CONSTRUCCIONES DE REGLAS GOLOMB, ARREGLOS COSTAS Y SECUENCIAS SONARES

UN ANÁLISIS ALGEBRAICO

SERGIO LUIS AGREDO OTERO

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN

PROGRAMA DE MATEMÁTICAS

POPAYÁN

2014

CONSTRUCCIONES DE REGLAS GOLOMB, ARREGLOS COSTAS Y SECUENCIAS SONARES

UN ANÁLISIS ALGEBRAICO

Trabajo de grado como requisito parcial para optar el título de Matemático

SERGIO LUIS AGREDO OTERO

Director: Dr. Carlos Alberto Trujillo Solarte

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN

PROGRAMA DE MATEMÁTICAS

POPAYÁN

2014

Nota de aceptación

_____

_____

_____

_____

Director: Dr Carlos Alberto Trujillo

_____

Jurado: Diego Fernando Ruiz Solarte

_____

Jurado: Alfredo Gómez Calvache

Fecha de sustentación: 29 de abril del 2014.

AGRADECIMIENTOS

Mis más sinceros agradecimientos al Dios verdadero por permitirme avanzar esta etapa de mi vida, quien me ha brindado las fuerzas necesarias para sobrellevar la tribulación, la angustia. Muchas gracias Jehová por entrar en mi vida y por darme el tiempo y el espacio de terminar, por brindarme un pequeño núcleo familiar.

Le agradezco enormemente a mi querida madre Mercedes, por escucharme y apoyarme en los momentos que nadie más lo hacía, por ser ese oido sincero ante mis palabras, por ser ese alguien que me cuidó y me protegió de mis problemas y mis aflixiones.

Gracias a todas mis queridas y amadas amigas que recorrieron este largo y tedioso camino junto conmigo, han sido mi mayor apoyo, mi mayor poder. Muchas gracias por brindarme esa amistad tan valiosa, espero el destino no nos separe y que nuestros caminos sigan entrelazados un tiempo más.

Gracias a todos mis maestros, por enseñarme la valiosa instrucción, gracias por enseñarme a luchar e ignorar las dificultades cuando éstas aparecen. De corazón, un abrazo muy grande a todos ustedes, los llevo en mi corazón.

Índice general

Capítulo 1

Introducción

En 1932, el matemático Húngaro Simon Sidon, quien estaba trabajando en análisis de Fourier, le planteó a Paul Erdös el siguiente problema:
¿Qué tan grande puede ser un subconjunto A de $\{1, 2, ..., n\}$ que tenga la propiedad de que la representación de cualquier número entero visto como suma de dos elementos del conjunto A es a lo sumo 1? Esto se lo planteó Simon Sidon cuando trabajaba con la función $f_A(x) = \sum_{a \in A} x^a$, porque al elevar al cuadrado esa expresión aparece el número de representaciones mediante suma de dos elementos.

Debido a esta discusión, el matemático Simon Sidon creó el concepto de *conjunto de Sidon* definido como un conjunto de enteros que cumple la propiedad de que todas las sumas de dos elementos del conjunto son todas distintas, sin embargo, este concepto será ampliado a un marco teórico mucho mayor a este.

Existe una relación directa entre los conjuntos de Sidon con las *reglas Golomb*, cuyos origenes datan en la resolución de problemas de trabajos en paralelo, soluciones buscadas para resolver problemas computacionales en paralelo y formas lineales de trabajo en paralelo, como ejemplo el posicionamiento de antenas de radio, *phased array radio antennas* (antenas radiales con arreglos en fase) [4].

El problema de los sistemas de radar es que deben hacer frente a la presencia de diferentes tipos de señales indeseadas; aquí es donde emerge el problema general planteado por Babcock (1953) en relación con radio interferencia, la introducción de las reglas Golomb a la aplicación en comunicación.

Estos conjuntos especiales resultan ser una solución para evitar interferencias de tercer grado.

En su amplia gama, los conjuntos de Sidon se abren paso igualmente con los arreglos Costas que fueron propuestos por John P. Costas en el año 1965, quien motivado por una novedosa aplicación al sonar, empezó a buscar matrices de permutación con propiedades de auto ambigüedad óptimas. Él encontró ejemplos de tales matrices de tamaño n, con $1 \leq n \leq 12$. Al no poder encontrar una matriz de tamaño 13 contactó al profesor Solomon Golomb; éste último le respondió creando técnicas para construir tales matrices basadas en campos finitos [10].

De manera intuitiva, un arreglo Costas se refiere geométricamente a un conjunto de n puntos en la malla $n \times n$ ubicados de tal forma que en cada fila y en cada columna hay un solo punto y los $n(n-1)$ vectores que se forman entre cada par de puntos son todos distintos [7].

Tras la invención de estos nuevos conjuntos surge uno más seguido del arreglo Costas, la secuencia sonar; esta vez siendo permisivo en un arreglo rectángular, donde se permiten repeticiones (puntos extra) sólo en las filas.

El estudio de estos conjuntos se debe a la creciente investigación en la teoría de la comunicación en conjunto de la teoría de la criptografía, acelerando todos los procesos investigativos que se relacionan con estos tópicos. Las relaciones entre los problemas fundamentales de las reglas Golomb, arreglos Costas y secuencias sonares acorde a estas teorías se entrelazan de manera directa: Los conjuntos óptimos de reglas Golomb en relación a el posicionamiento de antenas radiales en fase, los arreglos Costas en relación a las aplicaciones de los diseños de experimentos o diseños experimentales, además de aplicaciones en la ingeniería de radares con arreglos en fase, y por último las secuencias sonares en relación a las aplicaciones a la comunicación [4].

Teniendo en cuenta que las construcciones existentes dan una solución parcial a los problemas fundamentales anteriormente mencionados, éstas brindan soporte igualmente a las aplicaciones que de éstas dependen; consecuentemente un estudio algebraico de estas construcciones abrirá campo ante este terreno identificando los puntos sobresalientes y comunes de aquellas construcciones para su uso en las aplicaciones.

Como objetivo básico, se pretende mostrar una perspectiva algebraica distinta de las construcciones como se presentan en la actualidad, para ello se presenta el segundo capítulo como los preliminares para ahondar el conocimiento de los conjuntos que se van a trabajar.

Las construcciones, siendo objetivo de mucho interés, se presentan en el capítulo tres. Se pretende proporcionar cada demostración con el fin de mostrar las técnicas usuales para probar si un conjunto es de Sidon, con el fin de recalcar como aparecen los problemas fundamentales de éstas al hacer las construcciones.

La sección de mayor relevancia es el capítulo cuatro, donde se enseña tanto una técnica para transformar un conjunto de Sidon de dimensión dos a otro de dimensión uno como las relaciones que unen a algunas de las construcciones vistas como grafos de funciones especiales.

Capítulo 2

Preliminares

2.1. Conceptos fundamentales

Sean $(G, +)$ un grupo conmutativo notado aditivamente y A un subconjunto no vacío de G.

Definición 2.1 ***(Conjunto de Sidon).*** *A es un conjunto de Sidon en el grupo G si para todo $a, b, c, d \in A$*

$$a + b = c + d \Longrightarrow \{a, b\} = \{c, d\}.$$

Una forma equivalente a esta propiedad es:

A es un conjunto de Sidon en el grupo G si para todo $x \in G$, la ecuación $x = a + b$ con $a, b \in A$ tiene a lo sumo dos soluciones $(a, b), (b, a) \in A \times A$.

Los conjuntos de Sidon en los enteros módulo n se llaman *conjuntos de Sidon modular o conjuntos de Sidon módulo n.*

Ejemplo 1. El conjunto

$$\{2^i : i = 1, 2, 3, ..., n\} \text{ para cualquier } n \in \mathbb{N},$$

es un conjunto de Sidon, y si tomamos el conjunto

$$\bigcup_{n=1}^{\infty}\{2^i : i = 1, 2, 3, ..., n\},$$

obtenemos un conjunto de Sidon infinito.

Demostración.

Primer paso. Tome el primer elemento del conjunto que se desea construir, a saber 1. Llame a su conjunto A_1.
Se desea agregar un nuevo elemento al conjunto que se está formando, por eso se debe evitar que las sumas del nuevo elemento con los elementos anteriores se repitan, para ello una técnica puede ser trasladar las nuevas sumas a números más grandes a las sumas anteriores, así que:

Segundo paso. Tome el elemento más grande del conjunto suma del conjunto. En este caso 2.

Este paso asegura que las nuevas sumas $2+A_1$ son superiores a cualquier elemento perteneciente a $A_1 + A_1$, ya que la suma más pequeña formada es $1 + 2 > 2$ el elemento más grande del conjunto $A_1 + A_1$.

Tercer paso. Llame $A_2 = \{2\} \bigcup A_1$ el nuevo conjunto de Sidon.

Continue el proceso realizando el paso dos y tres para obtener un conjunto de Sidon de tamaño n para cualquier n natural. Los elementos agregados son claramente potencias de 2.

■

Esta construcción muestra la existencia de conjuntos de Sidon infinitos si se toma el límite de n cuando tiende a infinito.

Ejemplo 2. El conjunto de los números primos es un conjunto de Sidon infinito en el grupo $(\mathbb{Q}^*, \times)$.

Ejemplo 3. El conjunto

$$\{0, 5, 15, 34, 35, 42, 73, 75, 86, 89, 98, , 134, 151, 155, 177, 183, 201\}$$

es un conjunto de Sidon módulo 273.

Cuando G es un conjunto finito, el problema fundamental sobre conjuntos de Sidon consiste en investigar la función

$$S(G) := \text{máx}\{|A| : A \text{ es Sidon en } G\},$$

donde $|A|$ denota el cadinal del conjunto A. En particular, investigar y decidir sobre la existencia del límite

$$\lim_{|G|\longrightarrow\infty} \frac{S(G)}{\sqrt{|G|}}.$$

Cuando G es el grupo de los enteros, la función a investigar es

$$S(n) := \text{máx}\{|A| : A \subseteq [1,n] \wedge A \in B_2\},$$

donde B_2 denota a la familia de todos los conjuntos de Sidon, y $[1,n] := \{1,2,...,n\}$ es el intervalo entero de 1 a n.

Sin embargo, se sabe que

$$\lim_{n\longrightarrow\infty} \frac{S(n)}{\sqrt{n}} = 1.$$

Los conjuntos de Sidon usan la operación del grupo para definir su propiedad, aún así, en los grupos existen los inversos aditivos, una forma similar a una resta. Con ello se define un nuevo concepto partiendo de la misma propiedad de Sidon.

Definición 2.2 ***(Regla Golomb).*** *A es una regla Golomb en el grupo G si para todo $a,b,c,d \in A$ con $a \neq b, c \neq d$*

$$a - b = c - d \Longrightarrow a = c \wedge b = d.$$

Una forma equivalente a esta propiedad es:
A es una regla Golomb en el grupo G si para todo $x \in G \setminus \{0\}$ la ecuación $x = a - b$ con $a,b \in A$ tiene a lo sumo una solución $(a,b) \in A \times A$.

En el contexto entero, las reglas Golomb tienen atributos extra que se definen a continuación.

Definición: El *orden* de una regla Golomb es el número de marcas o elementos que ésta posea, y su *longitud* es la distancia más grande entre un par de marcas de la regla.

Definición: Una regla Golomb es *óptima* si no existe otra regla Golomb del mismo orden con longitud menor.

El número máximo de marcas que posee una regla Golomb óptima de longitud n es asintóticamente igual a $\sqrt{n}$ [1].

De acuerdo con este criterio se buscan reglas Golomb con un número de marcas relativamente cercano a la raíz cuadrada de su longitud.

Una regla Golomb de longitud n es *asintóticamente óptima* si el número de marcas que posee es asintóticamente igual a $\sqrt{n}$; mientras que para un número real positivo α, la regla es *α-cercanamente óptima* si el número de marcas que posee es asintóticamente igual a $\alpha\sqrt{n}$.

El problema fundamental en las reglas Golomb cuando $G = \mathbb{Z}$ es el siguiente.
Dado el número de marcas, determinar la regla Golomb con longitud más corta, es decir se trata de estudiar la función

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

Proposición 2.1 *La cota superior trivial para las reglas Golomb de orden m y longitud n en $\mathbb{Z}$ está dada por*

$$m < \sqrt{2n} + 1.$$

Demostración.

Cualquier regla Golomb de longitud n define a lo más n posibles distancias, y si ésta tiene m marcas, entonces las $\frac{m(m-1)}{2}$ distancias que éstas definen deben ser únicas. Así que

$$\frac{(m-1)^2}{2} < \frac{m(m-1)}{2} \leq n$$

$$(m-1)^2 < 2n$$

$$m - 1 < \sqrt{2n}$$

$$m < \sqrt{2n} + 1.$$

■

Los conceptos de conjunto de Sidon en G y regla Golomb en G son equivalentes.

Lema 2.1 *A es un conjunto de Sidon en G si y sólo si A es una regla Golomb en G.*

Demostración.

Sean $A \subseteq G$ una regla Golomb y G un grupo conmutativo notado aditivamente. Suponga que $a, b, c, d \in A$.

Si $a + b = c + d$ y $a \neq c \ \wedge d \neq b$, entonces

$$a - c = d - b \text{ con } a \neq c \ \wedge d \neq b.$$

Como A es una regla golomb se obtiene que $a = d \ \wedge c = b$.

Luego,

$$\{a, b\} = \{c, d\},$$

por tanto A es un conjunto de Sidon en G.

Suponga ahora que A es un conjunto de Sidon en G y que $a, b, c, d \in A$.

Si $a - b = c - d$, con $a \neq b \ \wedge c \neq d$, entonces $a + d = c + b$.

De donde

$$\{a, d\} = \{c, b\},$$

pero como $a \neq b \ \wedge c \neq d$, entonces $a = c \ \wedge b = d$, luego A es una regla Golomb en G.

■

Ejemplo 4. Como los conjuntos de Sidon y las reglas Golomb son equivalentes, el ejemplo 3 sirve de referencia como una regla Golomb.

Definición 2.3 ***(Regla Golomb modular).*** *Sea A un subconjunto de $\mathbb{Z}$ y $N \in \mathbb{Z}^+, N > 1$. A es una regla Golomb módulo N (en el grupo $\mathbb{Z}_n$) si para todo $a, b, c, d \in A$, con $a \neq b, c \neq d$*

$$a - b \equiv c - d \pmod{N} \Longrightarrow a = c \wedge b = d.$$

Nota. Como la propiedad de estos conjuntos involucra solamente adiciones o diferencias, las traslaciones y las reflexiones mantienen la propiedad.

Proposición 2.2 *A es una regla Golomb modular si y sólo si A es una regla Golomb finita.*

Demostración.

Sean A una regla Golomb finita (es decir que posee un número finito de elementos), y N la distancia más grande; defina $M = 2N + 1$.

A es una regla Golomb módulo M. En efecto, si $a, b, c, d \in A$ y $a \neq b$ y $c \neq d$ y $a - b \equiv c - d \pmod{M}$, entonces

$$(a - b) - (c - d) = k(2N + 1) \text{ con } k \in \mathbb{Z}.$$

Pero $-2N \leq (a - b) - (c - d) \leq 2N$, luego

$$-2N - 1 < (a - b) - (c - d) < 2N + 1,$$

por consiguiente

$$k = 0 \ \wedge \ a - b = c - d.$$

Como A es regla Golomb entonces

$$a = c \wedge b = d.$$

El caso inverso es inmediato de la definición.

■

En casos especiales cuando el grupo G es producto de dos grupos, los conjuntos de Sidon se llaman conjuntos de Sidon en dos dimensiones. Ahora, se desea darle una estructura funcional al conjunto bi-dimensional, así al restringir al conjunto se obtiene un objeto especial: Los arreglos Costas.

Un **Arreglo Costas** de orden n se refiere geométricamente al conjunto de n puntos (parejas) sobre la malla $n \times n$ ubicados de tal forma que en cada fila y en cada columna hay un solo punto y los $n(n-1)$ vectores que se forman entre cada par de puntos son todos distintos [7].

Definición 2.4 ***(Arreglo Costas).*** *Una biyección $f : [1,n] \longrightarrow [1,n]$ es un arreglo Costas (Permutación Costas) de orden n si para todo i, j, k tales que $1 \leq i, j, i+k, j+k \leq n$,*

$$(f(i+k) - f(i) = f(j+k) - f(j)) \Longrightarrow (i = j \ \vee \ k = 0).$$

Nota. Esta implicación se suele llamar *la propiedad de diferencias distintas.*

A continuación se muestra una prueba de relación entre los arreglos Costas con los conjuntos de Sidon.

Proposición 2.3 *Los arreglos Costas son conjuntos de Sidon en dos dimensiones.*

Demostración.

Sea una biyección $f : [1,n] \longrightarrow [1,n]$ un arreglo Costas. El grafo de esta función

$$\mathfrak{g}_f = \{(i, f(i)) : i \in [1,n]\},$$

es un conjunto de Sidon en dos dimensiones.

En efecto, sean $i, j, k, l \in [1,n]$. Suponga que

$$(i, f(i)) + (j, f(j)) = (k, f(k)) + (l, f(l)),$$

se sigue

$$i + j = k + l$$

$$i - k = l - j.$$

Defina $h := i - k$, así se obtiene $i = h + k$ y $l = h + j$. Por otra parte,

$$f(i) + f(j) = f(k) + f(l)$$

$$f(i) - f(k) = f(l) - f(j)$$

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

de donde $h = 0$ o $k = j$, luego

$$\{i, j\} = \{k, l\}$$

$$\{(i, f(i)), (j, f(j))\} = \{(k, f(k)), (l, f(l))\}.$$

■

Aquí, el problema fundamental consiste en probar o refutar la existencia de un arreglo Costas de orden n para todo entero positivo n. Se desconocen construcciones que generen arreglos Costas de orden 32 y 33, éstos son los valores mínimos para los cuales no se sabe si existen o no arreglos Costas de tal orden [7].

Otra representación de los arreglos Costas se presenta como un arreglo matricial $[a_{ij}]_{i,j=1}^{n}$ de tamaño $n \times n$ tal que:

$$a_{ij} = \begin{cases} 1, & \text{si } j = f(i); \\ 0, & \text{en caso contrario.} \end{cases}$$

En esta perspectiva, se espera que de las $n!$ permutaciones de la matriz identidad de tamaño $n \times n$, exista al menos un arreglo Costas, sin embargo se tiene este resultado.

Proposición 2.4

$$\lim_{n \longrightarrow \infty} \frac{\mathfrak{C}(n)}{n!} = 0$$

donde $\mathfrak{C}(n)$ es el número total de arreglos Costas de orden n [3].

Nota. La Proposición 4 aclara que la densidad de los arreglos Costas tiende a cero, es decir, si se escoge una matriz permutación de la identidad de tamaño $n \times n$ de manera aleatoria la probabilidad de haber escogido un arreglo Costas es casi nula.

Ejemplo 5. Considere la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 6 & 3 \end{pmatrix}$$

Esta permutación define un arreglo Costas, se puede verificar que los 15 vectores diferencia asociados son todos distintos. También se puede ver como un arreglo matricial de 1's y 0's como sigue

$$\begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 \end{pmatrix}$$

En esta matriz, los 1's determinan las marcas y los 0's los vacíos. También puede ser representada como el conjunto de puntos en la malla $n \times n$:

	1	**2**	**3**	**4**	**5**	**6**
1	•					
2		•				
3						•
4				•		
5			•			
6					•	

Figura 1: Arreglo Costas de orden 6

Una extensión de los arreglos Costas son las secuencias sonares que se define a continuación.

Definición 2.5 ***(Secuencia sonar).*** *Una secuencia sonar de tamaño $m \times n$ es una función $f : [1, n] \longrightarrow [1, m]$ tal que para todo i, j, k tales que $1 \leq i, j, i + k, j + k \leq n$, se satisface*

$$(f(i + k) - f(i) = f(j + k) - f(j)) \Longrightarrow (i = j \ \vee \ k = 0).$$

Observe que este arreglo es rectangular, con mucha más libertad que los arreglos Costas. En el caso particular que la función sea biyectiva y el arreglo sea cuadrado se obtienen: Un arreglo Costas y una secuencia sonar.

El problema fundamental en las secuencias sonares es el siguiente.
"Para un m fijo, encontrar el n más grande para el cual existe una secuencia sonar de tamaño $m \times n$".

Ejemplo 6. Sea $f : [1, 5] \longrightarrow [1, 6]$ definida por:
$f(1) = 1 = f(5)$, $f(2) = 3 = f(4)$ y $f(3) = 6$, se puede denotar en forma funcional como

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 6 & 3 & 1 \end{bmatrix}$$

o como una secuencia (1 3 6 3 1); o como un arreglo de puntos en la malla $[1, 5] \times [1, 6]$:

	1	**2**	**3**	**4**	**5**
1	•				•
2					
3		•		•	
4					
5					
6			•		

Figura 2: Secuencia sonar 6×5

Los 10 vectores diferencia asociados con los pares de puntos son todos distintos. Por lo tanto f es una secuencia sonar 6×5.

Una *secuencia sonar modular* de tamaño $m \times n$ es una función
$f : [1, n] \longrightarrow [1, m]$ tal que para todo i, j, k con $1 \leq i, j, i + k, j + k \leq n$

$$f(i + k) - f(i) \equiv f(j + k) - f(j) \pmod{m} \Longrightarrow (i = j \ \vee \ k = 0).$$

2.2. Transformaciones elementales

Para todos estos arreglos existen algunas operaciones o transformaciones que se aplican a ellos o entre ellos para formar nuevos arreglos de la misma clase.

Transformaciones para conjuntos de Sidon/reglas Golomb.

Propiedad 1. Sea $B \subseteq A$. Si A es una regla Golomb entonces B también es una regla Golomb. Para construir una regla golomb con cualquier número de marcas $m \in \mathbb{N}$, se construye primero una regla Golomb con a marcas, $a \in \mathbb{N}$, tal que $a > m$. Con ello, se trunca la regla, es decir se remueven las $a - m$ marcas para obtener m marcas [1].

¿Cómo se puede construir una regla Golomb (razonablemente densa) con un número de marcas arbitrarias?

Propiedad 2. Sea $m \in \mathbb{N}$. $m = a_1 \cdot \cdots a_l$, donde las a_i son potencias primas para todo $i = 1, 2, ..., l$. Con ello, se construyen l reglas Golomb con a_i marcas cada una, así se combinan todas para formar una regla Golomb con m marcas como sigue [1].

Proposición 2.5 *Sean* $f_i : [0, m_i - 1] \longrightarrow [0, n_i]$ *reglas Golomb módulo* N_i *para todo* $i = 1, 2, ..., l$, *tales que* $mcd(N_i, N_j) = 1$ *para todo* $1 \leq i < j \leq l$. *Entonces el conjunto*

$$C := \left\{ N \sum_{i=1}^{l} \frac{f_i(x_i)}{N_i} : x_i \in [0, m_i - 1], i \in [1, l] \right\},$$

con $N := \prod_{i=1}^{l} N_i$, *forma una regla Golomb con* $m := \prod_{i=1}^{l} m_i$ *marcas y longitud* $n := N \sum_{i=1}^{l} \frac{n_i}{N_i}$.

Demostración.

Considere la siguiente ecuación

$$N \sum_{i=1}^{l} \frac{f_i(x_i)}{N_i} - N \sum_{i=1}^{l} \frac{f_i(y_i)}{N_i} = a, \tag{2.1}$$

con $a \in \mathbb{N}$. Se debe probar que (2.1) tiene a lo más una solución.
Module la ecuación (2.1) por $\pmod{N_i}$, para todo $i \in [1, l]$, así se obtienen las ecuaciones

$$\frac{N}{N_i} f_i(x_i) - \frac{N}{N_i} f_i(y_i) \equiv a \pmod{N_i}. \tag{2.2}$$

Note que $\text{mcd}(\frac{N}{N_i}, N_i) = 1$, luego $\frac{N}{N_i}$ tiene inversa $\pmod{N_i}$, así se obtiene

$$\frac{N}{N_i}(f_i(x_i) - f_i(y_i)) \equiv a \pmod{N_i}$$
$$f_i(x_i) - f_i(y_i) \equiv \frac{N_i}{N} a \pmod{N_i}.$$

Como f_i es una regla Golomb módulo N_i la ecuación anterior tiene como máximo una solución. Luego la ecuación (2.1) tiene como máximo una solución dado $a \in \mathbb{N}$.

Con esto C es una regla Golomb; en particular si $a = 0$ entonces $x_i = y_i$ para todo $i \in [1, l]$, así C tiene m distintos elementos, desde 0 hasta n.

■

Transformaciones para arreglos Costas.

Proposición 2.6 *Si $P = (f(1) \cdots f(n))$ es una permutación correspondiente a un arreglo Costas con $n \in \mathbb{Z}^+, n > 1$, entonces para cada s, t tales que $1 \leq s < t \leq n$, la sección $P' = (f(s) \cdots f(t))$ conserva la propiedad de diferencias distintas. Si además los números en P' son enteros consecutivos, como se sigue*

$$\{f(i) : i = s, s+1, ..., t\} = \{a, a+1, ..., a+t-s\},$$

para algún $a \in \mathbb{N}$, entonces la permutación

$$P'' = ([f(s) - a + 1] \cdots [f(t) - a + 1]),$$

representa un arreglo Costas de orden $t - s + 1$ [2].

Lema 2.2 *Si un arreglo Costas de orden n visto matricialmente tiene un 1 en cualquiera de sus cuatro esquinas, las correspondientes filas y columnas pueden ser removidas para obtener un arreglo Costas de orden* $n-1$.

Demostración.

Cualquier violación de las condiciones de los arreglos Costas en la patente reducida presentaría en principio una violación en la patente original.

■

Comentario. Los arreglos Costas vistos como un arreglo de puntos y vacíos no es afectado bajo traslaciones horizontales, verticales y alrededor de la diagonal principal, es decir, no pierde la propiedad de diferencias distintas. Así que cada construcción de arreglos Costas viene en paquetes de 4 arreglos disjuntos en el caso que el arreglo sea simétrico, o de 8 arreglos disjuntos en el caso que el arreglo no sea simétrico [2].

Transformaciones para secuencias sonares.

Proposición 2.7 ***(Transformación al sonar).*** *Si* $f : [1,n] \longrightarrow [1,m]$ *es una secuencia sonar módulo* m*, entonces*

1. *Adicionando* $a \pmod m$, *con* $a \in \mathbb{Z}$, $f_{+a}(i) := f(i) + a \pmod m$ *resulta ser una nueva secuencia sonar módulo* m *correspondiente a una rotación cíclica de las filas del arreglo por* a *unidades. Las filas vacías contiguas son rotadas a la parte superior del sonar y son eliminadas para producir mejores sonares.*

2. *Multiplicando por una unidad* u *módulo* m, $f_{\times u}(i) := uf(i) \pmod m$ *resulta ser una secuencia sonar módulo* m *la cual corresponde a una permutación de las filas del arreglo con la intención de incrementar el número de filas vacías contiguas en el arreglo.*

3. *Agregando un aumento lineal* s *módulo* m, $f_{shear\ s}(i) := f(i) + si \pmod m$ *resulta ser una secuencia sonar modular la cual corresponde a un movimiento de columnas con el mismo fin, producir un número mayor de filas vacías contiguas en el arreglo [8].*

Demostración.

1. Sean $i, j, k, i+k, j+k \in [1,n]$ tales que

$$f_{+a}(i+k) - f_{+a}(i) \equiv f_{+a}(j+k) - f_{+a}(j) \pmod{m}.$$

Se sigue que

$$f(i+k) + a - f(i) - a \equiv f(j+k) + a - f(j) - a \pmod{m}$$

$$f(i+k) - f(i) \equiv f(j+k) - f(j) \pmod{m},$$

con lo cual se obtiene que $i = j$.

2. Sean $i, j, k, i+k, j+k \in [1, n]$ tales que

$$f_{\times u}(i+k) - f_{\times u}(i) \equiv f_{\times u}(j+k) - f_{\times u}(j) \pmod{m}.$$

Se sigue que

$$uf(i+k) - uf(i) \equiv uf(j+k) - uf(j) \pmod{m}$$

$$f(i+k) - f(i) \equiv f(j+k) - f(j) \pmod{m},$$

con lo cual se obtiene que $i = j$.

3. Sean $i, j, k, i+k, j+k \in [1, n]$ tales que

$$f_{shear\ s}(i+k) - f_{shear\ s}(i) \equiv f_{shear\ s}(j+k) - f_{shear\ s}(j) \pmod{m}.$$

Se sigue que

$$f(i+k) + s(i+k) - f(i) - si \equiv f(j+k) + s(j+k) - f(j) - sj \pmod{m}$$

$$f(i+k) - f(i) \equiv f(j+k) - f(j) \pmod{m},$$

con lo cual se obtiene que $i = j$.

■

Capítulo 3

Construcciones generales de los conjuntos de Sidon

3.1. Construcciones de reglas Golomb

Esta sección está dedicada a las construcciones conocidas de reglas Golomb [1].

Teorema 3.1 ***(Construcción de Erdös-Turán).*** *Para cada primo p impar, el conjunto*

$$\{2pk + (k^2 \text{ mód } p) : \ k = 0, 1, ..., p-1\},$$

es una regla Golomb, donde k^2 mód p es el menor entero no negativo x tal que $k^2 \equiv x \pmod{p}$.

Demostración.

Sean $x, y \in [0, p-1]$ y $a \in \mathbb{N}$ fijo, tales que

$$2px + (x^2 \text{ mód } p) + 2py + (y^2 \text{ mód } p) = a$$

$$2p(x+y) + (x^2 \text{ mód } p) + (y^2 \text{ mód } p) = a. \tag{3.1}$$

Se debe demostrar que los enteros x y y pueden ser escogidos a lo más de una sola manera.

Divida entre $2p$ la ecuación (3.1)

$$(x+y)+\frac{(x^2 \bmod p)}{2p}+\frac{(y^2 \bmod p)}{2p}=\frac{a}{2p}.$$

Como $(x+y)\in\mathbb{Z}$ y $(x^2 \bmod p),(y^2 \bmod p)<p$, entonces

$$\frac{(x^2 \bmod p)}{2p}<\frac{p}{2p}=\frac{1}{2};\qquad \frac{(y^2 \bmod p)}{2p}<\frac{p}{2p}=\frac{1}{2},$$

así que

$$\frac{(x^2 \bmod p)}{2p}+\frac{(y^2 \bmod p)}{2p}<1,$$

y por tanto

$$\left\lfloor (x+y)+\frac{(x^2 \bmod p)}{2p}+\frac{(y^2 \bmod p)}{2p}\right\rfloor=\left\lfloor\frac{a}{2p}\right\rfloor,$$

de donde

$$x+y=\left\lfloor\frac{a}{2p}\right\rfloor.$$

Sea $A:=\left\lfloor\frac{a}{2p}\right\rfloor$. De la ecuación (3.1) se tiene

$$x^2+y^2\equiv a \pmod p$$

$$(x+y)^2-2xy\equiv a \pmod p$$

$$\frac{1}{2}[(x+y)^2-a]\equiv xy \pmod p,$$

dado que p es impar, $\mathrm{mcd}(2,p)=1$ y así 2 tiene inverso multiplicativo módulo p.

Como $x+y=A$, $B:=\frac{1}{2}[A^2-a]=\frac{1}{2}[(x+y)^2-a]$, es una constante.

Dado que

$$x+y\equiv A \pmod p$$

$$xy\equiv B \pmod p,$$

multiplique por x y y a la primera congruencia.

$$x^2 + xy \equiv Ax \pmod{p} \quad \text{y} \quad y^2 + xy \equiv Ay \pmod{p}.$$

De aquí se obtiene

$$x^2 - Ax + B \equiv 0 \pmod{p} \quad \text{y} \quad y^2 - Ay + B \equiv 0 \pmod{p}.$$

En otras palabras, el polinomio $f(z) := z^2 - Az + B \in \mathbb{F}_p[Z]$ tiene como raíces a x y a y. Sin embargo $f(z)$ es un polinomio de grado 2, así que o es irreducible o se factoriza por 2 productos lineales, es decir tiene dos raíces.

Por lo tanto, para todo $a \in \mathbb{N}$ si existen $x, y \in [0, p-1]$ que satisfacen (3.1), son únicos, luego el conjunto es una regla Golomb.

■

Comentario. El conjunto definido en el Teorema 3.1 posee p elementos, la ubicación de la marca mínima es en 0, cuando $k = 0$; y la ubicación de la marca máxima es menor a $2p^2$, puesto que

$$2pk + (k^2 \bmod p) \leq 2p^2 - 2p + p - 1 = 2p^2 - p - 1,$$

así la longitud de esta regla es menor a $2p^2$, luego la regla generada en el Teorema 3.1 es $\sqrt{2}$-cercanamente óptima.

Teorema 3.2 ***(Construcción de Apostolos)***. *Sean n un entero positivo y $c \in \{1, 2\}$ fijo. El conjunto*

$$\{cnk^2 + k, \text{ con } k \in [0, n-1]\},$$

es una regla Golomb.

Demostración.

Sean $c = 2$; $x, y \in [0, n-1]$ tales que

$$2n(x^2 + y^2) + (x + y) = a. \tag{3.2}$$

Divida por $2n$.

$$x^2 + y^2 + \frac{x+y}{2n} = \frac{a}{2n}$$

$$\left\lfloor x^2 + y^2 + \frac{x+y}{2n} \right\rfloor = \left\lfloor \frac{a}{2n} \right\rfloor.$$

Como $x, y \in [0, n-1]$ entonces $0 \leq \frac{x+y}{2n} < 1$, luego

$$\left\lfloor x^2 + y^2 + \frac{x+y}{2n} \right\rfloor = x^2 + y^2 = \left\lfloor \frac{a}{2n} \right\rfloor,$$

sustituyendo lo anterior en (3.2) se obtiene

$$2n \left\lfloor \frac{a}{2n} \right\rfloor + (x+y) = a$$

De donde

$$x + y = a - 2n \left\lfloor \frac{a}{2n} \right\rfloor := A.$$

Observe que

$$xy = \frac{1}{2}[(x+y)^2 - (x^2+y^2)] = \frac{1}{2}\left[A^2 - \left\lfloor \frac{a}{2n} \right\rfloor\right].$$

Por tanto el conjunto $\{x, y\}$ son raíces de un polinomio de grado 2 en $\mathbb{Z}[X]$, que están determinadas a lo más de una manera posible, se sigue que el conjunto es una regla Golomb.

Para el caso $c = 1$ suponga que

$$a = n(x^2 - y^2) + (x - y) \text{ con } x \geq y;\ x, y \in [0, n-1]. \tag{3.3}$$

Como $0 \leq x - y \leq n$ se sigue

$$\left\lfloor \frac{a}{n} \right\rfloor = \left\lfloor x^2 - y^2 + \frac{x-y}{n} \right\rfloor = x^2 - y^2.$$

Reemplazando en (3.3)

$$a = n \left\lfloor \frac{a}{n} \right\rfloor + (x - y)$$

$$x - y = a - n \left\lfloor \frac{a}{n} \right\rfloor := A.$$

Note que

$$x + y = \frac{x^2 - y^2}{x - y} = \frac{\left\lfloor \frac{a}{n} \right\rfloor}{A}.$$

De estas últimas tengo un sistema lineal, de lo cual se definen los únicos valores de x, y.

■

Nota. Este teorema no induce una regla Golomb óptima, mas bien, produce reglas Golomb de todos los ordenes con longitudes bastante largas.

Teorema 3.3 ***(Construcción de Ruzsa-Lindström).*** *Sean p un primo, g un elemento primitivo de $\mathbb{F}_p$ y s un entero primo relativo con $p-1$. El conjunto*

$$\{(psk + (p-1)g^k) \text{ mód } p(p-1) : \ k = 0, 1, ..., p-2\},$$

es una regla Golomb.

Demostración.

Sean $a \in \mathbb{N}$ fijo y $x, y \in [0, p-2]$ tales que

$$(psx + (p-1)g^x) \text{ mód } p(p-1) + (psy + (p-1)g^y) \text{ mód } p(p-1) = a. \quad (3.4)$$

Tome módulo p en ambos lados

$$(p-1)g^x + (p-1)g^y \equiv a \pmod{p}$$

$$g^x + g^y \equiv -a \pmod{p}. \quad (3.5)$$

Tome módulo $p-1$ en ambos lados de la ecuación (3.4)

$$psx + psy \equiv a \pmod{p-1}$$

$$p(s(x+y)) \equiv a \pmod{p-1}.$$

Dado que $p \equiv 1 \pmod{p-1}$, se sigue que

$$s(x+y) \equiv a \pmod{p-1}$$

$$x + y \equiv s^{-1}a \pmod{p-1}.$$

Luego $(p-1)|(x+y-s^{-1}a)$, esto es, existe $k \in \mathbb{Z}$ tal que

$$x + y = s^{-1}a + k(p-1),$$

$$g^{x+y} = g^{s^{-1}a}(g^{(p-1)})^k,$$

donde g es elemento primitivo de $\mathbb{F}_p$.
Así

$$g^x g^y \equiv g^{s^{-1}a} \pmod{p}. \tag{3.6}$$

De (3.5) y (3.6), se construye un polinomio de grado 2 en el campo $\mathbb{F}_p[X]$ el cual tiene únicamente dos raíces, a saber: g^x y g^y, que están unívocamente relacionadas con x, y por ser g elemento primitivo; luego el conjunto obtenido es una regla Golomb.

■

Comentario. En este caso, la marca mínima es mayor o igual a 0, mientras que la marca máxima es menor o igual a $p(p-1)$, y así la distancia más lejana posible es $p(p-1)$. Dado que el número de marcas que tiene esta regla es $p-1$ se obtiene una construcción asintóticamente óptima.

Teorema 3.4 ***(Construcción de Bose-Chowla).*** *Sean $q = p^n$ una potencia prima y g un elemento primitivo de $\mathbb{F}_{q^2}$, entonces los q enteros en el conjunto*

$$S = \{i \in [1, q^2 - 2] : g^i - g \in \mathbb{F}_q\},$$

tienen todas sus diferencias, dos a dos, distintas módulo $q^2 - 1$. Además, el conjunto de los $q(q-1)$ diferencias de dos elementos distintos en S, reducidas (mód $q^2 - 1$)*, es igual al conjunto de todos los enteros no negativos menores que $q^2 - 1$ que no son divisibles por $q + 1$.*

Demostración.

Sean $x_i \in S$, con $i = 1, 2, 3, 4$. Suponga que $x_1 + x_2 = x_3 + x_4$.

Luego en $\mathbb{F}_{q^2}$

$$g^{x_1+x_2} = g^{x_3+x_4}$$

$$g^{x_1} g^{x_2} = g^{x_3} g^{x_4}. \tag{3.7}$$

Como $x_i \in S$ entonces $g^{x_i} - g \in \mathbb{F}_q$, consecuentemente existen $u_i \in \mathbb{F}_q$ tales que

$$g^{x_i} - g = u_i,$$

$$g^{x_i} = u_i + g. \tag{3.8}$$

Reemplazando (3.8) en (3.7) se obtiene

$$(g + u_1)(g + u_2) = (g + u_3)(g + u_4),$$

$$g^2 + gu_2 + u_1 g + u_1 u_2 = g^2 + gu_4 + gu_3 + u_3 u_4$$

$$g(u_2 + u_1 - u_3 - u_4) = u_3 u_4 - u_1 u_2. \tag{3.9}$$

Note que si $u_2 + u_1 - u_3 - u_4 \neq 0$, entonces
$g = (u_3 u_4 - u_1 u_2)(u_2 + u_1 - u_3 - u_4)^{-1}$; ya que $\mathbb{F}_q$ es un campo.

Por consiguiente $g \in \mathbb{F}_q$ [no es posible puesto que g es un elemento primitivo de $\mathbb{F}_{q^2}$].

De ese modo

$$u_2 + u_1 - u_3 - u_4 = 0$$

$$u_1 + u_2 = u_3 + u_4. \tag{3.10}$$

Reemplazando (3.10) en (3.9) se obtiene $u_3 u_4 = u_1 u_2$.

En consecuencia

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

$$\{x_1, x_2\} = \{x_3, x_4\},$$

porque los x_i están determinados por los $u_i,\ i \in \{1, 2, 3, 4\}$. Con esto queda probado que S es una regla Golomb.

Resta probar que el conjunto diferencia es el conjunto de todos los enteros no negativos menores que $q^2 - 1$ que no son divisibles por $q + 1$.

Usando la notación:

$$g^{x_1 - x_2} = \frac{g^{x_1}}{g^{x_2}} = \frac{g + u_1}{g + u_2} \text{ con } x_1, x_2 \in S,\ u_1, u_2 \in \mathbb{F}_q;$$

si $g^{x_1 - x_2} \in \mathbb{F}_q$, existe $u \in \mathbb{F}_q$ tal que $u = g^{x_1 - x_2}$. Observe que

$$u = \frac{g + u_1}{g + u_2} \Longleftrightarrow ug + uu_2 = g + u_1$$

$$\iff g(u-1) = u_1 - uu_2.$$

Si $u-1 \neq 0$ entonces $g = (u-1)^{-1}(u_1 - uu_2)$, de lo cual $g \in \mathbb{F}_q$(no es posible).

Luego $u-1=0$, esto es $u=1$ y $g^{x_1-x_2}=1$.

En consecuencia, se tiene que $x_1 - x_2 = k(q^2-1)$, para algún $k \in \mathbb{Z}$. Pero $x_1, x_2 \in [1, q^2-2]$, así que: $-(q^2-2) \leq x_1 - x_2 \leq q^2-2$; luego $k=0$ y $x_1 = x_2$.

Con esto $g^{x_1-x_2} \notin \mathbb{F}_q$ para todo $x_1, x_2 \in S$ con $x_1 \neq x_2$.

Note que $g^i \in \mathbb{F}_q \iff (q+1)|i$. De esto se sigue que $q+1$ no puede dividir a $x_1 - x_2$.

Además si $x_1 + x_2 \equiv x_3 + x_4 \pmod{q^2-1}$ con $x_1, x_2, x_3, x_4 \in S$,

entonces

$$(x_1 + x_2) - (x_3 + x_4) = (q^2-1)d \text{ para algún } d \in \mathbb{Z}.$$

Luego $g^{(x_1+x_2)-(x_3+x_4)} = (g^{q^2-1})^d = 1$.

De donde

$$\frac{g^{(x_1+x_2)}}{g^{(x_3+x_4)}} = 1$$
$$g^{x_1+x_2} = g^{x_3+x_4}.$$

Siguiendo el argumento anterior se concluye que

$$\{x_1, x_2\} = \{x_3, x_4\}.$$

Es decir, S es una regla Golomb módulo q^2-1.

Con esto, todas las $q(q-1)$ diferencias 2 a 2 de elementos de S reducidas (mód q^2-1) son distintas. Al reorganizar el número q^2-1 se obtiene

$$q^2 - 1 = q(q-1) + q - 1,$$

donde q^2-1 denota el número total de los elementos de $\mathbb{Z}_{q^2-1}$, $q(q-1)$ las diferencias formadas por el conjunto S que son todas distintas y $q-1$ el número total de múltiplos de $q+1$.

■

Comentario. En la literatura, este método es referido como la construcción del plano afín de una regla Golomb.

Si se define

$$S \ominus S := \{s_1 - s_2 : s_1, s_2 \in S,\ s_1 \neq s_2\},$$

entonces el conjunto $S \ominus S$ que indica el Teorema 3.4 se puede escribir de la siguiente manera:

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

con $M_{q+1} = \{0, q+1, 2(q+1), ..., (q-2)(q-1)\}$.

Note un dato importante sobre esta construcción.
$S \subseteq [1, q^2-2] \subseteq [0, q^2]$ por lo tanto $S \subseteq [0, q^2]$. Como la longitud más grande de $[0, q^2]$ es q^2 se concluye que la longitud de S es menor o igual a q^2, y como posee exactamente q elementos, esta construcción genera una regla Golomb asintóticamente óptima.

Teorema 3.5 ***(Construcción de Singer).*** *Sea $q = p^n$ una potencia prima. Existen $q+1$ enteros $\{d_i : i = 0, ..., q\}$ tales que las q^2+q diferencias $d_i - d_j,\ i, j = 0, ..., q,\ i \neq j$ son todas distintas. En particular éstas coinciden con los enteros no cero módulo q^2+q+1 cuando se reducen módulo q^2+q+1.*

Nota. La demostración original de este teorema usa geometría proyectiva, tema que está fuera del alcance de este trabajo. Sin embargo existe una forma más elocuente de presentar este teorema que se presentará en el siguiente capítulo.

Teorema 3.6 ***(Lindström).*** *Sean $q = p^n$ una potencia prima y g un elemento primitivo de $\mathbb{F}_{q^2}$. El conjunto*

$$S = \{i \in [1, q^2-2] : g^i + g^{qi} = 1\},$$

contiene exactamente q enteros los cuales tienen distintas distancias dos a dos módulo $q^2 - 1$.

Demostración.

Sean $m, n, u, v \in S$ tales que $m + n \equiv u + v \pmod{q^2 - 1}$.
Luego existe $k \in \mathbb{Z}$ tal que

$$\begin{aligned} m + n - (u + v) &= (q^2 - 1)k \\ g^{m+n-(u+v)} &= (g^{(q^2-1)})^k \\ g^{m+n-(u+v)} &= 1 \\ g^{m+n} &= g^{u+v}. \end{aligned} \tag{3.11}$$

Por hipótesis: $g^m + g^{qm} = 1 = g^n + g^{qn} = g^u + g^{qu} = g^v + g^{qv}$.
Luego,

$$(g^m + g^{qm})(g^n + g^{qn}) = (g^u + g^{qu})(g^v + g^{qv})$$

$$g^m g^{qn} + g^{qm} g^n = g^u g^{qv} + g^{qu} g^v,$$

pero $g^{qi} = 1 - g^i$ para $i = n, m, u, v$. Así se obtiene

$$g^m + g^n = g^u + g^v. \tag{3.12}$$

De (3.11) y (3.12) se concluye que $\{g^u, g^v\} = \{g^m, g^n\}$, y así

$$\{u, v\} = \{m, n\},$$

por tanto, el conjunto S es una regla Golomb.

Ahora se debe probar que la ecuación

$$x^q + x = 1; x \in \mathbb{F}_{q^2}. \tag{3.13}$$

tiene exactamente q raíces.

Se necesita demostrar primero que $T : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2}$ con $T(x) = x^q + x$; $x \in \mathbb{F}_{q^2}$ (la función traza) es una función lineal en el espacio vectorial $\mathbb{F}_{q^2}$ sobre el campo $\mathbb{F}_q$.

En efecto, sean $x, y \in \mathbb{F}_{q^2}, a, b \in \mathbb{F}_q$.

$$\begin{aligned} T(ax+by) &= (ax+by)^q + (ax+by) \\ &= a^q x^q + b^q y^q + ax + by \\ &= a(x^q + x) + b(y^q + y) \\ &= aT(x) + bT(y). \end{aligned}$$

Así queda probado que T es lineal. Luego el núcleo y la imagen de T son subespacios de $\mathbb{F}_{q^2}$.

Observe cuántos elementos tiene el núcleo de T.

Sea $z \in KerT \setminus \{0\}$, se tiene que $z^q = -z$.

En $\mathbb{F}_p$ cuando $p = 2$, se cumple que $z = -z$, de donde $z^q = z$, consecuentemente $z^{q-1} = 1$. Esto indica que $z \in \mathbb{F}_q$; se ve claramente que la recíproca también es cierta, es decir, si $z \in \mathbb{F}_q$ entonces $z \in KerT$.

Cuando $p > 2$, $z^q = -z \Longrightarrow (z^2)^q = z^2$.

De nuevo $z^2 \in \mathbb{F}_q$, porque z^2 es raíz del polinomio $x^q - x$, el cual es el polinomio de descomposición de $\mathbb{F}_q$. También se concluye que $z \notin \mathbb{F}_q$ porque no es raíz del polinomio $x^q - x$. Con esto, basta escoger todos los $w \in \mathbb{F}_{q^2}$ tales que $w^2 \in \mathbb{F}_q$ y $w \notin \mathbb{F}_q$, para que el $KerT$ coincida con el conjunto

$$\{0\} \cup \{w \in \mathbb{F}_{q^2} : w^2 \in \mathbb{F}_q, w \notin \mathbb{F}_q\} = KerT.$$

¿Cuántos elementos tiene el conjunto $\{w \in \mathbb{F}_{q^2} : w^2 \in \mathbb{F}_q, w \notin \mathbb{F}_q\}$?

Note que $< g^{q+1} >= \mathbb{F}_q^*$, donde $< g^{q+1} >$ denota el grupo cíclico generado por el elemento g^{q+1}. Como p es impar entonces q también lo es, consecuentemente $q + 1$ es par.

Además $\{g^{\frac{(2n+1)(q+1)}{2}} : n = 0, 1, 2, ..., q-2\} = \{w \in \mathbb{F}_{q^2} : w^2 \in \mathbb{F}_q, w \notin \mathbb{F}_q\}$.

Se obtiene que $|\{g^{\frac{(2n+1)(q+1)}{2}} : n = 0, 1, 2, ..., q-2\}| = q - 1$, luego $|KerT| = q$.

En ambos casos $|KerT| = q$, y como $KerT$ es un subespacio sobre $\mathbb{F}_{q^2}$ tiene al menos una base, pero como su cardinal es q debe ser generado sólo por un elemento, esto es, $\dim(KerT) = 1$.

Como $|\mathbb{F}_{q^2}| = q^2$; $\dim(\mathbb{F}_{q^2}) = 2$ sobre $\mathbb{F}_q$, entonces por Teorema de la dimensión, $\dim(ImT) = 1$ lo cual es equivalente a que $|ImT| = q$.

Note una peculiaridad, si existe $q \in \mathbb{F}_{q^2}$ tal que $T(q) = 1$ entonces para todo $a \in KerT$ se tiene

$T(q + a) = T(q) + T(a) = 1 + 0 = 1$ con el cual se tendría q raíces de (3.13).

Observe que

$$[T(x)]^q = (x^q + x)^q = x^{q^2} + x^q = x^q + x = T(x) \text{ para todo } x \in \mathbb{F}_{q^2}.$$

Luego $T(x) \in \mathbb{F}_q$, pero $|ImT| = q$, así se obtiene que $ImT = \mathbb{F}_q$. Con ello se concluye que existe un $x \in \mathbb{F}_{q^2}$ tal que $T(x) = 1$.

■

El argumento para este teorema es similar al Teorema 3.4, es un conjunto que posee q elementos y su longitud es como máximo $q^2 - 3$, con lo cual estipula que la construcción es asintóticamente óptima.

Teorema 3.7 ***(Construcción de Golomb, generalización de Bose).*** *Sean $q = p^n$ una potencia prima, g un elemento primitivo de $\mathbb{F}_{q^2}$, $h \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ y $a \in \mathbb{F}_{q^2}^*$, entonces el conjunto*

$$S_{a,h} = \{i \in [0, q^2 - 2] : ag^i + h \in \mathbb{F}_q\},$$

tiene q elementos, y es una regla Golomb módulo $q^2 - 1$; de hecho es un cambio cíclico de la construcción de Bose-Chowla.

Demostración.

Como $\mathbb{F}_q$ tiene q elementos distintos y $h \notin \mathbb{F}_q$ se tiene que el conjunto $K := \{b - h;\ b \in \mathbb{F}_q\}$ tiene q elementos.

Dado que $\mathbb{F}_q^*$ es cíclico, es generado por g, al igual que ag. Así, todo elemento de K tiene una representación como sigue

$$ag^j = b - h \text{ para algún } j \in [0, q^2 - 2]$$

$$ag^j + h = b$$

Esto es, $ag^j + h \in \mathbb{F}_q$ para algunos $j \in [0, q^2 - 2]$. Luego $S_{a,h}$ tiene q elementos.

Se debe probar que $S_{a,h}$ es Sidon.

Sean $i_k \in S_{a,h}; k \in [1, 4]$ tales que $i_1 + i_2 = i_3 + i_4$.

Se sigue que

$$a^2 g^{i_1+i_2} = a^2 g^{i_3+i_4}.$$

Existen $u_k \in \mathbb{F}_q$ tales que $ag^{i_k} + h = u_k$ para $k \in [1, 4]$, luego

$$(u_1 - h)(u_2 - h) = (u_3 - h)(u_4 - h)$$

$$u_1u_2 - h(u_1 + u_2) = u_3u_4 - h(u_3 + u_4)$$

$$h(u_1 + u_2 - u_3 - u_4) = u_1u_2 - u_3u_4.$$

Si $u_1 + u_2 - u_3 - u_4 \neq 0$ se obtiene que $h \in \mathbb{F}_q$ (no es posible), luego

$$u_1 + u_2 = u_3 + u_4 \text{ y } u_1u_2 = u_3u_4.$$

Siguiendo el mismo argumento se obtiene

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

de donde

$$\{i_1, i_2\} = \{i_3, i_4\},$$

Con ello, se concluye la prueba.

¿Cuántos conjuntos $S_{a,h}$ distintos hay?

Sean $i \in S_{a,h},\ h' \in \mathbb{F}_q$ y $t \in \mathbb{F}_q^*$.

$$ag^i + h \in \mathbb{F}_q \text{ para algún } i \in [0, q^2 - 2],$$

$$tag^i + th + h' \in \mathbb{F}_q.$$

Así, $i \in S_{ta,th+h'}$. De manera inversa al proceso se llega a que
Si $j \in S_{ta,th+h'}$ entonces $j \in S_{a,h}$.

Con esto $S_{a,h} = S_{ta,th+h'}$, para todo $h^{'} \in \mathbb{F}_q$ y $t \in \mathbb{F}_q^*$.

Como $h \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ se tiene $q^2 - q$ posibles valores de escogencia para h.
Sea $A_h = \{th + h^{'} : h^{'} \in \mathbb{F}_q \text{ y } t \in \mathbb{F}_q^*\}$ con h fijo.
se debe probar que $|A_h| = q^2 - q$.

Como A_h tiene $q^2 - q$ entradas, basta probar que todos sus elementos son distintos.

Sean $t_1, t_2 \in \mathbb{F}_q^*$ y $h_1^{'}, h_2^{'} \in \mathbb{F}_q$ tales que : $t_1h + h_1^{'}, t_2h + h_2^{'} \in A_h$.
Si $t_1h + h_1^{'} = t_2h + h_2^{'}$ entonces

$$(t_1 - t_2)h = h_2^{'} - h_1^{'},$$

si $t_1 \neq t_2$ entonces $h \in \mathbb{F}_q$ (no es posible) luego $t_1 = t_2$ y $h_1^{'} = h_2^{'}$.

Ahora si $A_h \bigcap \mathbb{F}_q \neq \emptyset$, existen $t_1 \in \mathbb{F}_q^*, h_1^{'} \in \mathbb{F}_q$ tales que

$$t_1h + h_1^{'} \in \mathbb{F}_q$$

$$t_1h \in \mathbb{F}_q$$

$$h \in \mathbb{F}_q \text{ (no es posible)},$$

luego $A_h \bigcap \mathbb{F}_q = \emptyset$, así que, $A_h = \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

En otras palabras, para cualesquiera $h_1, h_2 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ se puede encontrar un t y $h^{'}$ tal que

$$h_2 = th_1 + h^{'}.$$

Consecuentemente, escogiendo $h_2 = -g$ se observa que el conjunto de familias de conjuntos

$\{S_{a,h} : h \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q, a \in \mathbb{F}_q^*\}$ coincide con la familia de conjuntos

$$\{S_{a,-g} : a \in \mathbb{F}_q^*\},$$

aclarando que $S_{a,-g}$ es solo un cambio cíclico de $S_{1,-g}$ mód $q^2 - 1$, la construcción de Bose-Chowla.

■

3.2. Construcciones de arreglos Costas

Las construcciones que se listan a continuación son todas las construcciones que se conocen hasta el momento [5].

Teorema 3.8 ***(Construcción de Welch).*** *Sea g un elemento primitivo de $\mathbb{F}_p$. La matriz $A = (a_{ij})$ de tamaño $(p-1) \times (p-1)$, definida mediante*

$$a_{ij} = \begin{cases} 1, & \text{si } j \equiv g^i \pmod{p} \text{ con } 1 \leq i \leq p-1,\ 1 \leq j \leq p-1; \\ 0, & \text{en caso contrario.} \end{cases}$$

es un arreglo Costas.

Demostración.

Suponga que $g^{i+k} - g^i = g^{j+k} - g^j$ con $1 \leq k \leq p-2$, de donde

$$g^i(g^k - 1) = g^j(g^k - 1).$$

Dado que $1 \leq k \leq p-2$ se tiene que $g^k \neq 1 \pmod{p}$. Luego $g^k - 1 \neq 0 \pmod{p}$, así se puede cancelar y obtener

$$g^i = g^j.$$

Con lo cual $i = j$.

■

Lema 3.1 *De la construcción de Welch se puede eliminar la primera columna a la izquierda y la última fila de la matriz de tamaño $(p-1) \times (p-1)$, para obtener un arreglo Costas de orden $(p-2)$.*

Demostración.

Como $g^{p-1} \equiv 1 \pmod{p}$, el arreglo original de grado $p-1$ visto matricialmente tiene un 1 en la posición $a_{p-1,1}$ en la esquina inferior mano izquierda. Por el lema 2.2, el arreglo puede ser reducido a grado $p-2$.

■

Lema 3.2 *Si 2 es un elemento primitivo de $\mathbb{F}_p$, entonces un arreglo Costas de orden $(p-3)$ puede ser obtenido de la construcción de Welch.*

Demostración.

Por el Lema 3.1, se elimina el 1 en la posición $a_{p-1,1}$. Como 2 es elemento primitivo, éste genera los puntos del arreglo, en particular genera el punto $a_{1,2}$ que está en la esquina superior izquierda del nuevo arreglo, éste también puede ser removido por el lema 2.2.

■

Lema 3.3 *Cada permutación cíclica de las filas de un arreglo Costas de la construcción de Welch es de nuevo un arreglo Costas de orden $(p-1)$.*

Demostración.

Sean g un elemento primitivo módulo p y c un entero positivo fijo. El arreglo Costas de orden $(p-1)$ con

$$a_{ij} = \begin{cases} 1, & \text{si } j \equiv g^{i+c} \pmod{p}; \\ 0, & \text{en caso contrario.} \end{cases}$$

es un arreglo Costas (La misma demostración de la construcción de Welch), y los valores de c dan las permutaciones cíclicas sucesivas de las filas en el teorema anterior.

■

Teorema 3.9 ***(Construcción de Lempel).*** *Sea α un elemento primitivo en el campo $\mathbb{F}_q$ para cualquier $q > 2$. La matriz $A = (a_{ij})$ de tamaño $(q-2) \times (q-2)$ con*

$$a_{ij} = \begin{cases} 1, & \textit{si } \alpha^i + \alpha^j = 1\textit{;} \\ 0, & \textit{en caso contrario.} \end{cases}$$

es un arreglo Costas.

Demostración.

Dado que $1 = \alpha^i + \alpha^j = \alpha^j + \alpha^i$, se puede contemplar que a_{ij} y a_{ji} son 1 en el arreglo matricial, así la matriz prueba ser simétrica de orden $q-2$, ya que el índice $q-1$ no puede ser tomado debido a que $\alpha^{q-1} = 1$.

Si $\alpha^i + \alpha^j = 1$ entonces esta expresión se escribe en forma de función:

$$j = \log_\alpha(1 - \alpha^i).$$

Si $\log_\alpha(1 - \alpha^{i+k}) - \log_\alpha(1 - \alpha^i) = \log_\alpha(1 - \alpha^{l+k}) - \log_\alpha(1 - \alpha^l)$, con $1 \leq k \leq q - 3$ entonces

$$\log_\alpha\left(\frac{1 - \alpha^{i+k}}{1 - \alpha^i}\right) = \log_\alpha\left(\frac{1 - \alpha^{l+k}}{1 - \alpha^l}\right)$$

$$\frac{1 - \alpha^{i+k}}{1 - \alpha^i} = \frac{1 - \alpha^{l+k}}{1 - \alpha^l}$$

$$1 - \alpha^l - \alpha^{i+k} + \alpha^{i+k+l} = 1 - \alpha^i - \alpha^{l+k} + \alpha^{i+k+l}$$

$$\alpha^{i+k} - \alpha^i = \alpha^{l+k} - \alpha^l$$

$$\alpha^i(\alpha^k - 1) = \alpha^l(\alpha^k - 1).$$

Como $\alpha^k - 1 \neq 0$, se obtiene que $\alpha^i = \alpha^l$ con lo cual se concluye que $i = l$.

■

Teorema 3.10 ***(Construcción Golomb).*** *Sean α y β elementos primitivos en el campo $\mathbb{F}_q$, para cualquier $q > 2$. La matriz $A = (a_{ij})$ de tamaño $(q-2) \times (q-2)$ con*

$$a_{ij} = \begin{cases} 1, & \text{si } \alpha^i + \beta^j = 1; \\ 0, & \text{en caso contrario.} \end{cases}$$

es un arreglo Costas.

Demostración.

De $\alpha^i + \beta^j = 1$ se puede ver la relación en forma de función como sigue: $j = \log_\beta(1 - \alpha^i)$. El resto de la prueba se sigue exactamente de la prueba del Teorema 3.9.

■

Teorema 3.11 ***(Moreno).*** *Sea $q > 2$. El campo $\mathbb{F}_q$ posee 2 elementos primitivos α, β (no necesariamente distintos) tales que*

$$\alpha + \beta = 1.$$

La demostración de este teorema fue resuelta hace poco, así que no será presentada en el presente trabajo, solo será referenciado el Teorema por su gran uso.

Lema 3.4 *La construcción de Golomb puede ser reducida a un arreglo Costas de orden* $(q-3)$.

Demostración.

Del Teorema 3.11, existen $\alpha, \beta \in \mathbb{F}_q$ tales que $\alpha + \beta = 1$. Tomando estos elementos primitivos y aplicando la construcción de Golomb con ellos, obtenemos que $a_{11} = 1$, por lema 2.2, se elimina la primer fila y la primer columna a la izquierda y se obtiene un arreglo Costas de orden $(q-3)$.

■

3.3. Construcciones de secuencias sonares

Las construcciones listadas a continuación pueden ser encontradas en [8].

Teorema 3.12 ***(Construcción cuadrática).*** *Sea p un primo impar; sean a, b y c enteros constantes con a no congruente con $0 \bmod p$. La función $f : [1, p+1] \longrightarrow [1, p]$ definida por*

$$f(i) = (ai^2 + bi + c) \bmod p,$$

es una secuencia sonar modular de tamaño $p \times (p+1)$.

Demostración.

Suponga que $f(i+h) - f(i) = f(j+h) - f(j)$ para algunos $i, j, h \in [1, p+1]$ con $1 \leq h \leq p$ y $1 \leq i, j \leq p+1-h$.

Se obtiene

$$a(i+h)^2+b(i+h)+c-(ai^2+bi+c) = a(j+h)^2+b(j+h)+c-(aj^2+bj+c),$$

de donde

$$2aih + ah^2 + bh \equiv 2ajh + ah^2 + bh \pmod{p}$$

$$2aih \equiv 2ajh \pmod{p}$$

$$aih \equiv ajh \pmod{p}$$

$$ih \equiv jh \pmod{p}$$

$$(i-j)h \equiv 0 \pmod{p}.$$

Si $1 \leq h \leq p-1$ entonces se obtiene que $i = j$.

Si $h = p$, de la hipótesis general $1 \leq i, j \leq p+1-p$ se tiene que

$$1 \leq i, j \leq 1$$

$$i = j,$$

completando la prueba.

■

Teorema 3.13 ***(Construcción Shift).*** *Sean p un primo, $q = p^n$, α un elemento primitivo de $\mathbb{F}_{q^2}$ y β un elemento primitivo de $\mathbb{F}_q$.*

Para $p = 2$, sea $f : [1, q] \longrightarrow [1, q-1]$ definida por

$$f(i) := \log_\beta((\alpha^i)^q + \alpha^i).$$

Para un primo p impar, defina a f similarmente, pero cambiando el dominio por $(-(q-1)/2 \leq i \leq (q-1)/2)$.
De esta manera, f es una secuencia sonar modular de tamaño $(q-1) \times q$.

Demostración.

Asuma que p es impar. Del Teorema 3.6 de Lindström, la función $T(x) = x^q + x$ (La función traza) es una función lineal de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$ y $ImT = \mathbb{F}_q$.

Sea $x = \alpha^i$ con $(-(q-1)/2 \leq i \leq (q-1)/2)$.

Llame $L(i) := (\alpha^i)^q + \alpha^i$ con $(-(q-1)/2 \leq i \leq (q-1)/2)$.
Para asegurar que la función $\log_\beta L(i)$ está bien definida se debe probar que $L(i) \neq 0$ para todo i.

Si $(\alpha^i)^q + \alpha^i = 0$, entonces

$$\begin{aligned} \alpha^i((\alpha^i)^{q-1} + 1) &= 0 \\ (\alpha^i)^{q-1} + 1 &= 0 \\ (\alpha^i)^{q-1} &= -1 \\ (\alpha)^{2i(q-1)} &= 1. \end{aligned}$$

Como $(-(q-1)/2 \leq i \leq (q-1)/2)$, entonces $-(q-1) \leq 2i \leq (q-1)$.

$$-q^2 + 1 < (-(q-1)^2 \leq 2i(q-1) \leq (q-1)^2 < q^2 - 1.$$

Note que α es un elemento primitivo de orden q^2-1, así de $(\alpha)^{2i(q-1)}=1$ se tiene una contradicción.

Luego f está bien definida.

Se debe probar que f es una secuencia sonar.

Sean h,i,j con $1\leq h\leq q-1$ y $-(q-1)/2\leq i\leq j\leq (q-1)/2-h$ tales que

$$\begin{aligned}\log_\beta L(i+h)-\log_\beta L(i)&\equiv \log_\beta L(j+h)-\log_\beta L(j) \pmod q\\ \log_\beta \frac{L(i+h)}{L(i)}&\equiv \log_\beta \frac{L(j+h)}{L(j)} \pmod q\\ \log_\beta \frac{L(i+h)}{L(i)}&= \log_\beta \frac{L(j+h)}{L(j)}+k(q-1), k\in\mathbb{Z}.\end{aligned}$$

De la anterior igualdad, se toma a β como base, para obtener

$$\begin{aligned}\frac{(\alpha^{i+h})^q+\alpha^{i+h}}{(\alpha^i)^q+\alpha^i}&=\frac{(\alpha^{j+h})^q+\alpha^{j+h}}{(\alpha^j)^q+\alpha^j}\\ \frac{\alpha^i\alpha^h((\alpha^{i+h})^{q-1}+1)}{\alpha^i((\alpha^i)^{q-1}+1)}&=\frac{\alpha^j\alpha^h((\alpha^{j+h})^{q-1}+1)}{\alpha^j((\alpha^j)^{q-1}+1)}\\ [(\alpha^{i+h})^{q-1}+1]((\alpha^j)^{q-1}+1)&=[(\alpha^{j+h})^{q-1}+1]((\alpha^i)^{q-1}+1)\\ (\alpha^{i+j+h})^{q-1}+(\alpha^{i+h})^{q-1}+(\alpha^j)^{q-1}+1&=(\alpha^{i+j+h})^{q-1}+(\alpha^{j+h})^{q-1}+(\alpha^i)^{q-1}+1\\ (\alpha^{i+h})^{q-1}+(\alpha^j)^{q-1}&=(\alpha^{j+h})^{q-1}+(\alpha^i)^{q-1}\\ (\alpha^{i+h})^{q-1}-(\alpha^i)^{q-1}&=(\alpha^{j+h})^{q-1}-(\alpha^j)^{q-1}\\ (\alpha^i)^{q-1}[(\alpha^h)^{q-1}-1]&=(\alpha^j)^{q-1}[(\alpha^h)^{q-1}-1].\end{aligned}$$

Como $h\leq q-1$ tenemos que $(\alpha^h)^{q-1}\neq 1$, así se cancelan los términos y se obtiene

$$\begin{aligned}(\alpha^i)^{q-1}&=(\alpha^j)^{q-1}\\ 1&=(\alpha^{j-i})^{q-1}.\end{aligned}$$

Como $0\leq j-i\leq q-1$ se concluye que

$$i=j.$$

■

Capítulo 4

Análisis algebraico de los conjuntos B_2

4.1. Nuevas construcciones de conjuntos B_2

Se presenta la versión moderna del teorema de Singer exhibiendo la forma de su construcción, seguida del teorema CRT-2013 para la construcción de secuencias sonares, el cual transforma las reglas Golomb generadas por el Teorema 3.3 y 3.4 en secuencias sonares. Se recalca que la versión original o general del teorema de Singer se presenta de forma existencial, es decir, afirma que existe tal conjunto pero no muestra quien és.

Teorema 4.1 ***(Construcción de Singer, versión moderna).*** *Sean $q = p^n$ una potencia prima, α un elemento de grado 3 sobre el campo $\mathbb{F}_q$, y θ un elemento primitivo del campo $\mathbb{F}_{q^3}$. El conjunto*

$$(\log_\theta(\alpha + \mathbb{F}_q)) \pmod{q^2+q+1} \cup \{0\} :=$$
$$\{(\log_\theta(\alpha + a)) \pmod{q^2+q+1} : a \in \mathbb{F}_q\} \cup \{0\} \subseteq \mathbb{Z}_{q^2+q+1},$$

es una regla Golomb módulo q^2+q+1, con $q+1$ elementos.

Demostración.

El conjunto $\log_\theta(\alpha + \mathbb{F}_q)$ es el mismo conjunto tomado en la construcción de Bose-Chowla, así este conjunto es una regla Golomb.

Sean $x_1, x_2, x_3, x_4 \in (\log_\theta(\alpha + \mathbb{F}_q))\ (\text{mód } q^2+q+1)$.
Observe que para cada $i = 1, 2, 3, 4.$ los x_i se definen como sigue

$x_i = y_i - k_i(q^2+q+1)$ con $y_i \in \log_\theta(\alpha + \mathbb{F}_q), k_i \in \mathbb{Z}$.

Si $x_1 - x_2 \equiv x_3 - x_4\ (\text{mód } q^2+q+1)$, con $x_1 \neq x_2,\ x_3 \neq x_4$,

entonces

$$\begin{aligned} y_1 - y_2 &\equiv y_3 - y_4 \pmod{q^2+q+1} \\ y_1 - y_2 &= y_3 - y_4 + k(q^2+q+1),\ k \in \mathbb{Z} \\ \theta^{y_1-y_2} &= \theta^{y_3-y_4}(\theta^{q^2+q+1})^k. \end{aligned} \tag{4.1}$$

Note que como θ es un elemento primitivo de $\mathbb{F}_{q^3}$, θ^{q^2+q+1} genera la parte multiplicativa del campo de orden $q-1$ ya que $(q^2+q+1)(q-1) = q^3-1$, el ordel del elemento θ, pero el único campo de orden q es $\mathbb{F}_q$, luego θ^{q^2+q+1} genera su parte multiplicativa, por ende $(\theta^{q^2+q+1})^k \in \mathbb{F}_q$. Sea $U := (\theta^{q^2+q+1})^k$.

Dado que $y_i \in \log_\theta(\alpha + \mathbb{F}_q)$ con $i = 1, 2, 3, 4$, existen $u_i \in \mathbb{F}_q$, tales que $\theta^{y_i} = \alpha + u_i$. Reemplazando en (4.1):

$$\begin{aligned} \theta^{y_1-y_2} &= \theta^{y_3-y_4}U \\ \frac{\alpha+u_1}{\alpha+u_2} &= \left(\frac{\alpha+u_3}{\alpha+u_4}\right)U \\ \frac{\alpha+u_1}{\alpha+u_2} &= \frac{U\alpha+Uu_3}{\alpha+u_4} \\ \alpha^2 + u_4\alpha + u_1\alpha + u_4u_1 &= U\alpha^2 + Uu_3\alpha + Uu_2\alpha + Uu_2u_3 \end{aligned}$$

$$(1-U)\alpha^2 + (u_4 + u_1 - Uu_3 - Uu_2)\alpha + u_1u_4 - Uu_2u_3 = 0.$$

observe que α es raíz del polinomio de grado 2:
$(1-U)x^2 + (u_4+u_1-Uu_3-Uu_2)x + u_1u_4 - Uu_2u_3 \in \mathbb{F}_q[X]$(no es posible); ya que α fue elegido como un elemento de grado 3 sobre $\mathbb{F}_q$; luego el polinomio anterior es el polinomio constante cero, implicando

$$U = 1;\ u_4 + u_1 = u_3 + u_2;\ u_4u_1 = u_3u_2.$$

Con lo cual, se sigue

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

de donde

$$\{\theta^{y_4}, \theta^{y_1}\} = \{\theta^{y_3}, \theta^{y_2}\}$$

$$\{y_4, y_1\} = \{y_3, y_2\}$$

$$\{x_4, x_1\} = \{x_3, x_2\}.$$

Como $x_1 \neq x_2,\ x_3 \neq x_4$ se obtiene que $x_1 = x_3,\ x_2 = x_4$, con lo que se concluye que $(\log_\theta(\alpha + \mathbb{F}_q))\ (\text{mód } q^2+q+1)$ es una regla Golomb modular.

Resta probar que el nuevo conjunto posee q elementos.

Sean $y_1, y_2 \in \log_\theta(\alpha + \mathbb{F}_q)$ tales que

$$\begin{aligned} y_1 &\equiv y_2 \pmod{q^2+q+1} \\ y_1 &= y_2 + k(q^2+q+1),\ k \in \mathbb{Z} \\ y_1 - y_2 &= k(q^2+q+1). \end{aligned}$$

Pasando al campo $\mathbb{F}_{q^3}$:

$$\theta^{y_1-y_2} = u, \text{ donde } u := (\theta^{q^2+q+1})^k \in \mathbb{F}_q.$$

Existen $u_i \in \mathbb{F}_q$, con $i = 1, 2$, tales que

$$\theta^{y_i} = \alpha + u_i, \text{ con ello se obtiene que}$$

$$u = \frac{\alpha + u_1}{\alpha + u_2} \Longleftrightarrow u\alpha + uu_2 = \alpha + u_1$$

$$\Longleftrightarrow \alpha(u-1) = u_1 - uu_2.$$

Si $u - 1 \neq 0$ entonces $\alpha = (u-1)^{-1}(u_1 - uu_2)$, de lo cual $\alpha \in \mathbb{F}_q$ (no es posible).

Luego $u - 1 = 0$, esto es $u = 1$ y $\theta^{y_1-y_2} = 1$.

Sin embargo para que θ se vuelva 1, el valor más pequeño para la potencia de θ debe ser $\pm(q^3-1)$ dado que θ es elemento primitivo de $\mathbb{F}_{q^3}$.

Dado que $y_1, y_2 \in [1, q^3-2]$ se satisface $-(q^3-2) \leq y_1 - y_2 \leq q^3 - 2$; así que $y_1 = y_2$. De aquí se tiene que el conjunto $\log_\theta(\alpha+\mathbb{F}_q)\ (\text{mód } q^2+q+1)$ tiene q elementos.

Ahora, se agrega el cero al conjunto. Se debe probar que el conjunto sigue siendo regla Golomb.

Si $x_1, x_2, x_3 \in (\log_\theta(\alpha + \mathbb{F}_q)) \pmod{q^2+q+1}$, con $x_2 \neq x_3$ tales que

$$x_1 \equiv x_2 - x_3 \pmod{q^2+q+1},$$

entonces

$$x_1 = x_2 - x_3 + k(q^2+q+1), k \in \mathbb{Z},$$

pasando a $\mathbb{F}_{q^3}$

$$\theta^{x_1} = \theta^{x_2 - x_3} u, \text{ donde } u := (\theta^{q^2+q+1})^k \in \mathbb{F}_q.$$

Existen $u_1, u_2, u_3 \in \mathbb{F}_q$ tales que $\theta^{x_i} = \alpha + u_i$, para $i = 1, 2, 3$.

Luego

$$\alpha + u_1 = \frac{u\alpha + u_2 u}{\alpha + u_3}$$

$$\alpha^2 + (u_3 + u_1 - u)\alpha + u_1 u_3 - u_2 u = 0.$$

Esta última ecuación es un polinomio de grado dos sobre $\mathbb{F}_q$ (no es posible).

Por lo tanto

$$x_1 \neq x_2 - x_3 \pmod{q^2+q+1} \text{ para todo}$$
$$x_1, x_2, x_3 \in (\log_\theta(\alpha + \mathbb{F}_q)) \pmod{q^2+q+1},$$

de modo que el conjunto $(\log_\theta(\alpha + \mathbb{F}_q)) \pmod{q^2+q+1} \cup \{0\}$ es una regla Golomb modular.

■

El Teorema 4.1 fue desarrollado por el grupo ALTENUA de la Universidad del Cauca.

El siguiente teorema fue desarrollado por el grupo de investigación ALTENUA en el año 2013, creando una relación directa entre los conjuntos de Sidon y las secuencias sonares como sigue.

Teorema 4.2 ***(CRT-2013).*** *Sean $m, b \in \mathbb{N}$ y $\mathcal{A} = \{a_1, ..., a_n\}$ un conjunto de Sidon en el grupo aditivo $\mathbb{Z}_{mb}$. Si $\mathcal{A}$ (mód b) $:= \{a \bmod b : a \in \mathcal{A}\} = [1, n]$, entonces la función $F : [1, n] \longrightarrow \mathbb{Z}_m$ definida mediante $F(i) = \left\lfloor \frac{a_i}{b} \right\rfloor$, donde a_i es el único elemento de $\mathcal{A}$ tal que $a_i \equiv i$ (mód b), es una secuencia sonar $m \times n$ modular.*

Demostración.

Sean h, i, j con $1 \leq h \leq n-1$ y $1 \leq i, j \leq n-h$ tales que

$$\begin{aligned} &F(i+h) - F(i) \equiv F(j+h) - F(j) \pmod{m}. \\ &F(i+h) - F(i) = F(j+h) - F(j) + tm, \text{ con } t \in \mathbb{Z} \\ &\left\lfloor \frac{a_{i+h}}{b} \right\rfloor - \left\lfloor \frac{a_i}{b} \right\rfloor = \left\lfloor \frac{a_{j+h}}{b} \right\rfloor - \left\lfloor \frac{a_j}{b} \right\rfloor + tm. \end{aligned}$$

Multiplique por b, así se tiene

$$\left\lfloor \frac{a_{i+h}}{b} \right\rfloor b - \left\lfloor \frac{a_i}{b} \right\rfloor b = \left\lfloor \frac{a_{j+h}}{b} \right\rfloor b - \left\lfloor \frac{a_j}{b} \right\rfloor b + tmb.$$

Al sumar h a ambos lados de la igualdad se llega a

$$\left\lfloor \frac{a_{i+h}}{b} \right\rfloor b - \left\lfloor \frac{a_i}{b} \right\rfloor b + (h+i) - i = \left\lfloor \frac{a_{j+h}}{b} \right\rfloor b - \left\lfloor \frac{a_j}{b} \right\rfloor b + (h+j) - j + tmb.$$

Note que para todo entero s y todo entero c se tiene que existe el residuo l tal que

$$s = \left\lfloor \frac{s}{c} \right\rfloor c + l. \tag{4.2}$$

Así, reorganizando la ecuación anterior se obtiene

$$\left\lfloor \frac{a_{i+h}}{b} \right\rfloor b + (i+h) - \left(\left\lfloor \frac{a_i}{b} \right\rfloor b + i \right) = \left\lfloor \frac{a_{j+h}}{b} \right\rfloor b + (j+h) - \left(\left\lfloor \frac{a_j}{b} \right\rfloor b + j \right) + tmb.$$

Por hipótesis se tiene que

$$a_{i+h} \equiv i + h \pmod{b},\ a_i \equiv i \pmod{b}$$
$$a_{j+h} \equiv j + h \pmod{b},\ a_j \equiv j \pmod{b}.$$

Con ello y (4.2) se llega a

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

Modulando por mb se obtiene

$$a_{i+h} - a_i \equiv a_{j+h} - a_j \pmod{mb}.$$

Por hipótesis $\mathcal{A}$ es un conjunto de Sidon en $\mathbb{Z}_{mb}$, así que

$$i = j.$$

■

A este teorema le siguen tres corolarios importantes en la creación de secuencias sonares.

Corolario 4.1 ***(Construcción desde Sidon tipo Bose).*** *Sean q una potencia prima y $b = q + 1$, $m = q - 1$ y $\mathcal{A} = \{a_1, ..., a_q\}$ el conjunto de Sidon módulo $q^2 - 1$ obtenido en Teorema 3.4. La función definida en el Teorema 4.2 (CRT-2013):*

$$F : [1, q] \longrightarrow \mathbb{Z}_{q-1},$$

$$F(i) := \left\lfloor \frac{a_i}{q+1} \right\rfloor,$$

es una secuencia sonar $(q-1) \times q$ modular.

Demostración.

Se debe probar que el conjunto de Sidon proveniente del Teorema 3.4 módulo $q + 1$ es igual a $[1, q]$.

Dado el conjunto S definido en el Teorema 3.4 tiene q elementos, basta probar que al reducirlo módulo $q + 1$ el conjunto sigue con q elementos.

Si $a \equiv b \pmod{q+1}$ donde $a, b \in S$, entonces

$$a - b \equiv 0 \pmod{q+1}) \text{ (no es posible)},$$

ya que el conjunto $(S \ominus S) \pmod{q^2-1} = \mathbb{Z}_{q^2-1} \setminus M_{q+1}$.

Así $S \pmod{q+1} = [1, q]$, aplicando el Teorema 4.2 se sigue el resultado.

■

Corolario 4.2 ***(Construcciones desde Sidon tipo Ruzsa).*** *Sean p un primo, $b = p, m = p-1$, y $\mathcal{A} = \{a_1, ..., a_{p-1}\}$ el conjunto de Sidon módulo $(p-1)p$ obtenido en el Teorema 3.3. La función definida en el Teorema 4.2 (CRT-2013):*

$$F : [1, p-1] \longrightarrow \mathbb{Z}_{p-1},$$

$$F(i) := \left\lfloor \frac{a_i}{p} \right\rfloor,$$

es una secuencia sonar $(p-1) \times (p-1)$ modular.

Demostración.

Los elementos del conjunto construido en el Teorema 2.3 son de la forma:

$$[psk + (p-1)g^k] \text{ mód } p(p-1) \text{ con } k = 0, ..., p-2,$$

si

$$[psa + (p-1)g^a] \text{ mód } p(p-1) \equiv [psb + (p-1)g^b] \text{ mód } p(p-1) \pmod{p} \text{ con } a, b \in \{0, 1, ..., p-2\},$$

entonces

$$(p-1)g^a \equiv (p-1)g^b \pmod{p}$$

$$g^a \equiv g^b \pmod{p}.$$

Dado que g es un elemento primitivo, se concluye que $a = b$. Por lo tanto el conjunto generado por el Teorema 3.3 módulo p es igual a $[1, p-1]$.

■

Corolario 4.3 ***(Construcciones desde Sidon tipo Ruzsa).*** *Sean p un primo, $b = p-1, m = p$, y $\mathcal{A} = \{a_1, ..., a_{p-1}\}$ el conjunto de Sidon módulo $(p-1)p$ obtenido en el Teorema 3.3. La función definida en el Teorema 4.2 (CRT-2013):*

$$F : [1, p-1] \longrightarrow \mathbb{Z}_p,$$

$$F(i) := \left\lfloor \frac{a_i}{p-1} \right\rfloor,$$

es una secuencia sonar $p \times (p-1)$ modular.

Demostración.

Si

$$[psa + (p-1)g^a] \text{ mód } p(p-1) \equiv [psb + (p-1)g^b] \text{ mód } p(p-1) \pmod{p-1}$$
$$\text{con } a, b \in \{0, 1, ..., p-2\},$$

entonces

$$\begin{aligned} psa &\equiv psb \pmod{p-1} \\ a &\equiv b \pmod{p-1} \\ a &= b. \end{aligned}$$

Luego el conjunto posee $p-1$ elementos, terminando así la prueba.

■

4.2. Funciones y construcciones algebraicas generalizadas

Las reglas Golomb, los arreglos Costas y las secuencias sonares son conjuntos B_2 que poseen una propiedad común: La propiedad de diferencias distintas. Cada construcción presentada en este trabajo tiene un origen en los campos finitos, lo que no es muy claro es que provienen de sus grupos bases como sigue.

La tripla $(\mathbb{F}, +, \times)$ denota al campo $\mathbb{F}$ con operaciones suma y producto. Se obtienen sus grupos bases: $(\mathbb{F}, +)$ y $(\mathbb{F}^*, \times)$ donde $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$.

De estos dos grupos conmutativos se obtienen en esencia tres grupos productos que son:

1. $(\mathbb{F}, +) \times (\mathbb{F}^*, \times)$

2. $(\mathbb{F}^*, \times) \times (\mathbb{F}^*, \times)$

3. $(\mathbb{F}, +) \times (\mathbb{F}, +)$.

PARA LA CONSTRUCCIÓN DE WELCH

Se define la función

$I : \mathbb{F}^* \longrightarrow \mathbb{F}^*$ como sigue. Si $x \in \mathbb{F}^*, I(x) = x$.

El grafo de la función I es un conjunto de Sidon en el grupo: $(\mathbb{F}, +) \times (\mathbb{F}^*, \times)$.

Demostración.

Sean $(x_1, x_1), (x_2, x_2), (x_3, x_3), (x_4, x_4) \in \mathfrak{g}_I$ donde $\mathfrak{g}_I := \{(x, I(x)) : x \in \mathbb{F}^*\}$ es llamado el grafo de I.

Si $(x_1, x_1) \bigoplus (x_2, x_2) = (x_3, x_3) \bigoplus (x_4, x_4)$, entonces

$$x_1 + x_2 = x_3 + x_4 \quad \text{y} \quad x_1 x_2 = x_3 x_4,$$

con $\bigoplus$ la operación del grupo $(\mathbb{F}, +) \times (\mathbb{F}^*, \times)$.

Luego

$$\{x_1, x_2\} = \{x_3, x_4\},$$

verificandose de la siguiente manera.

Ya que $x_1 \neq 0$ se obtiene que $x_2 = x_1^{-1} x_3 x_4$, luego

$$\begin{aligned} x_1 + x_1^{-1} x_3 x_4 &= x_3 + x_4 \\ x_1 + x_1^{-1} x_3 x_4 - (x_3 + x_4) &= 0 \\ x_1^2 + x_3 x_4 - x_1(x_3 + x_4) &= 0 \\ (x_1 - x_3)(x_1 - x_4) &= 0. \end{aligned}$$

En $\mathbb{F}$ no hay divisores de cero, por tanto

$$x_1 = x_3 \text{ o } x_1 = x_4 \text{ y } x_2 = x_3 \text{ o } x_2 = x_4.$$

■

Se toma el campo más básico finito: $\mathbb{F} = \mathbb{F}_p$ con p un primo.

Así la función $I : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$ con $I(x) = x, x \in \mathbb{F}_p^*$ define al grafo $\mathfrak{g}_I \subseteq (\mathbb{F}_p, +) \times (\mathbb{F}_p^*, \times)$ como un conjunto de Sidon en ese grupo.

Se debe probar lo siguiente:

$$(\mathbb{F}_p, +) \times (\mathbb{F}_p^*, \times) \equiv (\mathbb{Z}_p, +) \times (\mathbb{Z}_{p-1}, +).$$

En efecto, se define la función G_1 como sigue

$$\begin{array}{rl} G_1 : (\mathbb{F}_p, +) \times (\mathbb{F}_p^*, \times) & \longrightarrow (\mathbb{Z}_p \times \mathbb{Z}_{p-1}) \\ (n, \theta^j) & \longrightarrow G_1(n, \theta^j) = (n, j). \end{array}$$

G_1 **es homomorfismo.**

Sean $(n_1, \theta^{j_1}), (n_2, \theta^{j_2}) \in (\mathbb{F}_p, +) \times (\mathbb{F}_p^*, \times)$.

$$\begin{aligned} G_1[(n_1, \theta^{j_1}) \bigoplus (n_2, \theta^{j_2})] &= G_1(n_1 + n_2, \theta^{j_1 + j_2}) \\ &= (n_1 + n_2, j_1 + j_2) \\ &= (n_1, j_1) + (n_2, j_2) \\ &= G_1(n_1, \theta^{j_1}) + G_1(n_2, \theta^{j_2}). \end{aligned}$$

G_1 **es inyectivo.**

$$G_1(n_1, \theta^{j_1}) = G_1(n_2, \theta^{j_2})$$

$$(n_1, j_1) = (n_2, j_2)$$

$$n_1 = n_2 \text{ y } j_1 = j_2.$$

G_1 **es sobreyectivo.**

De $|\mathbb{F}_p \times \mathbb{F}_p^*| = |\mathbb{Z}_p \times \mathbb{Z}_{p-1}|$ y el hecho que sea G_1 inyectivo se obtiene lo deseado.

Así G_1 es un isomorfismo de grupos.

El siguiente teorema es extremamente útil para esta sección, dado que es la herramienta que se usa para pasar un conjunto de Sidon en un grupo a otro.

Teorema 4.3 *Sean $\psi : G \longrightarrow G^{'}$ un homomorfismo inyectivo de grupos, $(G, +_1), (G^{'}, +_2)$ dos grupos conmutativos y A un B_2 en G. Se tiene que $\psi(A)$ es B_2 en $\psi(G^{'})$.*

Demostración.

Sean $a, b, c, d \in A$. Si $\psi(a) +_2 \psi(b) = \psi(c) +_2 \psi(d)$, entonces

$$\psi(a +_1 b) = \psi(c +_1 d),$$

dado que ψ es inyectiva se sigue

$$a +_1 b = c +_1 d,$$

Luego

$$\{a, b\} = \{c, d\},$$

finalmente $$\{\varphi(a), \varphi(b)\} = \{\varphi(c), \varphi(d)\}.$$

■

Por el Teorema 4.3, se garantiza que $G_1(\mathfrak{g}_I)$ es un conjunto de Sidon en el grupo: $(\mathbb{Z}_p \times \mathbb{Z}_{p-1}, +)$.

De $\mathfrak{g}_I = \{(x, x) : x \in \mathbb{F}_p^*\}$, existe $j \in \mathbb{Z}_{p-1}$ tal que $x \equiv \theta^j \pmod{p}$. Así el conjunto

$$G_1(\mathfrak{g}_I) = \{(x, j) : x \equiv \theta^j \pmod{p}\},$$

es Sidon en el grupo $(\mathbb{Z}_p \times \mathbb{Z}_{p-1}, +)$, el mismo definido en el Teorema 3.8.

PARA LA CONSTRUCCIÓN DE RUZSA

Se requiere demostrar que

$$\mathbb{Z}_p \times \mathbb{Z}_{p-1} \equiv \mathbb{Z}_{p(p-1)}.$$

Se define la función G_2 como sigue

$$\begin{aligned} G_2 : \mathbb{Z}_p \times \mathbb{Z}_{p-1} &\longrightarrow \mathbb{Z}_{p(p-1)} \\ (a, b) &\longrightarrow G_2(a, b) = x, \end{aligned}$$

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

G_2 está bien definida. En efecto, por el Teorema chino de los restos, para cada pareja $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_{p-1}$ existe una única clase residual $x \in \mathbb{Z}_{p(p-1)}$ tal que satisface la propiedad de la función G_2, dado que $\text{mcd}(p, p-1) = 1$.

G_2 es inyectiva.

Del Teorema chino de los restos se sigue de inmediato la inyectividad.

G_2 es sobreyectiva.

Dado que $|\mathbb{Z}_p \times \mathbb{Z}_{p-1}| = |\mathbb{Z}_{p(p-1)}|$ y G_2 es inyectiva se obtiene la sobreyectividad.

G_2 es homomorfismo.

Sean $(a, b), (c, d) \in \mathbb{Z}_p \times \mathbb{Z}_{p-1}$. Luego

$G_2[(a, b) + (c, d)] = G_2(a + c, b + d)$

$$= x_1$$

tal que

$$\begin{aligned} x_1 &\equiv a + c \pmod{p} \\ x_1 &\equiv b + d \pmod{p-1}. \end{aligned}$$

Por otro lado,
$G_2(a, b) = x_2$, donde

$$\begin{aligned} x_2 &\equiv a \pmod{p} \\ x_2 &\equiv b \pmod{p-1}, \end{aligned} \tag{4.3}$$

y $G_2(c, d) = x_3$, donde

$$\begin{aligned} x_3 &\equiv c \pmod{p} \\ x_3 &\equiv d \pmod{p-1}. \end{aligned} \tag{4.4}$$

De (4.3) y (4.4) se sigue

$$\begin{aligned} x_2 + x_3 &\equiv a + c \pmod{p} \\ x_2 + x_3 &\equiv b + d \pmod{p-1}. \end{aligned}$$

Luego

$$\begin{aligned} x_1 &\equiv x_2 + x_3 \pmod{p} \\ x_1 &\equiv x_2 + x_3 \pmod{p-1}. \end{aligned}$$

Por consiguiente

$$x_1 = x_2 + x_3 + kp \text{ con } k \in \mathbb{Z}.$$

Si se modula por $(p-1)$ se obtiene

$$x_1 \equiv x_2 + x_3 + k \pmod{p-1},$$

pero por la anterior equivalencia se obtiene que:

$$k \equiv 0 \pmod{p-1}.$$

Así $k = j(p-1)$ con $j \in \mathbb{Z}$. Con ello se concluye que

$$x_1 = x_2 + x_3.$$

Por tanto la función G_2 es un isomorfismo de grupos.

Como $G_1(\mathfrak{g}_I)$ es Sidon en $(\mathbb{Z}_p \times \mathbb{Z}_{p-1})$ entonces por Teorema 4.3, $G_2[G_1(\mathfrak{g}_I)]$ es un conjunto de Sidon en $\mathbb{Z}_{p(p-1)}$.

Note que

$$\begin{aligned} G_2[G_1(\mathfrak{g}_I)] &= G_2(\{(x,j) : x \equiv \theta^j \pmod{p}\}) \\ &= \{x' : x' \equiv x \pmod{p} \ \wedge x' \equiv j \pmod{p-1}\} \\ &= \{x' : x' \equiv \theta^j \pmod{p} \ \wedge x' \equiv j \pmod{p-1}\}. \end{aligned}$$

Observe que la solución está dada por

$$x' = (p-1)\theta^j + jp,$$

la misma construcción del Teorema 3.3 con $s = 1$.

Para el caso general, sea s primo relativo con $p-1$. Se redefine la función G_2 como sigue

$$\begin{aligned} G_2' : \mathbb{Z}_p \times \mathbb{Z}_{p-1} &\longrightarrow \mathbb{Z}_{p(p-1)} \\ (a,b) &\longrightarrow G_2'(a,b) = x, \end{aligned}$$

donde $x \equiv a \pmod{p}$ y $x \equiv sb \pmod{p-1}$.

La escogencia del s es para garantizar inyectividad y sobreyectividad, de este modo:

Dado que b recorre todos los elementos de $\mathbb{Z}_{p-1}$, sb también los recorre todos, así el Teorema chino de los restos aplica y se sigue que G_2' es un isomorfismo de grupos.

Con ello

$$G_2'[G_1(\mathfrak{g}_I)] = \{x' : x' \equiv \theta^j \pmod{p} \ \wedge x' \equiv sb \pmod{p-1}\},$$

donde la solución está dada por:

$$x' = (p-1)\theta^j + jsp,$$

la construcción general del Teorema 3.3.

PARA LA CONSTRUCCIÓN DE LEMPEL

Se define otra función especial; sea $a \in \mathbb{F}^*$.

$I_a : \mathbb{F}^* \longrightarrow \mathbb{F}^*$
$\quad x \longrightarrow x + a$, con $x \neq -a$.

El grafo $\mathfrak{g}_{I_a}$ es un conjunto de Sidon en $(\mathbb{F}^*, \times) \times (\mathbb{F}^*, \times)$.

Demostración.

En efecto; sean $(b, b+a), (c, c+a), (d, d+a), (e, e+a) \in \mathfrak{g}_{I_a}$.
Si $(b, b+a) \bigoplus (c, c+a) = (d, d+a) \bigoplus (e, e+a)$, entonces

$$bc = ed$$

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

Se sigue

$$bc + ab + ac + a^2 = de + ad + ae + a^2$$

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

$$b + c = d + e.$$

Esto implica que

$$\{b, c\} = \{d, e\}.$$

■

Sea $\mathbb{F} = \mathbb{F}_q$ con $q > 2$ una potencia prima. Se define G_3 como sigue

$G_3 : (\mathbb{F}_q^*, \times) \times (\mathbb{F}_q^*, \times) \longrightarrow (\mathbb{Z}_{q-1}, +) \times (\mathbb{Z}_{q-1}, +)$
$\qquad (\alpha^i, \alpha^j) \qquad \longrightarrow G_3(\alpha^i, \alpha^j) = (i, j)$,

con $< \alpha >= \mathbb{F}_q^*$. Se necesita probar que G_3 es un isomorfismo.

Sean $(\alpha^{i_1}, \alpha^{j_1}), (\alpha^{i_2}, \alpha^{j_2}) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$.

Inyectividad.

Si $G_3(\alpha^{i_1}, \alpha^{j_1}) = G_3(\alpha^{i_2}, \alpha^{j_2})$, entonces

$$(i_1, j_1) = (i_2, j_2)$$

$$i_1 = i_2 \text{ y } j_1 = j_2.$$

Sobreyectividad.

Viene dada por $|\mathbb{F}_q^* \times \mathbb{F}_q^*| = |\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}|$ y la inyectividad.

Homomorfismo.

$$\begin{aligned} G_3[(\alpha^{i_1}, \alpha^{j_1}) \bigoplus (\alpha^{i_2}, \alpha^{j_2})] &= G_4(\alpha^{i_1+i_2}, \alpha^{j_1+j_2}) \\ &= (i_1 + i_2, j_1 + j_2) \\ &= (i_1, j_1) + (i_2, j_2) \\ &= G_3(\alpha^{i_1}, \alpha^{j_1}) + G_3(\alpha^{i_2}, \alpha^{j_2}). \end{aligned}$$

Con esto se concluye que G_3 es un isomorfismo de grupos.

Sea $a = 1$, así el conjunto

$\mathfrak{g}_{I_1} = \{(\alpha^i, \alpha^i + 1) : \alpha^i : \mathbb{F}_q^*, \alpha^i \neq -1\}$ es un conjunto de Sidon en el grupo $(\mathbb{F}_q^*, \times) \times (\mathbb{F}_q^*, \times)$.

Luego $G_3(\mathfrak{g}_{I_1})$ es un conjunto de Sidon en $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$.
Note que $G_3(\mathfrak{g}_{I_1})$ está dado por:

$G_3(\mathfrak{g}_{I_1}) = \{(k, j) : \alpha^k + 1 = \alpha^j\}$.
Pero $\alpha^k = -\alpha^i$ para algún $i \in \mathbb{Z}_{q-1}$. Luego

$G_3(\mathfrak{g}_{I_1}) = \{(i, j) : 1 = \alpha^i + \alpha^j\}$ es la misma construcción del Teorema 3.9.

La estrategia se conserva para la construcción de Golomb salvo que la función G_3 es cambiada como sigue

$$\begin{aligned} G_3' : (\mathbb{F}_q^*, \times) \times (\mathbb{F}_q^*, \times) &\longrightarrow (\mathbb{Z}_{q-1}, +) \times (\mathbb{Z}_{q-1}, +) \\ (\alpha^i, \beta^j) &\longrightarrow G_3(\alpha^i, \beta^j) = (i, j), \end{aligned}$$

con α, β elementos primitivos de $\mathbb{F}_q$.

PARA LA CONSTRUCCIÓN CUADRÁTICA

Se define la función

$C : \mathbb{F} \longrightarrow \mathbb{F}$
$\quad x \longrightarrow ax^2 + bx + c,$
con $a \neq 0$ y $a, b, c \in \mathbb{F}$.

El grafo $\mathfrak{g}_C = \{(x, ax^2 + bx + c) : x, a, b, c \in \mathbb{F}, a \neq 0\}$ es un conjunto de Sidon en $(\mathbb{F}, +) \times (\mathbb{F}, +)$.

Demostración.

Sean $(x_1, ax_1^2 + bx_1 + c), (x_2, ax_2^2 + bx_2 + c), (x_3, ax_3^2 + bx_3 + c)$, $(x_4, ax_4^2 + bx_4 + c) \in \mathfrak{g}_C$.

Si
$(x_1, ax_1^2+bx_1+c)+(x_2, ax_2^2+bx_2+c) = (x_3, ax_3^2+bx_3+c)+(x_4, ax_4^2+bx_4+c)$,
entonces

$$x_1 + x_2 = x_3 + x_4$$

$$ax_1^2 + bx_1 + c + ax_2^2 + bx_2 + c = ax_3^2 + bx_3 + c + ax_4^2 + bx_4 + c,$$

$$a(x_1^2 + x_2^2) = a(x_3^2 + x_4^2)$$

$$x_1^2 + x_2^2 = x_3^2 + x_4^2.$$

Como $x_1 + x_2 = x_3 + x_4$ entonces

$$(x_1 + x_2)^2 = (x_3 + x_4)^2,$$

$$x_1^2 + 2x_1x_2 + x_2^2 = x_3^2 + 2x_3x_4 + x_4^2$$

$$2x_1x_2 = 2x_3x_4,$$

si 2 es invertible en $\mathbb{F}$ se obtiene

$$x_1x_2 = x_3x_4$$

$$x_1 + x_2 = x_3 + x_4,$$

lo cual implica que $\{x_1, x_2\} = \{x_3, x_4\}$.

■

Tome $\mathbb{F} = \mathbb{F}_p$ con p impar para obtener el inverso multiplicativo de 2, y cambie el representante de la clase 0 por p.

Así la función

$C : \mathbb{F}_p \longrightarrow \mathbb{F}_p$
$\quad x \longrightarrow ax^2 + bx + c,$
con $a \neq p$ y $a, b, c \in \mathbb{F}_p$,

define al grafo $\mathfrak{g}_C$ como un conjunto de Sidon en $\mathbb{Z}_p \times \mathbb{Z}_p$. (Note que $\mathbb{F}_p \equiv \mathbb{Z}_p$).

Se debe expandir este conjunto un poco para alcanzar la construcción cuadrática.

Agrege al grafo de C el punto $(p+1, (a+b+c) \text{ mód } p)$. Se debe probar que el nuevo conjunto continua siendo un conjunto de Sidon.

Sean $x_1, x_2, x_3 \in \mathbb{Z}_p$ tales que

$$(p+1, a+b+c) + (x_1, ax_1^2 + bx_1 + c) = (x_2, ax_2^2 + bx_2 + c) + (x_3, ax_3^2 + bx_3 + c),$$

entonces

$$\begin{gathered} p + 1 + x_1 = x_2 + x_3 \\ a + b(p+1) + c + ax_1^2 + bx_1 + c \equiv ax_2^2 + bx_2 + c + ax_3^2 + bx_3 + c \pmod{p} \\ a + ax_1^2 \equiv ax_2^2 + ax_3^2 \pmod{p} \\ 1 + x_1^2 \equiv x_2^2 + x_3^2 \pmod{p}, \end{gathered}$$

pero

$$1 + x_1 \equiv x_2 + x_3 \pmod{p},$$

así que

$$\begin{gathered} (1 + x_1)^2 \equiv (x_2 + x_3)^2 \pmod{p} \\ 1 + 2x_1 + x_1^2 \equiv x_2^2 + 2x_2x_3 + x_3^2 \pmod{p}, \end{gathered}$$

se obtiene

$$1x_1 \equiv x_2x_3 \pmod{p}$$

$$1 + x_1 \equiv x_2 + x_3 \pmod{p}.$$

Dado que $1, x_1, x_2, x_3 \in \mathbb{Z}_p$ se sigue

$$\{1, x_1\} = \{x_2, x_3\}.$$

Suponga sin pérdida de generalidad que $x_3 = 1$. Así que

$$\begin{aligned} p + 1 + x_1 &= x_2 + 1 \\ p + x_1 &= x_2 \text{ (no es posible)}, \end{aligned}$$

ya que $x_1, x_2 \in [1, p]$. Por lo tanto el nuevo conjunto

$\mathfrak{g}_C \bigcup (p + 1, (a + b + c) \text{ mód } p)$ es un conjunto de Sidon en $\mathbb{Z} \times \mathbb{Z}_p$, la construcción cuadrática.

PARA LA CONSTRUCCIÓN DE BOSE

Conside ahora un elemento α de grado 2 sobre el campo $\mathbb{F}$, así se obtiene la siguiente extensión:

$$\begin{array}{c} \mathbb{F}(\alpha) \\ | \\ \mathbb{F}. \end{array}$$

Sea el conjunto $A := \alpha + \mathbb{F}$. Se debe probar que A es un conjunto de Sidon en el grupo $(\mathbb{F}(\alpha)^*, \times)$.

Demostración.

Sean $(\alpha + a), (\alpha + b), (\alpha + c), (\alpha + d) \in A$. Si

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

entonces

$$\alpha^2 + (a + b)\alpha + ab = \alpha^2 + (b + d)\alpha + cd,$$

se sigue

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

Es decir α es raiz del polinomio $[(a+b)-(c+d)]x+[ab-cd] \in \mathbb{F}[X]$. Como α es de grado 2 sobre $\mathbb{F}$ se tiene que

$$a+b=c+d$$

$$ab=cd,$$

con lo cual

$$\{a,b\}=\{c,d\}$$

$$\{\alpha+a,\alpha+b\}=\{\alpha+c,\alpha+d\}.$$

■

Tome $\mathbb{F}=\mathbb{F}_q$ y $\mathbb{F}(\alpha)=\mathbb{F}_{q^2}$.

Defina la función
$\log_\theta : (\mathbb{F}^*_{q^2},\times) \longrightarrow \mathbb{Z}_{q^2-1}$
$\theta^i \longrightarrow \log_\theta(\theta^i)=i$, con $<\theta>=\mathbb{F}^*_{q^2}$.

Como se ha visto, ésto es un isomorfismo de grupos, así que el conjunto $\log_\theta(A)$ es un conjunto de Sidon en $\mathbb{Z}_{q^2-1}$, con $A:=\theta+\mathbb{F}_q$. Pero,

$$\begin{aligned}\log_\theta(A) &= \{\log_\theta(\theta+a) : a\in\mathbb{F}_q\}\\ &= \{j\in[0,q^2-2] : \theta^j=\theta+a, a\in\mathbb{F}_q\}\\ &= \{j\in[0,q^2-2] : \theta^j-\theta=a, a\in\mathbb{F}_q\}\\ &= \{j\in[0,q^2-2] : \theta^j-\theta\in\mathbb{F}_q\},\end{aligned}$$

la misma construcción del Teorema 3.4.

4.3. Comparación: Conjuntos Bose, Golomb y Shift

Lo que se destaca de las 3 construcciones antes mencionadas, es que las 3 se basan en campos finitos y en el mismo campo $\mathbb{F}_q$, con $q>2$.

Sin embargo, las construcciones de Bose y Shift se basan en su campo de extensión $\mathbb{F}_{q^2}$ para formar el conjunto requerido en $\mathbb{F}_q$ o en su traslación $(\alpha + \mathbb{F}_q, < \alpha >= \mathbb{F}_{q^2})$, mas la construcción Golomb no usa esa herramienta en su construcción.

En el recorrido del presente trabajo se estudió un teorema que liga las construcciones de Bose y Shift, a saber, el Teorema 3.6(el teorema de la traza). Por su forma, se nota claramente la relación del Teorema 3.6 con el Teorema 3.13, lo que no se ve claramente es el uso adecuado de unas trazas en particular, y que ese conjunto de trazas fijas es un conjunto de Bose.

El estudio de estas propiedades y el desarrollo de esa relación se postergará en el trabajo de JOVEN INVESTIGADOR que el presente autor desarrollará en este año.

Conclusiones

Se analizaron las construcciones propuestas identificando los ligamentos que las unen: La construcción de Ruzsa con la de welch, por medio de la función generalizadora $I(x) = x$, la construcción de Lempel con la de Golomb, por medio de la función generalizadora $I_a = x + a$ y la construcción de Bose con la construcción Singer, por medio de la construcción $\alpha + \mathbb{F}$ siendo α un elemento de grado 2 sobre $\mathbb{F}$ en el caso de la construcción de Bose, y un elemento de grado 3 sobre $\mathbb{F}$ en el caso de la construcción de Singer.

El estudio detallado de los fundamentos algebraicos abrió el camino para la identificación de las construcciones "semejantes"que se acabaron de mencionar, dando la posibilidad de encontrar las funciones generalizadoras de algunas de estas construcciones.

Se construyó una función G_2 capaz de transformar un conjunto de Sidon de dimensión 2 a un conjunto de Sidon de dimensión 1.

En la comparación de las construcciones de los teoremas, se encontró que el Teorema de Singer versión moderna usa de una manera particular el Teorema 3.6, puesto que toma la función traza de un conjunto distinto al conjunto de traza 1. En adición, el teorema 3.6 viene siendo otra representación del Teorema 3.4, la construcción de Bose.

Apéndice A

Campos finitos

Se proporcionan algunos resultados de grupos que serán decisivos a lo largo del presente trabajo.

Teorema. Sean $(G, +)$ un grupo cíclico finito notado aditivamente, a un generador de G y $k \in \mathbb{Z}^+$.

1. Cada subgrupo del grupo cíclico G es cíclico.

2. En el grupo cíclico finito $< a >$ de orden m, el elemento a^k genera un subgrupo de orden $\frac{m}{\text{mcd}(k,m)}$, donde $\text{mcd}(k, m)$ denota el máximo común divisor entre k y m.

3. Si d es un divisor positivo de orden m del grupo cíclico G, entonces el grupo G contiene uno y sólo un subgrupo de índice d. Para cada divisor positivo f de m, G contiene precisamente un subgrupo de orden f.

4. Sea f un divisor positivo del orden del grupo m. Entonces G contiene $\phi(f)$ elementos de orden f, donde la función $\phi(x)$ denota la función phi de Euler.

5. G contiene $\phi(m)$ generadores (esto es, elementos del grupo G, a^r tales que $< a^k >=< a >$). Los generadores son las potencias a^r con $\text{mcd}(r, m) = 1$.

Definición (Campo Galois). Para un primo p,
sean $\mathbb{F}_p := \{0, 1, 2, ..., p-1\}$ un subconjunto de $\mathbb{Z}$ y $\varphi := \mathbb{Z}\backslash < p > \longrightarrow \mathbb{F}_p$ una función definida por $\varphi([a]) = a$ para $a = 0, 1, ..., p-1$. $\mathbb{F}_p$ dotado con la estructura de campo inducida por φ, es un campo finito llamado el campo de Galois de orden p.

Definición (Característica). Si R es un anillo arbitrario y existe un entero positivo n tal que $nr = 0$ para cada $r \in R$, entonces el entero positivo n más pequeño es llamado la característica de R y se dice que R tiene característica n. Si no existe tal entero positivo, R tiene característica 0.

Teorema. Sea R un anillo conmutativo con característica p. Entonces

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \text{ y } (a-b)^{p^n} = a^{p^n} - b^{p^n},$$

para $a, b \in R$ y $n \in \mathbb{N}$.

Apéndice B

Algunas propiedades de los conjuntos B_2

La propiedad de diferencias distintas, al igual que la propiedad de los conjuntos de Sidon, es una forma formal de darle unicidad al conjunto formado por las sumas o diferencias de dos elementos. Razón por la cual se definen maneras análogas a estas propiedades, como por ejemplo el conjunto solución a la ecuación $x = a + b$ o $x = a - b$ con $a, b \in A$, $x \in G$ y $A \subseteq G$ como máximo una sola vez, así se estipula que el elemento $x \in G$ se puede escribir como la suma o diferencia de dos elementos de A como máximo de una forma posible.

Cotas para las secuencias sonares

- Una cota superior trivial para el máximo n dado m es $n = 2m$ para las secuencias sonares.
- Una cota superior trivial para el máximo n dado m es $n = m + 1$ para las secuencias sonares modulares.

Demostración.

1. Cuando $k = 1$, se hacen las comparaciones correspondientes, y dado que $f(i+1) - f(i) \in [-m+1, m-1]$ se tiene como máximo $2m - 1$ posibles valores para las diferencias, así que

$f(n) - f(n-1)$	1
$f(n-1) - f(n-2)$	2
$f(n-2) - f(n-3)$	3
...	...
$f(2) - f(1)$	$2m-1$

Se puede observar que de la sucesión se tiene

$$n - (2m - 1) = 1$$

$$n - 2m + 1 = 1$$

$$n = 2m.$$

2. Nuevamente tomando $k = 1$ se hacen las diferencias correspondientes, esta vez $f(i+1) - f(i) \in [0, m-1]$, así se obtiene

$f(n) - f(n-1)$	1
$f(n-1) - f(n-2)$	2
$f(n-2) - f(n-3)$	3
...	...
$f(2) - f(1)$	m

Se puede observar que de la sucesión se tiene

$$n - m = 1$$

$$n = m + 1.$$

■

Bibliografía

[1] Drakakis, Konstantinos. "A review of the available construction methods for Golomb Rulers". Advances in Mathematics of Communications, Vol. 3, No. 3, (2009) 235-250.

[2] Drakakis, Konstantinos. "A review of Costas arrays". Hindawi Publishing Corporation, Journal of Applied Mathematics, Volume 2006, Article ID 26385, Pages 1-32.

[3] Drakakis, Konstantinos. "Three challenges in Costas Arrays". Preprint (2008).

[4] en.wikipedia.org/wiki/Golomb_ruler, visitado el 03/04/2014.

[5] Golomb Solomon W. "Algebraic Constructions for Costas Arrays". Journal of Combinatorial Theory, series A 37 (1984), 13-21.

[6] Golomb Solomon W, and Taylor Herbert. "Constructions and Properties of Costas Arrays". Proceedings of the IEEE, Vol. 72, No.9 (1984), 1143-1163.

[7] en.wikipedia.org/wiki/Costas_array, visitado el 03/04/2014.

[8] Moreno Oscar, Games Richard, and Taylor Herbert. "Sonar Sequences from Costas Arrays and the Best Known Sonar Sequences with up to 100 symbols". IEEE Transactions Information Theory, Vol. 39, No.6, (1993), 1985-1987.

[9] Rudolf Lidl and Harald Niederreiter. " Finite Fields". Encyclopedia of Mathematics and Its Applications. Cambridge University Press, 1997.

[10] www.costasarrays.org, visitado el 09/02/2011.