NUEVAS CONSTRUCCIONES DE SECUENCIAS SONAR Y SUS PROPIEDADES

NIDIA YADIRA CAICEDO BRAVO
Universidad del Valle

CARLOS ALBERTO TRUJILLO
Universidad del Cauca

ALTENCOA 6 - 2014
Universidad de Nariño
San Juan de Pasto
Agosto de 2014

Conjunto de Sidon o B_2

Definición

Sea $(G, *)$ un grupo. El conjunto, $\mathcal{A} = \{a_1, \ldots, a_n\} \subset G$ es un conjunto de Sidon si para todo $x \in G$ y todo $a_i, a_j \in \mathcal{A}$ con $1 \leq i \leq j \leq n$, el número de soluciones de la ecuación $x = a_i * a_j$ es 0 o 1.

Definición

Sea $(G, *)$ un grupo. El conjunto, $\mathcal{A} = \{a_1, \ldots, a_n\} \subset G$ es un conjunto de Sidon si para todo $x \in G$ y todo $a_i, a_j \in \mathcal{A}$ con $1 \leq i \leq j \leq n$, el número de soluciones de la ecuación $x = a_i * a_j$ es 0 o 1.

Por ejemplo, en el grupo $(\mathbb{Z}, +)$ el conjunto:

$$\mathcal{A} = \{0, 1, 4, 9, 11\}$$

Definición

Sea $(G, *)$ un grupo. El conjunto, $\mathcal{A} = \{a_1, \ldots, a_n\} \subset G$ es un conjunto de Sidon si para todo $x \in G$ y todo $a_i, a_j \in \mathcal{A}$ con $1 \leq i \leq j \leq n$, el número de soluciones de la ecuación $x = a_i * a_j$ es 0 o 1.

Por ejemplo, en el grupo $(\mathbb{Z}, +)$ el conjunto:

$$\mathcal{A} = \{0, 1, 4, 9, 11\}$$

+	0	1	4	9	11
0	0	1	4	9	11
1		2	5	10	12
4			8	13	15
9				18	20
11					22

Problema

Estudiar el comportamiento asintótico de la función:

$$f_2(G) := \max\{|\mathcal{A}| : \mathcal{A} \subseteq G \text{ es un conjunto de Sidon}\}.$$

Problema

Estudiar el comportamiento asintótico de la función:

$$f_2(G) := \max\{|\mathcal{A}| : \mathcal{A} \subseteq G \text{ es un conjunto de Sidon}\}.$$

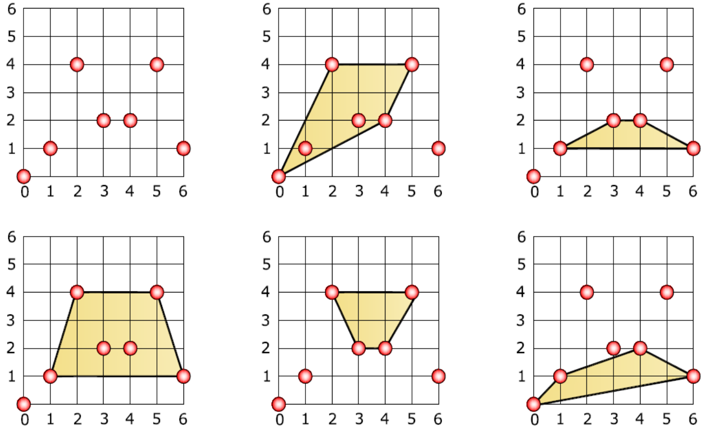
Existen tres construcciones de conjuntos de Sidon que proporcionan conjuntos maximales.

- La construcción de Singer (1938) que implica $f_2(\mathbb{Z}_{q^2+q+1}) = q+1$,
- La construcción de Bose (1942) que implica $f_2(\mathbb{Z}_{q^2-1}) = q$,
- La construcción de Ruzsa (1993) que implica $f_2(\mathbb{Z}_{p^2-p}) = p-1$.

Conjunto de Sidon en dos dimensiones

Los conjuntos de Sidon enteros en dos dimensiones tienen una interesante interpretación geométrica: se pueden ver como aquellos que tienen la propiedad especial que no es posible "dibujar" un paralelogramo usando sus puntos como vértices.

Los conjuntos de Sidon enteros en dos dimensiones tienen una interesante interpretación geométrica: se pueden ver como aquellos que tienen la propiedad especial que no es posible “dibujar” un paralelogramo usando sus puntos como vértices.



Conjunto de Sidon o B_2

Dado cualquier campo F con las operaciones de adición y multiplicación $(F, +, \cdot)$ tenemos dos grupos $(F, +)$ y $(F^*, \cdot)$, donde $F^* = F \setminus \{0\}$.

Con estos dos grupos podemos formar los siguientes grupos producto:

1. $(F, +) \times (F, +)$,
2. $(F, +) \times (F^*, \cdot) \cong (F^*, \cdot) \times (F, +)$,
3. $(F^*, \cdot) \times (F^*, \cdot)$.

Dado cualquier campo F con las operaciones de adición y multiplicación $(F, +, \cdot)$ tenemos dos grupos $(F, +)$ y $(F^*, \cdot)$, donde $F^* = F \setminus \{0\}$.

Con estos dos grupos podemos formar los siguientes grupos producto:

1. $(F, +) \times (F, +)$,
2. $(F, +) \times (F^*, \cdot) \cong (F^*, \cdot) \times (F, +)$,
3. $(F^*, \cdot) \times (F^*, \cdot)$.

En estos grupos es posible construir algunos conjuntos de Sidon en dimensión dos:

1. $\mathcal{C}(F) = \{(x, x^2) : \ x \in F\} \subset (F, +) \times (F, +)$.
2. $\mathcal{D}_1(F) = \{(x, x) : \ x \in F^*\} \subset (F^*, \cdot) \times (F, +)$ y

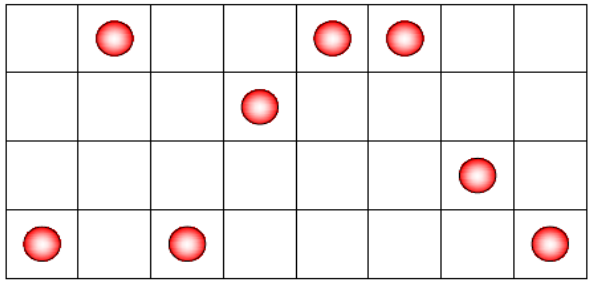
   $\mathcal{D}_2(F) = \{(x, x) : \ x \in F^*\} \subset (F, +) \times (F^*, \cdot)$.
3. $\mathcal{D}_a(F) = \{(x - a, x) : \ x \in F^*, \ x \neq a, \ a \in F^*\} \subset (F^*, \cdot) \times (F^*, \cdot)$.

En particular, si consideramos el cuerpo finito $F = \mathbb{F}_q$, donde $q = p^n$, $n \in \mathbb{N}$ y p primo, y usando algunos isomorfismos conocidos tenemos:

1. $\mathcal{C}(\mathbb{F}_q) = \{(x, x^2) : \ x \in \mathbb{F}_q\} \subset (\mathbb{F}_q \times \mathbb{F}_q, +)$,
2. $\mathcal{D}_1(\mathbb{F}_q \times \mathbb{Z}_{q-1}) = \{(x, \log_\theta x) : \ x \in \mathbb{F}_q^*\} \subset (\mathbb{F}_q \times \mathbb{Z}_{q-1}, +)$,

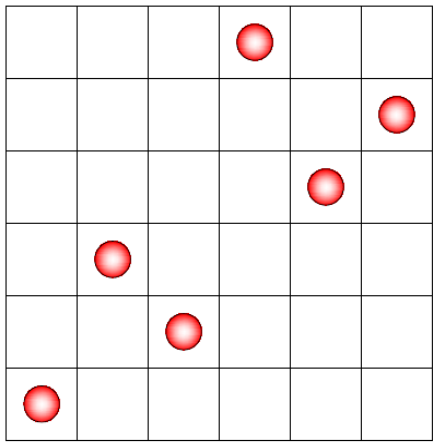
   $\mathcal{D}_2(\mathbb{Z}_{q-1} \times \mathbb{F}_q) = \{(k, \theta^k) : \ k \in \mathbb{Z}_{q-1}^*\} \subset (\mathbb{Z}_{q-1} \times \mathbb{F}_q, +)$,
3. $\mathcal{D}_a(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}) = \{(\log_\theta(\theta^k - a), k) : \ k \in \mathbb{Z}_{q-1}\} \subset (\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}, +)$.

Las secuencias sonar, son un tipo de conjuntos de Sidon en dos dimensiones que se definen en términos de funciones; estas secuencias fueron introducidas por Golomb y Taylor en 1982, 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.



Secuencia Sonar 4×8

Los arreglos Costas aparecen por primera vez en 1965 en el contexto de la detección sonar con J. Costas.



Arreglo Costas 6×6

Definición (Propiedad de Diferencias Distintas)

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:

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

Definición (Propiedad de Diferencias Distintas)

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:

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

Equivalentemente, si $G_f = \{(x, f(x)) : x \in [1, n]\}$ es un conjunto de Sidon en el grupo aditivo $\mathbb{Z} \times \mathbb{Z}$.

Definición (Propiedad de Diferencias Distintas)

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:

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

Equivalentemente, si $G_f = \{(x, f(x)) : x \in [1, n]\}$ es un conjunto de Sidon en el grupo aditivo $\mathbb{Z} \times \mathbb{Z}$.

Definición (Propiedad de Diferencias Distintas Modulares)

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 $1 \leq h \leq n-1$ y $1 \leq i, j \leq n-h$,

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

Definición

Una **secuencia sonar** de orden $m \times n$ es una función $f : [1, n] \to [1, m]$ que tiene la propiedad de diferencias distintas; dicho de otro modo, una secuencia sonar es una función Sidon de $[1, n]$ en $[1, m]$.

Definición

Una **secuencia sonar** de orden $m \times n$ es una función $f : [1, n] \to [1, m]$ que tiene la propiedad de diferencias distintas; dicho de otro modo, una secuencia sonar es una función Sidon de $[1, n]$ en $[1, m]$.

Definición

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

Definición

Una **secuencia sonar** de orden $m \times n$ es una función $f : [1, n] \to [1, m]$ que tiene la propiedad de diferencias distintas; dicho de otro modo, una secuencia sonar es una función Sidon de $[1, n]$ en $[1, m]$.

Definición

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

Definición

Un **arreglo Costas** de orden n es una permutación $f : [1, n] \to [1, n]$ que tiene la propiedad de diferencias distintas; es decir, un arreglo Costas es una función Sidon biyectiva de $[1, n]$ en $[1, n]$.

Problema 1

Para m fijo encontrar el mayor n para el cual existe una secuencia sonar $m \times n$.

Problema 1

Para m fijo encontrar el mayor n para el cual existe una secuencia sonar $m \times n$.

Problema 2

¿Existen secuencias sonar modular para todo m con m elementos?

Problema 1

Para m fijo encontrar el mayor n para el cual existe una secuencia sonar $m \times n$.

Problema 2

¿Existen secuencias sonar modular para todo m con m elementos?

Problema 3

¿Existen arreglos Costas para todo n?

Teorema (Construcción cuadrática)

Sean p un primo impar, a, b, c enteros tales que $a \not\equiv 0 \pmod{p}$. 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 (Construcción Shift)

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

Teorema (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 $p \times p$. Si $s = 0$, la función $f : [1, p-1] \to \mathbb{Z}_p$ definida como antes es una secuencia sonar modular $p \times (p-1)$.

Teorema (Construcción Welch Logarítmica)

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

Teorema (Construcción Golomb-Lempel)

Sea $q \geq 2$ una potencia prima, y sean α, β elementos primitivos de $\mathbb{F}_q$. La función $f : [1, q-2] \to \mathbb{Z}_{q-1}$ 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.

Nuevas construcciones de Secuencias Sonar Modulares, que provienen de los conjuntos de Sidon tipo Bose y tipo Ruzsa.

Teorema

Sean $m, b \in \mathbb{N}$ *y* $A = \{a_1, \ldots, a_n\}$ *un conjunto de Sidon en el grupo aditivo* $\mathbb{Z}_{mb}$. *Si* $A \bmod b := \{a \bmod b : a \in A\} = [1, n]$, *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* A *tal que* $a_i \equiv i \bmod b$.

Ejemplo

Sean $q = 9$, $mb = 80 = 8 * 10$.

Un conjunto de Sidon con 9 elementos en el grupo aditivo $\mathbb{Z}_{80}$ que proviene de la construcción de Bose es:

$$\mathcal{B} = \{1, 6, 13, 14, 28, 49, 52, 75, 77\}$$

Ejemplo

Sean $q = 9$, $mb = 80 = 8 * 10$.

Un conjunto de Sidon con 9 elementos en el grupo aditivo $\mathbb{Z}_{80}$ que proviene de la construcción de Bose es:

$$\mathcal{B} = \{1, 6, 13, 14, 28, 49, 52, 75, 77\}$$

Este conjunto satisface que

$$\mathcal{B}(\mathrm{mod}\, 10) = \{1, 6, 3, 4, 8, 9, 2, 5, 7\} = [1, 9].$$

Entonces por el Teorema anterior si consideramos $m = 8$, $b = 10$ la función

$$\begin{aligned} f : [1, 9] &\to \mathbb{Z}_8 \\ i &\mapsto f(i) = \lfloor b_i/8 \rfloor \end{aligned}$$

donde $b_i \in \mathcal{B}$, es una secuencia sonar modular 8×9.

Explícitamente,

$$
\begin{aligned}
1 \equiv 1(\mathrm{mod}\,10) \rightarrow b_1 = 1 \quad &\rightarrow f(1) = \lfloor 1/10 \rfloor = 0 \\
52 \equiv 2(\mathrm{mod}\,10) \rightarrow b_2 = 52 \quad &\rightarrow f(2) = \lfloor 52/10 \rfloor = 5 \\
13 \equiv 3(\mathrm{mod}\,10) \rightarrow b_3 = 13 \quad &\rightarrow f(3) = \lfloor 13/10 \rfloor = 1 \\
14 \equiv 4(\mathrm{mod}\,10) \rightarrow b_4 = 14 \quad &\rightarrow f(4) = \lfloor 14/10 \rfloor = 1 \\
75 \equiv 5(\mathrm{mod}\,10) \rightarrow b_5 = 75 \quad &\rightarrow f(5) = \lfloor 75/10 \rfloor = 7 \\
6 \equiv 6(\mathrm{mod}\,10) \rightarrow b_6 = 6 \quad &\rightarrow f(6) = \lfloor 6/10 \rfloor = 0 \\
77 \equiv 7(\mathrm{mod}\,10) \rightarrow b_7 = 77 \quad &\rightarrow f(7) = \lfloor 77/10 \rfloor = 7 \\
28 \equiv 8(\mathrm{mod}\,10) \rightarrow b_8 = 28 \quad &\rightarrow f(8) = \lfloor 28/10 \rfloor = 2 \\
49 \equiv 9(\mathrm{mod}\,10) \rightarrow b_9 = 49 \quad &\rightarrow f(9) = \lfloor 49/10 \rfloor = 4
\end{aligned}
$$

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

BOSE

Corolario 1

Sean q una potencia prima, θ un elemento primitivo del cuerpo finito $\mathbb{F}_q$ y $B(q,\theta)$ un conjunto de Sidon tipo Bose en el grupo aditivo $\mathbb{Z}_{q^2-1}$.
La función $f : [1, q] \to \mathbb{Z}_q$ 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 $b_i \equiv i \bmod (q+1)$.

RUZSA

Corolario 2

Sean p un número primo, θ un elemento primitivo del cuerpo finito $\mathbb{F}_p$ y $R(p,\theta)$ 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 $r_i \equiv i \bmod p$.

RUZSA

Corolario 3

Sea $R(p,\theta)$ 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 $r_i \equiv i \bmod (p-1)$.

Propiedades de las secuencias sonar modulares

Se pueden hacer algunas transformaciones en las secuencias sonar modulares $m \times n$ para obtener mejores secuencias sonar, estas transformaciones son:

1. Agregar a módulo m, $f_{+a}(i) = [f(i) + a] \,(\mathrm{mod} m)$.
2. Multiplicación por u módulo m, $f_{\times u}(i) = uf(i)(\mathrm{mod} m)$.
3. Cizallamiento por s módulo m, $f_{schear(s)}(i) = [f(i) + si] \,(\mathrm{mod} m)$.

Se pueden combinar las anteriores transformaciones obteniendo el siguiente resultado.

Teorema

Si f es una secuencia sonar modular $m \times n$ y u es una unidad módulo m , entonces g definida por

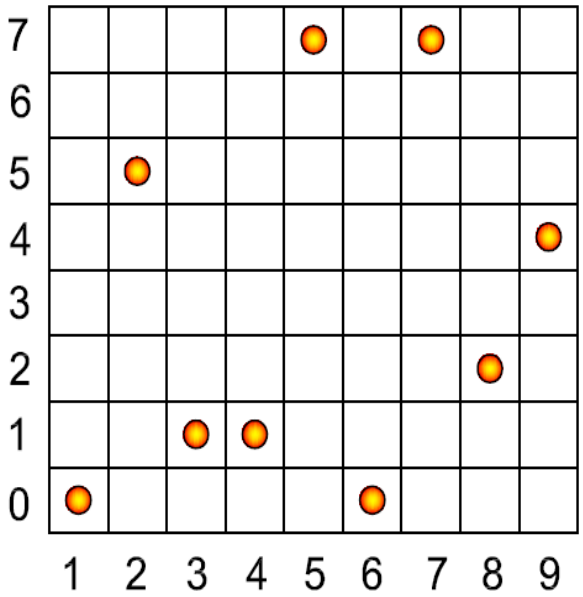
$$g(i) = uf(i) + si + a$$

es una secuencia sonar modular $m \times n$.

Ejemplo

Usando el ejemplo que proviene de la construcción de Bose, tenemos la secuencia sonar modular 8×9

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



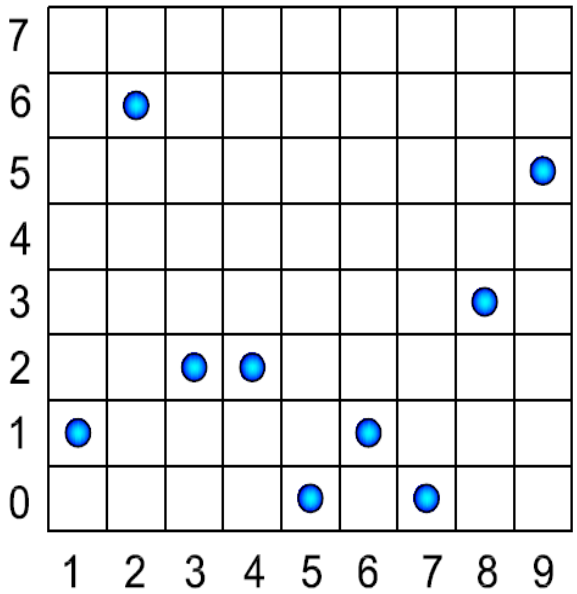
Ejemplo

Si aplicamos la propiedad (1) a la secuencia sonar anterior tenemos que la función:

$f_{+1} : [1, 9] \to \mathbb{Z}_8$ definida por $f_{+1}(i) = f(i) + 1$

produce la secuencia sonar modular:

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

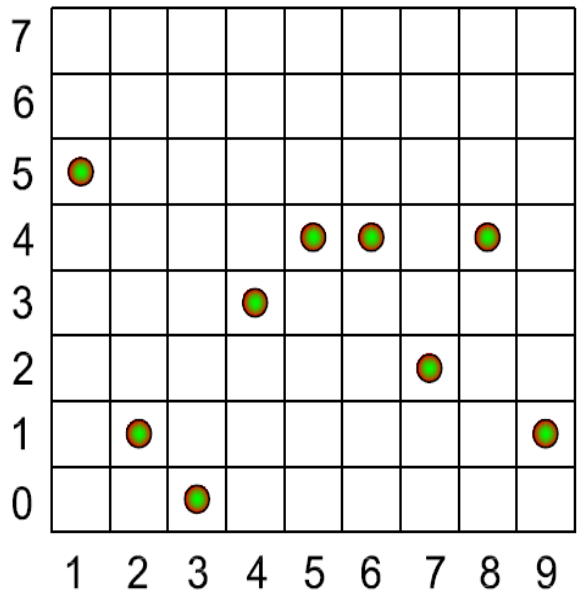


Ahora si aplicamos el último teorema y consideramos la función:

$g : [1, 9] \to \mathbb{Z}_8$ definida por $g(i) = 5f(i) + 3i + 2$

obtenemos la siguiente secuencia sonar modular

$$S_1 = \{(1, 5), (2, 1), (3, 0), (4, 3), (5, 4), (6, 4), (7, 2), (8, 4), (9, 1)\}$$



Bibliografía

- O. Moreno, R. A. Games y H. Taylor, *Sonar Sequences from Costas Arrays and the Best Know Sonar Sequences with up to 100 Symbols*, IEEE Trans. Inform. Theory, vol 39, N° 6, 1985-1987. Nov. 1993.

- Golomb y Taylor S. Golomb y H. Taylor, *Two-dimensional synchronization patterns for minimum ambiguity*, IEEE Transactions on Information Theory, vol IT-28, 263-272. July 1982. ISSN :0018-9448.

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

15 AÑOS

MUCHAS GRACIAS