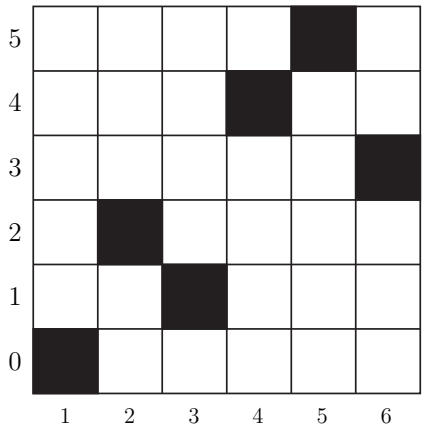

Figura 2.5: Construcción asociada al Teorema 2.4.1 y su respectivo arreglo rectangular.

2.5. Construcción de Golomb

Teorema 2.5.1. *Sean* $q = p^r > 2$ *una potencia prima con* $r \geq 1$ *y* α , β *elementos primitivos de* $\mathbb{F}_q^*$. *La función* $f : [q-2]^* \longrightarrow [q-1]^*$, *definida por* $f(i) = j$ *si y sólo si* $\alpha^i + \beta^j = 1$, *es una secuencia sonar módulo* $q-1$ *con* $q-2$ *elementos.*

Demostración. Sean $q = p^r$, potencia de un primo impar con $r \geq 1$ y $\langle\alpha\rangle = \langle\beta\rangle = \mathbb{F}_q^*$. Note que f así definida es equivalente a decir que $f(i) = \log_\beta\left(1-\alpha^i\right)$. Además se tiene que $1-\alpha^i \neq 0$ ya que $1 \leq i \leq q-2$. Ahora, sean h, j, i enteros tales que $1 \leq h \leq q-3$ y $1 \leq j \leq i \leq q-2-h$. Suponga que

$$f(i+h) - f(i) \equiv f(j+h) - f(j) \pmod{q}$$

es decir,

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

de donde

$$\log_\beta\Big((1-\alpha^{i+h})(1-\alpha^{j})\Big) \equiv \log_\beta\Big((1-\alpha^{j+h})(1-\alpha^{i})\Big) \quad (\text{mód } q),$$
$$(1-\alpha^{i+h})(1-\alpha^{j}) = (1-\alpha^{j+h})(1-\alpha^{i}),$$
$$1-\alpha^{i+h}-\alpha^{j}+\alpha^{i+j+h} = 1-\alpha^{j+h}-\alpha^{i}+\alpha^{i+j+h},$$
$$\alpha^{i}-\alpha^{i+h} = \alpha^{j}-\alpha^{j+h},$$
$$\alpha^{i}(1-\alpha^{h}) = \alpha^{j}(1-\alpha^{h}).$$

Dado que $1 \leq h \leq q-3$ se tiene que $\alpha^h \neq 1$ y por lo tanto $\alpha^i = \alpha^j$, es decir $\alpha^{i-j} = 1$. Como $h \geq 1$ entonces $i-j \leq q-3$, luego debe ser que $i-j=0$, y así $i=j$. Por lo tanto f define una secuencia sonar módulo $q-1$ con $q-2$ elementos. ■

Ejemplo 2.5.1. *Considere $p=11$ y $\langle 2\rangle = \langle 8\rangle = \mathbb{F}_{11}^*$. La función $f:[9]^* \longrightarrow [10]^*$ definida por $f(i)=\log_8(1-2^i)$ permite construir el conjunto*

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

el cual es una secuencia sonar módulo 10 con 9 elementos. En la Figura 2.6 se observa la aplicación de la función f junto con su arreglo rectangular asociado.

i	$f(i)$ (mód 11)
1	$\log_8(1-2) = \log_8 10 = 5$
2	$\log_8(1-4) = \log_8 8 = 1$
3	$\log_8(1-8) = \log_8 4 = 4$
4	$\log_8(1-16) = \log_8 7 = 9$
5	$\log_8(1-32) = \log_8 2 = 7$
6	$\log_8(1-64) = \log_8 3 = 6$
7	$\log_8(1-128) = \log_8 5 = 8$
8	$\log_8(1-256) = \log_8 9 = 2$
9	$\log_8(1-512) = \log_8 6 = 3$

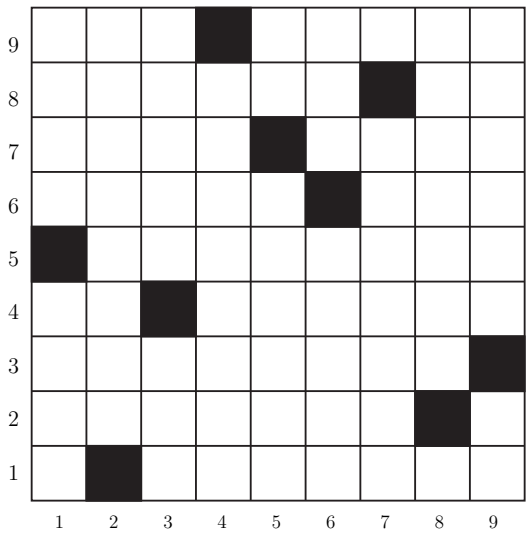

Figura 2.6: Construcción asociada al Teorema 2.5.1 y su respectivo arreglo rectangular.

Observación 2.5.1. *En el Teorema anterior, cuando $\alpha = \beta$, la construcción se debe a Lempel [6, 3].*

2.6. Construcción Exponencial Extendida de Welch

Teorema 2.6.1. *Sea α una raíz primitiva en $\mathbb{Z}_p^*$ y $s \in \mathbb{Z}$. La función*

$$\begin{aligned} f : [p-1] &\longrightarrow [p]^* \\ i &\longmapsto \alpha^{i+s} \end{aligned}$$

es una secuencia sonar módulo p con p elementos.

Demostración. Sean p un primo, s un entero y $\langle\alpha\rangle = \mathbb{Z}_p^*$. Considere h, i, j enteros tales que $1 \leq h \leq p-2$ y $1 \leq j \leq i \leq p-1-h$. Suponga que

$$f(i+h) - f(i) \equiv f(j+h) - f(j) \pmod{p}$$

A partir de la definición de f se sigue que

$$\begin{aligned} \alpha^{i+h+s} - \alpha^{i+s} &\equiv \alpha^{j+h+s} - \alpha^{j+s} \pmod{p} \\ \alpha^i \left(\alpha^{h+s} - \alpha^s\right) &\equiv \alpha^j \left(\alpha^{h+s} - \alpha^s\right) \pmod{p} \end{aligned}$$

Dado que $1 \leq h \leq p-2$ entonces $\alpha^{h+s} \not\equiv \alpha^s \pmod{p}$ y así $\alpha^i \equiv \alpha^j \pmod{p}$, esto es $\alpha^{i-j} \equiv 1 \pmod{p}$. De otro lado, $i - j \leq p-2$, y por tanto $i = j$. ■

Ejemplo 2.6.1. *Considere $p = 7$, $s = 1$ y $\langle 3\rangle = \mathbb{Z}_7^*$. La función $f : [6] \longrightarrow [7]^*$ definida por $f(i) = 3^{i+1}$ permite construir el conjunto*

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

el cual es una secuencia sonar módulo 7 con 7 elementos. En la Figura 2.7 se observa la aplicación de la función f junto con su arreglo rectangular asociado.

i	$f(i)$ (mód 7)
0	$3^1 = 3$
1	$3^2 = 2$
2	$3^3 = 6$
3	$3^4 = 4$
4	$3^5 = 5$
5	$3^6 = 1$
6	$3^7 = 3$

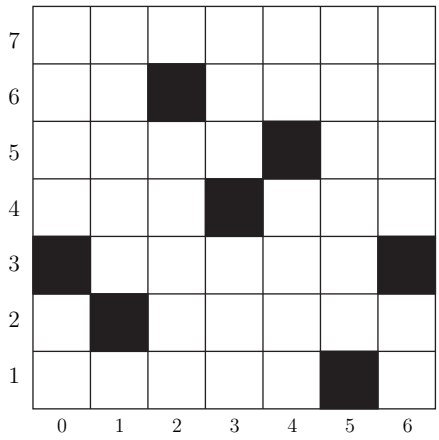

Figura 2.7: Construcción asociada al Teorema 2.6.1 y su respectivo arreglo rectangular.

2.7. Nuevas Construcciones

En esta sección se darán a conocer dos nuevas construcciones de secuencias sonar modulares, las cuales se basan esencialmente en las construcciones de conjuntos de Sidon tipo Bose y tipo Ruzsa. Estas dos nuevas construcciones son producto del proyecto de investigación titulado "Construcción de Conjuntos $B_h[g]$, Propiedad de Midy y Algunas Aplicaciones" con código VRI: 3744 al cual se encuentra adjunto este trabajo y además son producción intelectual del profesor Carlos Trujillo.

A continuación se presentan las construcciones de conjunto de Sidon tipo Bose y tipo Ruzsa junto con ciertas características relevantes que serán de gran ayuda para la construcción de las dos nuevas secuencias sonar. Un estudio más amplio y detallado de las construcciones tipo Bose y tipo Ruzsa se realiza en [9].

Teorema 2.7.1 (**Construcción Tipo Bose**). *Sea q una potencia prima, θ un elemento primitivo en $\mathbb{F}_{q^2}^*$ y $u \in \mathbb{F}_q \setminus \{0\}$. Entonces, el conjunto*

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

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

Observación 2.7.1. *El conjunto B satisface las siguientes propiedades.*

B1) Dados $b_i, b_j \in B$, se tiene que $b_i - b_j \not\equiv 0 \pmod{q+1}$ si $i \neq j$.

B2) $b \not\equiv 0 \pmod{q+1}$, para todo $b \in B$.

De estas dos propiedades se puede concluir que $B \pmod{q+1} = [q]^*$. Es decir, para cada $i \in [q]^*$ existe un único $b_i \in B$ tal que $b_i \equiv i \pmod{q+1}$, con lo que es posible escribir b_i como $b_i = \lfloor b_i/(q+1) \rfloor (q+1) + i$ para todo $i = 1, 2, \ldots, q$, donde $\lfloor x \rfloor$ denota la parte entera del número real x.

Considere la construcción del Teorema 2.3.1. Sea p un primo y α una raíz primitiva en $\mathbb{Z}_p$, mediante la pareja (i, α^i), con $i = 1, 2, \ldots, p-1$ se plantea el siguiente sistema de congruencias

$$x \equiv i \pmod{p-1}$$
$$x \equiv \alpha^i \pmod{p}$$

el cual tiene solución única módulo $p(p-1)$ mediante el Teorema Chino de los Restos. El conjunto de puntos que solucionan dicho sistema forman un conjunto de Sidon en $\mathbb{Z}_{p(p-1)}$. Formalmente este resultado se presenta en el siguiente teorema.

Teorema 2.7.2 (Construcción Tipo Ruzsa). *El conjunto*

$$R := R(p, \alpha) = \{x \in \mathbb{Z}_{p(p-1)} \,:\, x \equiv i \pmod{p-1} \;\; y \;\; x \equiv \alpha^i \pmod{p}; i = 1, 2, \ldots, p-1\},$$

es un conjunto de Sidon con $p-1$ elementos, sobre el grupo $\mathbb{Z}_{p(p-1)}$.

Observación 2.7.2. *El conjunto R satisface satisface las siguientes propiedades*

R1) $r \not\equiv 0 \pmod{p}$ para todo $r \in R$.

R2) Dados $r_i, r_j \in R$ se tiene que $r_i \not\equiv r_j \pmod{p}$ si $i \neq j$.

R3) Dados $r_i, r_j \in R$ se tiene que $r_i \not\equiv r_j \pmod{p-1}$ si $i \neq j$.

De las Propiedades $R1$) y $R2$) se puede concluir que $R \pmod{p} = [p-1]^*$. Es decir, para cada $i \in [p-1]^*$ existe un único $r_i \in R$ tal que $r_i \equiv i \pmod{p}$. Luego r_i se puede escribir como $r_i = \lfloor r_i/p \rfloor p + i$, para todo $i = 1, 2, \ldots, p-1$.

Además de $R3$) se tiene que $R \pmod{p-1} = [p-1]^*$. Es decir, para cada $j \in [p-1]^*$ existe un único $r_j \in R$ tal que $r_j \equiv j \pmod{p-1}$. Así r_j se puede escribir como $r_j = \lfloor r_j/(p-1) \rfloor (p-1)+j$, para todo $j = 1, 2, \ldots, p-1$.

Las anteriores propiedades son mostradas con mayor detalle en [11].

2.7.1. Primera Construcción

En adelante, para $m \in \mathbb{Z}$ se concidera $[m] = \{0, 1, 2, \ldots, m\}$. Haciendo uso de el Teorema 2.7.1 y de la Observación 2.7.1 se obtiene el siguiente resultado.

Teorema 2.7.3. *La función*

$$\begin{aligned} f : [q]^* &\longrightarrow [q-2] \\ i &\longmapsto \lfloor b_i/(q+1) \rfloor , \end{aligned}$$

define una secuencia sonar módulo $q-1$ con q elementos.

Demostración. Sean h, i, j enteros tales que $1 \leq h \leq q-1$ y $1 \leq i, j \leq q-h$. Suponga que $f(i+h) - f(i) \equiv f(j+h) - f(j) \pmod{q-1}$, es decir

$$\left\lfloor \frac{b_{i+h}}{q+1} \right\rfloor - \left\lfloor \frac{b_i}{q+1} \right\rfloor \equiv \left\lfloor \frac{b_{j+h}}{q+1} \right\rfloor - \left\lfloor \frac{b_j}{q+1} \right\rfloor \pmod{q-1}.$$

Luego existe $t \in \mathbb{Z}$ tal que

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

Así,

$$\left\lfloor \frac{b_{i+h}}{q+1} \right\rfloor (q+1) - \left\lfloor \frac{b_i}{q+1} \right\rfloor (q+1) = \left\lfloor \frac{b_{j+h}}{q+1} \right\rfloor (q+1) - \left\lfloor \frac{b_j}{q+1} \right\rfloor (q+1) + t(q^2-1)$$

Sumando $h = (h+i) - i = (h+j) - j$ a ambos lados de la ecuación se tiene

$$\begin{aligned} \left(\left\lfloor \frac{b_{i+h}}{q+1} \right\rfloor (q+1) + (h+i) \right) - \left(\left\lfloor \frac{b_i}{q+1} \right\rfloor (q+1) + i \right) &= \left(\left\lfloor \frac{b_{j+h}}{q+1} \right\rfloor (q+1) + (h+j) \right) \\ &\quad - \left(\left\lfloor \frac{b_j}{q+1} \right\rfloor (q+1) + j \right) + t(q^2-1) \end{aligned}$$

Con lo que $b_{i+h} - b_i \equiv b_{j+h} - b_j \pmod{q^2-1}$. Ya que B es un conjunto de Sidon módulo q^2-1 entonces $i = j$. Por lo tanto f define una secuencia sonar módulo $q-1$ con q elementos. ■

Ejemplo 2.7.1. *Considere* $q = 7$, $q^2 - 1 = 48 = 6 * 8$ *y* $\langle 2\theta + 6 \rangle = \mathbb{F}_{7^2}$. *Se obtiene el conjunto de Sidon tipo Bose,* $B(7, 2\theta + 6, 1) = \{1, 5, 11, 12, 14, 26, 31\}$. *Mediante la función* $f : [7]^* \longrightarrow [5]$ *definida por* $f(i) = \lfloor b_i/8 \rfloor$ *donde* $b_i \in B(7, 2\theta + 6, 1)$, *se construye el conjunto*

$$\{(1,0), (2,3), (3,1), (4,1), (5,0), (6,1), (7,3)\},$$

el cual es una secuencia sonar módulo 6 con 7 elementos. En la Figura 2.8 se observa la aplicación de la función f junto con su arreglo rectangular asociado.

$$\begin{array}{rcrcrl} 1 & \equiv & 1 \text{ (mód 8)} & \rightarrow & \lfloor 1/8 \rfloor & = 0 \\ 26 & \equiv & 2 \text{ (mód 8)} & \rightarrow & \lfloor 26/8 \rfloor & = 3 \\ 11 & \equiv & 3 \text{ (mód 8)} & \rightarrow & \lfloor 11/8 \rfloor & = 1 \\ 12 & \equiv & 4 \text{ (mód 8)} & \rightarrow & \lfloor 12/8 \rfloor & = 1 \\ 5 & \equiv & 5 \text{ (mód 8)} & \rightarrow & \lfloor 5/8 \rfloor & = 0 \\ 14 & \equiv & 6 \text{ (mód 8)} & \rightarrow & \lfloor 14/8 \rfloor & = 1 \\ 31 & \equiv & 7 \text{ (mód 8)} & \rightarrow & \lfloor 31/8 \rfloor & = 3 \end{array}$$

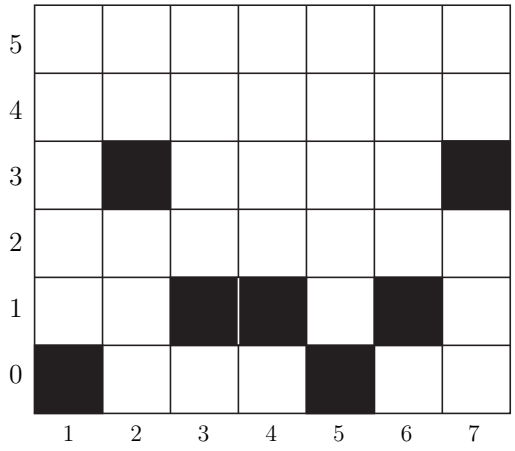

Figura 2.8: Construcción asociada al Teorema 2.7.3 y su respectivo arreglo rectangular.

2.7.2. Segunda Construcción

Haciendo uso del Teorema 2.7.2 y de la Observación 2.7.2 se obtienen los siguientes resultados.

Teorema 2.7.4. *La función*

$$\begin{aligned} f : [p-1]^* &\longrightarrow [p-2] \\ i &\longmapsto \lfloor r_i/p \rfloor \end{aligned}$$

define una secuencia sonar módulo $p - 1$ *con* $p - 1$ *elementos.*

Teorema 2.7.5. *La función*

$$\begin{aligned} g : [p-1]^* &\longrightarrow [p-1] \\ i &\longmapsto \lfloor r_i/(p-1) \rfloor \end{aligned}$$

define una secuencia sonar módulo p *con* $p - 1$ *elementos.*

Nota 2.7.1. *Las demostraciones de estos dos teoremas son similares a la prueba del Teorema 2.7.3, por lo cual se omiten.*

Ejemplo 2.7.2. *Considere* $p = 11$ *y* $\alpha = 2$. *Se obtiene el conjunto de Sidon tipo Ruzsa,* $R(11,2) = \{101, 92, 63, 104, 65, 86, 7, 58, 39, 100\}$. *Mediante la función* $f : [10]^* \longrightarrow [9]$ *definida por* $f(i) = \lfloor r_i/11) \rfloor$ *donde* $r_i \in R(11,2)$, *se construye el conjunto*

$$\{(1,9),(2,9),(3,5),(4,8),(5,9),(6,3),(7,0),(8,5),(9,7),(10,5)\},$$

el cual es una secuencia sonar módulo 10 *con* 10 *elementos. En la Figura 2.9, se observa la aplicación de la función* f *junto con su arreglo rectangular asociado.*

$$\begin{aligned}
100 &\equiv 1 \ (\text{mód } 11) \rightarrow \lfloor 100/11 \rfloor = 9 \\
101 &\equiv 2 \ (\text{mód } 11) \rightarrow \lfloor 101/11 \rfloor = 9 \\
58 &\equiv 3 \ (\text{mód } 11) \rightarrow \lfloor 58/11 \rfloor = 5 \\
92 &\equiv 4 \ (\text{mód } 11) \rightarrow \lfloor 92/11 \rfloor = 8 \\
104 &\equiv 5 \ (\text{mód } 11) \rightarrow \lfloor 104/11 \rfloor = 9 \\
39 &\equiv 6 \ (\text{mód } 11) \rightarrow \lfloor 39/11 \rfloor = 3 \\
7 &\equiv 7 \ (\text{mód } 11) \rightarrow \lfloor 7/11 \rfloor = 0 \\
63 &\equiv 8 \ (\text{mód } 11) \rightarrow \lfloor 63/11 \rfloor = 5 \\
86 &\equiv 9 \ (\text{mód } 11) \rightarrow \lfloor 86/11 \rfloor = 7 \\
65 &\equiv 10 \ (\text{mód } 11) \rightarrow \lfloor 65/11 \rfloor = 5
\end{aligned}$$

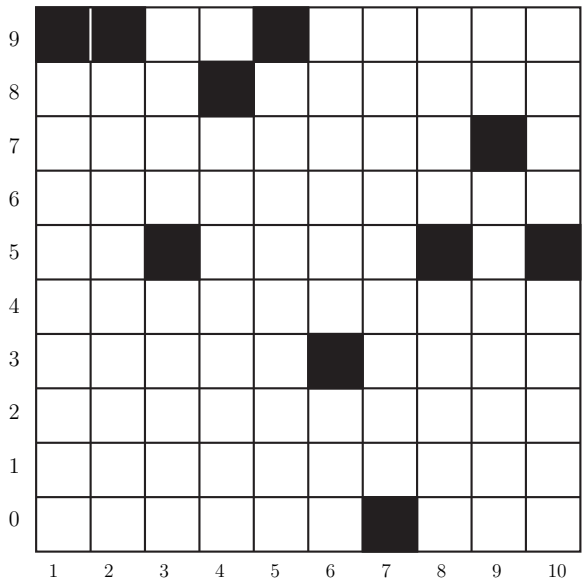

Figura 2.9: Construcción Asociada al Teorema 2.7.4 y su Respectivo Arreglo Rectangular.

De otro lado, mediante la función $g : [10]^* \longrightarrow [10]$ *definida por* $g(i) = \lfloor r_i/10 \rfloor$ *donde* $r_i \in R(11, 2)$*, se construye el conjunto*

$$\{(1, 10), (2, 9), (3, 6), (4, 10), (5, 6), (6, 8), (7, 0), (8, 5), (9, 3), (10, 10)\},$$

el cual es una secuencia sonar módulo 11 *con* 10 *elementos. En la Figura 2.10, se observa la aplicación de la función g junto con su arreglo rectangular asociado.*

$$\begin{aligned}
101 &\equiv 1 \ (\text{mód } 10) \rightarrow \lfloor 101/10 \rfloor = 10 \\
92 &\equiv 2 \ (\text{mód } 10) \rightarrow \lfloor 92/10 \rfloor = 9 \\
63 &\equiv 3 \ (\text{mód } 10) \rightarrow \lfloor 63/10 \rfloor = 6 \\
104 &\equiv 4 \ (\text{mód } 10) \rightarrow \lfloor 104/10 \rfloor = 10 \\
65 &\equiv 5 \ (\text{mód } 10) \rightarrow \lfloor 65/10 \rfloor = 6 \\
86 &\equiv 6 \ (\text{mód } 10) \rightarrow \lfloor 86/10 \rfloor = 8 \\
7 &\equiv 7 \ (\text{mód } 10) \rightarrow \lfloor 7/10 \rfloor = 0 \\
58 &\equiv 8 \ (\text{mód } 10) \rightarrow \lfloor 58/10 \rfloor = 5 \\
39 &\equiv 9 \ (\text{mód } 10) \rightarrow \lfloor 39/10 \rfloor = 3 \\
100 &\equiv 10 \ (\text{mód } 10) \rightarrow \lfloor 100/10 \rfloor = 10
\end{aligned}$$

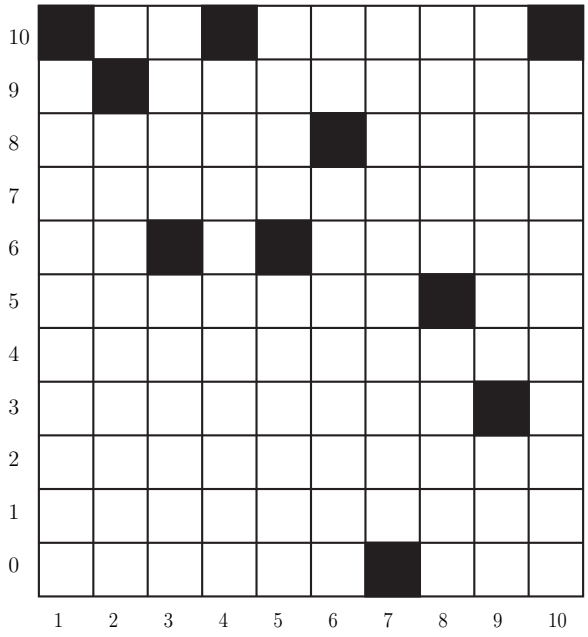

Figura 2.10: Construcción Asociada al Teorema 2.7.5 y su Respectivo Arreglo Rectangular.

Capítulo 3

Problema Fundamental

En este capítulo se dará a conocer el Teorema 3.3.1 que mejora asíntoticamente la cota hallada en el Teorema 4 de [4]. El resultado que se presenta en este capítulo se obtiene haciendo uso de una técnica relativamente nueva conocida como "Energía Aditiva", éste tema se desarrolla de una manera más amplia y detallada en [12].

3.1. La Función $G(m)$

El problema fundamental en secuencias sonar consiste en determinar, para un m fijo, el máximo n para el cual existe una secuencia $m \times n$, es decir, se trata de investigar la función

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

En principio se establece una cota trivial para $G(m)$. Para lograr esta cota se necesitará de la definición de triángulo de diferencias.

Definición 3.1.1. *Sea $f : [n]^* \to [m]^*$, $n, m \in \mathbb{N}$. El triángulo de diferencias $T(f)$ está definido como las colección de los vectores $[t_k(f) : \ 1 \leq k \leq n-1]$, donde $t_k(f) = f(i+k) - f(i)$ con $1 \leq i \leq n-k$ define la k-ésima fila del triángulo de diferencias.*

En la Figura 3.1 se ilustra el triángulo de diferencias para $n = 5$.

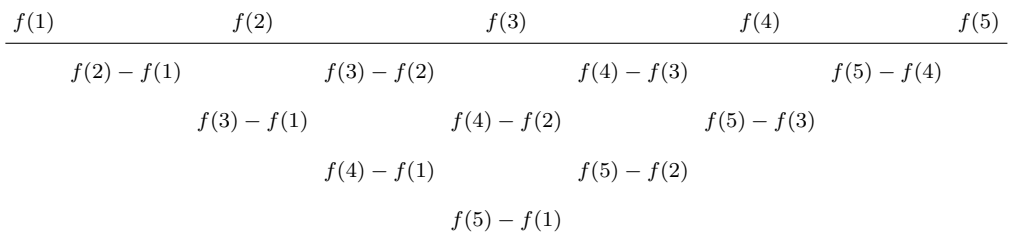

Figura 3.1: $T(f)$ para $n = 5$.

Teorema 3.1.1. *Si $f : [n]^* \longrightarrow [m]^*$ define una secuencia sonar entonces $n \leq 2m$. En consecuencia $G(m) \leq 2m$.*

Demostración. Note que por ser f una secuencia sonar, en la primera fila del triángulo de diferencias, Figura 3.2, hay $n-1$ entradas distintas las cuales se quedan en el intervalo entero $[-m+1, m-1]$. Ya que $|[-m+1, m-1]| = 2m-1$, se tiene que $n-1 \leq 2m-1$, es decir $n \leq 2m$. ■

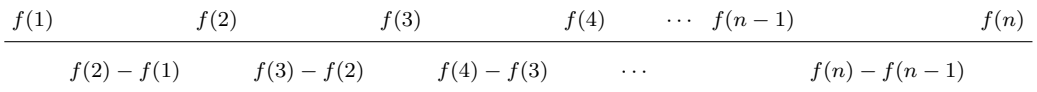

Figura 3.2: Primera fila de $T(f)$.

Ejemplo 3.1.1. *La cota del Teorema 3.1.1 se alcanza cuando $m = 4$ a través de la siguiente secuencia sonar entera con 8 elementos, la cual es construida utilizando el método exhaustivo*

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

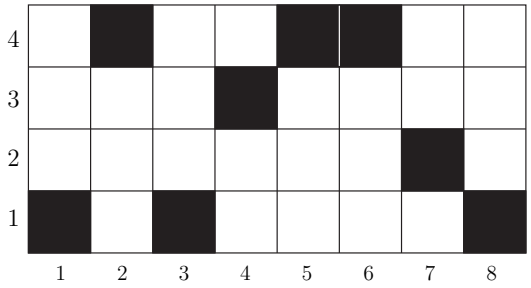

Figura 3.3: Secuencia sonar 4×8.

3.2. Energía Aditiva

Dado un grupo conmutativo $(G,+)$, $\mathcal{A} \subseteq G$ y $x \in G$, se define la función representación de x con respecto al conjunto $\mathcal{A}-\mathcal{A}$ como

$$R_{\mathcal{A}-\mathcal{A}}(x) := |\{(a,b) \in \mathcal{A}\times\mathcal{A} :\ x = a-b\}| = |\mathcal{A} \cap (\mathcal{A}+x)|\,,$$

donde $\mathcal{A}+x$ es la traslación de $\mathcal{A}$ mediante x. En general, la función de representación de x se puede definir con respecto a los conjuntos $\mathcal{A}-\mathcal{B}$ y $\mathcal{A}+\mathcal{B}$, donde $\mathcal{A}$ y $\mathcal{B}$ son subconjuntos de G distintos, de la siguiente manera

$$R_{\mathcal{A}+\mathcal{B}}(x) := |\{(a,b) \in \mathcal{A}\times\mathcal{B} :\ x = a+b\}| = |\mathcal{A} \cap (x-\mathcal{B})|$$

$$R_{\mathcal{A}-\mathcal{B}}(x) := |\{(a,b) \in \mathcal{A}\times\mathcal{B} :\ x = a-b\}| = |\mathcal{A} \cap (\mathcal{B}+x)|\,,$$

donde $x-\mathcal{B}$ es la reflexión de $\mathcal{B}$ mediante x. Se puede probar que R satisface las siguientes identidades

$$\begin{aligned} R_{\mathcal{A}-\mathcal{A}}(0) &= |\mathcal{A}|. \\ \sum_{x\in\mathcal{A}+\mathcal{B}} R_{\mathcal{A}+\mathcal{B}}(x) &= |\mathcal{A}||\mathcal{B}|. \\ \sum_{x\in\mathcal{A}-\mathcal{B}} R_{\mathcal{A}-\mathcal{B}}(x) &= |\mathcal{A}||\mathcal{B}|. \end{aligned} \tag{3.1}$$

Con estas herramientas es posible establecer y definir algunas propiedades básicas de la energía aditiva.

Definición 3.2.1. *Sean $(G,+)$ un grupo conmutativo notado aditivamente y $\mathcal{A},\mathcal{B} \subseteq G$. Se define la energía aditiva entre $\mathcal{A}$ y $\mathcal{B}$ como*

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

En general $E(\mathcal{A},\mathcal{B})$ cuenta el número de soluciones de la ecuación $a+b=a'+b'$, que coincide con el número de soluciones de la ecuación $a-a'=b-b'$. Esta observación permite establecer

las siguientes identidades, las cuales se demuestran en [12] mediante argumentos combinatorios

$$\begin{aligned} E(\mathcal{A},\mathcal{B}) &= \sum_{x\in\mathcal{A}+\mathcal{B}} R^2_{\mathcal{A}+\mathcal{B}}(x) \\ &= \sum_{x\in\mathcal{A}-\mathcal{B}} R^2_{\mathcal{A}-\mathcal{B}}(x) \\ &= \sum_{x\in(\mathcal{A}-\mathcal{A})\cap(\mathcal{B}-\mathcal{B})} R_{\mathcal{A}-\mathcal{A}}(x)R_{\mathcal{B}-\mathcal{B}}(x). \end{aligned} \tag{3.2}$$

El siguiente lemma se debe a Ruzsa [10], y relaciona el cardinal de un conjunto de Sidon con el cardinal de un conjunto cualquiera, en el mismo grupo.

Lema 3.2.1. *Sea $\mathcal{A}$ un conjunto de Sidon en un grupo conmutativo G y sea $\mathcal{B}$ cualquier subconjunto de G. Entonces*

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

Demostración. Mediante la desigualdad de Cauchy y las identidades (3.1) y (3.2) se tiene que

$$\begin{aligned} (|\mathcal{A}||\mathcal{B}|)^2 &= \left(\sum_{x\in\mathcal{A}+\mathcal{B}} R_{\mathcal{A}+\mathcal{B}}(x)\right)^2 \\ &\leq |\mathcal{A}+\mathcal{B}| \sum_{x\in\mathcal{A}+\mathcal{B}} R^2_{\mathcal{A}+\mathcal{B}}(x) \\ &= |\mathcal{A}+\mathcal{B}| \sum_{x\in(\mathcal{A}-\mathcal{A})\cap(\mathcal{B}-\mathcal{B})} R_{\mathcal{A}-\mathcal{A}}(x)R_{\mathcal{B}-\mathcal{B}}(x). \end{aligned} \tag{3.3}$$

Como $\mathcal{A}$ es de Sidon entonces $R_{\mathcal{A}-\mathcal{A}}(x) \leq 1$ para todo $x \neq 0$, por lo tanto la suma de la desigualdad (3.3) está acotada por

$$R_{\mathcal{A}-\mathcal{A}}(0)R_{\mathcal{B}-\mathcal{B}}(0) + \sum_{\substack{x\in(\mathcal{A}-\mathcal{A})\cap(\mathcal{B}-\mathcal{B}) \\ x\neq 0}} R_{\mathcal{B}-\mathcal{B}}(x) \leq |\mathcal{A}||\mathcal{B}| + |\mathcal{B}|^2 - |\mathcal{B}|,$$

lo que implica que

$$\begin{aligned} (|\mathcal{A}||\mathcal{B}|)^2 &\leq |\mathcal{A}+\mathcal{B}|(|\mathcal{A}||\mathcal{B}| + |\mathcal{B}|^2 - |\mathcal{B}|) \\ |\mathcal{A}|^2 &\leq |\mathcal{A}+\mathcal{B}|\left(\frac{|\mathcal{A}|}{|\mathcal{B}|} + 1 - \frac{1}{|\mathcal{B}|}\right) \\ |\mathcal{A}|^2 &\leq |\mathcal{A}+\mathcal{B}|\left(1+\frac{|\mathcal{A}|-1}{|\mathcal{B}|}\right) \end{aligned}$$

probando así la desigualdad deseada. ■

3.3. El Problema Fundamental

El estado actual del problema en arreglos sonar establece que $G(m) \leq m + 3m^{2/3} + 2m^{1/3} + 9$, resultado que se menciona en [4] pero del cual no se conoce (al menos de nuestra parte) una prueba formal. En el Teorema 4 de [4] se demuestra que $G(m) \leq m + 5m^{2/3}$, resultado que se mejora a continuación.

Teorema 3.3.1. *Si $f : [n]^* \longrightarrow [m]^*$ define una secuencia sonar entonces*

$$G(m) \leq m + 3{,}78m^{2/3} + 4{,}76m^{1/3} + 2.$$

Demostración. Dado que f es una secuencia sonar el grafo de f es un conjunto de Sidon. Además se tiene que $|G_f| = n$ y $G_f \subseteq [n]^* \times [m]^*$.

Considere el conjunto $\mathcal{B} = [u] \times [u]$, donde $u = \lfloor cm^{2/3} \rfloor$. Más adelante se mostrará cuál es el valor de c. Note que $G_f + \mathcal{B} \subseteq [n+u]^* \times [m+u]^*$, y por tanto $|G_f + \mathcal{B}| \leq (n+u)(m+u)$ y $|\mathcal{B}| = (u+1)^2$. Así, de acuerdo al Lema 3.2.1 se sigue la siguiente desigualdad

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

de donde se tiene que

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

Ahora considere $h(c) = \frac{2c^3+2}{c^2}$. Se tiene que $h'(c) = \frac{2c^3-4}{c^3}$, por lo tanto $h'(c) = 0$ implica que $c = \sqrt[3]{2}$. De otro lado, se tiene que $h''(c) = \frac{12}{c^4}$; es decir $h''(c) > 0$ para todo c y en conclusión, por el criterio de la segunda derivada h tiene un mínino relativo en $c = \sqrt[3]{2} \approx 1{,}26$. Luego con $c = 1{,}26$ se tiene el resultado requerido. ■

Contribuciones

A continuación se mencionan las contribuciones relevantes que fueron posibles gracias a la realización de este trabajo y fueron hechas dentro del desarrollo del mismo. Estas contribuciones están ligadas a los objetivos propuestos en un principio y conforman, junto con una visión de proyectos futuros, las conclusiones de este trabajo.

3.4. Contribuciones

1. Se muestra en la primera parte de este trabajo el papel de los conjuntos de Sidon dentro del sistema del sonar, lo cual hasta el momento no se había hecho en detalle y representa una contribución a tener en cuenta para trabajos futuros en aplicaciones de los conjuntos estudiados.

2. Se determinan tres nuevas construcciones de secuencias sonar, las cuales están descritas en detalle en los teoremas 2.7.3, 2.7.4, 2.7.5, y que son resultado del proyecto de investigación coordinado por el profesor Carlos Trujillo. Estas son basadas originalmente en las construcciones de conjuntos de Sidon tipo Bosse y tipo Ruzsa. Cabe resaltar que estos resultados pueden ser generalizados a partir de cualquier construcción de conjuntos de Sidon que satisfagan algunas propiedades especiales.

3. El resultado obtenido por Paul Erdös, Ron Graham, Irme Ruzsa y Herbert Taylor en el Teorema 4 de [4] se mejora asintóticamente con la cota hallada en el Teorema 3.3.1 usando energía aditiva. En el Apéndice A, se muestra la relación entre las cotas de los dos teoremas antes mencionados y la cota trivial del Teorema 3.1.1.

4. De la realización de este trabajo se desprendieron charlas en congresos especializados. La primera se tituló "Conjuntos de Sidon y Arreglos Radar" y fue presentada el 3 de diciembre de 2012 en el marco del encuentro internacional de Álgebra, Teoría de Números, Aplicaciones y Combinatoria-ALTENCOA5- en la ciudad de Bogotá. La segunda charla se titula "Aplicación de los conjuntos de Sidon a las telecomunicaciones" y será presentada en noviembre de 2013 en la isla de San Andres Colombia dentro del marco del II Congreso Internacional de Matemática Aplicada y Computación ICAMI.

3.5. Trabajos futuros

1. Continuar el estudio de la aplicación al sonar, la cual puede ser descrita con mayor detalle valiéndose del análisis de Fourier en el tratamiento de señales. Así como también, realizar un estudio de las aplicaciones de los conjuntos de Sidon en dimensión dos dentro de las telecomunicaciones, enfocándose en el problema de evitar la intermodulacion de tercer orden en la recepción de señales [2]. Además, mostrar en detalle la aplicación de los conjuntos de Sidon en dimensión uno en la ubicación de radiotelescopios en un arreglo lineal e intentar hallar nuevas aplicaciones de los conjuntos de Sidon.

2. Realizar un estudio detallado de las nuevas construcciones aquí presentadas y de su posible generalización.

3. Llegar al estado actual del problema fundamental de secuencias sonar (o mejorarlo), mediante el uso de energía aditiva.

Apéndice A

Comparación de las Cotas

A continuación se muestran tablas que comparan los primeros 200 valores de las cotas $G_1 = 2m$, $G_2 = m + 5m^{2/3}$ y $G_3 = m + 3{,}78m^{2/3} + 4{,}76m^{1/3} + 2$, en donde se puede observar fácilmente las siguientes relaciones entre estas cotas: $G_1 \leq G_2 \leq G_3$ para $1 \leq m \leq 78$, $G_1 \leq G_3 \leq G_2$ para $79 \leq m \leq 113$, $G_3 \leq G_1 \leq G_2$ para $114 \leq m \leq 125$ y finalmente $G_3 \leq G_2 \leq G_1$ para $m \geq 126$, con lo que se muestra la mejora que se logra con la nueva cota.

m	G_1	G_2	G_3
1	2	6	11,54204263
2	4	9,93700526	16,00010253
3	6	13,40041912	19,73063211
4	8	16,5992105	23,08407188
5	10	19,62008869	26,19550144
6	12	22,50963624	29,13416789
7	14	25,29652855	31,94125572
8	16	28	34,64365041
9	18	30,63374355	37,26006948
10	20	33,20794417	39,80417486
11	22	35,73043722	42,28630668
12	24	38,20741394	44,71451913
13	26	40,64387407	47,09523396
14	28	43,04392867	49,43367133
15	30	45,41100998	51,73414436
16	32	47,74802104	54,00026671
17	34	50,05744509	56,23510259
18	36	52,34142728	58,44127773
19	38	54,60183679	60,62106305
20	40	56,84031499	62,77643871

m	G_1	G_2	G_3
21	42	59,05831306	64,9091441
22	44	61,25712205	67,02071714
23	46	63,437897	69,1125258
24	48	65,60167646	71,18579338
25	50	67,74939867	73,2416193
26	52	69,88191478	75,28099604
27	54	72	77,30482333
28	56	74,10436292	79,31391987
29	58	76,19565339	81,30903334
30	60	78,27446923	83,29084875
31	62	80,34136202	85,25999566
32	64	82,396842	87,21705427
33	66	84,44138239	89,16256076
34	68	86,47542311	91,09701184
35	70	88,49937403	93,02086875
36	72	90,51361778	94,93456075
37	74	92,51851234	96,83848811
38	76	94,51439318	98,73302488
39	78	96,50157526	100,6185212
40	80	98,48035476	102,4953055

m	G_1	G_2	G_3
41	82	100,4510107	104,3636861
42	84	102,4138062	106,2239532
43	86	104,3689898	108,0763803
44	88	106,3167968	109,9212254
45	90	108,2574499	111,7587323
46	92	110,1911602	113,5891315
47	94	112,1181284	115,4126417
48	96	114,038545	117,2294699
49	98	115,9525914	119,0398131
50	100	117,8604404	120,8438581
51	102	119,7622568	122,6417829
52	104	121,6581977	124,4337571
53	106	123,5484133	126,2199423
54	108	125,4330473	128,0004926
55	110	127,3122371	129,7755553
56	112	129,1861142	131,5452713
57	114	131,0548048	133,3097753
58	116	132,9184298	135,0691963
59	118	134,7771055	136,8236579
60	120	136,6309432	138,5732786
61	122	138,4800504	140,3181721
62	124	140,32453	142,0584478
63	126	142,1644813	143,7942106
64	128	144	145,5255614
65	130	145,8311781	147,2525974
66	132	147,6581045	148,975412
67	134	149,4808649	150,6940954
68	136	151,2995419	152,4087344
69	138	153,1142154	154,1194127
70	140	154,9249626	155,8262111
71	142	156,7318582	157,5292077
72	144	158,5349742	159,2284777
73	146	160,3343806	160,9240941
74	148	162,1301449	162,6161272
75	150	163,9223326	164,3046451
76	152	165,7110072	165,9897138
77	154	167,4962301	167,671397
78	156	169,2780611	169,3497567
79	158	171,0565579	171,0248526
80	160	172,8317767	172,6967429

m	G_1	G_2	G_3
81	162	174,603772	174,3654838
82	164	176,3725969	176,0311301
83	166	178,1383027	177,6937346
84	168	179,9009395	179,353349
85	170	181,6605558	181,0100232
86	172	183,417199	182,6638058
87	174	185,1709151	184,3147439
88	176	186,9217489	185,9628836
89	178	188,6697438	187,6082694
90	180	190,4149425	189,2509448
91	182	192,1573862	190,890952
92	184	193,8971153	192,5283322
93	186	195,6341689	194,1631255
94	188	197,3685855	195,7953708
95	190	199,1004023	197,4251062
96	192	200,8296558	199,0523688
97	194	202,5563814	200,6771947
98	196	204,280614	202,2996191
99	198	206,0023873	203,9196764
100	200	207,7217345	205,5374
101	202	209,4386878	207,1528228
102	204	211,1532787	208,7659766
103	206	212,8655382	210,3768926
104	208	214,5754963	211,9856013
105	210	216,2831825	213,5921323
106	212	217,9886255	215,1965148
107	214	219,6918537	216,7987772
108	216	221,3928945	218,3989472
109	218	223,0917749	219,9970518
110	220	224,7885212	221,5931178
111	222	226,4831594	223,187171
112	224	228,1757147	224,7792368
113	226	229,8662118	226,3693401
114	228	231,554675	227,9575051
115	230	233,2411281	229,5437557
116	232	234,9255943	231,1281151
117	234	236,6080965	232,7106063
118	236	238,2886569	234,2912514
119	238	239,9672976	235,8700725
120	240	241,6440399	237,4470909

m	G_1	G_2	G_3
121	242	243,318905	239,0223277
122	244	244,9919135	240,5958035
123	246	246,6630856	242,1675384
124	248	248,3324413	243,7375523
125	250	250	245,3058646
126	252	251,6657809	246,8724942
127	254	253,3298028	248,43746
128	256	254,9920842	250,0007801
129	258	256,652643	251,5624725
130	260	258,3114972	253,122555
131	262	259,9686641	254,6810447
132	264	261,624161	256,2379588
133	266	263,2780047	257,7933138
134	268	264,9302116	259,3471262
135	270	266,5807982	260,899412
136	272	268,2297804	262,4501871
137	274	269,8771738	263,9994669
138	276	271,522994	265,5472667
139	278	273,1672561	267,0936016
140	280	274,809975	268,6384861
141	282	276,4511654	270,1819347
142	284	278,0908418	271,7239618
143	286	279,7290184	273,2645812
144	288	281,3657091	274,8038068
145	290	283,0009277	276,341652
146	292	284,6346876	277,87813
147	294	286,2670023	279,4132541
148	296	287,8978847	280,947037
149	298	289,5273478	282,4794914
150	300	291,1554043	284,0106297
151	302	292,7820667	285,5404642
152	304	294,4073472	287,069007
153	306	296,0312579	288,5962698
154	308	297,6538109	290,1222643
155	310	299,2750178	291,6470022
156	312	300,8948901	293,1704945
157	314	302,5134394	294,6927525
158	316	304,1306768	296,2137872
159	318	305,7466133	297,7336094
160	320	307,3612599	299,2522296

m	G_1	G_2	G_3
161	322	308,9746274	300,7696584
162	324	310,5867262	302,2859061
163	326	312,1975668	303,8009828
164	328	313,8071596	305,3148986
165	330	315,4155146	306,8276633
166	332	317,0226418	308,3392867
167	334	318,6285511	309,8497783
168	336	320,2332522	311,3591475
169	338	321,8367547	312,8674038
170	340	323,439068	314,3745563
171	342	325,0402015	315,8806139
172	344	326,6401642	317,3855858
173	346	328,2389654	318,8894805
174	348	329,8366139	320,3923069
175	350	331,4331186	321,8940734
176	352	333,0284882	323,3947886
177	354	334,6227312	324,8944606
178	356	336,2158562	326,3930979
179	358	337,8078715	327,8907083
180	360	339,3987854	329,3873
181	362	340,988606	330,8828807
182	364	342,5773413	332,3774584
183	366	344,1649994	333,8710406
184	368	345,751588	335,3636349
185	370	347,3371149	336,8552488
186	372	348,9215877	338,3458898
187	374	350,5050141	339,835565
188	376	352,0874014	341,3242816
189	378	353,668757	342,8120468
190	380	355,2490881	344,2988676
191	382	356,8284021	345,7847508
192	384	358,4067058	347,2697034
193	386	359,9840065	348,753732
194	388	361,5603109	350,2368434
195	390	363,135626	351,719044
196	392	364,7099585	353,2003404
197	394	366,283315	354,6807391
198	396	367,8557022	356,1602463
199	398	369,4271266	357,6388684
200	400	370,9975947	359,1166114

Apéndice B

Implementación en MuPAD Pro 4.0

B.1. Algoritmos

En este apéndice se presentan algunos algoritmos implementados en **MuPAD Pro 4.0** que han sido utilizados en éste trabajo para verificar ciertos cálculos que suelen ser un poco largos, o simplemente tediosos cuando no se hace uso de una herramienta computacional.

B.1.1. Algoritmo 1: Verificar Sonar

Entrada: Una lista `L` de enteros.

Descripción: Este algoritmo verifica si una lista `L` es una secuencia sonar en $\mathbb{Z} \times \mathbb{Z}$, mediante el uso del triángulo de diferencias (Definición 3.1.1).

Salida: `TRUE` si `L` es una secuencia sonar o `FALSE` en caso contrario.

```
essonar:=proc(L)
begin
n:=nops(L);
cont1:=1; cont2L:=1; Sonar:=TRUE; N:=n-1;
for i from 1 to N do
    S:={};
    N1:=n-i;
    for j from 1 to N1 do
        S:={op(S),L[j+i]-L[j]};
```

```
    end_for:
    if (nops(S)<>N1) then
        Sonar:=FALSE;
        break
    end_if
end_for:
Sonar
end_proc
```

Ejemplo B.1.1. `L:=[1,4,7,3,6,8]:`

```
essonar(L)
FALSE
```

B.1.2. Algoritmo 2: Verificar Sonar Modular

Entrada: Una lista `L` de enteros y un entero p.

Descripción: Este algoritmo verifica si una lista `L` es una secuencia sonar módulo p, mediante el uso del triángulo de diferencias (Definición 3.1.1).

Salida: `TRUE` si `L` es una secuencia sonar módulo p o `FALSE` en caso contrario.

```
essonarMod:=proc(L,p)
begin
n:=nops(L);
cont1:=1; cont2:=1; Sonar:=TRUE; N:=n-1;
for i from 1 to N do
    S:={};
    N1:=n-i;
    for j from 1 to N1 do
        S:={op(S),(L[j+i]-L[j])mod p};
    end_for:
    if (nops(S)<>N1) then
        Sonar:=FALSE;
        break
    end_if
```

```
end_for:
Sonar
end_proc
```

Ejemplo B.1.2. `L:=[9, 1, 8, 8, 1, 9, 10, 4, 2, 4, 10, 9]:`

```
essonarMod(L,11)
TRUE
```

B.1.3. Algoritmo 3: Construcción Cuadrática

Entrada: Un primo p y enteros `a,b,c` donde `a` no es congruente con cero módulo p.

Descripción: Siguiendo la construcción presentada en el Teorema 2.1.1, el algoritmo construye una secuencia sonar módulo p con $p+1$ elementos.

Salida: Una lista `S` de enteros, la cual será la secuencia sonar requerida.

```
SonarQuad:=proc(p,a,b,c)
begin
    S:=[]; P:=p+1;
    for i from 1 to P do
        S:=[op(S),(a*i^2+b*i+c)mod p];
    end_for:
end_proc
```

B.1.4. Algoritmo 4: Construcción Shift

Entrada: Un primo p y un entero r.

Descripción: Encuentra una secuencia sonar con la construcción Shift del Teorema 2.2.1. El algoritmo hace la distinción de la paridad del primo p para generar una construcción tipo Shift par o impar según corresponda. Además, construye el campo $\mathbb{F}_{p^{2r}}$ mediante `GaloisField(p,2*r)`.

Salida: Una lista `S` de enteros que será una secuencia sonar tipo Shift correspondiente a la paridad del primo de entrada.

```
SonarShift:=proc(p,r)
begin
S:=[]; q:=p^r;
```

```
F:=Dom::GaloisField(p,2*r);
Alfa:=F::randomPrimitive();
Beta:=Alfa^(q+1);
if p=2 then
  a:=1;b:=q;
else
    a:=-(q-1)/2; b:=(q-1)/2;
end_if;
for i from a to b do
    alfai:=Alfa^i;
    S:=[op(S),F::ln(alfai^(q)+alfai,Beta) mod q-1];
end_for;
S
end_proc
```

B.1.5. Algoritmo 5: Construcción Logarítmica de Welch

Entrada: Un primo p

Descripción: Este algoritmo encuentra una secuencia sonar módulo $p-1$ con $p-1$ elementos usando la construcción logarítmica de Welch del Teorema 2.4.1. Usa la función interna de MuPAD `GaloisField()` para crear el campo finito con p elementos y el cual guarda en la variable `F`. Luego, en `Alfa` asigna una raíz primitiva aleatoria mediante la función `randomPrimitive()`.

Salida: Una lista `LW` de enteros que será una secuencia sonar tipo Welch logarítmica.

```
LogWelch:=proc(p)
begin
   P:=p-1;
   F:=Dom::GaloisField(p);
   Alfa:=F::randomPrimitive();
   LW:=[];
   for i from 1 to P do
       LW:=[op(LW),F::ln(i,Alfa)];
   end_for;
```

```
   LW;
end_proc;
```

B.1.6. Algoritmo 6: Construcción de Golomb

Entrada: Un primo p y un entero r.

Descripción: Encuentra una secuencia sonar módulo $q-1$ con $q-2$ elementos usando la construcción Golomb del Teorema 2.5.1. Usa la función `GaloisField()` para construir el campo $\mathbb{F}_q$ con $q = p^r$. En `Alfa` y `Beta` asigna elementos primitivos aleatorios. Si los dos elementos primitivos coinciden, la construcción hecha es tipo Lempel, de lo contrario es tipo Golomb.

Salida: Una lista `G` de enteros que será una secuencia sonar tipo Golomb o Lempel según sea el caso.

```
Golombq:=proc(p,r)
begin
   q:=p^r;
   F:=Dom::GaloisField(p,r);
   Alfa:=F::randomPrimitive();
   Beta:=F::randomPrimitive();
   Q:=q-2; cont:=1;G:=[];
   for i from 1 to Q do
       G:=[op(G),F::ln(1-Alfa^i,Beta) mod q-1];
   end_for;
   if(Alfa=Beta)then
      print("Construcción Lempel");
   else
      print("Construcción Golomb");
   end_if;
end_proc
```

B.1.7. Algoritmo 7: Raíces Primitivas

Este algoritmo fue necesario implementarlo debido a que el comando `mod` de MuPAD Pro 4.0, creaba conflicto al utilizar las funciones internas `GaloisField()` y `randomPrimitive()` en la

implementación del Algoritmo B.1.8.

Entrada: Un primo p.

Descripción: Este algoritmo encuentra los elementos primitivos del grupo multiplicativo $\mathbb{F}_p^*$ para el primo p.

Salida: Una lista `Pr` que contiene todas la raíces primitivas módulo p.

```
primitiveprimes:=proc(p)
begin
cont:=1;cont2:=1;
P:=p-1;
Pr:=[]; Fp:={$1..P};
prim:=numlib::phi(p-1);
while (cont<=prim and cont2<=P) do
      S:={};
      for i from 1 to P do
          S:={op(S),(cont2^i)mod p}
      end_for:
      if (S=Fp) then
          cont:=cont+1;
          Pr:=[op(Pr),cont2]
      end_if;
      cont2:=cont2+1;
end_while:
Pr
end_proc
```

B.1.8. Algoritmo 8: Construcción Exponencial Extendida de Welch

Entrada: Un primo p y un entero s

Descripción: Este algoritmo encuentra una secuencia sonar módulo p con p elementos, usando la construcción del Teorema 2.6.1 genera las raíces primitivas mediante `primitiveprimes(p)` descrito en el Algoritmo 7 y las guarda en la variable `Pr`. Posteriormente, en la variable `B` se

asigna una raíz primitiva de manera aleatoria mediante la función interna de MuPAD `random()`.

Salida: Una lista `EW` de enteros, que será una secuencia sonar Welch exponencial extendida.

```
ExpoWelchX:=proc(p,s)
begin
   Pr:=primitiveprimes(p);
   B:=random(1..nops(Pr));
   Alfa:=Pr[B(1)]; print(Alfa);P:=p-1;
   EW:=[];
   for i from 0 to P do
       EW:=[op(EW),(Alfa^(i+s))mod p];
   end_for:
   EW
end_proc;
```

Bibliografía

[1] Michael A. Ainslie, *Principles of sonar performance modelling*, Springer Praxis Books, Jointly published with Praxis Publishing, 2010.

[2] Wallace C. Babcock, *Intermodulation interference in radio systems*, Bell System Technical Journal **32** (1953), no. 1, 63–73.

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

[4] Paul Erdős, Ron Graham, Imre Z. Ruzsa, and Herbert Taylor, *Bounds for arrays of dots with distinct slopes on lengths*, Combinatorica **12** (1992), no. 1, 39–44. MR 1167474 (93k:05182)

[5] Solomon Golomb and Herbert Taylor, *Two-dimensional synchronization patterns for minimum ambiguity*, Information Theory, IEEE Transactions on **28** (1982), no. 4, 600–604.

[6] Solomon W Golomb and Herbert Taylor, *Constructions and properties of Costas arrays*, Proceedings of the IEEE **72** (1984), no. 9, 1143–1163.

[7] Oscar Moreno, Richard A Games, and Herbert Taylor, *Sonar sequences from Costas arrays and the best known sonar sequences with up to 100 symbols*, Information Theory, IEEE Transactions on **39** (1993), no. 6, 1985–1987.

[8] J Robinson, *Golomb rectangles*, Information Theory, IEEE Transactions on **31** (1985), no. 6, 781–787.

[9] Carlos Alexis Gómez Ruiz and Carlos Alberto Trujillo Solarte, *Una nueva construcción de conjuntos B_h modulares*, Enseñanza **19** (2011), no. 1.

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

[11] Carlos Alberto Trujillo Solarte, Diego Fernando Ruiz Solarte, and Yadira Caicedo, *New constructions of sonar sequences*, Preprint.

[12] Terence Tao and Van H Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 2006.

[13] Ken Taylor, Scott Rickard, and Konstantinos Drakakis, *Costas arrays: survey, standardization, and matlab toolbox*, ACM Transactions on Mathematical Software (TOMS) **37** (2011), no. 4, 41.

[14] Hugh D. Young and Roger A. Freedman, *Fisica universitaria*, Pearson, Pearson Educacion, 2009.