Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(185):1024-1044, octubre-diciembre de 2023. doi: https://doi.org/10.18257/raccefyn.1900

Artículo original

Conjuntos Sidon en Contextos Finitos

Sidon Sets in Finite Contexts

Carlos Alberto Trujillo Solarte

Grupo de Investigación: Álgebra, Teoría de Números y Aplicaciones:ERM COL0017217, Universidad del Cauca, FACNED, Departamento de Matemáticas

Artículo de posesión como miembro correspondiente de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.

Resumen

Un conjunto A de enteros se llama *conjunto Sidon* si todas las sumas de dos elementos en A son distintas; es decir si para todo $a, b, c, d \in A$

$$(a + b = c + d) \Rightarrow \{a, b\} = \{c, d\}.$$

Estos conjuntos los consideró el analista Simon Sidon, a principios de los años 1930, en sus investigaciones sobre análisis de Fourier. Una *regla Golomb* es un conjunto de enteros (no negativos) con la propiedad que todas las diferencias no cero son distintas. Estas reglas especiales aparecieron en el estudio de interferencias en radiofrecuencias, realizado por Wallace Babcock, a principios de los años 1950. En este artículo se realiza un recorrido a través de contextos finitos en los que intervienen estos objetos matemáticos. Los contextos considerados son: conjuntos finitos de números enteros, grupos cíclicos, retículos bidimensionales de coordenadas enteras (arreglos Costas, secuencias Sonar) y funciones APN.

En buena parte, estas notas son resultado parcial de actividades realizadas durante mi actual año sabático en la Universidad del Cauca, y son también una versión ampliada de la conferencia invitada, que con el mismo título presenté durante el "55 Congreso Nacional de la Sociedad Matemática Mexicana", realizado en la Universidad de Guadalajara del 23 al 28 de octubre de 2022 (https://www.smm.org.mx/congreso).

Palabras clave: Conjuntos Sidon; Reglas Golomb; Funciones Sidon; Arreglos Costas; Funciones APN; Espacios Sidon.

Abstract

A set of integers A is called a *Sidon set* if all the sums of two elements in A are distinct; that is, if for all $a, b, c, d \in A$, we have the implication $(a + b = c + d) \Rightarrow \{a, b\} = \{c, d\}$. The analyst Simon Sidon considered these sets, in the early 1930s, in his research on Fourier analysis. A *Golomb ruler* is a set of (nonnegative) integers with the property that all nonzero differences are distinct. Such special rules appeared in the study of radio frequency interference carried out byWallace Babcock, at the beginning of the 1950s. The article, of an informative nature, takes a tour through finite contexts in which these mathematical objects intervene. The contexts considered are: finite sets of integers, cyclic groups, two-dimensional integer coordinate lattices (Costas arrays, Sonar sequences) and APN functions.

To a large extent, these notes are the partial result of activities carried out during my current sabbatical year at the University of Cauca, and are also an expanded version of the invited conference, that with the same title present during the "55 National Congress of the Mexican Mathematical Society", held at the University of Guadalajara from 23 to 28 October, 2022 (https://www.smm.org.mx/congreso).

Keywords: Sidon Sets; Golomb Rulers;Sidon Functions; Costas Arrays; APN Functions; Sidon Spaces.

Citación: Trujillo Solarte CA. Conjuntos Sidon en Contextos Finitos. Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales. 47(185):1024-1044, octubre-diciembre de 2023. doi: https://doi.org/10.18257/raccefyn.1900

Editor: Clara Helena Sánchez

Correspondencia:
Carlos Alberto Trujillo;
trujillo@unicauca.edu.co

Recibido: 31 de marzo de 2023
Aceptado: 6 de diciembre de 2023
Publicado en línea: 15 de diciembre de 2023

Introducción

Un subconjunto A de los números enteros se llama *conjunto Sidon* si todas las sumas de dos elementos de A son distintas; es decir si

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

para todo $a,b,c,d \in A$. Estos conjuntos los consideró el analista Simon Sidon, a principios de los años 1930, en sus investigaciones sobre análisis de Fourier. Así, el contexto original de los conjuntos de Sidon son los números enteros, y también sus primeros resutados aparecen ligados al desarrollo de la teoría de números aditiva.

Una *regla Golomb* es un conjunto de enteros (no negativos) con la propiedad que todas las diferencias no cero son distintas. Estas reglas especiales aparecieron en el estudio de interferencias en radiofrecuencias, realizado por Wallace Babcock, a comienzos de los años 1950. El contexto en el que se originan las reglas Golomb puede ubicarse en el de algunas aplicaciones de las matemáticas a teoría de la comunicación e información.

Las presentes notas describen un recorrido personal a través de diversos contextos, tanto teóricos como aplicados, en los que intervienen los conjuntos Sidon y reglas Golomb, objetos matemáticos claramente equivalentes. El recorrido personal es producto de la experiencia obtenida por autor y su grupo de investigación durante el desarrollo de proyectos de investigación (Sucesiones de Sidon y conjuntos $B_h[g]$, código Colciencias 11030511450; Las funciones de Graham y Sloane problemas de cubrimiento y empaquetamiento, código Colciencias 1103516865; Construcción de conjuntos $B_h[g]$, propiedad de Midy y algunas aplicaciones, código Colciencias 1103569935047; Aplicaciones a teoría de información y comunicación de los conjuntos de Sidon y sus generalizaciones, código Colciencias 110371 250560); la dirección de tesis doctorales ver (**Caicedo Bravo**, 2016; **Delgado Ordoñez**, 2023; **Martos Ojeda**, 2019); y algunas publicaciones derivadas de ellas (**Caicedo**, **Martos**, & **Trujillo**, 2015, 2021; **Campo**, **Mutis**, & **Trujillo**, 2002; **Delgado**, **Martos**, & **Trujillo**, 2021; **Martos**, **Delgado**, & **Trujillo**, 2021; **Martos**, **Daza**, & **Trujillo**, 2021).

El contenido de las siguientes secciones se describe como sigue. En la Sección " Conjuntos Sidon en los Enteros " se presenta el problema original propuesto por Sidon, el Teorema de Erdös y Turán respecto al tamaño óptimo de un conjunto Sidon contenido en los primeros enteros positivos, concluyendo con una conjetura de Erdös relacionada. En " Reglas Golomb Enteras " se realiza un tratamiento similar para el caso de las reglas Golomb. En la Sección " Conjuntos Sidon en Grupos Finitos " se considera el problema de Sidon en el contexto abstracto de los grupos conmutativos finitos, comenzando con los problemas modulares, es decir en grupos cíclicos.

La Sección " En $\mathbb{Z}\times\mathbb{Z}$: Dimensión 2 " considera contextos bidimensionales desde la visión de Funciones Sidon enteras, se incluyen los arreglos Costas y las secuencias Sonar, que son conceptos originados en aplicaciones a teoría de la información y comunicación. Finalmente, " En Contexto Criptográfico " se mencionan algunas apariciones muy recientes de los conjuntos Sidon o análogos en contextos criptográficos: funciones Sidon entre grupos (funciones APN), espacios Sidon, y criptosistema Sidon.

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(185):1024-1044, octubre-diciembre de 2023. doi: https://doi.org/10.18257/raccefyn.1900

Conjuntos Sidon en los Enteros

Notación

Si a,b son números enteros, $a<b$, mediante $[a,b]$ se representa al conjunto de todos los números enteros comprendidos entre a y b, es decir

$$[a,b] := \{a, a+1, ..., b\}.$$

$|A|$ denota el cardinal del conjunto A. Los símbolos $\overline{\lim} f(x)$, $\underline{\lim} f(x)$ corresponden a los límites superior e inferior de $f(x)$, cuando $x \to \infty$. Para funciones $f,g:\ g(x) = O(f(x))$ significa que $g(x)$ es acotada superiormente por un múltiplo constante de $f(x)$; $g(x) \sim f(x)$ significa que $\lim_{x\to\infty}(f(x)/g(x)) = 1$. Otra notación usada se aclara cuando sea necesario.

En esta sección se presenta la definición original de conjunto Sidon, el problema finito relacionado, el primer resultado y la primera conjetura que originaron la temática que nos ocupa.

Orígenes: Simon Sidon y Paul Erdös

¿ Cuál es el máximo número de enteros positivos que pueden seleccionarse entre los primeros N, en forma tal que *todas las sumas de dos de ellos sean distintas* ?

Conjuntos con esta propiedad se llaman **Conjuntos** B_2, nombre asignado por Simon Sidon (**Sidon**, 1932), o **Conjuntos Sidon,** como los denominó Paul Erdös (**Erdös** & **Turán**, 1941).

Problema finito de Sidon

Sean N un entero positivo y $[1,N]$ el intervalo entero correspondiente.

Estimar tan exactamente como sea posible la función

$$S(N) := \max\{|A| : A \subseteq [1,N],\ A \text{ es conjunto Sidon}\}.$$

En muchos de sus artículos sobre teoría de números aditiva y combinatoria, Paul Erdös hace referencia a problemas propuestos por el analista húngaro Simon Sidon ver, por ejemplo, (**Erdos**, 1995; **Erdös**, 1992; **Erdős**, 1994).

En 1941, Erdös y Turán escriben: "Sea $a_1 < a_2 < ...$ una secuencia de enteros positivos, y suponga que las sumas $a_i + a_j$ (donde $i \le j$) son todas diferentes. Tales secuencias, llamadas secuencias B_2 por Sidon, aparecen en la teoría de series de Fourier. La pregunta propuesta por Sidon es: ¿Qué tan grande puede ser $S(N)$? Es decir, ¿cuántos términos que no exceden a N puede tener una secuencia B_2?" (**Erdös** & **Turán**, 1941, p. 212).

Mediante una construcción que utiliza residuos cuadráticos módulo un primo, prueban que

$$S(N) > \left(\frac{1}{\sqrt{2}} - \varepsilon\right)\sqrt{N},$$

para todo $\varepsilon > 0$ y $N > N_0(\varepsilon)$. Por el otro lado, contando diferencias pequeñas, demuestran que

$$S(N) < (1+\varepsilon)\sqrt{N},$$

para todo $\varepsilon > 0$ y $N > N_0(\varepsilon)$. Así,

$$\frac{1}{\sqrt{2}} \le \underline{\lim}\left(\frac{S(N)}{\sqrt{N}}\right) \le \overline{\lim}\left(\frac{S(N)}{\sqrt{N}}\right) \le 1 \text{(}\textbf{Erdös} \text{ \& } \textbf{Turán}\text{, 1941, pp. 212–213).}$$

Erdös y Turán afirman: "Es muy probable que $\lim(S(N)/\sqrt{N})$ exista, pero no hemos sido capaces de probar esto" (**Erdös** & **Turán**, 1941, p. 212). Posteriormente, Erdös escribe: "Recientemente noté que J. Singer en su artículo (**Singer**, 1938), probó que si m es una potencia de un primo entonces existen $m+1$ números $a_1 < a_2 < ... < a_{m+1} < m^2+m+1$ tales que las diferencias $a_i - a_j$ son congruentes, $mod\left(m^2+m+1\right)$, a los enteros $1,2,...,m^2+m$. Claramente las sumas $a_i + a_j$ son todas diferentes, y como el cociente de dos primos consecutivos tiende a 1, la construcción de Singer dá, para algún N grande, un conjunto con $S(N) > N^{1/2}(1-\varepsilon)$, para todo $\varepsilon > 0$. Este resultado demuestra que la cota superior anterior para $S(N)$ es lo mejor posible, excepto quizás por el término error $O\left(N^{1/4}\right)$", (**Erdös**, 1944, p. 208). De los comentarios anteriores se deduce el siguiente resultado.

Teorema 1 *(**Erdös**, 1944; **Erdös** & **Turán**, 1941)*

$$\lim_{N\to\infty}\left(\frac{S(N)}{\sqrt{N}}\right) = 1.$$

Cota superior para $S(N)$ y una Conjetura de Erdös

Hay varias pruebas para la cota superior de la función $S(N)$. Para todo entero positivo N:

$$\begin{aligned} S(N) &< N^{1/2} + O\left(N^{1/4}\right) \text{ (**Erdös**, 1944, p. 208),} \\ &< N^{1/2} + N^{1/4} + 1 \text{ (**Linström**, 1969, p. 211),} \\ &< N^{1/2} + N^{1/4} + \frac{1}{2} \text{ (**Cilleruelo**, 2010, Cor 2, p. 860).} \end{aligned}$$

Mientras que, si N es suficientemente grande:

$$\begin{aligned} S(N) &< N^{1/2} + 0.998N^{1/4} \text{(**Balogh**, **Füredi**, & **Roy**, 2021, Thm 1.1, p. 2),} \\ S(N) &< N^{1/2} + 0.99703N^{1/4} \text{ (**O'Bryant**, 2022, Thm 2, p. 2).} \end{aligned}$$

Todos los métodos utilizan la idea de Erdös y Turán: contar "diferencias pequeñas"; además la cota de Lindström también se deduce, con un poco de cuidado, de la prueba de Erdös y Turan (**Campo**, **Mutis**, & **Trujillo**, 2002).

El Teorema 1 prueba que: El máximo cardinal de un conjunto Sidon contenido en los primeros N enteros positivos se comporta asintóticamente como la raíz cuadrada de N, esto es: $S(N) \sim N^{1/2}$. Sin embargo, aún permancen sin resolver problemas relacionados con la siguiente conjetura.

Conjetura 1 *(**Erdős**, 1994, p. 264) Para todo $\varepsilon > 0$*

$$S(N) < \sqrt{N} + O(N^{\varepsilon}). \tag{1}$$

Paul Erdös se refiere a esta conjetura en casi todos sus artículos sobre problemas. En algunos ofrece premios por resolverla. Por ejemplo, (**Erdos**, 1995, p. 4): "Ofrezco \$500 dólares por una prueba o refutación de (1), conjeturo que para todo t y $n > n_0(t)$

$$S(N+t) \leq S(N) + 1, \tag{2}$$

y quizás para $t < \varepsilon N^{1/2}$

$$S(N+t) \leq S(N) + 1. \tag{3}$$

La verdad de (2) y (3) implicaría que el crecimiento de $S(N)$ es familiarmente regular".

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(185):1024-1044, octubre-diciembre de 2023. doi: https://doi.org/10.18257/raccefyn.1900

Reglas Golomb Enteras

Orígenes: Wallace Babcock y Solomon Golomb

En un reporte técnico (**Babcock**, 1953), sobre interferencia en sistemas de radio frecuencia Wallace Babcock escribió: "La forma más general de interferencia de tercer orden ocurre cuando tres frecuencias A, B, y C intermodulan de tal forma que producen interferencia sobre un canal que opera en frecuencia D. En este caso

$$A+B-C=D.$$

Otra forma de interferencia de tercer orden ocurre cuando el segundo armónico de A intermodula con B produciendo interferencia sobre un canal que opera en frecuencia C. En este caso

$$2A-B=C.$$

Esta sección se propone determinar si el espacio de frecuencias se puede conservar seleccionando cuidadosamente los canales en operación en forma tal que los productos de intermodulación que se forman caigan en canales diferentes a los que están operando. Esto se logra seleccionando los canales en forma tal que la diferencia de frecuencias entre cualquier par de esos canales es distinta a la de cualquier otro par". Veinte años después Martin Gardner utilizó el nombre de **reglas Golomb,** (**Gardner**, 1972), para referirse a conjuntos de enteros con diferencias distintas, en el contexto de rotulamiento de grafos (**Bloom** & **Golomb**, 1977; **Golomb**, 1972).

En 1986, se describe uno de los problemas formulados por Babcock (**Atkinson**, **Santoro**, & **Urrutia**, 1986): "Para todo m dado, encontrar enteros $0 \leq a_0 < a_1 < \ldots < a_m$ tales que no se cumple ninguna igualdad no trivial $a_r + a_s - a_t = a_u$. Los enteros son radio frecuencias y como es deseable tener un rango espectral pequeño, se buscan soluciones en las que a_m sea lo mínimo posible (soluciones óptimas) o al menos probablemente cercanas a ser óptimas (soluciones subóptimas)". Utilizando los conjuntos con diferencias distintas obtenidos por James Singer, (**Singer**, 1938) y un resultado análogo (**Bose**, 1942), en (**Atkinson**, **Santoro**, & **Urrutia**, 1986), se demuestra que:

$$1-\frac{2}{\sqrt{m}} < \frac{a_m}{m^2} < 1+\frac{m^{19/12}}{m^2}.$$

Un conjunto A de enteros no negativos se llama una *regla Golomb* si todas las diferencias no cero entre dos de sus elementos son distintas,es decir si para todo $a,b,c,d \in A$, con $a \neq b$ y $c \neq d$

$$(a-b=c-d) \Longrightarrow (a=b) \text{ y } (c=d).$$

Sus elementos se llaman *marcas*, el número de marcas *orden*, la máxima diferencia entre dos marcas, $l(A) := \max A - \min A$, se llama *longitud* de la regla.

Problema Golomb

. ¿Cuál es la mínima longitud de una regla Golomb con m marcas? Determinar la(s) regla(s) Golomb más corta(s) para un número fijo de marcas, calcular el valor de la función **OEIS (A003022)**

$$G(m) := \min\{l(A) : |A| = m, \text{ y } A \text{ es regla Golomb}\}.$$

Teorema 2 *(**Atkinson**, **Santoro**, & **Urrutia**, 1986, p. 615).*

$$\lim_{m\to\infty}\left(\frac{G(m)}{m^2}\right) = 1.$$

Cota Inferior para $G(m)$ y Conjetura ASU

La cota inferior para la función $G(m)$ ha sido mejorada como sigue:

$$\begin{aligned} G(m) &> \frac{m(m-1)}{2} \text{ (trivial)}, \\ &> m^2 - 2m\sqrt{m} \text{ (**Atkinson**, **Santoro**, \& **Urrutia**, 1986, p. 615)}, \\ &> m^2 - 2m\sqrt{m} + \sqrt{m} - 2 \text{ (**Dimitromanolakis**, 2002, Tmh 4.9, p. 32)}, \\ &> m^2 - 2m\sqrt{m-1} + m - \frac{m}{\sqrt{m-1}} - 1 \text{ (**Caicedo**, **Martos**, \& **Trujillo**, 2015, p. 168)}, \\ &> m^2 - 2m\sqrt{m} + m + \sqrt{m} - 1 \text{ (**O'Bryant**, 2022, Thm 1, p.2)}. \end{aligned}$$

Las pruebas utilizan ideas similares a los métodos usados en la obtención de cotas superiores para $S(N)$.

Conjetura 2 *(**Atkinson**, **Santoro**, & **Urrutia**, 1986, p. 615) Para todo entero positivo m,*

$$G(m) > m^2 - m\sqrt{m}.$$

Las funciones $S(N)$ y $G(m)$ como "problemas inversos"

Apostolos Dimitromanolakis, en su Tesis de Maestría (**Dimitromanolakis**, 2002), dedica el Capítulo 4 a la equivalencia del problema finito de Sidon y del problema de Golomb, y establece relaciones entre las funciones $S(N)$ y $G(m)$. Específicamente, prueba los siguientes resultados.

- Para todo par de enteros positivos m,N

$$\begin{aligned} S(N) &= m \Longleftrightarrow (G(m) \leq N-1 \text{ y } G(m+1) > N). \\ G(m) &= n \Longleftrightarrow (S(N) = m-1 \text{ y } S(N+1) = m). \end{aligned}$$

- Si $L(N)$ y $U(N)$ son funciones invertibles en un intervalo contenido en los enteros positivos, se tiene la siguiente implicación.

$$L(N) < S(N) < U(N) \Longrightarrow U^{-1}(m) < G(m) + 1 < L^{-1}(m).$$

  En el otro sentido, si $L(m)$ y $U(m)$ son funciones invertibles en un intervalo contenido en los enteros positivos, entonces

$$L(m) < G(m) < U(m) \Longrightarrow U^{-1}(N) < S(N) < L^{-1}(N).$$

Utilizando la cota superior de Lindström para $S(N)$, obtiene su cota inferior para $G(m)$

$$G(m) \geq m^2 - 2m\sqrt{m} + \sqrt{m} - 2.$$

Con ayuda computacional, prueba que:

$$\begin{aligned} G(m) &< m^2, \text{ para todo } m \leq 65000; \\ S(N) &> N^{1/2}, \text{ para todo } N < 4.2 \times 10^9. \end{aligned}$$

Ver también la Tesis de Maestría de Carlos Martos (**Martos Ojeda**, 2015).

De aquí en adelante, se usan los conceptos equivalentes Conjuntos Sidon y Reglas Golomb, según se trate de sumas o diferencias, respectivamente.

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(185):1024-1044, octubre-diciembre de 2023. doi: https://doi.org/10.18257/raccefyn.1900

Conjuntos Sidon en Grupos Finitos

Es conveniente considerar el concepto de conjunto Sidon en el anillo de enteros módulo N, $(\mathbb{Z}_N,+,\cdot)$. Un subconjunto A de $\mathbb{Z}_N$, con $k=|A|$ elementos, se llama un *conjunto Sidon módulo N* si todas las $\binom{k+1}{2}=\frac{k(k+1)}{2}$ sumas de dos elementos de A son distintas módulo N; equivalentemente A se llama una *regla Golomb módulo N* si todas las $2\binom{k}{2}=k(k-1)$ diferencias no cero son distintas módulo N. Claramente, si A es un conjunto Sidon módulo N, con k elementos entonces, contando diferencias distintas de cero, tenemos

$$k(k-1)\leq N-1. \tag{4}$$

En estas estructuras se han construido conjuntos Sidon "óptimamente densos", es decir con un número de elementos aproximadamente igual a $N^{1/2}$. Las siguientes construciones muestran que existen familias infinitas de conjuntos Sidon módulo N para las cuales (4) es lo mejor posible.

Construcciones en Grupos Cíclicos

Una excelente referencia sobre los problemas de Sidon es el texto Sequences (**Halberstam** & **Roth**, 1983), presenta una buena descripción de las construcciones debidas a Singer y a Bose, ya mencionadas. En los siguientes resultados, q es una potencia prima.

Teorema 3 *(**Singer**, 1938, pp. 380–381) Existen $q+1$ enteros $s_1,s_2,...,s_{q+1}$ tales que las q^2+q diferencias no cero s_i-s_j representan todos los residuos no cero módulo q^2+q+1.*

Teorema 4 *(**Bose**, 1942, pp. 1–15). Existen q enteros $b_1,b_2,...,b_q$ tales que las $q(q-1)$ diferencias no cero b_i-b_j representan todos aquellos residuos módulo q^2-1 que no son divisibles entre $q+1$.*

Corolario 5 *(**Halberstam** & **Roth**, 1983, pp. 80–81) Existen $q+1$ enteros $s_1,s_2,...,s_{q+1}$ tales que las sumas s_i+s_j, donde $1\leq i\leq j\leq m+1$, son distintas módulo q^2+q+1 ; y existen q enteros $b_1,b_2,...,b_q$ tales que las sumas b_i+b_j, donde $1\leq i\leq j\leq q$, son distintas módulo q^2-1 .*

Más recientemente, Imre Ruzsa construye un conjunto Sidon "denso" para todo primo impar p, utiliza la existencia de raíces primitivas módulo p.

Teorema 6 *(**Ruzsa**, 1993, Thm 4.4, p. 267). Existen $p-1$ enteros $r_1,...,r_{p-1}$ tales que las sumas r_i+r_j son todas diferentes módulo $p(p-1)$. Contando las diferencias, es fácil ver que no pueden haber p de tales números.*

Como todo conjunto Sidon módulo N, induce un conjunto Sidon entero contenido en $[0,N-1]$, estas construcciones modulares " óptimas" se utilizan para obtener "buenas" construcciones enteras, tanto para conjuntos Sidon como para reglas Golomb "sub-óptimamente cortas".

Problemas Modulares: Implicaciones para $S(N)$ y $G(m)$

Sea

$$S(modN):=\max\{|A|:A \text{ es conjunto Sidon módulo } N\},$$

entonces

$$S(modN)\leq S(N).$$

Así, buenas construcciones modulares inducen buenas construcciones enteras.

Problema Sidon modular

En el contexto de los grupos cíclicos finitos, el problema (modular) de Sidon consiste en "estimar, lo más exactamente posible, la función $S(modN)$" .

Contando diferencias, las construcciones de Singer, Bose y Ruzsa, implican:

$$\begin{aligned} S(q^2+q+1) &\geq q+1 = S(mod\ q^2+q+1), \\ S(q^2-1) &\geq q = S(mod\ q^2-1), \\ S(p^2-p) &\geq p-1 = S(mod\ p^2-p), \end{aligned}$$

para toda potencia prima q y todo primo p. Por otro lado, como la función $S(N)$ es creciente y el cociente entre primos consecutivos tiende a 1, se sigue que

$$1 \leq \underline{\lim}\left(\frac{S(N)}{N^{1/2}}\right).$$

Problema Golomb modular

Dados m y N, cuando existe una regla Golomb módulo N con m marcas, proponemos el siguiente problema natural; **problema modular de Golomb** que consiste en estimar lo más exactamente posible la función

$$G(m,modN) := \min\{l(A) : |A| = m \text{ y } A \text{ es una regla Golomb módulo } N\}.$$

Contando diferencias, en las construcciones modulares:

$$\begin{aligned} G(q+1,mod\ q^2+q+1) &\leq q^2+q, \\ G(q,mod\ q^2-1) &\leq q^2-2, \\ G(p-1,mod\ p^2-p) &\leq p^2-p-1, \end{aligned}$$

para toda potencia prima q y todo primo p. También para el caso entero:

$$\begin{aligned} G(q+1) &\leq q^2+q, \\ G(q) &\leq q^2-2, \\ G(p-1) &\leq p^2-p-1. \end{aligned}$$

Así, es posible mejorar un poco las cotas superiores para el caso entero utilizando la estructura de los grupos cíclicos.

Como $G(p) < p^2$, para todo primo p, se sigue que:

$$\overline{\lim}\left(\frac{G(m)}{m^2}\right) \leq 1.$$

Observación. Aparentemente, la función $G(m,modN)$ no ha sido investigada.

Conjuntos B_2 en Grupos Finitos

Sea $(G,+)$ grupo conmutativo, notado aditivamente. Un subconjunto A de G se llama un *conjunto B2 (Conjunto Sidon o Regla Golomb) en G* si para todo $a,b,c,d \in A$:

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

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(185):1024-1044, octubre-diciembre de 2023. doi: https://doi.org/10.18257/raccefyn.1900

Equivalentemente si $a,b,c,d \in A$, con $a \neq b, c \neq d$,

$$(a-b=c-d) \Longrightarrow (a=c) \text{ y } (b=d).$$

Si se definen los conjuntos $A+A$ y $A \ominus A$ mediante

$$\begin{aligned} A+A &: = \{a+b : a,b \in A\}, \\ A \ominus A &: = \{a-b : a,b \in A, a \neq b\}, \end{aligned}$$

y si A es finito con $|A| = k$ elementos, se sigue que: A es un conjunto Sidon si y solo si $A+A$ y $A \ominus A$ tienen cardinales maximales:

$$|A+A| = \binom{k+1}{2}, \ |A \ominus A| = 2\binom{k}{2}.$$

Problema Sidon en grupos finitos

Si G es un grupo conmutativo finito, como antes, el problema general consiste en determinar la función

$$S(G) = S_2(G) := \max\{|A| : A \text{ es conjunto Sidon en } G\}.$$

Si A es un conjunto Sidon en G, con k elementos y el orden de G es N, entonces

$$\begin{aligned} k(k-1) &\leq N, \\ S(G) &\leq \sqrt{N}+1. \end{aligned}$$

Desde la desigualdad anterior y las construcciones " óptimas" en algunos grupos finitos, conocemos valores exactos:

G	$\mathbb{Z}_{p^{2n}+p^n+1}$	$\mathbb{Z}_{p^{2n}-1}$	$\mathbb{Z}_{p(p-1)}$	$\mathbb{Z}_p^{2n}$	$\mathbb{Z}_p^n \times \mathbb{Z}_{p^n-1}$	$\mathbb{Z}_{p^n-1}^2$
$S(G)$	p^n+1	p^n	$p-1$	p^n	p^n-1	p^n-2

.

Además, cuando G es finito, podemos definir un orden y considerar la función de Golomb relativa a la regla más corta. En particular, en el caso cíclico este problema es bastante interesante OEIS(A008404).

En $\mathbb{Z} \times \mathbb{Z}$: Dimensión 2

Esta sección presenta conjuntos Sidon y reglas Golomb en contexto bidimensional. Se retoman párrafos de uno de los artículos que originan la temática: *Two-Dimensional Synchronization Patterns for Minimum Ambiguity* (**Golomb** & **Taylor**, 1982).

"Hay numerosos problemas que aparecen en radar, sonar, alineación física y sincronización tiempo-posición, problemas que pueden formularse en términos de encontrar patrones bidimensionales de *unos* (puntos) y *ceros* (blancos) para los cuales la autocorrelación aperiódica bidimensional (espacial), llamada *función ambiguedad* del análisis radar, tiene mínimos valores fuera de fase. Un contexto típico es aquel en el cual se desea producir una secuencia de frecuencias distintas en intervalos consecutivos de tiempo, en tal forma que si un eco retornante se corre en tiempo y frecuencia debido a un objeto en movimiento, la única traslación del modelo original que tiene alta correlación con la configuración recibida será aquella cuyo corrimiento de tiempo corresponde al rango correcto y cuyo corrimiento de frecuencia corresponde con la velocidad correcta del objeto".

"Consideramos patrones de puntos en una malla rectangular bajo diferentes combinaciones de requisitos. El concepto unificador es el de un patrón que dé mayor coincidencia con copias corridas de sí mismo únicamente cuando ellas estén en posiciones especiales, y de otra forma únicamente coincidencias menores. En efecto, nuestros patrones básicos tienen la propiedad de que en cualquier posición alcanzable mediante corrimientos horizontales y verticales no cíclicos, diferentes a la posición original, el patrón coincidirá con el original en a lo sumo un punto localización".

Los conjuntos Sidon y reglas Golomb aparecen de manera natural en problemas originados en aplicaciones, en contextos bidimensionales tales como se sugiere en los párrafos anteriores (**Costas**, 1984, pp. 996–997) y (**Etzion**, 2009; **Gagliardi**, **Robbins**, & **Taylor**, 1987).

Arreglos Costas

Orígenes: John Costas y Solomon Golomb

Solomon Golomb (**Golomb**, 1984, p. 13), escribe: "Patrones bidimensionales de una clase especial, que aparecen en un problema sonar práctico, me fueron sugeridos por John Costas, quien preguntó sobre un patrón $n \times n$ de n puntos con un punto en cada fila y en cada columna, con la propiedad de que cualquier corrimiento horizontal y vertical debe coincidir en a lo sumo un punto posición. La aplicación original de esas constelaciones fue un problema sonar (**Costas**, 1975), pero también existen aplicaciones a radar, a sincronización y alineación". A esos arreglos, Golomb los denomina constelaciones, hoy se llaman arreglos Costas.

Definición 1 *(**Colbourn** & **Dinitz**, 2007, p. 357) Un arreglo Costas de orden n es un arreglo $n \times n$ de puntos negros y blancos que satisface dos condiciones:*

1. *Hay n puntos negros y $n(n-1)$ puntos blancos con exactamente un punto negro en cada fila y un punto negro en cada columna.*
2. *Todos los segmentos entre pares de puntos negros son diferentes en longitud o en pendiente.*

Problema Costas (**Golomb**, 1984, p. 13) ¿Existen arreglos Costas de cualquier orden? Si mediante $C(n)$ se denota al número de arreglos Costas de orden n, el problema fundamental consiste en determinar el valor de $C(n)$, en particular se trata de probar o refutar que $C(n) > 0$ para todo n ¿Existen arreglos Costas de orden 32? ¿De orden 33?

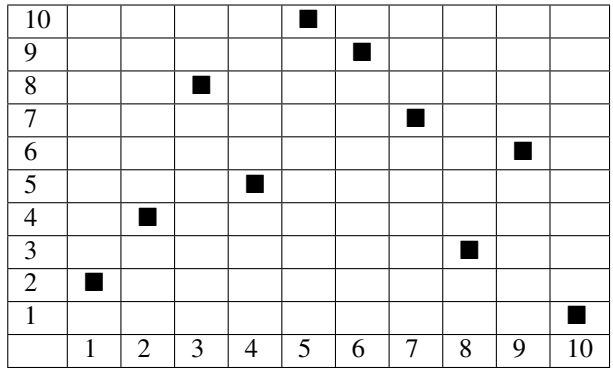
Sabemos que existen arreglos Costas de orden n para todo n, $1 \leq n < 359$, excepto para n en el siguiente conjunto (**Colbourn** & **Dinitz**, 2007, p. 359) OEIS(A008404).

$$32, 33, 43, 48, 49, 54, 63, 73, 74, 83, 84, 85, [89, 93], 97, 103, 109, [113, 117],$$
$$120, 121, 131, 132, 133, [139, 143], 151, 152, 153, 157, 158, 159, 163, 168, 169,$$
$$173, 174, [181, 186], 193, [199, 207], [211, 219], 223, 229, 233, 234, [242, 246],$$
$$251, 257, 258, 259, 263, 271, 272, 273, 277, 283, 284, 285, 288, 289, [293, 303],$$
$$313, [317, 327], 331, 332, 333, 337, 338, 339, 342, 349, 353, 354.$$

Construcciones Algebraicas de Arreglos Costas

Un ejemplo de un arreglo Costas de orden 10:

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(185):1024-1044, octubre-diciembre de 2023. doi: https://doi.org/10.18257/raccefyn.1900



Teorema 7 *Construcción Welch-Gilbert (**Gilbert**, 1965; **Golomb**, 1984, Thm 1, p.14). Sean p un primo, α una raíz primitiva módulo p, $n = p-1$ y a un entero no negativo Se obtiene un arreglo Costas de orden n colocando un punto en (i, j) si y solo si*

$$i = \alpha^j, \qquad a \leq j < n+a,\ i = 1,...,n.$$

Teorema 8 *Construcción Lempel-Golomb.(**Colbourn** & **Dinitz**, 2007; **Golomb**, 1984, Thm 3, p. 16). Sean q una potencia prima, α y β elementos primitivos en el campo $\mathbb{F}_q$ y $n = q-2$. Se obtiene un arreglo Costas de orden n, colocando un punto en (i, j) si y solo si*

$$\alpha^i + \beta^j = 1, \qquad 1 \leq i, j \leq n.$$

Cuando $\alpha = \beta$, se trata de la construcción de Lempel, generalizada por Golomb para todo α, β.

De las construcciones anteriores se sigue que: $C(p-1) \geq 1$ y $C(q-2) \geq 1$, para todo primo p y toda potencia prima $q \geq 4$.

Secuencias Sonar

Orígenes: Golomb, Taylor, Moreno, Games

En (**Golomb** & **Taylor**, 1982), Solomon Golomb y Herbert Taylor, comentan: " ...la aplicación Doppler sonar o radar no requiere la restricción de un punto por fila, únicamente la restricción de un punto por columna. En notación musical, el patrón puede verse como una secuencia de tonos, pero únicamente un tono en cada latido. Cuando los tonos retornan después de reflejarse en un objeto en movimiento, el corrimiento horizontal corresponde a tiempo transcurrido y el corrimiento vertical corresponde al Doppler. El número de filas será limitado por el contexto, pero generalmente el número de columnas será el que se desea maximizar". Oscar Moreno, Richard Games y Herbert Taylor, informalmente definen secuencia sonar como: "un arreglo $n \times m$ de puntos y blancos que tiene un punto por columna y valores autocorrelación menores o iguales que 1, esto es un arreglo que coincide en no más de un punto con cualquier corrimiento bidimensional no cero de sí mismo, se llama secuencia sonar" (**Moreno**, **Games**, & **Taylor**, 1991).

Paul Erdös, Ronald Graham, Imre Ruzsa y Herbert Taylor, presentan el concepto como sigue. "Un subconjunto de la cuadrícula $m \times n$ con exactamente un punto en cada columna, tal que los $\binom{m}{2}$ vectores determinados por ellos son todos distintos", refuerzan la defincón: " Una secuencia sonar $n \times m$ es un arreglo de puntos y blancos con n filas y exactamente un punto en cada una de sus m columnas, sujeto al requerimiento que pares distintos de puntos determinan vectores distintos. Cualquier dos de tales vectores deben diferenciarse en pendiente o en longitud" (**Erdős *et al***., 1992).

La referencia principal para esta sección es (**Moreno**, **Games**, & **Taylor**, 1993), de la cual se toman las definiciones y construcciones.

Definición 2 *Para m y n enteros, sean* $[1,m] = \{1,2,...,m\}$ *y* $[1,n] = \{1,2,...,n\}$.

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

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

2. *Considerando a* $[1,m]$ *como un conjunto de representantes de los enteros módulo m. Una función* $f : [1,n] \longrightarrow \mathbb{Z}_m$ *tiene la propiedad de diferencias modulares distintas si para todos los enteros* h,i,j, *con* $1 \leq h \leq n-1$ *y* $1 \leq i,j \leq n-h$,

$$f(i+h) - f(i) \equiv f(j+h) - f(j) \qquad (mod\ m) \qquad implica \qquad i = j.$$

3. *Una* ***secuencia Costas*** *de longitud n es una permutación* $f : [1,n] \longrightarrow [1,n]$ *con la propiedad de diferencias distintas.*

4. *Una* ***secuencia sonar*** $m \times n$ *es una función* $f : [1,n] \longrightarrow [1,m]$ *con la propiedad de diferencias distintas.*

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

Construcciones de Secuencias Sonar

Un ejemplo de secuencia sonar 11×6:

6						■	■			■	
5	■										
4					■						
3			■								
2		■						■			
1				■					■		■
	1	2	3	4	5	6	7	8	9	10	11

Las siguientes construcciones se describen en (**Moreno**, **Games**, & **Taylor**, 1993).

Secuencia Cuadrática (**Moreno**, **Games**, & **Taylor**, 1993, p. 1985). Sean p un primo impar; a,b,c enteros constantes con a no divisible entre p. Entonces

$$\begin{aligned} f &: [1,p+1] \longrightarrow [1,p], \\ f(x) &= ax^2 + bx + c\,(mod\ \ p), \end{aligned}$$

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

Secuencia Shift (**Moreno**, **Games**, & **Taylor**, 1993, p. 1985). Sean p un primo, $q = p^r$, α un elemento primitivo de $\mathbb{F}_{q^2}$, y β un elemento primitivo de $\mathbb{F}_q$. Para $p = 2$, sea

$$\begin{aligned} f &: [1,q] \longrightarrow [1,q-1], \\ f(x) &= \log_\beta \left((\alpha^i)^p + \alpha^i \right). \end{aligned}$$

Para p impar, definir f similarmente, cambiando el dominio por $\left[-\frac{q-1}{2}, \frac{q-1}{2}\right]$. Entonces f es una secuencia sonar modular $(q-1) \times q$.

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(185):1024-1044, octubre-diciembre de 2023. doi: https://doi.org/10.18257/raccefyn.1900

Secuencia Welch Exponencial (**Moreno**, **Games**, & **Taylor**, 1993, p. 1986). Sea α una raíz primitiva módulo el primo p. Entonces

$$\begin{aligned} f &: [1,p-1] \longrightarrow [1,p], \\ f(x) &= \alpha^x (mod\ p), \end{aligned}$$

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

Secuencia Welch Logarítmica (**Moreno**, **Games**, & **Taylor**, 1993, p. 1986). Sea α una raíz primitiva módulo el primo p. Entonces

$$\begin{aligned} f &: [1,p-1] \longrightarrow [1,p-1], \\ f(x) &= \log_\alpha x (mod\ p-1), \end{aligned}$$

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

Secuencia Lempel (**Moreno**, **Games**, & **Taylor**, 1993, p. 1986). Sea $q > 2$ una potencia prima y α un elemento primitivo de $\mathbb{F}_q$. Entonces

$$\begin{aligned} f &: [1,q-2] \longrightarrow [1,q-1], \\ f(x) &= y \Longleftrightarrow \alpha^x + \alpha^y = 1, \end{aligned}$$

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

Secuencia Golomb (**Moreno**, **Games**, & **Taylor**, 1993, p. 1986). Sea $q > 2$ una potencia prima y α, β elementos primitivos de $\mathbb{F}_q$. Entonces

$$\begin{aligned} f &: [1,q-2] \longrightarrow [1,q-1], \\ f(x) &= y \Longleftrightarrow \alpha^x + \beta^y = 1, \end{aligned}$$

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

Problemas Sonar

El problema principal para secuencias sonar es: "Para m fijo, encontrar el máximo n para el cual existe una secuencia sonar $m \times n$ ¿Cuál es el máximo número n tal que existe una secuencia sonar $m \times n$? Se trata entonces de estimar tan exactamente como sea posible la función

$$SS(m) := \max \{n \in \mathbb{N} : \text{ existe una secuencia sonar } m \times n\}.$$

Se han realizado extensas computaciones para determinar $SS(m)$:

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

m	14	15	16-18	19	20	21	22	23	24-27	28-31
$SS(m)$	21	22	≥ 23	25	26	28	30	31	32	37

La cota superior trivial es: $SS(m) \leq 2m$; igualdad para $1 \leq m \leq 4$, proponemos los siguientes dos problemas.

Problema sonar 1. Mejorar la cota superior trivial para valores "pequeños" de m (útiles en aplicaciones). Probar que $SS(m) \leq 2m-1$ para todo $m \geq 5$.

Problema sonar 2. Construir secuencias sonar que permitan probar que $SS(m) \geq m+2$, $m+3$ para infinitos m.

Teorema 9 *(**Erdős et al.**, 1992, Thm 4, p. 42). Si existe una secuencia sonar $m \times n$, entonces $n < m + 5m^{2/3}$.*

Su prueba utiliza un método similar a la del Teorema de Erdös y Turán para la cota superior de $S(N)$. En verdad, ellos demuestran que

$$SS(m) \leq m + 4m^{2/3} + 4n^{1/3} + 1.$$

Además, en el comentario siguiente a la demostración del teorema afirman: "Computación más cuidadosa demuestra que actualmente

$$SS(m) < m + 3m^{2/3} + 2m^{1/3} + 9,$$

para todo m."

Por el otro lado, utilizando la construcción cuadrática y un resultado sobre el menor no residuo cuadrático entre 1 y p, prueban el siguiente resultado.

Teorema 10 *(**Erdős et al.**, 1992, Thm 5, p. 43). Para algún $c > 0$, constante, existen infinitos enteros m tales que existe una secuencia sonar $m \times n$ con $n > m + c \log m \log\log m$.*

Al finalizar proponen el siguiente problema.

Problema abierto (**Erdős *et al***., 1992, p. 43). ¿Para todo n, existe un arreglo $n \times n$, con n puntos en el cual pares distintos de puntos determinan vectores que difieren en pendiente o en longitud?

Arreglos Costas y Secuencias Sonar como Funciones Sidon

En situaciones especiales, por ejemplo arreglos Costas y secuencias sonar, consideramos importante ubicar los contexto desde las que llamamos funciones Sidon que provienen de los grafos de funciones.

Definición 3 *Sean m y n enteros positivos. Una función*

$$F : [1,n] \longrightarrow [1,m]$$

se llama función Sidon, de orden $m \times n$, si su grafo

$$\mathscr{G}_F := \{(x, F(x)) : x \in [1,n]\}$$

es un conjunto Sidon en el grupo $(\mathbb{Z} \times \mathbb{Z}, +)$. Equivalentemente, si $\mathscr{G}_F$ es libre de paralelogramos (no hay vectores iguales entre pares de sus puntos). Vectorialmente, la definición prohibe igualdades "no triviales" de la forma

$$\begin{aligned} \mathbf{a} + \mathbf{b} &= \mathbf{c} + \mathbf{d}, \\ \mathbf{a} - \mathbf{c} &= \mathbf{d} - \mathbf{b}, \end{aligned}$$

entre puntos $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in \mathscr{G}_F$..

Con esta definición, es claro que el concepto de arreglo Costas de orden n es equivalente al concepto de función Sidon biyectiva de $[1,n]$ en $[1,n]$, entonces los términos *permutación Costas de orden n* y *permutación Sidon de orden n*, se pueden usar indistintamente. En términos de funciones Sidon se tienen las siguientes definiciones de arreglo Costas y secuencias sonar.

- Un *arreglo (secuencia, función, permutación) Costas de orden n*, es una *función Sidon biyectiva* de $[1,n]$ en $[1,n]$.

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(185):1024-1044, octubre-diciembre de 2023. doi: https://doi.org/10.18257/raccefyn.1900

- Una *secuencia (función, arreglo) sonar $m \times n$, es una función Sidon de* $[1,n]$ *en* $[1,m]$.
- Una *secuencia sonar modular $m \times n$, es una función Sidon de* $[1,n]$ *en los enteros módulo m ,* $\mathbb{Z}_m$.

Los problemas y resultados sobre arreglos Costas y secuencias sonar pueden trasladarse al contexto de funciones Sidon, y recíprocamente.

Conjuntos Sidon Bidimensionales y Rectángulos Golomb.

Las funciones Sidon, los arreglos Costas y las secuencias sonar son casos especiales de conjuntos Sidon en el grupo $(\mathbb{Z} \times \mathbb{Z}, +)$, extensión natural de los originales conjuntos Sidon en el grupo de los enteros, $(\mathbb{Z}, +)$, ver tesis doctorales de Carlos Trujillo (**Trujillo Solarte**, 1998) y Yadira Caicedo (**Caicedo Bravo**, 2016).

En 1995, James Shearer escribe: "Robinson define un *rectángulo Golomb* como un arreglo $n \times m$ de unos y ceros tal que la autocorrelación bidimensional tiene tres valores: 0, 1 y k, donde k es el número de unos en el arreglo (**Robinson**, 1985). Esto significa que las posiciones de los unos en cualquier traslación entera no cero del rectángulo coincide con las posiciones de los unos en la posición original del rectángulo en a lo sumo un lugar. Equivalentemente, la diferencia entre las posiciones de todo par de unos en el rectángulo, consideradas como vectores, son distintas" (**Shearer**, 1995, p. 1).

Es decir, se trata de un conjunto Sidon, en dos dimensiones, contenido en la malla $[1,n] \times [1,m]$. Es entonces natural preguntar por el máximo cardinal de un conjunto contenido en el rectángulo:

$$G(n,m) := \max\{|A| : A \subset [1,n] \times [1,m] \text{ y } A \text{ es arreglo Golomb}\}.$$

Robinson define un *rectángulo óptimo* (**Shearer**, 1995, p. 1) como aquel que contiene $G(n,m)$ unos. El mismo Robinson utiliza el nombre de *cuadrado Golomb* para el caso en que $n = m$ y presenta la siguiente tabla

$n =$	3	4	5	6	7	8	9	10	11	12	13
$G(n,n) \leq$	5	6	8	10	11	13	15	17	19	21	23

Demuestra además las siguientes cotas superiores:

$$\begin{aligned} G(n,n) &< 2n \\ G(n,n) &\leq 2n-2, \text{ para } n > 3. \\ G(n,n) &\leq 2n-3, \text{ para } n > 6. \end{aligned}$$

Finalmente afirma que el argumento de (**Erdös** & **Turán**, 1941) se puede usar para demostrar que

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

para n suficientemente grande.

James Shearer actualiza algunos valores para $G(n,n)$ y define $GS(n,n)$ como el máximo número de unos en un cuadrado Golomb "Simétrico" $n \times n$ (**Shearer**, 2004).

$n =$	2	3	4	5	6	7	8	9	10	11	12
$G(n,n) \leq$	3	5	6	8	9	11	12	13	15	16	17
$GS(n,n)$	3	5	6	8	9	10	12	13	15	16	17

$n =$	13	14	15	16	17	18	19	20	21	22
$G(n,n) \leq$										
$GS(n,n)$	18	19	21	22	23	24	25	26	27	29

Para otros valores de $G(n,m)$ ver (**Robinson**, 1997; **Shao *et al***., 2013, pp. 67–68).

Conjuntos Sidon en dimensión d

En 1972, Bernt Lindström considera conjuntos Sidon en el contexto de vectores en dimensión d. "Decimos que una secuencia de vectores $v_1, v_2, ..., v_n$ es una B_2-*secuencia* si todas las sumas $v_i + v_j$, con $1 \leq i \leq j \leq n$, son diferentes. Si la dimensión de todos los vectores es d y las componentes se toman en $\{0,1,2,...,N-1\}$, sea $F_2(N,d)$ el máximo número de vectores en una B_2-secuencia".

Teorema 11 *(**Linström**, 1969, p. 211) Cuando* $N \to \infty$,

$$F_2(N,d) \leq N^{d/2} + O\left(N^{d^2/(2d+2)}\right).$$

Al finalizar, sección Problemas no Resueltos, como una generalización de la conjetura de Paul Erdös, propone el siguiente problema.

Probar que, cuando $N \to \infty$,

$$F_2(N,d) = N^{d/2} + O(1).$$

Javier Cilleruelo (**Cilleruelo**, 2010, p. 858) refuta la conjetura anterior de Lindström para $d = 2$ demostrando que la desigualdad

$$F_2(N,2) > N + \log N \log\log\log N$$

vale infinitamente.

El Teorema 11 para $d = 2$ implica que

$$F_2(N,2) \leq N + O\left(N^{2/3}\right).$$

En la tesis doctoral De Yadira Caicedo se muestra una constante explícita para el término $N^{2/3}$ (**Caicedo Bravo**, 2016). Para todo entero positivo N, se tiene que:

$$F_2(N,2) \leq N + 1.9N^{2/3} + 1.6N^{1/3} + 1.$$

En Contexto Criptográfico

En los últimos dos años han aparecido relaciones entre funciones con buenas propiedades criptográficas, funciones que tienen resitencia frente a los denominados "ataques lineales y/o diferenciales", y funciones Sidon. En esta sección consideramos algunas de tales conexiones.

Funciones APN

Una función $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ se llama APN (Almost Perfect Nonlinear) si para todo $a \in \mathbb{F}_{2^n}$, no cero, y todo $b \in \mathbb{F}_{2^n}$, la ecuación

$$F(x+a) + F(x) = b,$$

tiene a lo sumo dos soluciones. Equivalentemente, si el sistema de ecuaciones

$$\begin{aligned} x+y+z+t &= 0, \\ F(x)+F(y)+F(z)+F(t) &= 0, \end{aligned} \tag{5}$$

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(185):1024-1044, octubre-diciembre de 2023. doi: https://doi.org/10.18257/raccefyn.1900

tiene soluciones únicas para cuaternas (x,y,z,t) cuyos elementos no son todos distintos (es decir, hay pares iguales) (**Carlet** & **Picek**, 2021).

Por otro lado, el grafo de F

$$\mathscr{G}_F := \{(x,F(x)) : x \in \mathbb{F}_{2^n}\},$$

es conjunto Sidon en el grupo $(\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, +)$ si y solo si la ecuación

$$(x,F(x)) + (y,F(y)) = (z,F(z)) + (t,F(t)),$$

tiene soluciones no triviales. Equivalentemente, el sistema

$$\begin{aligned} x+y &= z+t, \\ F(x)+F(y) &= F(z)+F(t), \end{aligned} \tag{6}$$

tiene únicamente soluciones no triviales. Es bastante clara la equivalencia de los sistemas (5) y (6). Claude Carlet y Sihem Mesnager escriben lo siguiente (**Carlet** & **Mesnager**, 2022, p. 2). "Existe una conexión natural entre aquellas funciones (n,n) que van de $\mathbb{F}_{2^n}$ en sí mismo, que son funciones APN de la criptografía y los conjuntos Sidon. Por defínción, una función (n,n) es APN si y solo si su grafo es un conjunto Sidon en el grupo $(\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, +)$. En (**Carlet** & **Picek**, 2021) hay otra conexión entre los exponentes de funciones APN potencias, esto es $F(x) = x^d$, sobre $\mathbb{F}_{2^n}$ (llamados exponentes APN) y aquellos subgrupos de $\mathbb{F}_{2^n}^*$ que son al mismo tiempo conjuntos Sidon y conjuntos libres de sumas en el grupo $(\mathbb{F}_2^n, +)$:

Teorema 12 *(**Carlet** & **Picek**, 2021, Thm 4.1, p.5-6). Si d es un exponente APN, entonces para todo entero j el subgrupo multiplicativo de orden mcd $\left(d-2^j, 2^n-1\right)$ es un conjunto Sidon y libre de sumas en el grupo aditivo $(\mathbb{F}_{2^n}, +)$.*

Nota. En $(\mathbb{F}_{2^n}, +) \equiv (\mathbb{F}_2^n, +)$ (aditivamente), se tiene que S es un conjunto Sidon, respectivamente libre de sumas, si no contiene 4 elementos, respectivamente 3 elementos, distintos cuya suma sea cero.

En el último Simposio Latinoamericano sobre Informática Teórica (LATIN 2022), Claude Carlet presenta dos resultados y una conjetura que relacionan funciones APN y conjuntos Sidon "maximales" (es decir, no contenidos en otro conjunto Sidon).

Proposición 13 *(**Carlet**, 2022, Prop. 1, p. 247) El grafo de una función APN, $F : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ es un conjunto Sidon maximal en $\left((\mathbb{F}_2^n)^2, +\right)$ si y solo si el conjunto*

$$\mathscr{G}_F + \mathscr{G}_F + \mathscr{G}_F = \{(x+y+z, F(x)+F(y)+F(z)) : x,y,z \in \mathbb{F}_2^n\}$$

cubre el espacio completo $(\mathbb{F}_2^n)^2$.

Proposición 14 *(**Carlet**, 2022, Prop. 2, p. 249) Sean n cualquier entero positivo y $F : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ una función APN. El grafo de F no es maximal como un conjunto Sidon si y solo si existe una función APN, $G : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$, que puede obtenerse desde F cambiando su valor en un solo punto (es decir, que G está a distancia Hamming 1 de F).*

Conjetura 3 *(**Carlet**, 2022, Conj 3, p. 250) Los grafos de todas las funciones APN son conjuntos Sidon maximales.*

Espacios Sidon

Hoy hay gran interés en investigar estructuras q-análogas de estructuras combinatorias en las que vectores y subconjuntos se reemplazan por espacios vectoriales sobre un campo

finito. Ejemplos de tales estructuras q-análogas son códigos de dimensión constante y t-diseños sobre campos finitos. "Lo que comenzó como un área de investigación puramente teórica, ha encontrado importantes aplicaciones a codificación aleatoria de redes, la teoría de códigos y diseños subespacio se ha desarrollado rápidamente" (**Zhang** & **Ge**, 2022). Los espacios Sidon, que pueden mirarse como q-análogos de conjuntos de Sidon, fueron introducidos en (**Bachoc**, **Serra**, & **Zémor**, 2017) para estudiar ciertas propiedades multiplicativas de subespacios.

Sean $\mathbb{F}_q$ el campo finito con q elementos y $\mathbb{F}_{q^n}$ el campo extensión de grado n sobre $\mathbb{F}_q$, el cual puede verse como un espacio vectorial de dimensión n. Mediante $\mathscr{G}_q(n,k)$ se denota al conjuntos de todos los subespacios k-dimensionales de $\mathbb{F}_{q^n}$, un (n,k) espacio Grassmanniano sobre $\mathbb{F}_q$.

Definición 4 *(**Bachoc**, **Serra**, & **Zémor**, 2017, pp. 425–426). Un subespacio $V \in \mathscr{G}_q(n,k)$ se llama espacio Sidon si para todo $a,b,c,d \in V$, no cero,*

$$ab = cd \Longrightarrow \left\{a\mathbb{F}_q, b\mathbb{F}_q\right\} = \left\{c\mathbb{F}_q, d\mathbb{F}_q\right\},$$

donde para $u \in \mathbb{F}_{q^n}$, $u\mathbb{F}_q = \left\{u\lambda : \lambda \in \mathbb{F}_q\right\}$ es el "corrimiento" cíclico de $\mathbb{F}_q$ mediante u.

Informalmente, esto significa que un espacio Sidon es un subespacio $V \in \mathscr{G}_q(n,k)$ tal que el producto de cualquier par de elementos no cero de V tiene factorización única sobre V, excepto por un múltiplo constante de $\mathbb{F}_q$.

Los siguientes dos teoremas muestran la estrecha relación entre conjuntos Sidon y espacios Sidon: cada construcción de uno de estos objetos puede utilizarse para obtener una construcción del otro.

Teorema 15 *(**Raviv**, **Langton**, & **Tamo**, 2021; **Zhang** & **Ge**, 2022, Thm 2.4, p. 783). Sea $S = \{n_1, n_2, ..., n_k\} \subseteq [1,m]$ un conjunto Sidon en los enteros tal que $k = m^2(1+o_k(1))$. Entonces, para un entero $n > 2m$ y un elemento propio γ de $\mathbb{F}_{q^n}$ (que no pertenece a algún subcampo propio de $\mathbb{F}_{q^n}$),*

$$V := \langle\{\gamma^{n_i} : i \in [1,k]\}\rangle,$$

es un espacio Sidon.

Teorema 16 *(**Raviv**, **Langton**, & **Tamo**, 2021; **Zhang** & **Ge**, 2022, Thm 2.5, p. 784). Si $V \in \mathscr{G}_q(n,k)$ es un espacio Sidon, γ es un elemento primitivo en $\mathbb{F}_{q^n}$ y*

$$A = \{\gamma^{n_i} : i \in [1, (q^n-1)/(q-1)]\},$$

es un conjunto de representantes no cero de todos los subespacios con dimensión uno de V, entonces $S := \{n_i : \gamma^{n_i} \in A\}$ es un conjunto Sidon en $\mathbb{Z}_{(q^n-1)/(q-1)}$.

Hoy, muchos investigadores publican resultados relacionados con algoritmos y métodos para construir espacios Sidon, además de los artículos mencionados, el lector puede consultar (**Niu**, **Xiao**, & **Gao**, 2022; **Zhang** & **Cao**, 2022; **Zhang** & **Tang**, 2023), y las referencias en ellos. El reciente concepto de *Espacio Multi-Sidon* (**Zullo**, 2021, 2023) puede considerarse como una generalización de la noción presentada en esta sección. No podemos dejar de mencionar una reciente aplicación criptográfica de los conjuntos Sidon: *Cryptosistemas Sidon* (**Briaud**, **Tillich**, & **Verbel**, 2022; **Raviv**, **Langton**, & **Tamo**, 2021).

Conclusiones

Se realizó un recorrido a través de algunos contextos finitos en los que intervienen conjuntos Sidon y reglas Golomb, desde sus origenes puramente matemáticos (1930) y sus aplicaciones (1950) hasta nuestros días en seguridad de información (criptografía).

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(185):1024-1044, octubre-diciembre de 2023. doi: https://doi.org/10.18257/raccefyn.1900

Los contextos considerados son: conjuntos finitos de números enteros, grupos cíclicos, retículos bidimensionales de coordenadas enteras (arreglos Costas y secuencias Sonar); finalizando en contextos criptográficos (funciones APN).

Estos contextos fueron identificados por integrantes del grupo de investigación durante el desarrollo de proyectos, dirección de tesis y publicación de artículos.

Propyectos de Investigación: (Sucesiones de Sidon y conjuntos $B_h[g]$, código Colciencias 11030511450; Las funciones de Graham y Sloane problemas de cubrimiento y empaquetamiento, código Colciencias 1103516865; Construcción de conjuntos $B_h[g]$, propiedad de Midy y algunas aplicaciones, código Colciencias 1103569935047; Aplicaciones a teoría de información y comunicación de los conjuntos de Sidon y sus generalizaciones, código Colciencias 110371 250560).

La dirección de tesis doctorales ver (**Caicedo Bravo**, 2016; **Delgado Ordoñez**, 2023; **Martos Ojeda**, 2019); y algunas publicaciones derivadas de ellas (**Caicedo**, **Martos**, & **Trujillo**, 2015, 2021; **Campo**, **Mutis**, & **Trujillo**, 2002; **Delgado**, **Martos**, & **Trujillo**, 2021; **Martos**, **Delgado**, & **Trujillo**, 2021; **Martos**, **Daza**, & **Trujillo**, 2021).

Queda pendiente un recorrido similar en otros contextos tales como: combinatoria (diseños, conjuntos diferencia y configuraciones), teoría de códigos y teoría de grafos entre otros. También se deben considerar contextos que se derivan de las aplicaciones.

Agradecimientos

El autor agradece a la Universidad del Cauca, Facultad de Ciencias Naturales, Exactas y de la Educación, Departamento de Matemáticas, por el apoyo recibido durante la aprobación y desarrollo de su Año Sabático (2022-2023); y al grupo de investigación " Álgebra, Teoría de Números y Aplicaciones: ERM" por su continua colaboración durante más de veinte años de trabajo conjunto.

También agradece a los evaluadores anónimos, cuyas sugerencias mejoraron la calidad del artículo.

Conflicto de intereses

El autor certifica que no tiene conflicto de intereses con respecto al contenido de este artículo.

References

Atkinson, M., Santoro, Urrutia. (1986). Integer sets with distinct sums and differences and carrier frequency assignments for nonlinear repeaters. *Transactions on Communications, 34*(6), 614-617.

Babcock, W. C. (1953). Intermodulation interference in radio systems frequency of occurrence and control by channel selection. *The Bell System Technical Journal, 32*(1), 63-73.

Bachoc, C., Serra, O., Zémor, G. (2017). An analogue of vosper's theorem for extension fields. *Mathematical Proceedings of the Cambridge Philosophical Society, 163*(3), 423-452.

Balogh, J., Füredi, Z., Roy, S. (2021). An upper bound on the size of sidon sets. *arXiv preprint arXiv:2103.15850.*

Bloom, G. S., Golomb, S. W. (1977). Applications of numbered undirected graphs. *Proceedings of the IEEE, 65*(4), 562-570.

Bose, R. (1942). An affine analogue of singer's theorem. *J. Indian Math. Soc, 6*(1), 1-15.

Briaud, P., Tillich, J.-P., Verbel, J. (2022). A polynomial time key-recovery attack on the sidon cryptosystem. *Selected Areas in Cryptography: 28th International Conference, Virtual Event, September 29-October 1, 2021, Revised Selected Papers,* 419-438.

Caicedo, Y., Martos, C. A., Trujillo, C. A. (2015). g− Golomb rulers. *Revista Integración, 33*(2), 161-172.

Caicedo, Y., Martos, C. A., Trujillo, C. A. (2021). Construcci´on de conjuntos bh en varias dimensiones. *Ciencia en Desarrollo, 12*(2), 73-81.

Caicedo Bravo, N. Y. (2016). Conjuntos de sid´on en dimensión dos. *Tesis de Doctorado, Universidad del Valle.*

Campo, L., Mutis,W., Trujillo, C. (2002). Cotas superiores para conjuntos de sidon finitos. *Unicauca Ciencia, 7, 95-108.*

Carlet, C. (2022). On apn functions whose graphs are maximal sidon sets. *Latin American Symposium on Theoretical Informatics,* 243-254.

Carlet, C., Mesnager, S. (2022). On those multiplicative subgroups of F2n which are sidon sets and/or sum-free sets. *Journal of Algebraic Combinatorics, 55*(1), 43-59.

Carlet, C., Picek, S. (2021). On the exponents of APN power functions and sidon sets, sumfree sets, and dickson polynomials. *Advances in Mathematics of Communications,* 1-19.

Cilleruelo, J. (2010). Sidon sets in Nd. *Journal of Combinatorial Theory, Series A, 117*(7), 857-871.

Colbourn, C., Dinitz, J. (2007). *Handbook of combinatorial designs.* CRC press Boca Raton, FL.

Costas, J. P. (1975). Medium constraints on sonar design and performance. *IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS, 11*(5), 973-973.

Costas, J. P. (1984). A study of a class of detection waveforms having nearly ideal range— doppler ambiguity properties. *Proceedings of the IEEE, 72*(8), 996-1009.

Delgado, L. M. D., Martos, C. A., Trujillo, C. A. (2021). New constructions of extended sonar sequences from sidon sets. *IEEE Access, 10*, 3343-3350.

Delgado Ordoñez, L. M. (2023). Reglas golomb generalizadas y la teoría de ramsey. *Tesis de Doctorado, Departamento de Matemáticas, Universidad del Cauca.*

Dimitromanolakis, A. (2002). Analysis of the golomb ruler and the sidon set problems, and determination of large, near-optimal golomb rulers. *Master's Thesis, Department of Electronic and Computer Engineering, Technical University of Crete.*

Erdos, P. (1995). Some of my favourite problems in number theory, combinatorics, and geometry. *Resenhas do Instituto de Matemática e Estatıstica da Universidade de São Paulo, 2*(2), 165-186.

Erdös, P. (1944). On a problem of sidon in additive number theory and on some related problems addendum. *Journal of The London Mathematical Society-second Series* 19, 208-208.

Erdös, P. (1992). Some of my forgotten problems in number theory. *Hardy-Ramanujan Journal, 15,* 34-50.

Erdös, P. (1994). Some problems in number theory, combinatorics and combinatorial geometry. Mathematica Pannonica, 5, 261-269.

Erdös, P., Graham, R., Ruzsa, I. Z., Taylor, H. (1992). Bounds for arrays of dots with distinct slopes or lengths. *Combinatorica, 12*(1), 39-44.

Erdös, P., Turán, P. (1941). On a problem of sidon in additive number theory, and on some related problems. J*ournal of The London Mathematical Society-second Series, 16,* 212-215.

Etzion, T. (2009). Problems on two-dimensional synchronization patterns. *Coding and Cryptology: Second InternationalWorkshop, IWCC 2009, Zhangjiajie, China, June* 1-5, 2009. Proceedings *2,* 52-62.

Gagliardi, R., Robbins, J., Taylor, H. (1987). Acquisition sequences in ppm communications (corresp.) *IEEE Transactions on Information Theory, 33*(5), 738-744.

Gardner, M. (1972). Graceful graphs of solomon golomb, or how to number a graph parsimoniously. *Scientific American, 226*(3), 108.

Gilbert, E. N. (1965). Latin squares which contain no repeated digrams. *Siam Review, 7*(2), 189-198.

Golomb, S., Taylor, H. (1982). Two-dimensional synchronization patterns for minimum ambiguity. *IEEE Transactions on Information Theory, 28*(4), 600-604.

Golomb, S. W. (1972). How to number a graph. *In Graph theory and computing* (pp. 23-37). Elsevier.

Golomb, S.W. (1984). Algebraic constructions for costas arrays. *Journal of CombinatorialmTheory, Series A, 37*(1), 13-21.

Halberstam, H., Roth, K. F. (1983). *Sequences*. Springer Science & Business Media.

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(185):1024-1044, octubre-diciembre de 2023. doi: https://doi.org/10.18257/raccefyn.1900

Linström, B. (1969). An inequality for B2-sequences. *Journal of Combinatorial Theory, 6*(2), 211-212.

Martos, C. A., Delgado, L. M., Trujillo, C. A. (2021). Bh sets as a generalization of golomb rulers. *IEEE Access, 9,* 118042-118050.

Martos, C. A. M., Daza, D. F., Trujillo, C. A. (2021). Near-optimal g-golomb rulers. *IEEE Access, 9,* 65482-65489.

Martos Ojeda, C. A. (2015). Reglas g− golomb. Tesis de Maestría, Departamento de Matemáticas, Universidad del Cauca.

Martos Ojeda, C. A. (2019). Conjuntos Bh y reglas g− golomb cortas. *Tesis de Doctorado, Departamento de Matem´aticas, Universidad del Valle.*

Moreno, O., Games, R., Taylor, H. (1991). New constructions and bounds on sonar sequences. *Proceedings. 1991 IEEE International Symposium on Information Theory,* 283-283.

Moreno, O., Games, R. A., 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.

Niu, M., Xiao, J., Gao, Y. (2022). New constructions of large cyclic subspace codes via sidon spaces. *Advances in Mathematics of Communications,* 1-15.

O'Bryant, K. (2022). On the size of finite sidon sets. *arXiv preprint arXiv:2207.07800.*

Raviv, N., Langton, B., Tamo, I. (2021). Multivariate public key cryptosystem from sidon spaces. *Public-Key Cryptography–PKC 2021: 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10–13, 2021, Proceedings, Part I,* 242-265.

Robinson, J. (1985). Golomb rectangles. *IEEE transactions on information theory, 31*(6), 781-787.

Robinson, J. P. (1997). Golomb rectangles as folded rulers. *IEEE Transactions on Information Theory, 43*(1), 290-293.

Ruzsa, I. Z. (1993). Solving a linear equation in a set of integers i. *Acta arithmetica, 65*(3), 259-282.

Shao, Z., Zhou, J., Liang, M., Lang, F., Xu, X. (2013). Some new golomb rectangles. *Journal of Computational and Theoretical Nanoscience, 10*(1), 66-68.

Shearer, J. B. (1995). Some new optimum golomb rectangles. *The electronic journal of combinatorics,* R12.

Shearer, J. B. (2004). Symmetric golomb squares. *IEEE transactions on information theory, 50*(8), 1846-1847.

Sidon, S. (1932). Ein satz über trigonometrische polynome und seine anwendung in der theorie der fourier-reihen. *Mathematische Annalen, 106,* 536-539.

Singer, J. (1938). A theorem in finite projective geometry and some applications to number theory. *Transactions of the American Mathematical Society, 43*(3), 377-385.

Trujillo Solarte, C. A. (1998). Sucesiones de sidon. *Tesis de Doctorado, Facultad de Informática, Universidad Politecnica de Madrid.*

Zhang, H., Cao, X. (2022). Constructions of sidon spaces and cyclic subspace codes. *Frontiers of Mathematics in China, 17*(2), 275-288.

Zhang, H., Tang, C. (2023). Constructions of large cyclic constant dimension codes via sidon spaces. *Designs, Codes and Cryptography, 91*(1), 29-44.

Zhang, T., Ge, G. (2022). New constructions of sidon spaces. *Journal of Algebraic Combinatorics,* 1–14.

Zullo, F. (2021). Multi-sidon spaces over finite fields. *arXiv preprint arXiv:2112.08781.*

Zullo, F. (2023). Multi-orbit cyclic subspace codes and linear sets. *Finite Fields and Their Applications, 87,* 102-153.