JTN 2015
Universidad de Valladolid
June 29-July 3, 2015

Secuencias sonar como conjuntos de Sidon y nuevas construcciones

Nidia Yadira Caicedo[1], Carlos Alberto Trujillo[2]

[1] *Universidad del Tolima, Colombia, nycaicedob@ut.edu.co*
[2] *Universidad del Cauca, Colombia, trujillo@unicauca.edu.co*

1 Secuencias sonar

Sean $a,b \in \mathbb{Z}$, con $a < b$, mediante $[a,b]$ denotamos el conjunto de todos los enteros x tales que $a \leq x \leq b$.

Una función $f : [1,n] \longrightarrow [1,m]$ tiene la *propiedad de diferencias distintas* si para todo $i,j,h \in \mathbb{N}$, $1 \leq h \leq n-1$, $1 \leq i,j \leq n-h$,

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

Si además, identificamos a $[1,m]$ con $\mathbb{Z}_m$, una función $f : [1,n] \longrightarrow \mathbb{Z}_m$ tiene la *propiedad de diferencias distintas módulo m* si para todo $i,j,h \in \mathbb{N}$, $1 \leq h \leq n-1$, $1 \leq i,j \leq n-h$,

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

Una *secuencia sonar* $m \times n$ es una función $f : [1,n] \longrightarrow [1,m]$ que tiene la propiedad de diferencias distintas. Mientras que una *secuencia sonar modular* $m \times n$ es una función $f : [1,n] \longrightarrow \mathbb{Z}_m$ con la propiedad de diferencias distintas módulo m. Ver [2].

Secuencias sonar fueron introducidas en [3] como ejemplos de modelos de sincronización bidimensional con ambigüedad mínima. Una secuencia sonar puede dibujarse como un arreglo $m \times n$ en el cual cada columna i tiene un único punto$(i, f(i))$, es decir en el grafo de la función hay un y solo un punto en cada vertical. La propiedad de diferencias distintas es equivalente al hecho que cualquier copia corrida horizontal o verticalmente coincide con el arreglo original en a lo sumo un punto (propiedad de ambigüedad o de autocorrelación mínima). Esta es una propiedad muy útil en las aplicaciones y en muchos problemas de sincronización ([3]).

El problema principal de las secuencias sonar es: *para m fijo, encontrar el máximo n para el cual existe una secuencia sonar* $m \times n$.

La cota superior trivial es $n \leq 2m$, la cual se logra hasta $m = 4$. En [4] se afirma que es posible probar $n < m + 3m^{2/3} + 2m^{1/3} + 9$. Para valores de m de interés en ingeniería, $m \leq 100$, las cotas anteriores no son adecuadas. Mejorar estas cotas para m pequeño es un problema abierto.

Búsquedas computacionales han determinado el valor óptimo de n para $m \leq 15$:

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
n	2	4	6	8	9	11	12	13	14	16	17	18	19	21	22

Las construcciones conocidas de secuencias sonar hasta ahora se han realizado "directamente" en dos dimensiones (ver [2]). A continuación las describimos.

Construcción Cuadrática (extendida). Sea p un primo impar, la función

$$\begin{array}{rccc} C: & [1,p+1] & \longrightarrow & \mathbb{Z}_p \\ & i & \mapsto & i^2 \end{array},$$

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

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

$$\begin{array}{rccc} S: & [1,q] & \longrightarrow & \mathbb{Z}_{q-1} \\ & i & \mapsto & \log_\beta(\alpha^{qi}+\alpha^i) \end{array},$$

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

Construcción exponencial (extendida) de Welch. Sean p un primo y α una raíz primitiva módulo p, la función

$$\begin{array}{rccc} W_e: & [0,p-1] & \longrightarrow & \mathbb{Z}_p \\ & i & \mapsto & \alpha^{i+1} \end{array},$$

es una secuencia modular $p \times p$.

Construcción logarítmica de Welch. Sean p un primo y α una raíz primitiva módulo p, la función

$$\begin{array}{rccc} W_l: & [1,p-1] & \longrightarrow & \mathbb{Z}_{p-1} \\ & i & \mapsto & \log_\alpha i \end{array},$$

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

Construcción de Golomb. Sean q una potencia prima mayor que 2, α y β elementos primitivos de $\mathbb{F}_q$, la función

$$\begin{array}{rccc} G: & [1,q-2] & \longrightarrow & \mathbb{Z}_{q-1} \\ & i & \mapsto & \log_\beta(1-\alpha^i) \end{array},$$

es una secuencia sonar modular $(q-1) \times (q-2)$.

2 Conjuntos de Sidon

Un *conjunto de Sidon* es un conjunto de enteros A con la propiedad de que todas las sumas de dos elementos de A son distintas (excepto por la conmutatividad). Este concepto puede extenderse claramente a grupos conmutativos.

Si G es un grupo conmutativo, notado aditivamente, y A es un subconjunto de G, entonces A es un *conjunto de Sidon en* G si para todo $a,b,c,d \in A$,

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

Es decir, si todas las sumas de dos elementos de A producen elementos distintos en G.

Si G es el grupo de los enteros módulo m, solo se conocen tres construcciones de conjuntos de Sidon, describimos las dos que necesitamos en esta comunicación.

Construcción de Bose. Sean q una potencia prima y θ un elemento primitivo de $\mathbb{F}_{q^2}$, el conjunto

$$B(q,\theta) := \left\{ k \in \left[1, q^2-1\right] : \theta^k - \theta \in \mathbb{F}_q \right\},$$

es un conjunto de Sidon en $\left(\mathbb{Z}_{q^2-1},+\right)$, con q elementos. Además, este conjunto es tal que:

$$B(q,\theta)(\mathrm{mod}\, q+1) := \{k(\mathrm{mod}\, q+1) : k \in B(q,\theta)\} = [1,q]\,.$$

Construcción de Ruzsa. Sean p un primo y α una raíz primitiva módulo p, el conjunto

$$R(p,\alpha) := \left\{r_i := \left[ip - \alpha^i\,(p-1)\right](\mathrm{mod}\, p^2-p) : 1 \le i \le p-1\right\},$$

es un conjunto de Sidon en $\left(\mathbb{Z}_{p^2-p},+\right)$, con $p-1$ elementos. Además, este conjunto es tal que:

$$\begin{aligned} R(p,\alpha)(\mathrm{mod}\, p) &= [1,p-1]\,, \\ R(p,\alpha)(\mathrm{mod}\, p-1) &= [1,p-1]\,. \end{aligned}$$

En la siguiente sección, después de presentar el resultado principal de la comunicación, mostramos como a partir de estas dos contrucciones podemos obtener secuencias sonar.

3 Secuencias sonar como conjuntos de Sidon

No es difícil demostrar que una función $f : [1,n] \longrightarrow [1,m]$ es *una secuencia sonar si y sólo si su grafo es un conjunto de Sidon en el grupo aditivo* $\mathbb{Z}\times\mathbb{Z}$ (ver [5, 6]).

El siguiente resultado permite construir secuencias sonar a partir de conjuntos de Sidon especiales.

Theorem 1 *Sean m y b enteros positivos, y $A = \{a_1, a_2, \ldots, a_n\}$ un conjunto de Sidon en $(\mathbb{Z}_{mb},+)$. Si $\{a(\mathrm{mod}\, b) : a \in A\} = [1,n]$, entonces la función $f : [1,n] \longrightarrow \mathbb{Z}_m$ definida por $f(i) = \lfloor a_i/b \rfloor$, donde a_i es el único elemento de A tal que $a_i \equiv i(\mathrm{mod}\, p)$, es una secuencia sonar modular $m \times n$.*

Este teorema aplicado a las construcciones de Bose y Ruzsa, nos permiten obtener las siguiente construcciones de secuencias sonar.

Construcción de secuencias sonar a partir de conjuntos de Sidon tipo Ruzsa. Sea $R(p,\alpha)$ el conjunto de Sidon de la construcción de Ruzsa, entonces:

1. la función
$$\begin{array}{rccc} R_1: & [1,p-1] & \longrightarrow & \mathbb{Z}_{p-1} \\ & i & \mapsto & \left\lfloor \frac{r_i}{p} \right\rfloor \end{array},$$
donde r_i es el único elemento de $R(p,\alpha)$ tal que $r_i \equiv i(\mathrm{mod}\, p)$, es una secuencia sonar modular $(p-1)\times(p-1)$; y
2. la función
$$\begin{array}{rccc} R_2: & [1,p-1] & \longrightarrow & \mathbb{Z}_{p} \\ & i & \mapsto & \left\lfloor \frac{r_i}{p-1} \right\rfloor \end{array},$$
donde r_i es el único elemento de $R(p,\alpha)$ tal que $r_i \equiv i(\mathrm{mod}\, p-1)$, es una secuencia sonar modular $p\times(p-1)$.

Construcción de secuencias sonar a partir de conjuntos de Sidon tipo Bose. Sea $B(q,\theta)$ el connunto de Sidon de la construcción de Bose, entonces la función

$$\begin{array}{rccc} B: & [1,q] & \longrightarrow & \mathbb{Z}_{q-1} \\ & i & \mapsto & \left\lfloor \frac{b_i}{q+1} \right\rfloor \end{array},$$

donde b_i es el único elemento de $B(q,\theta)$ tal que $b_i \equiv i(\mathrm{mod}\, q-1)$ es una secuencia sonar modular $(q-1)\times q$.

4 Algunos problemas abiertos

El problema principal en secuencias sonar consiste en investigar las siguientes funciones:

$$\begin{aligned} G(m) &: = \max\{n \in \mathbb{N} : \text{existe una secuencia sonar } m \times n\}, \\ G(\text{mod}\, m) &: = \max\{n \in \mathbb{N} : \text{ existe una secuencia sonar modular } m \times n\}. \end{aligned}$$

Claramente $G(m) \geq G(\text{mod}\, m)$. Como m,encionamos, el primer problema consiste en mejorar la cota superior para la función $G(m)$.

De las construcciones conocidas, sabemos que:

$$\begin{aligned} G(\text{mod}\, p) &= p+1 \Longrightarrow G(p) \geq p+1, \\ G(\text{mod}\, q-1) &= q \Longrightarrow G(q-1) \geq q, \end{aligned}$$

para todo primo p y toda potencia prima q.

Problema 2. Probar o refutar que: $G(m) \geq G(\text{mod}\, m) \geq m$, para todo m.

El cuadro siguiente resume las construcciones de secuencias sonares modulares conocidas.

Construcciones Anteriores	Longitud	Módulo
Cuadrática (extendida)	$p+1$	p
Welch Exponencial (extendida)	p	p
Welch Logarítmica	$p-1$	$p-1$
Golomb/Lempel	$q-2$	$q-1$
Shift	q	$q-1$
Construcciones Nuevas	Longitud	Módulo
Sidon tipo Ruzsa 1	$p-1$	$p-1$
Sidon tipo Ruzsa 2	$p-1$	p
Sidon tipo Bose	q	$q-1$

Problema 3. ¿Existen otras construcciones modulares similarmente óptimas? ¿Existe alguna relación estrecha entre las construcciones anteriores y las recientemente obtenidas?

References

[1]

[2] Oscar Moreno, Richard A. Games and Herbert Taylor, *Sonar sequences from Costas arrays and the best known sonar sequences with up to 100 symbols*, IEEE Trans. Inform. Theory **39**, 6, pp. 1985-1987 (1993).

[3] S. W. Golomb and H. Taylor, *Two –dimensional synchronization patterns form minimum ambiguity*, IEEE Trans. Inform. Theory **28**, pp. 262-172 (1982).

[4] P. Erdos, R. I. Graham, I. Z. Rusza and H. Taylor, *Bounds for arrays of dots with distinc slopes for lenghts*, Combinatorica **12**, pp. 1-6 (1992).

[5] Yadira Caicedo, Diego Ruiz and Carlos Trujillo, *New constructions of sonar sequences*, IJBAS-IJENS, **14**, pp. 2-16 (2014).

[6] Julian Osorio, Diego Ruiz, Carlos Trujillo and Cristhian Urbano, *Secuencias sonar y conjuntos de Sidon*, Revista de Ciencias, Universidad del Valle, **18**, 1, pp. 73-83 (2014).