Ciencia en Desarrollo, Vol. 10 No. 1
ISSN 0121 - 7488 - Enero a Junio de 2019

Secuencia Sonar Bose y algunas aplicaciones

Bose Sonar sequence and some applications

Héctor Andrés Granada Díaz [a*]
Nidia Yadira Caicedo Bravo [b*]

Fecha de Recepción: 05.10.2018
Fecha de aceptación: 06.12.2018
DOI:https://doi.org/10.19053/01217488.v10.n1.2019.8714

Resumen

Se presenta la secuencia sonar *Bose* y se muestra que satisfacen algunas de las características de las secuencias sonar conocidas, las cuales se relacionan mediante algunas propiedades geométricas y algebraicas de los conjuntos de Sidon. Se especifica una metodología para la obtención de la secuencia Bose utilizando el software Matlab, estas secuencias pueden ser aplicadas a diversos campos de la ingeniería que involucren técnicas Radar y/o Sonar.

Palabras clave: Secuencias Sonar, Conjuntos de Sidon, Campos finitos, Teoría de Galois.

Abstract

This article presents the *Bose* sonar sequence and we will show that it satisfy some of the characteristics of know sonar sequences, which are related by some geometric and algebraic properties of the Sidon sets. We specify a methodology for obtaining the Bose sequence using the Matlab software, this sequeces can be applied to various fields of engineering that involve Radar and Sonar techniques.

Key words: Sonar sequences, Sidon sets, Finite fields, Galois theory.

a Universidad del Tolima, A.A. 546, Ibagué, Colombia.
* Correo electrónico: hagranadad@ut.edu.co
b Universidad del Tolima, A.A. 546, Ibagué, Colombia.
* Correo electrónico: nycaicedob@ut.edu.co

1. INTRODUCCIÓN

Las secuencias sonar fueron introducidas por Golomb y Taylor [4] como ejemplos de patrones de sincronización dos dimensional de mínima ambigüedad. Una *secuencia sonar* $m \times n$ es un arreglo de puntos y espacios que tienen m filas y exactamente un punto en cada una de sus n columnas, sujeto a la restricción que cada par de puntos determinan vectores distintos.

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

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

Los arreglos Costas aparecen por primera vez en 1965 en el contexto de la detección sonar [1] cuando J. P. Costas decepcionado por los malos resultados de los sistemas sonar, los usó para describir un nuevo patrón de saltos de frecuencia [10] para los sistemas sonar con óptimas propiedades de autocorrelación. J. Costas encontró arreglos Costas hasta de orden 12 utilizando lápiz y papel, pero no pudo continuar, mucho menos pudo encontrar una técnica general de construcción de los mismos. Golomb desarrolló dos técnicas de generación de arreglos Costas, ambas basadas en la teoría de Campos Finitos, conocidos hoy en día como Método Welch y Método Golomb [11, 3, 2]. Además, éstas construcciones son las únicas que se conocen en la actualidad, pese a los esfuerzos de muchos investigadores.

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

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

Los dos primeros n para los cuales no se conoce nada son $n = 32$ y $n = 33$.

2. FUNCIÓN SIDON, SECUENCIAS SONAR Y ARREGLOS COSTAS.

Un conjunto de enteros positivos se llama conjunto de Sidon si las sumas de dos elementos del conjunto son todas distintas, excepto por la conmutatividad. Esta definición se puede extender a cualquier grupo aditivo, en particular podemos definir conjuntos de Sidon en dimensión dos; por ejemplo las secuencias sonar y los arreglos Costas son un tipo de conjuntos de Sidon en dimensión dos. Para dar la definición formal de éstos conceptos, vamos a definir lo que es una función Sidon. En lo que sigue, consideremos G_1 y G_2 dos grupos conmutativos finitos notados aditivamente, $A \subseteq G_1$, $B \subseteq G_2$, $f : A \to B$, una función. Recordemos que el grafo de f es el conjunto

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

Definición 2.1. *$f : A \to B$, es una función Sidon si $\mathscr{G}_f$ es un conjunto de Sidon en el grupo $G_1 \times G_2$.*

Definición 2.2. *Una secuencia sonar de orden $m \times n$, es una función Sidon $f : A \to B$, donde $|A| = n$ y $|B| = m$.*

Debido a que las secuencias sonar tienen diversas aplicaciones, también presentamos la definición clásica de secuencia sonar [5], pero antes definimos los siguientes conceptos.

Definición 2.3. *Sean $n, m \in \mathbb{N}$ y $f : [1, n] \to [1, m]$ una función. Se dice que f tiene la propiedad de diferencias distintas si para todo i, j, k tales que $1 \leq k \leq n - 1$, $1 \leq i, j \leq n - k$, se cumple que:*

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

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

Proposición 2.4. *f tiene la propiedad de diferencias distintas si y sólo si el grafo de f, $G_f := \{(x, f(x)) : x \in [1, n]\}$, es un conjunto de Sidon en el grupo aditivo $\mathbb{Z} \times \mathbb{Z}$.*

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

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

esto implica que

$$x - y = z - w, \tag{1}$$

$$f(x) - f(y) = f(z) - f(w). \tag{2}$$

Entonces sin pérdida de generalidad podemos considerar $x-y = z-w>0$, pues el caso negativo se analiza de manera similar, así tenemos que $x>y, z>w$, luego existen enteros positivos a, b tales que $x = y + a$, $z = w + b$, luego como $x - y = z - w$ entonces $a = b$, por lo tanto reemplazando x = $y + a$ y $z = w + b$ en (2) tenemos

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

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

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

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

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

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

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

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

implica que $i = j$ y por lo tanto f satisface la propiedad de diferencias distintas.

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

Definición 2.5. *Una función Sidon modular, es una función* $f : [1, n] \to \mathbb{Z}_m$ *tal que tiene la propiedad de diferencias modulares distintas; esto es, si para todo h, i, j con* $1 \le h \le n - 1$ *y* $1 \le i, j \le n - h$, *se cumple que:*

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

Definición 2.6. *Una secuencia sonar de orden m* × *n es una función* $f : [1, n] \to [1, m]$ *que tiene la propiedad de diferencias distintas.*

Definición 2.7. *Una secuencia sonar modular m* × *n es una función* $f : [1, n] \to \mathbb{Z}_m$ *con la propiedad de diferencias modulares distintas.*

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

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

y para el caso modular el problema es determinar si existen secuencias sonar modulares $m \times m$, para todo m entero positivo.

Definición 2.8. *Un arreglo Costas de orden n, es una función Sidon biyectiva* $f : A \to B$, *donde* $|A| = |B| = n$.

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

Definición 2.9. U*n arreglo Costas de orden n es una permutación* $f : [1, n] \to [1, n]$ *que tiene la propiedad de diferencias distintas.*

Si $\mathscr{C}(n)$ cuenta el número de arreglos Costas de orden n, entonces el problema principal de estudio en los enteros para el caso de los arreglos Costas es determinar si $\mathscr{C}(n) > 0$, para todo n. El primer n para el cual no se conoce es $n = 32$.

2.1. Construcciones de Secuencias Sonar

Ahora vamos a describir algunas construcciones conocidas de secuencias sonar [5], consideremos p un número primo, r un entero positivo y $q = p^r$, sea además $\mathbb{F}_q$ el campo finito con q elementos.

Teorema 2.10 (Construcción cuadrática). *Sean p un primo impar, y a, b, c enteros tales que $a \not\equiv 0$ (mód p). La función $f:[1, p+1] \to \mathbb{Z}_p$ definida por $f(i) = ai^2 + bi + c$ es una secuencia sonar modular $p \times (p+1)$.*

Teorema 2.11 (Construcción Shift). *Sean $q = p^r$ una potencia prima, α un elemento primitivo de $\mathbb{F}_{q^2}$ y β un elemento primitivo de $\mathbb{F}_q$. La función $f:[1, q] \to \mathbb{Z}_{p-1}$ definida por $f(i) = \log_\beta(\alpha^{iq} + \alpha^i)$ es una secuencia sonar modular $(q-1) \times q$.*

Teorema 2.12 (Construcción Welch Exponencial). *Sean α un elemento primitivo modulo p. La función $f:[0, p-1] \to \mathbb{Z}_p$ definida por $f(i) = \alpha^i$ es una secuencia sonar modular $p \times (p-1)$.*

Teorema 2.13 (Construcción Welch Exponencial Extendida). *Sean α un elemento primitivo modulo p y s un entero. La función $f:[0, p-1] \to \mathbb{Z}_p$ definida por $f(i) = \alpha^{i+s}$ es una secuencia sonar modular $p \times p$.*

Teorema 2.14 (Construcción Welch Logarítmica). *Sea α un elemento primitivo modulo p. La función $f:[1, p-1] \to \mathbb{Z}_{p-1}$ definida por definida por $f(i) = \log_\alpha i$ es una secuencia sonar modular $(p-1) \times (p-1)$.*

Teorema 2.15 (Construcción Golomb-Lempel). *Sea q una potencia prima mayor que 2, y sean α, β elementos primitivos de $\mathbb{F}_q$. La función $f:[1, q-2] \to \mathbb{Z}_{p-1}$ definida por definida por $f(i) = j$ si y sólo si $\alpha^i + \beta^j = 1$ es una secuencia sonar modular $(q-1) \times (q-2)$. Si $\alpha = \beta$ esta construcción se conoce con el nombre de construcción Lempel.*

En el artículo [7], se presentan nuevas construcciones de secuencias sonar que provienen del análisis de ciertas propiedades que satisfacen los conjuntos de Sidon de tipo Bose y Ruzsa.

Teorema 2.16. *Sean m, $b \in \mathbb{N}$ y $\mathscr{A} = \{a_1, \ldots, a_n\}$ un conjunto de Sidon en el grupo aditivo $\mathbb{Z}_{mb}$.* Si $\mathscr{A} \bmod b := \{a \bmod b : a \in \mathscr{A}\} = [1, n]$, *entonces la función $f:[1, n] \to \mathbb{Z}_m$ definida por $f(i) = \left\lfloor \frac{a_i}{b} \right\rfloor$,* es *una secuencia sonar $m \times n$, donde a_i es el único elemento en $\mathscr{A}$ tal que $a_i \equiv i$ mód b.*

El siguiente corolario viene de la construcción tipo Bose de conjuntos de Sidon.

Corolario 2.17. *Sean q una potencia prima, θ un elemento primitivo del cuerpo finito $\mathbb{F}_q$ y $B(q, \theta) = \{\log_\theta(\theta + a) : a \in \mathbb{F}_q\}$, un conjunto de Sidon tipo Bose en el grupo aditivo $\mathbb{Z}_{q^2-1}$. La función $f:[1, q] \to \mathbb{Z}_{q-1}$ definida por*

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

es una secuencia sonar modular $(q-1) \times q$, donde b_i es el único elemento en $B(q, \theta)$ tal que $b_i \equiv i$ mód $(q+1)$.

Corolario 2.18. *Sean p un número primo, θ un elemento primitivo del cuerpo finito $\mathbb{F}_p$ y $R(p, \theta) = \{ip - \theta^i(p-1) / 1 \le i \le p-1\}$ un conjunto de Sidon tipo Ruzsa en el grupo aditivo $\mathbb{Z}_{p^2-p}$. La función $f:[1, p-1] \to \mathbb{Z}_{p-1}$ definida por*

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

es una secuencia sonar modular $(p-1) \times (p-1)$, donde r_i es el único elemento en $R(p, \theta)$ tal que $r_i \equiv i$ mód p.

Corolario 2.19. *Sean p un número primo, θ un elemento primitivo del cuerpo finito $\mathbb{F}_p$ y $R(p, \theta) = \{ip - \theta^i(p-1) / 1 \le i \le p-1\}$ un conjunto de Sidon tipo Ruzsa en el grupo aditivo $\mathbb{Z}_{p^2-p}$. La función $f:[1, p-1] \to \mathbb{Z}_p$ definida por*

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

es una secuencia sonar modular $p \times (p-1)$, donde r_i es el único elemento en $R(p, \theta)$ tal que $r_i \equiv i$ mód $(p-1)$.

Ejemplo 2.20. *Sean q=9, $q^2 - 1 = 80 = 10 \times 8$. Un conjunto de Sidon de tipo Bose con 9 elementos es*

$$B(9, \theta) = \{1, 4, 37, 38, 49, 53, 55, 62, 76\}.$$

Usando la función $f:[1, 9] \to \mathbb{Z}_8$, definida por $f(i) = \lfloor b_i/8 \rfloor$, donde $b_i \in B(9, \theta)$, del Corolario 2.17 tenemos una secuencia sonar modular 8×9 dada por $\{(1, 0), (2, 6), (3, 5), (4, 0), (5, 5), (6, 7), (7, 3), (8, 3), (9, 4)\}$.

Ejemplo 2.21. *Sean* $p = 7$, $p^2 - p = 42 = 6 \times 7$. *Un conjunto de Sidon de tipo Ruzsa con 6 elementos es*

$$R_1 = \{2, 4, 5, 27, 31, 36\}.$$

Usando la función $f : [1, 6] \rightarrow \mathbb{Z}_6$, *definida por* $f(i) = \lfloor r_i/7 \rfloor$, *donde* $r_i \in R_1$, *del Corolario 2.18 tenemos una secuencia sonar modular* 6×6 *dada por*

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

Ejemplo 2.22. *Sean* $p = 13$, $p^2 - p = 156 = 13 \times 12$. *Un conjunto de Sidon de tipo Ruzsa con 12 elementos es* $R_2 = \{10, 16, 57, 59, 90, 99, 115, 134, 144, 145, 149, 152\}$.

Usando la función $f : [1, 12] \rightarrow \mathbb{Z}_{13}$, *definida por* $f(i) = \lfloor r_i/12 \rfloor$, *donde* $r_i \in R_2$, *del Corolario 2.19 tenemos una secuencia sonar modular* 13×12 *dada por* $\{(1, 12), (2, 12), (3, 11), (4, 8), (5, 1), (6, 12), (7, 7), (8, 9), (9, 12), (10, 4), (11, 0), (12, 4)\}$.

3. EJEMPLO DE UNA CONSTRUCCIÓN DE LA SECUENCIA BOSE CON AYUDA DEL SOFTWARE MATLAB

Para entender la construcción de la secuencia sonar Bose presentada a continuación, lo primero que debemos notar es un polinomio en forma vectorial. A manera de ejemplo, el polinomio $P(x) = 1 + 2x^2 + 3x^4$ será interpretado vectorialmente como [1 0 2 0 3].

Mostraremos una secuencia sonar tipo Bose para $p = 2$ y r = 3 por medio de los siguientes pasos:

1. Para calcular todos los polinomios primitivos del cuerpo $\mathbb{F}_{p^k}$ empleando Matlab se puede hacer con el comando **Pk=gfprimfd(k,'all',p)**. Escogemos un polinomio primitivo sobre cada cuerpo de Galois $\mathbb{F}_{p^{2r}}$ y $\mathbb{F}_{p^r}$ arbitrarios. En el caso del cuerpo $\mathbb{F}_{2^3}$ los dos polinomios primitivos están conformados por las filas de la matriz:

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

y seleccionamos uno arbitrario, por ejemplo tomamos la segunda fila P = [1 0 1 1]. Análogamente, calculamos los polinomios primitivos en $\mathbb{F}_{2^6}$:

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

y escogemos uno arbitrario, por ejemplo el de la primera fila:

$$Q = [1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1]$$

2. Para calcular las raíces del polinomio **P** sobre el cuerpo $\mathbb{F}_{p^k}$ se puede hacer mediante la siguiente función **[potencia,raiz]=gfroots(P,k,p)**. El polinomio Q = [1 1 0 0 0 0 1] tendrá 2×3 raíces como se muestran en las filas de la matriz:

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

Posteriormente escogemos un elemento primitivo arbitrario sobre $\mathbb{F}_{p^{2r}}$. Por ejemplo la quinta fila, α = [1 1 0 0 1 0] .

3. Calculamos todas las potencias de α desde $k = 0, 1, 2, \cdots p^{2r} - 2$, lo que nos genera un grupo cíclico de orden $k = p^{2r} - 1$ como se muestra en la Tabla 1.

Tabla 1. Potencias de α

k	1	x	x^2	x^3	x^4	x^5
0	1	0	0	0	0	0
1	1	1	0	0	1	0
2	1	0	0	1	0	0
3	1	0	1	1	0	0
4	0	1	0	0	0	0
5	0	1	1	0	0	1

6	0	1	0	0	1	0
7	0	1	0	1	1	0
8	0	0	1	0	0	0
9	1	1	1	1	0	0
10	0	0	1	0	0	1
11	0	0	1	0	1	1
12	0	0	0	1	0	0
13	0	1	1	1	1	0
14	1	1	0	1	0	0
15	1	1	0	1	0	1
16	0	0	0	0	1	0
17	0	0	1	1	1	1
18	0	1	1	0	1	0
19	1	0	1	0	1	0
20	0	0	0	0	0	1
21	1	1	0	1	1	1
22	0	0	1	1	0	1
23	0	1	0	1	0	1
24	1	1	0	0	0	0
25	1	0	1	0	1	1
26	1	1	0	1	1	0
27	1	1	1	0	1	0
28	0	1	1	0	0	0
29	1	0	0	1	0	1
30	0	1	1	0	1	1
31	0	1	1	1	0	1
32	0	0	1	1	0	0
33	1	0	0	0	1	0
34	1	1	1	1	0	1
35	1	1	1	1	1	0
36	0	0	0	1	1	0
37	0	1	0	0	0	1
38	1	0	1	1	1	0
39	0	1	1	1	1	1
40	0	0	0	0	1	1
41	1	1	1	0	0	0
42	0	1	0	1	1	1
43	1	1	1	1	1	1
44	1	1	0	0	0	1
45	0	1	1	1	0	0
46	1	1	1	0	1	1
47	1	0	1	1	1	1
48	1	0	1	0	0	0
49	0	0	1	1	1	0
50	1	0	1	1	0	1
51	1	0	0	1	1	1
52	0	1	0	1	0	0
53	0	0	0	1	1	1
54	1	0	0	1	1	0
55	1	0	0	0	1	1
56	0	0	1	0	1	0
57	1	1	0	0	1	1
58	0	1	0	0	1	1
59	1	0	0	0	0	1
60	0	0	0	1	0	1
61	1	0	1	0	0	1
62	1	1	1	0	0	1

4. Resolvemos la ecuación $P(\alpha^k) = 0$ sobre $\mathbb{F}_{p^{2r}}$, donde P es el polinomio primitivo en $\mathbb{F}_{p^r}$ y obtenemos las siguientes potencias:

$$\begin{bmatrix} k & 1 & x & x^2 & x^3 & x^4 & x^5 \\ 9 & 1 & 1 & 1 & 1 & 0 & 0 \\ 18 & 0 & 1 & 1 & 0 & 1 & 0 \\ 36 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Escogemos arbitrariamente un elemento primitivo β sobre $\mathbb{F}_{p^r}$. A manera de ejemplo tomamos $\beta = \alpha^9 = [1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0]$ y calculamos las potencias de β para formar el grupo cíclico $< \beta >$ de orden $k = 23 - 1$

$$< \beta >= \begin{bmatrix} k & 1 & x & x^2 & x^3 & x^4 & x^5 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 2 & 0 & 1 & 1 & 0 & 1 & 0 \\ 3 & 1 & 1 & 1 & 0 & 1 & 0 \\ 4 & 0 & 0 & 0 & 1 & 1 & 0 \\ 5 & 0 & 1 & 1 & 1 & 0 & 0 \\ 6 & 1 & 0 & 0 & 1 & 1 & 0 \\ 7 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

5. Se construye el conjunto $\mathscr{A}$ dado en el Teorema 2.16 como:

$$\mathscr{A} = \text{ mód } (\alpha + < \beta >, p) \cup \alpha$$
$$= \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

6. Buscamos las potencias de α en la Tabla 1 del paso 3 que coinciden con los elementos del paso 6 para construir el conjunto
$B = \{b_i\} = \{49 \quad 48 \quad 8 \quad 14 \quad 38 \quad 52 \quad 6 \quad 1\}$

7. Se calculan los valores de x e y como en el Corolario 2.17:

$$x = \text{ mód } (B, p^r + 1)$$
$$= \{ \ 4 \quad 3 \quad 8 \quad 5 \quad 2 \quad 7 \quad 6 \quad 1 \ \}$$

$$y = \text{ mód } \left(\left[\left| \frac{b_i}{p^r + 1} \right| \right], p^r - 1 \right)$$
$$= \{ \ 5 \quad 5 \quad 0 \quad 1 \quad 4 \quad 5 \quad 0 \quad 0 \ \}$$

y finalmente se organiza la secuencia mediante el orden de x para obtener la secuencia sonar Bose: $SB = \left[\begin{array}{c|cccccccc} x & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline y & 0 & 4 & 5 & 5 & 1 & 0 & 5 & 0 \end{array} \right]$

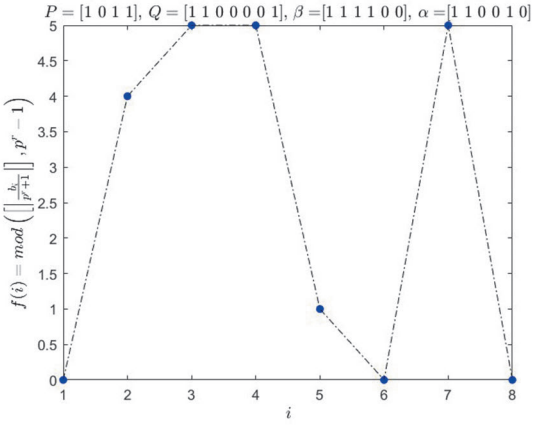


Figura 1. Secuencia sonar Bose

Podemos notar en el gráfico que los vectores diferencia entre cada par de puntos de la secuencia son distintos en magnitud y dirección, lo que hace que no se generen paralelogramos; propiedad que cumplen los conjuntos de Sidon en dimensión dos. Para observar esto calculamos el conjunto diferencia $SB{-}SB = \{(x_1 - x_2, y_1 - y_2) : (x_i, y_i) \in SB, \ i = 1, 2\}$ y verificamos que el tamaño del conjunto diferencia sea $|SB - SB| = 2\binom{|SB|}{2} + 1 = 2\binom{8}{2} + 1 = 57$. En efecto, calculamos las matrices antisimétricas X y Y de diferencias en x e y respectivamente:

$$X = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ -1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 \\ -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 \\ -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 \\ -5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 \\ -6 & -5 & -4 & -3 & -2 & -1 & 0 & 1 \\ -7 & -6 & -5 & -4 & -3 & -2 & -1 & 0 \end{bmatrix},$$

$$Y = \begin{bmatrix} 0 & 4 & 5 & 5 & 1 & 0 & 5 & 0 \\ -4 & 0 & 1 & 1 & -3 & -4 & 1 & -4 \\ -5 & -1 & 0 & 0 & -4 & -5 & 0 & -5 \\ -5 & -1 & 0 & 0 & -4 & -5 & 0 & -5 \\ -1 & 3 & 4 & 4 & 0 & -1 & 4 & -1 \\ 0 & 4 & 5 & 5 & 1 & 0 & 5 & 0 \\ -5 & -1 & 0 & 0 & -4 & -5 & 0 & -5 \\ 0 & 4 & 5 & 5 & 1 & 0 & 5 & 0 \end{bmatrix}$$

y conformamos el conjunto de todas las parejas (X_i, Y_i), contando solamente una vez a la pareja (0, 0). De esta forma se generan 57 puntos como se muestran en la Figura 2

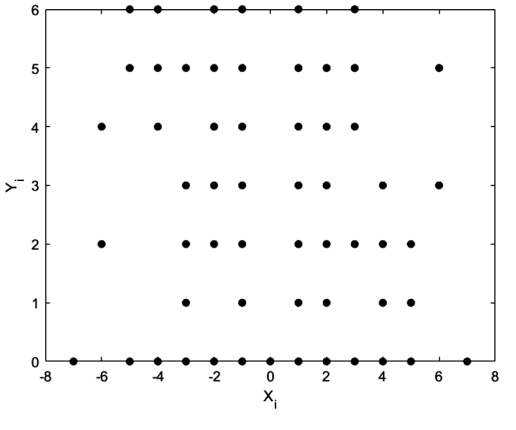


Figura 2. Diagrama de diferencia

Se puede evidenciar que manteniendo los polinomios primitivos P y Q fijos y seleccionando

dos elementos primitivos diferentes en los cuerpos $\mathbb{F}_{p^r}$ y en $\mathbb{F}_{p^{2r}}$, la secuencia sonar Bose será la misma, por ejemplo al tomar $\alpha = [0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0]$ y $\beta = [0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0]$, se obtiene la misma secuencia sonar presentada en la Figura 1. Ahora al cambiar los polinomios primitivos, podemos obtener otra secuencia sonar tipo Bose como se muestra en la Figura 3, lo cual evidencia que se puede obtener más de una secuencia sonar para cada valor de p y r.

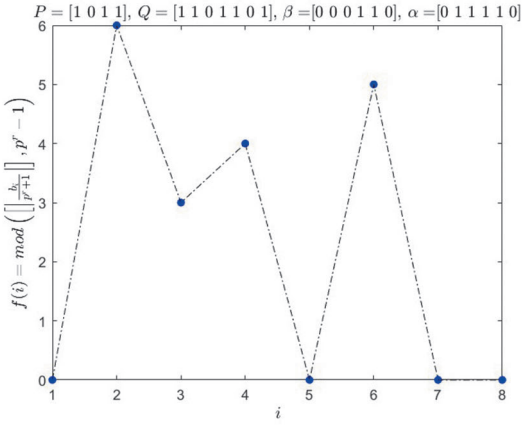
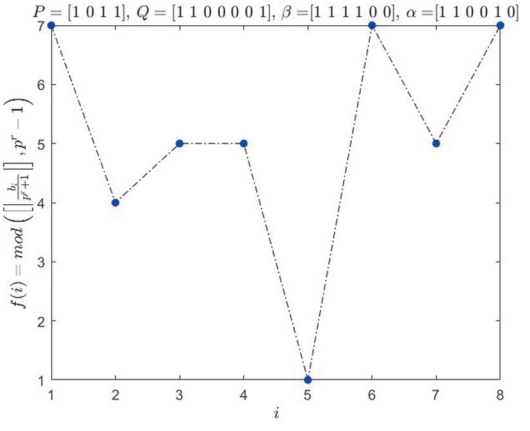


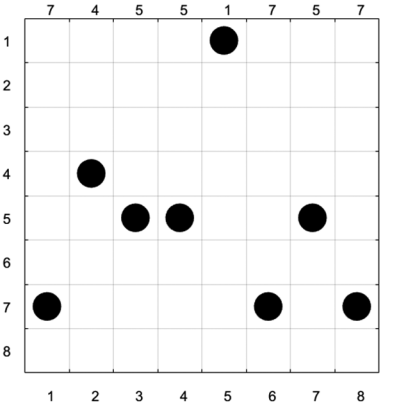
Figura 3. Secuencia Sonar cambiando polinomios primitivos

3.1 Representación de la secuencia Sonar Bose

La secuencia Sonar Bose es el conjunto de puntos de la forma $(i, f(i))$ donde i $\in \{1, 2, \cdots, p^r\}$ y $f(i)$ es la correspondiente imagen de la secuencia en el punto i. Para efectos computacionales es conveniente cambiar el cero de la secuencia por su correspondiente valor $p^r - 1$, esto se aplica en el cálculo de la matriz de energía y posteriormente realizar correlaciones de secuencias. En la Figura 4(a) se presenta la secuencia de la Figura 1 reemplazando el 0 por el 7 y en la Figura 4(b) se presenta el diagrama de puntos de blancos y negros como se hace en [6], la numeración inferior representa los valores de i mientras la numeración lateral izquierda representa las imágenes $f(i)$ de la secuencia, la numeración superior representa la secuencia simplificada, la cual significa que el primer valor es $f(1)$, el segundo $f(2)$ y así hasta el valor $f(p^r)$. En el diagrama de puntos de blancos y negros se puede evidenciar que no se forman paralelogramos entre los puntos, en este diagrama se puede verificar fácilmente si la secuencia es biyectiva, basta con observar si en cada fila o columna aparece un sólo punto. En el caso en que sea biyectiva se obtienen arreglos Costas. La construcción de la secuencia sonar Bose no es biyectiva pues es de orden $(p^r-1) \times p^r$ lo que garantiza que se va a repetir en alguna fila un punto.



(a) Secuencia reemplazando 0 por $p^r - 1$



(b) Diagrama de puntos de blancos y negros

Figura 4. Representación de la secuencia sonar

De la secuencia sonar Bose de orden $(p^r-1)\times p^r$ se puede extraer la matriz de energía A del mismo orden, definida como $A(f(i), i) = 1$ y el resto de las componentes en cero. La matriz de energía de la secuencia presentada en la Figura 4(b) viene dada por:

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

Se considera la función de correlación de dos matrices de energía A y B como se define en [11], $\Psi_{A,B}(u, v) = |\{A(i, j) = B(i + u, j + v)\}|$, que representa el número de coincidencias de puntos de la matriz A con la matriz B trasladada por u filas y v columnas. Para el caso de la secuencia sonar se analiza la función de autocorrelación, es decir $B = A$ que genera una superficie de autocorrelación donde la característica principal es que al sobreponer una matriz con la otra al trasladarla u filas y v columnas el número de coincidencias es a lo más uno, salvo cuando las dos matrices coinciden para cierta traslación como se puede observar en la Figura 5.

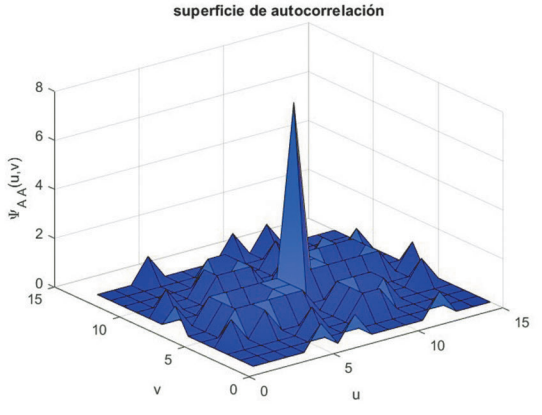


Figura 5. Superficie de autocorrelación

4. DISCUSIÓN

La metodología presentada en este artículo puede ser implementada para la obtención de otros tipo de secuencia sonar generadas por otras construcciones, ya que provienen de la teoría de cuerpos finitos. Del trabajo presentado se evidencia que al cambiar la elección del polinomio primitivo la secuencia sonar cambia, pero al cambiar el elemento primitivo se mantiene, esto sugiere realizar un análisis más detallado de la construcción del conjunto tipo Bose y su secuencia sonar correspondiente.

Por otra parte, los gráficos de superficie de autocorrelación permiten identificar si dada una secuencia arbitraria cumple la propiedad de ser secuencia sonar, para de esta manera obtener otros tipos de secuencias que no provienen de las secuencias conocidas. Respecto al costo computacional se pudo evidenciar que es elevado cuando p y r lo son, es interesante proponer otra metodología que permita reducir los costos computacionales.

Un problema interesante surge a partir de que la secuencia sonar tipo Bose no es biyectiva, ¿será posible conseguir un arreglo Costas de menor tamaño al eliminar un punto de la secuencia sonar tipo Bose para que sea una secuencia sonar biyectiva?, estas preguntas sugieren investigar más sobre nuevas técnicas sonar y sus propiedades.

REFERENCIAS

[1] J. P. Costas (1984). *A study of a class of detection waveforms having nearly ideal range-doppler ambiguity properties*, Proceedings of the IEEE, Vol. 72, No. 8, 996-1009.

[2] S. W. Golomb (1984). *Algebraic constructions for Costas arrays*, Journal of Combinatorial Theory, Series A, Volume 37, Issue 1, 13-21.

[3] S. W. Golomb and H. Taylor (1984). *Constructions and properties of Costas arrays*, Proceedings of the IEEE, vol. 72, No. 9,1143-1163.

[4] S. Golomb and H. Taylor (1982). *Two-dimensional synchronization patterns for minimum ambiguity*, IEEE Trans. on Information Theory, vol IT-28, Issue 4, 600-604.

[5] O. Moreno, R. A. Games and H. Taylor (1993). *Sonar Sequences from Costas Arrays and the Best Know Sonar Sequences with up to 100 Symbols*, IEEE Transactions on Information Theory, Vol 39, No. 6.

[6] O. Moreno, D. Bollman and L.Yuchun (2003), *Exhaustive search for Costas-type sequences for multi-target recognition*, Proceedings of the The Ninth IEEE Workshop on Future Trends of Distributed Computing Systems (FTDCS?03), 354 - 358.

[7] D. Ruiz, C. Trujillo and Y. Caicedo (2014). *New Constructions of Sonar Sequences*. IJBAS: International Journal of Basic & Applied Sciences. Vol. 14 Issue 01, 12-16.

[8] I. Ruzsa (1993). *Solving a linear equation in a set of integers I*. Acta Arithmetica. Vol. LXV, No. 3, 259-282.

[9] J. Singer (1938). *A theorem infinite projective geometry and some applications to number theory*, Transactions of the American Mathematical Society, Vol. 43, No. 3, 377-385.

[10] S. Haykin (2009). *Communication Systems*, 5th ed. New York, Wiley, 440 p.

[11] K. Taylor, S. Rickard, K. Drakakis (2011), *Costas arrays: Survey, standardization, and MATLAB toolbox*, ACM Trans. Math. Softw., Vol. 37 No. 4, 1-31.