Facultad de Ciencias Naturales y Exactas
Universidad del Valle

Sonar Sequences and Sidon Sets

Rigo Julián Osorio **Diego Fernando Ruiz**
Carlos Alberto Trujillo **Cristhian Leonardo Urbano**
Universidad del Cauca

Received: October 23, 2013 Accepted: February 3, 2014

Pag. 33-42

Abstract

$\mathcal{A}$ is a Sidon set in an additive commutative group G if the number of representations of each non-identity element in G, as a difference of two elements in $\mathcal{A}$ is at most 1. An $m \times n$ sonar sequence is a function $f : \{1, \ldots, n\} \to \{1, \ldots, m\}$ such that its associated graph $G_f := \{(x, f(x)) : 1 \leq x \leq n\}$ is a Sidon set in the group $\mathbb{Z} \times \mathbb{Z}$. If $G(m)$ denotes the maximum positive integer such that there exists an $m \times n$ sonar sequence, using additive energy and some of its properties. In this paper, we show that $G(m) \leq m + 3{,}78m^{2/3} + 4{,}76m^{1/3} + 2$. Furthermore, using the construction of Sidon sets type Bose in $\mathbb{Z}_{q^2-1}$ we construct $(q-1) \times q$ sonar sequences for all prime power q.

Keywords: Sidon sets, sonar sequences, additive energy.

Secuencias sonar y conjuntos de Sidon

Resumen

$\mathcal{A}$ es un conjunto de Sidon en un grupo conmutativo G notado aditivamente si el número de representaciones de todo elemento no identidad de G como diferencia de dos elementos de $\mathcal{A}$ es a lo sumo 1. Una secuencia sonar $m \times n$ es una función $f : \{1, \ldots, n\} \to \{1, \ldots, m\}$ tal que su grafo asociado $G_f := \{(x, f(x)) : 1 \leq x \leq n\}$ es un conjunto de Sidon en el grupo $\mathbb{Z} \times \mathbb{Z}$. Si $G(m)$ denota el máximo entero positivo n tal que existe una secuencia sonar $m \times n$, utilizando el concepto de energía aditiva y algunas de sus propiedades elementales. En este trabajo se prueba que $G(m) \leq m + 3{,}78m^{2/3} + 4{,}76m^{1/3} + 2$. Además, utilizando la construcción de conjuntos de Sidon tipo Bose en $\mathbb{Z}_{q^2-1}$ se construyen secuencias sonar $(q-1) \times q$, para toda potencia prima q.

Palabras clave: Conjuntos de Sidon, secuencias sonar, energía aditiva.

1 Introducción

En teoría de números aditiva, uno de los problemas que ha tenido gran impacto en el área de las telecomunicaciones es el de los conjuntos de Sidon, el cual data desde 1930. Su nombre es en honor al analista Simon Sidon quien los introdujo con el propósito de resolver un problema en análisis armónico [1]. Sidon investigaba conjuntos de enteros positivos con la propiedad que las sumas de dos

elementos son todas distintas. Esta propiedad equivale a que las diferencias no cero entre cualquier par de elementos del conjunto son todas distintas. El concepto de conjunto de Sidon puede considerarse en situaciones más generales, por ejemplo en grupos conmutativos. En dimensión dos, un caso particular de los conjuntos de Sidon es el de "secuencia sonar", una función $f : \{1, \ldots, n\} \to \{1, \ldots, m\}$ tal que su grafo asociado

$$G_f := \{(x, f(x)) : 1 \leq x \leq n\}$$

es un conjunto de Sidon en $(\mathbb{Z} \times \mathbb{Z}, +)$. Su nombre se debe a que tales funciones se usan en aplicaciones a dispositivos tales como el sonar, denominado así por sus siglas en inglés "Sound Navigation And Ranging", que se utiliza como medio de localización acústica. Otras aplicaciones de conjuntos de Sidon en dimensión dos se encuentran en sistemas de comunicaciones óptimos, en criptografía, en la distribución de claves en redes de celulares, e incluso en el campo militar [2].

Formalmente, un conjunto de Sidon se define como sigue.

Definición 1.1. *Un conjunto $\mathcal{A}$ en un grupo abeliano G notado aditivamente es un conjunto de Sidon, si todas las diferencias $a - a'$ con $a, a' \in \mathcal{A}$, $a \neq a'$, son distintas.*

Sean a, m enteros con $a < m$. Mediante $[a, m]$ se representa el conjunto $\{a, a + 1, a + 2, \ldots, m\}$. A continuación se define el concepto de secuencia sonar como en [3].

Definición 1.2. *Una función $f : [1, n] \to [1, m]$ tiene la propiedad de diferencias distintas si para todos los enteros h, i, j, con $1 \leq h \leq n - 1$, $1 \leq i,\ j \leq n - h$ se tiene que*

$$f(i + h) - f(i) = f(j + h) - f(j) \Longrightarrow i = j. \tag{1}$$

Si $[1, m]$ se identifica con el conjunto de representantes de los enteros módulo m y la condición (1) se cambia por

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

f tiene la propiedad de diferencias distintas modular.

Definición 1.3. *Una función $f : [1, n] \to [1, m]$ es una secuencia sonar $m \times n$ si tiene la propiedad de diferencias distintas. Mientras que f es una secuencia sonar modular $m \times n$ si tiene la propiedad de diferencias distintas modular. En este caso se suele decir que f es una secuencia sonar módulo m con n elementos.*

El siguiente lema, cuya prueba se sigue directamente de la Definición 1.1, la Definición 1.3 y del grafo asociado a una secuencia sonar G_f, establece la relación entre conjuntos de Sidon y secuencias sonar.

Lema 1.1. *Una función $f : [1, n] \to [1, m]$ es una secuencia sonar si y sólo si el grafo de f, G_f, es un conjunto de Sidon en $(\mathbb{Z} \times \mathbb{Z}, +)$. Similarmente, f es una secuencia sonar modular $m \times n$ si y sólo si G_f es un conjunto de Sidon en $(\mathbb{Z} \times \mathbb{Z}_m, +)$.*

El problema fundamental en secuencias sonar consiste en investigar el comportamiento asintótico de las siguientes funciones:

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

Note que $G(m) \geq G \pmod m$. El siguiente lema establece las cotas superiores triviales para dichas funciones.

Lema 1.2. *Para todo entero positivo m, se tiene que $G(m) \leq 2m$ y $G(\text{mód}\, m) \leq m+1$.*

Demostración 1.1. *Sea $f : [1,n] \to [1,m]$ una secuencia sonar. De acuerdo con el Lema 1.1, todas las parejas $(1, f(i+1) - f(i))$, con $1 \leq i \leq n-1$, son distintas. Así, se tienen $n-1$ enteros distintos contenidos en $[-m+1, m-1]$, de donde $n-1 \leq 2m-1$. El caso modular es similar, sólo que las $n-1$ diferencias se consideran módulo m.*

El Teorema 4 de [4] establece que

$$G(m) < m + 5m^{2/3},$$

para m suficientemente grande. Utilizando el concepto de energía aditiva y algunas de sus propiedades elementales, en la siguiente sección se prueba que

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

En la Sección 3 se usa la construcción de conjuntos de Sidon tipo Bose para construir secuencias sonar que implican que

$$G(\text{mód}(q-1)) = q,$$

para toda q potencia prima. Además se presentan los algoritmos correspondientes a cada construcción, los cuales han sido implementados en MuPAD Pro 4.0.

Finalmente, en la Sección 4 se presentan algunos problemas relacionados con el trabajo.

2 Energía aditiva y cota superior para *G(m)*

Sean $(G,+)$ un grupo conmutativo notado aditivamente, y $\mathcal{A}$, $\mathcal{B} \subseteq G$. El conjunto suma y conjunto diferencia asociados con $\mathcal{A}$ y $\mathcal{B}$ se definen como

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

La función representación de $x \in G$ con respecto al conjunto $\mathcal{A} + \mathcal{B}$, y $\mathcal{A} - \mathcal{B}$ se define respectivamente como

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

donde $x - \mathcal{B}$ es la reflexión de $\mathcal{B}$ mediante x, $\mathcal{B} + x$ es la traslación de $\mathcal{B}$ mediante x, y $|\mathcal{X}|$ denota el cardinal del conjunto finito $\mathcal{X}$.

Note que

$$R_{\mathcal{A}-\mathcal{A}}(0) = |\mathcal{A}|,$$
$$\sum_{x\in\mathcal{A}+\mathcal{B}} R_{\mathcal{A}+\mathcal{B}}(x) = \sum_{x\in\mathcal{A}-\mathcal{B}} R_{\mathcal{A}-\mathcal{B}}(x) = |\mathcal{A}||\mathcal{B}|. \tag{2}$$

Observación 2.1. *Note que $\mathcal{A}$ es un conjunto de Sidon en G si y sólo si $R_{\mathcal{A}-\mathcal{A}}(x) \leq 1$ para todo $x \in G$, $x \neq 0$.*

Definición 2.1. *La energía aditiva entre $\mathcal{A}$ y $\mathcal{B}$, que se denota $E(\mathcal{A}, \mathcal{B})$, se define como:*

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

Note que $E(\mathcal{A}, \mathcal{B})$ cuenta el número de soluciones de la ecuación $a+b = a'+b'$, que es equivalente al número de soluciones de la ecuación $a - b' = a' - b$ o de la ecuación $a - a' = b' - b$. Esta observación permite establecer las siguientes identidades (ver [5] para una prueba detallada)

$$E(\mathcal{A}, \mathcal{B}) = \sum_{x\in\mathcal{A}+\mathcal{B}} R^2_{\mathcal{A}+\mathcal{B}}(x) = \sum_{x\in\mathcal{A}-\mathcal{B}} R^2_{\mathcal{A}-\mathcal{B}}(x)$$
$$= \sum_{x\in(\mathcal{A}-\mathcal{A})\cap(\mathcal{B}-\mathcal{B})} R_{\mathcal{A}-\mathcal{A}}(x) R_{\mathcal{B}-\mathcal{B}}(x). \tag{3}$$

El siguiente lema, debido a Ruzsa [6], relaciona el cardinal de un conjunto de Sidon en G con el cardinal de un conjunto cualquiera en el mismo grupo.

Lema 2.1. *Sea $\mathcal{A}$ un conjunto de Sidon en G y sea $\mathcal{B}$ cualquier subconjunto de G. Entonces*

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

Demostración 2.1. *Mediante la desigualdad de Cauchy–Schwartz y las identidades* (2) *y* (3) *se tiene que*

$$(|\mathcal{A}||\mathcal{B}|)^2 = \left(\sum_{x\in\mathcal{A}+\mathcal{B}} R_{\mathcal{A}+\mathcal{B}}(x)\right)^2$$
$$\leq |\mathcal{A} + \mathcal{B}| \sum_{x\in\mathcal{A}+\mathcal{B}} R^2_{\mathcal{A}+\mathcal{B}}(x)$$
$$= |\mathcal{A} + \mathcal{B}| \sum_{x\in(\mathcal{A}-\mathcal{A})\cap(\mathcal{B}-\mathcal{B})} R_{\mathcal{A}-\mathcal{A}}(x) R_{\mathcal{B}-\mathcal{B}}(x). \tag{4}$$

Como $\mathcal{A}$ es un conjunto de Sidon, entonces $R_{\mathcal{A}-\mathcal{A}}(x) \leq 1$ para todo $x \neq 0$. Por lo tanto, la suma de la desigualdad (4) *está acotada por*

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

lo que implica que

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

probando así la desigualdad deseada.

Utilizando el Lema 2.1 se tiene el primer resultado.

Teorema 2.1. *Si* $f:[1,n]\longrightarrow[1,m]$ *es una secuencia sonar entonces*

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

Demostración 2.2. *Dado que* f *es una secuencia sonar, su grafo es un conjunto de Sidon. Además se tiene que* $|G_f|=n$ *y* $G_f\subseteq[1,n]\times[1,m]$. *Considere el conjunto* $\mathcal{B}=[0,u]\times[0,u]$, *donde* $u=\lfloor cm^{\alpha}\rfloor$ *con* $\alpha,c>0$. *Es claro que* $|\mathcal{B}|=(u+1)^2$. *Note que* $G_f+\mathcal{B}\subseteq[1,n+u]\times[1,m+u]$, *y por tanto* $|G_f+\mathcal{B}|\leq(n+u)(m+u)$. *Así, de acuerdo con el Lema 2.1 se sigue que*

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

de donde

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

Luego, con $\alpha=2/3$ *y* $c=\sqrt[3]{2}$ *se tiene el resultado deseado.*

3 Una nueva construcción de secuencias sonar

En esta sección se presenta una nueva construcción de secuencias sonar, la cual es un caso particular de la dada en [7]. Esta se basa en la construcción de conjuntos de Sidon tipo Bose y algunas propiedades que se desprenden de ella.

3.1 Conjuntos de Sidon tipo Bose

La prueba del Teorema 3.1 y de la Proposición 3.1 se presenta en [7].

Teorema 3.1. (**Construcción Tipo Bose**). *Sean q una potencia prima, θ un elemento primitivo en $\mathbb{F}_{q^2}$ y $u \in \mathbb{F}_q^*$. Entonces,*

$$\mathcal{B} = \mathcal{B}(q, \theta, u) := \{\log_\theta(u\theta + a) : a \in \mathbb{F}_q\}, \tag{5}$$

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

Proposición 3.1. *El conjunto $\mathcal{B}$ del Teorema 3.1 satisface las siguientes propiedades.*

1. *Dados $b, b' \in \mathcal{B}$, si $b \neq b'$ entonces $b \not\equiv b' \pmod{q+1}$.*
2. *Para todo $b \in \mathcal{B}$, $b \not\equiv 0 \pmod{q+1}$.*
3. *$\mathcal{B} \pmod{q+1} := \{b \pmod{q+1} : b \in \mathcal{B}\} = [1, q]$.*

El siguiente algoritmo calcula un conjunto de Sidon tipo Bose en el grupo aditivo $\mathbb{Z}_{q^2-1}$.

Algoritmo 3.1. *Bose:*

Entrada: *Un primo* `p` *y un entero positivo* `r`.
Descripción: *Mediante la función interna de MuPAD* `Dom::GaloisField()`, *se crea el campo finito $\mathbb{F}_{q^2}$ y de este se escoge al azar un elemento primitivo mediante* `randomPrimitive()`, *para así realizar la asignación mencionada en el Teorema 3.1.*
Salida: *Una lista de enteros positivos* `B`, *que corresponde a un conjunto de Sidon tipo Bose.*

```
Bose:=proc(p,r)
begin
 K:=Dom::GaloisField(p,2*r);
 teta:=K::randomPrimitive();
 alfa:=teta^(q+1); q:=p^r; B:=[1];
 for j from 1 to q-1 do
     B:=[op(B),K::ln(teta+alfa^j,teta)];
 end_for;
 return(B);
end_proc;
```

3.2 Construcción de secuencia sonar

Haciendo uso del Teorema 3.1 y de la Proposición 3.1 se obtiene el siguiente resultado.

Teorema 3.2. *Sean q una potencia prima, $\mathcal{B}$ el conjunto de Sidon tipo Bose, y para cada $i \in [1, q]$ sea b_i el único elemento de $\mathcal{B}$ tal que $b_i \equiv i \pmod{q+1}$. La función $f : [1, q] \longrightarrow [0, q-2]$ definida mediante $f(i) = \lfloor b_i/(q+1) \rfloor$, es una secuencia sonar módulo $q-1$ con q elementos.*

Demostración 3.1. *Sean h, i, j enteros tales que $1 \leq h \leq q-1$ y $1 \leq i, j \leq q-h$. Suponga que $f(i+h) - f(i) \equiv f(j+h) - f(j) \pmod{q-1}$, es decir*

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

Luego existe un entero t tal que

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

Así

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

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

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

Dado que $0 \leq i+h < q+1$ y $0 \leq j+h < q+1$, de la última igualdad se tiene que $b_{i+h} - b_i \equiv b_{j+h} - b_j \pmod{q^2-1}$. Ya que $\mathcal{B}$ es un conjunto de Sidon módulo q^2-1 entonces $i = j$. Por lo tanto f es una secuencia sonar módulo $q-1$ con q elementos.

El siguiente algoritmo construye una secuencia sonar aplicando el Teorema 3.2.

Algoritmo 3.2. *SonarN1:*

Entrada: *Un primo* `p` *y un entero positivo* `r`.
Descripción: *Mediante el uso del Algoritmo 3.1 y la asignación descrita en el Teorema 3.2 se construye la secuencia sonar.*
Salida: *Una lista* `N1` *la cual es una secuencia sonar módulo $q-1$ con q elementos.*

```
SonarN1:=proc(p,r)
begin
 B:=Bose(p,r); q:=p^r; N1:=[];
 for j from 1 to q do
     for b in B  do
         if (b mod q+1)=j then
             N1:=[op(N1), i div q+1];
         end_if;
     end_for;
 end_for;
 return(N1);
end_proc;
```

En el siguiente ejemplo se usa el Algoritmo 3.2 para construir una secuencia sonar módulo 6 con 7 elementos.

Ejemplo 3.1. *Sean $p = 7$ y $r = 1$. Mediante el Algoritmo 3.1 se construye un conjunto de Sidon tipo Bose con 7 elementos sobre el grupo aditivo $\mathbb{Z}_{48}$.*

```
B := Bose(7,1); B = [1, 26, 11, 5, 12, 14, 31].
```

Ahora, continuando con el Algoritmo 3.2 y basado en el conjunto de Sidon `B` *se construye una secuencia sonar módulo 6 con 7 elementos.*

```
N1 := SonarN1(7,1); N1 = [0, 3, 1, 1, 0, 1, 3].
```

4 Algunos problemas relacionados

Mediante búsqueda exhaustiva hoy se conocen valores exactos para la función $G(m)$ (algunos se muestran en la Tabla 1).

Tabla 1: Valores exactos de $G(m)$ y $2m - G(m)$, para $1 \leq m \leq 14$.

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$G(m)$	2	4	6	8	9	11	12	13	14	16	17	18	19	21
$2m - G(m)$	0	0	0	0	1	1	2	3	4	4	5	6	7	7

A partir de ellos es natural preguntarse si

Problema 1. ¿$G(m) \leq 2m - 1$ para todo entero $m \geq 5$
Note que el resolver este problema implica una mejora en la cota superior de $G(m)$ para valores pequeños de m.

De otro lado, por el Lema 1.2 y el Teorema 2.1, el comportamiento de la cota superior de la función $G(m)$, para todo m en el intervalo respectivo, es como sigue

$$G(m) \leq 2m \leq m + 5m^{2/3} \leq m + 3{,}78m^{2/3} + 4{,}76m^{1/3} + 2,\ m \in [1, 78].$$
$$G(m) \leq 2m \leq m + 3{,}78m^{2/3} + 4{,}76m^{1/3} + 2 \leq m + 5m^{2/3},\ m \in [79, 113].$$
$$G(m) \leq m + 3{,}78m^{2/3} + 4{,}76m^{1/3} + 2 \leq 2m \leq m + 5m^{2/3},\ m \in [114, 125].$$
$$G(m) \leq m + 3{,}78m^{2/3} + 4{,}76m^{1/3} + 2 \leq m + 5m^{2/3} \leq 2m,\ m \geq 126,$$

de donde se sigue el segundo problema.

Problema 2. Mejorar la cota superior para la función $G(m)$. Relacionado con este problema, en [4] se afirma que $G(m) \leq m + 3m^{2/3} + 2m^{1/3} + 9$, con lo que se mejoraría la cota superior de $G(m)$ para valores grandes de m. Ya que en [4] no se presenta una prueba de este resultado, y de nuestra parte no ha sido posible establecerla, un problema específico consiste en obtener una prueba formal de dicha cota.

De la construcción presentada en la Sección 3 se infiere que $G(q-1) \geq q$ para toda potencia prima q. Además, de los resultados dados en [3], también se observa que $G(m) \geq m$ para todo $m \leq 100$. De este modo se presentan los siguientes problemas.

Problema 3. Probar o refutar que $G(m) \geq m$ para todo entero positivo m. Nuestros cálculos para otros valores particulares de m nos hace conjeturar que la respuesta es afirmativa.

Problema 4. Para cuáles valores de m se tiene que $G \pmod m = m+1$ y para cuáles $G \pmod m = m$?

Problema 5. Finalmente, un problema que podría resolver el comportamiento asintótico de la función $G(m)$ para valores grandes de m sería el estudio del siguiente límite

$$\lim_{m\to\infty} \frac{G(m)}{m}$$

Conjeturamos que si el límite anterior existe, este debe ser 1.

Agradecimientos

Los autores agradecen al profesor Javier Cilleruelo por la sugerencia hecha en ALTENCOA5–2012 de usar energía aditiva con el fin de lograr una mejor cota superior para la función $G(m)$. Además, se agradece a Colciencias y a la Universidad del Cauca por el apoyo al grupo de investigación "Álgebra, Teoría de Números y Aplicaciones–ALTENUA ERM" bajo los proyectos de investigación con código 110356935047 y VRI 3744, respectivamente.

Referencias bibliográficas

[1] Drakakis K. (2006). *A review of Costas arrays*, Journal of Applied Mathematics, 32.

[2] Taylor K., Rickard S. and Drakakis K. (2011). *Costas arrays: survey, standardization, and matlab toolbox*, ACM Transactions on Math. Software 37, (4) 1–31.

[3] Moreno O., Games R. and Taylor H. (1993). *Sonar sequences from Costas arrays and the best known sonar sequences with up to 100 symbols*, IEEE Transactions on Information Theory, 39 (6) 1985–1987.

[4] Erdos P., Graham R., Ruzsa I. and Taylor H.(1992). *Bounds for arrays of dots with distinct slopes or lengths*, Combinatorica, Akadémiai Kiado-Springer-Verlag 12 (1) 39–44.

[5] Tao T. and Vu V. H. (2006). *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, Cambridge University Press.

[6] Ruzsa I. (1993). *Solving a linear equation in a set of integers I*, Acta Arithmetica 65 (3) 256–282.

[7] Ruiz D., Caicedo Y. and Trujillo C. (2014). *New constructions of sonar sequences*, International Journal of Basic and Applied Sciences IJBAS–IJENS 14 (1) 12–16.

Dirección de los autores

Rigo Julián Osorio
Departamento de Matemáticas, Universidad del Cauca, Popayán - Colombia
rosorio@unicauca.edu.co

Diego Fernando Ruiz
Departamento de Matemáticas, Universidad del Cauca, Popayán - Colombia
dfruiz@unicauca.edu.co

Carlos Alberto Trujillo
Departamento de Matemáticas, Universidad del Cauca, Popayán - Colombia
trujillo@unicauca.edu.co

Cristhian Leonardo Urbano
Departamento de Matemáticas, Universidad del Cauca, Popayán - Colombia
cristhianleon@unicauca.edu.co