Reglas g-Golomb

Carlos A. Martos O. Nidia Y. Caicedo
Universidad del Cauca - Universidad del Valle

ALGEBRA, TEORÍA DE NÚMEROS, COMBINATORIA Y APLICACIONES ALTENCOA-6
San Juan de Pasto
Colombia

Agosto 2014

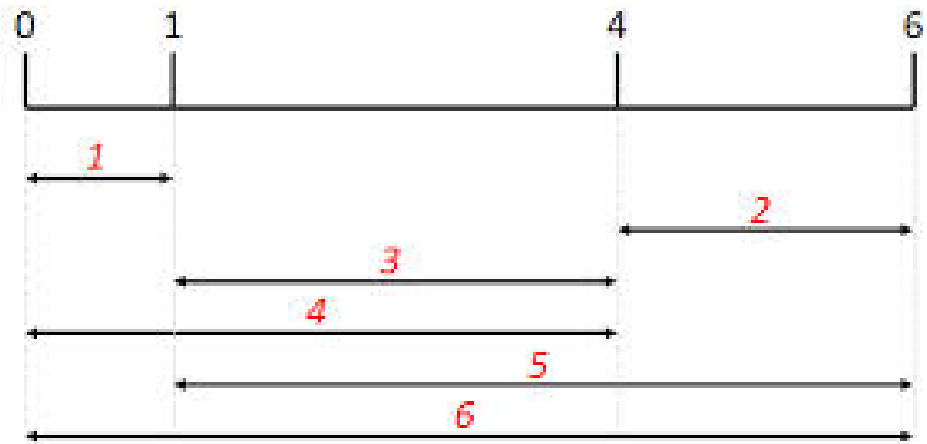
¿Qué es una regla Golomb?

¿Qué es una regla Golomb?

Una regla Golomb es un conjunto de enteros no negativos, llamados marcas, con la propiedad que todas las diferencias no nulas de dos elementos del conjunto son distintas.

¿Qué es una regla Golomb?

Una regla Golomb es un conjunto de enteros no negativos, llamados marcas, con la propiedad que todas las diferencias no nulas de dos elementos del conjunto son distintas.



Definición Formal

Definición

Una regla Golomb es un conjunto de enteros

$$A = \{a_1, a_2, \cdots, a_m\},$$

con la propiedad que para cada entero positivo d existe a lo más una solución de la ecuación $d = a_i - a_j$, con $i > j$.

Definición Formal

Definición

Una regla Golomb es un conjunto de enteros

$$A = \{a_1, a_2, \cdots, a_m\},$$

con la propiedad que para cada entero positivo d existe a lo más una solución de la ecuación $d = a_i - a_j$, con $i > j$.

Ejemplo:

Definición Formal

Definición

Una regla Golomb es un conjunto de enteros

$$A = \{a_1, a_2, \cdots, a_m\},$$

con la propiedad que para cada entero positivo d existe a lo más una solución de la ecuación $d = a_i - a_j$, con $i > j$.

Ejemplo:

El conjunto $A = \{0, 2, 6, 24, 29, 40, 43, 55, 68, 75, 76, 85\}$ es una regla Golomb.

Observaciones

Dada una regla Golomb A,

1. El número de marcas de la regla se denomina el *orden* .

Observaciones

Dada una regla Golomb A,

1. El número de marcas de la regla se denomina el *orden* .

2. La mayor distancia entre dos de sus marcas se llama *longitud* de la regla y se denota por $\ell(A)$.

Observaciones

Dada una regla Golomb A,

1. El número de marcas de la regla se denomina el *orden* .

2. La mayor distancia entre dos de sus marcas se llama *longitud* de la regla y se denota por $\ell(A)$.

$$\begin{aligned} \ell(A) &= \text{máx}\, A - \text{mín}\, A \\ &= a_m - a_1 \end{aligned}$$

Propiedades

1. Si A es una regla Golomb y x un entero, entonces

Propiedades

1. Si A es una regla Golomb y x un entero, entonces

$$A + x = \{a_i + x : a_i \in A\},$$

es una regla Golomb.

Propiedades

1. Si A es una regla Golomb y x un entero, entonces

$$A + x = \{a_i + x : a_i \in A\},$$

es una regla Golomb.

2. Si A es una regla Golomb y x un número entero, entonces

$$xA = \{xa_i : a_i \in A\},$$

es una regla Golomb.

Problema Fundamental

El problema fundamental en el estudio de las reglas Golomb, consiste en determinar la regla más corta para un número determinado de marcas . Estas se llaman **reglas Golomb óptimas.**

Problema Fundamental

El problema fundamental en el estudio de las reglas Golomb, consiste en determinar la regla más corta para un número determinado de marcas . Estas se llaman **reglas Golomb óptimas.**

0	3	15	41	66	95	97	106	142	152	220
221	225	242	295	330	338	354	382	388	402	415
486	504	523	546	553						

Función $G(m)$

Función $G(m)$

Definición

Se define la función $G(m)$ como la mínima longitud de una regla Golomb con m marcas, es decir,

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

Cotas Inferiores

- $G(m) \geq \frac{m(m-1)}{2}$ (Cota trivial).

Cotas Inferiores

- $G(m) \geq \frac{m(m-1)}{2}$ (Cota trivial).
- $G(m) \geq m^2 - 2m\sqrt{m}$, (M. D. Atkinson, N. Santoro y J. Urrutia [14]).

Cotas Inferiores

- $G(m) \geq \frac{m(m-1)}{2}$ (Cota trivial).
- $G(m) \geq m^2 - 2m\sqrt{m}$, (M. D. Atkinson, N. Santoro y J. Urrutia [14]).
- $G(m) \geq m^2 - 2m\sqrt{m} + \sqrt{m} - 2$, (A. Dimitromanolakis [1]).

Reglas g-Golomb

Reglas g-Golomb

Definición

Sean G un grupo abeliano aditivo, A, B subconjuntos de G, la función de representación con dominio el grupo G y codominio los enteros no negativos, se define por:

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

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

para todo $x \in G$.

Reglas g-Golomb

Definición

Sean G un grupo abeliano aditivo, A, B subconjuntos de G, la función de representación con dominio el grupo G y codominio los enteros no negativos, se define por:

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

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

para todo $x \in G$.

Note que

$$\sum_{x \in G} R_{A+B}(x) = \sum_{x \in G} R_{A-B}(x) = |A|\,|B|\,.$$

Definición (Regla g-Golomb)

Una regla g-Golomb o conjunto $B_2^-[g]$ es un conjunto A de enteros tal que

$$R_{A-A}(x) \leq g, \text{ para todo } x \text{ entero distinto de cero .}$$

Definición (Regla g-Golomb)

Una regla g-Golomb o conjunto $B_2^-[g]$ es un conjunto A de enteros tal que

$$R_{A-A}(x) \leq g, \text{ para todo } x \text{ entero distinto de cero .}$$

Ejemplo:

El conjunto $A_1 = \{0, 1, 4, 6, 8, 9\}$ es una regla 2-Golomb.

Problema fundamental

- **Problema 1. Reglas g-Golomb óptimamente Cortas**

Problema fundamental

- **Problema 1. Reglas g-Golomb óptimamente Cortas**
- **Problema 2. Reglas g-Golomb óptimamente Densas**

Función $G(g, m)$

Definición

Se define la función $G(g, m)$ como la mínima longitud de una regla g-Golomb con m marcas, es decir,

Función $G(g, m)$

Definición

Se define la función $G(g, m)$ como la mínima longitud de una regla g-Golomb con m marcas, es decir,

$$G(g, m) := \min \{\ell(A) : A \text{ es una regla } g\text{-Golomb}, |A| = m\}.$$

Definición $F_2^-(g,n)$

Definición

Se define la función $F_2^-(g,n)$ como

Definición $F_2^-(g,n)$

Definición

Se define la función $F_2^-(g,n)$ *como*

$$F_2^-(g,n) := \max\{|A| : A \subseteq [1,n],\ A \text{ es una regla } g\text{-Golomb}\},$$

donde $[1,n] := \{1,2,\ldots,n\}$.

Definición (Energía Aditiva)

Sea G un grupo abeliano aditivo, A, B subconjuntos de G,se define la energía aditiva, $E(A,B)$,entre A y B como,

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

Definición (Energía Aditiva)

Sea G un grupo abeliano aditivo, A, B subconjuntos de G,se define la energía aditiva, $E(A,B)$,entre A y B como,

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

Note que

$$E(A,B) = \sum_{x \in A+B} R^2_{A+B}(x)$$

Lema

(Ruzsa-Cilleruelo) Sea G un grupo abeliano aditivo y A, B subconjuntos de G. Si $R_{A-A}(x) \leq g$ para todo $x \in G$, $x \neq 0$, entonces

Lema

(Ruzsa-Cilleruelo) Sea G un grupo abeliano aditivo y A, B subconjuntos de G. Si $R_{A-A}(x) \leq g$ para todo $x \in G$, $x \neq 0$, entonces

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

Teorema

Si $A = \{a_i : 1 \leq i \leq m\}, \qquad 0 = a_1 < a_2 < \cdots < a_m,$ *es una regla* g*-Golomb de* m *marcas y* $\ell(A) = a_m$*, entonces*

Teorema

Si $A = \{a_i : 1 \leq i \leq m\}, \qquad 0 = a_1 < a_2 < \cdots < a_m,$ *es una regla* g*-Golomb de* m *marcas y* $\ell(A) = a_m$*, entonces*

$$G(g,m) \geq \frac{m^2}{g} - \frac{2m\sqrt{m-g}}{g} + \frac{m}{g} - \frac{m}{\sqrt{m-g}} - 1.$$

Corolario

Para todo entero positivo m

$$G(m) \geq m^2 - 2m\sqrt{m-1} + m - \frac{m}{\sqrt{m-1}} - 1.$$

Corolario

Para todo entero positivo m

$$G(m) \geq m^2 - 2m\sqrt{m-1} + m - \frac{m}{\sqrt{m-1}} - 1.$$

Corolario

Para todo entero $g \geq 1$ *tenemos.*

Corolario

Para todo entero positivo m

$$G(m) \geq m^2 - 2m\sqrt{m-1} + m - \frac{m}{\sqrt{m-1}} - 1.$$

Corolario

Para todo entero $g \geq 1$ *tenemos.*

$$\lim_{n\to\infty} \inf \frac{G(g,m)}{m^2} \geq \frac{1}{g}. \tag{1}$$

Teorema

Para todo número natural g y todo n, se tiene que

$$F_2^-(g,n) \leq (gn)^{1/2} + (gn)^{1/4} + 1. \tag{2}$$

Teorema

Para todo número natural g y todo n, se tiene que

$$F_2^-(g,n) \leq (gn)^{1/2} + (gn)^{1/4} + 1. \tag{2}$$

Corolario

$$\lim_{n\to\infty} \sup \frac{F_2^-(g,n)}{\sqrt{n}} \leq \sqrt{g}. \tag{3}$$

Construcciones

Construcciones

Teorema

Sean $g \in \mathbb{N}$ y $\varphi : G \to G'$ un homomorfsmo de grupos con $|ker(\varphi)| = g$. Si A es una regla Golomb en G entonces $\varphi(A)$ es una regla g-Golomb en $\varphi(G)$.

Por otro lado, se sabe que existen tres construcciones de reglas Golomb ó conjuntos B_2 muy conocidas, éstas son:

Por otro lado, se sabe que existen tres construcciones de reglas Golomb ó conjuntos B_2 muy conocidas, éstas son:

- La construcción de Singer que propociona una regla Golomb con $q+1$ elementos, módulo q^2+q+1.

Por otro lado, se sabe que existen tres construcciones de reglas Golomb ó conjuntos B_2 muy conocidas, éstas son:

- La construcción de Singer que propociona una regla Golomb con $q+1$ elementos, módulo q^2+q+1.
- La construcción de Bose que propociona una regla Golomb con q elementos, módulo q^2-1.

Por otro lado, se sabe que existen tres construcciones de reglas Golomb ó conjuntos B_2 muy conocidas, éstas son:

- La construcción de Singer que propociona una regla Golomb con $q+1$ elementos, módulo q^2+q+1.
- La construcción de Bose que propociona una regla Golomb con q elementos, módulo q^2-1.
- La construcción de Ruzsa que propociona una regla Golomb con $p-1$ elementos, módulo p^2-p.

Teorema (Bose, 1942)

Para cada potencia prima q, existe un conjunto $A \subseteq [1, q^2-1]$ con q elementos tal que $A \in B_2$ en $\mathbb{Z}_{q^2-1}$. Además, $A \ominus A = \mathbb{Z}_{q^2-1} \setminus M_{q+1}$, donde M_{q+1} indica el conjunto de múltiplos de $q+1$ en $\mathbb{Z}_{q^2-1}$.

Teorema (Bose, 1942)

Para cada potencia prima q, existe un conjunto $A \subseteq [1, q^2-1]$ con q elementos tal que $A \in B_2$ en $\mathbb{Z}_{q^2-1}$. Además, $A \ominus A = \mathbb{Z}_{q^2-1} \setminus M_{q+1}$, donde M_{q+1} indica el conjunto de múltiplos de $q+1$ en $\mathbb{Z}_{q^2-1}$.

Teorema (Ruzsa, 1993)

Para cada número primo p, existe un conjunto $R \subseteq [1, p^2-p]$ con $p-1$ elementos tal que $R \in B_2$ en $\mathbb{Z}_{p^2-p}$. Además, $R \ominus R = \mathbb{Z}_{p^2-p} \setminus (M_p \cup M_{p-1})$, donde M_p indica el conjunto de múltiplos de p y M_{p-1} indica el conjunto de múltiplos de $p-1$ en $\mathbb{Z}_{p^2-p}$.

Lema

Para cada entero $g \geq 2$ *y cada potencia prima* $q \equiv 1(\text{ mód } g)$, *existe un conjunto* $B \in B_2^-[g]$ *tal que* $|B| = q$ *y* $B \subseteq \left[1, \frac{q^2-1}{g}\right]$

Lema

Para cada entero $g \geq 2$ *y cada potencia prima* $q \equiv 1(\text{ mód } g)$, *existe un conjunto* $B \in B_2^-[g]$ *tal que* $|B| = q$ *y* $B \subseteq \left[1, \frac{q^2-1}{g}\right]$

Lema

Para cada entero $g \geq 2$ *y cada prima* $p \equiv 1(\text{mód } g)$, *existe un conjunto* $S \in B_2^-[g]$ *tal que* $|S| = p$ *y* $S \subseteq \left[1, \frac{p^2-p}{g}\right]$

Corolario

Para todo entero $g \geq 1$ *tenemos.*

Corolario

Para todo entero $g \geq 1$ *tenemos.*

$$\lim_{n\to\infty} \sup \frac{G(g,m)}{m^2} \leq \frac{1}{g}. \tag{4}$$

Corolario

Para todo entero $g \geq 1$ *tenemos.*

$$\lim_{n\to\infty} \sup \frac{G(g,m)}{m^2} \leq \frac{1}{g}. \tag{4}$$

Demostración.

Sabemos que $G(g,p) \leq \frac{p^2-1}{g}$, luego

Corolario

Para todo entero $g \geq 1$ *tenemos.*

$$\lim_{n\to\infty} \sup \frac{G(g,m)}{m^2} \leq \frac{1}{g}. \tag{4}$$

Demostración.

Sabemos que $G(g,p) \leq \frac{p^2-1}{g}$, luego

$$\frac{G(g,p)}{p^2} \leq \frac{1}{g},$$

□

por otro lado, sean p y p', primos tales que:

por otro lado, sean p y p', primos tales que:

$$G(g,p') \leq G(g,m) \leq G(g,p),$$

por otro lado, sean p y p', primos tales que:

$$G(g,p') \leq G(g,m) \leq G(g,p),$$

de donde.

$$\frac{G(g,m)}{m^2} \leq \left(\frac{p}{p'}\right)^2 \frac{1}{g}$$

Teorema

Sea $g \geq 2$ un entero. Para infinitos valores de n, existe un conjunto $A \subseteq [1, n]$, $A \in B_2^-[g]$, con $|A| \geq (gn)^{1/2}$

Teorema

Sea $g \geq 2$ un entero. Para infinitos valores de n, existe un conjunto $A \subseteq [1, n]$, $A \in B_2^-[g]$, con $|A| \geq (gn)^{1/2}$

Demostración.

Sea $g \geq 2$ un entero, por el Teorema de Dirichlet sobre primos en progresiones aritméticas, existen infinitos primos p que satisfacen $p \equiv 1 (\mathrm{mód}\, g)$.

Teorema

Sea $g \geq 2$ un entero. Para infinitos valores de n, existe un conjunto $A \subseteq [1, n]$, $A \in B_2^-[g]$, con $|A| \geq (gn)^{1/2}$

Demostración.

Sea $g \geq 2$ un entero, por el Teorema de Dirichlet sobre primos en progresiones aritméticas, existen infinitos primos p que satisfacen $p \equiv 1 (\mathrm{mód}\, g)$.

Para cada uno de estos primos p , sea $n = \frac{p^2-1}{g}$; por el Lema 2 existe un conjunto $B \subseteq [1, n]$ en la clase $B_2^-[g]$ con

$$|B| = p \geq \sqrt{p^2 - 1} = \sqrt{gn}.$$

Teorema

Para infinitos enteros positivos n, existe un conjunto de Sidon $A \subseteq [1, n]$ con $|A| \geq \sqrt{n}$.

Teorema

Para infinitos enteros positivos n, existe un conjunto de Sidon $A \subseteq [1, n]$ con $|A| \geq \sqrt{n}$.

Demostración.

Como existen infinitos primos, tenemos infinitas potencias de primos q. Sea $n = q^2 - 1$, por la construcción de Bose, para cada q, existe un conjunto $A \subseteq [1, n]$ en la clase B_2, tal que $|A| = q = \sqrt{q^2} \geq \sqrt{q^2 - 1} = \sqrt{n}$.

$\square$

En consecuencia, tenemos

En consecuencia, tenemos

$$F_2^-(g,n) \geq (gn)^{1/2},$$

para todo $g \in \mathbb{N}$ e infinitos n.

Corolario

$$\lim_{n\to\infty} \inf \frac{F_2^-(g,n)}{\sqrt{n}} \geq \sqrt{g}. \tag{5}$$

Teorema

Para cada entero $g \geq 1$, se tiene que

1. $$\lim_{n\to\infty} \frac{F_2^-(g,n)}{\sqrt{n}} = \sqrt{g}.$$

Teorema

Para cada entero $g \geq 1$, se tiene que

1. $$\lim_{n\to\infty} \frac{F_2^-(g,n)}{\sqrt{n}} = \sqrt{g}.$$

2. $$\lim_{n\to\infty} \frac{G(g,m)}{m^2} = \frac{1}{g}.$$

Problemas Abiertos

- Mejorar la cota superior de la función F_2^-, dada por

$$F_2^-(g,n) \leq (gn)^{1/2} + (gn)^{1/4} + \frac{1}{2}.$$

Problemas Abiertos

- Mejorar la cota superior de la función F_2^-, dada por

$$F_2^-(g,n) \leq (gn)^{1/2} + (gn)^{1/4} + \frac{1}{2}.$$

- Mejorar la cota inferior de la función G, dada por

$$G(g,m) \geq \frac{m^2}{g} - \frac{2m\sqrt{m-g}}{g} + \frac{m}{g} - \frac{m}{\sqrt{m-g}} - 1.$$

Problemas Abiertos

- Mejorar la cota superior de la función F_2^-, dada por

$$F_2^-(g,n) \leq (gn)^{1/2} + (gn)^{1/4} + \frac{1}{2}.$$

- Mejorar la cota inferior de la función G, dada por

$$G(g,m) \geq \frac{m^2}{g} - \frac{2m\sqrt{m-g}}{g} + \frac{m}{g} - \frac{m}{\sqrt{m-g}} - 1.$$

- Construir conjuntos $B_2^+[g]$ enteros.

- A. Dimitromanolakis, Analysis of the Golomb Ruler and the Sidon set Problems, and Determination of Large, near-optimal Golomb rulers. Master's thesis, Departement of Electronic and Cumputer Engineering, Techical University of Crete, June 2002.
- R. C. Bose, *An afine analogue of Singer's theorem*, J. Indian Math. Soc. (N.S.) 6 (1942), 1-15.
- J. Cilleruelo, *Sidon sets in* $\mathbb{N}^d$. J. Combin. Theory Ser. A 117 (2010), N° 7, 857-871.
- J. Gómez, *Construcción de conjuntos* $B_h[g]$, Tesis de Maestría en Ciencias Matemáticas, Universidad del Valle, 2011.
- B. Lindström, *An inequality for* B_2*-sequences*, J. Combinatorial Theory 6 (1969), 211-212.
- T. Tao and V.H. Vu. Additive Combinatorics. Cambridge University Press, New York (2006).
- C. A. Trujillo, G. García, J. M. Velásquez, $B_2^-[g]$ *Finite Sets*,

15 años

Gracias