CONJUNTOS B_h, ALGUNOS PROBLEMAS Y APLICACIONES

CARLOS ALBERTO TRUJILLO
Universidad del Cauca

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

Sea $A \subseteq \mathbb{N}$, se define

$$f_A(x) := \sum_{a \in A} x^a.$$

Sea $A \subseteq \mathbb{N}$, se define

$$f_A(x) := \sum_{a \in A} x^a.$$

$$f_A(x)^2 = \left(\sum_{a \in A} x^a \right)^2 = \sum_{n \in \mathbb{N}} R_A(n) x^n,$$

donde $R_A(n) := |\{(a,b) \in A \times A : \ n = a + b\}| = |A \cap (n - A)|$.

Ejemplo

Sea $A = \{1, 2, 3, 5, 7\}$, entonces

$$f_A(x) = x + x^2 + x^3 + x^5 + x^7$$

$+$	1	2	3	5	7
	2	3	4	6	8
	3	4	5	7	9
	4	5	6	8	10
	6	7	8	10	12
	8	9	10	12	14

Ejemplo

n	2	3	4	5	6	7	8	9	11	12	14
$R_A(n)$	1	2	3	2	3	2	3	2	3	2	1

$$f_A(x)^2 = x^2 + 2x^3 + 3x^4 + 2x^5 + 3x^6 + 2x^7 + 3x^8 + 2x^9 + 3x^{11} + 2x^{12} + x^{14}.$$

Ejemplo

n	2	3	4	5	6	7	8	9	11	12	14
$R_A(n)$	1	2	3	2	3	2	3	2	3	2	1

$$f_A(x)^2 = x^2 + 2x^3 + 3x^4 + 2x^5 + 3x^6 + 2x^7 + 3x^8 + 2x^9 + 3x^{11} + 2x^{12} + x^{14}.$$

Sea $D = \{1, 2, 4, 8, 16, 32, \ldots\}$, entonces

$$f_D(x)^2 = x^2 + 2x^3 + x^4 + 2x^5 + \cdots = \sum_{n \in \mathbb{N}} R_D(n) x^n$$

En particular: $R_D(n) \leq 2$ para todo n.

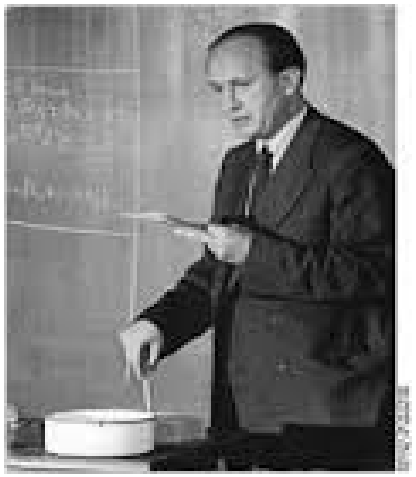
Conjuntos A tales que $R_A(n)$ es "pequeño"

Sidon pregunta a Erdös (1932)

¿Cuál es el máximo número de enteros seleccionados de $\{1, 2, \ldots, N\}$ en forma tal que las sumas de dos elementos sean todas distintas?

Erdös los llama **Conjuntos de Sidon**

Teorema Paul Erdös y Paul Turán (1942)



$$\lim_{N\to\infty} \frac{F_2(N)}{\sqrt{N}} = 1$$

Inicia investigación sobre conjuntos B_h.

Definición general de conjuntos B_h

Sean $(G, +)$ un grupo conmutativo y $A \subseteq G$.

A es un conjunto B_h (en G) si todas las sumas de h elementos de A producen elementos distintos en G. Notación: $A \in B_h$ (en G).

Definición general de conjuntos B_h

Sean $(G, +)$ un grupo conmutativo y $A \subseteq G$.

A es un conjunto B_h (en G) si todas las sumas de h elementos de A producen elementos distintos en G. Notación: $A \in B_h$ (en G).

Dados $a_1, \ldots, a_h; b_1, \ldots, b_h \in A$,

$a_1 + \cdots + a_h = b_1 + \cdots + b_h \Rightarrow (b_1, \ldots, b_h)$ es permutación de $(a_1, \ldots, a_h)$.

Definición general de conjuntos B_h

Sean $(G,+)$ un grupo conmutativo y $A \subseteq G$.

A es un conjunto B_h (en G) si todas las sumas de h elementos de A producen elementos distintos en G. Notación: $A \in B_h$ (en G).

Dados $a_1,\ldots,a_h; b_1,\ldots,b_h \in A$,

$a_1+\cdots+a_h = b_1+\cdots+b_h \Rightarrow (b_1,\ldots,b_h)$ es permutación de $(a_1,\ldots,a_h)$.

NOTACIÓN

$$hA := \underbrace{A+\cdots+A}_{h-\text{ copias}} := \{a_1+\cdots+a_h : a_1,\ldots,a_h \in A\}$$

Definición general de conjuntos B_h

Sea $A = \{a_1, \ldots, a_k\}$, se tiene

$$A \in B_h \text{ sii } |hA| = \binom{k+h-1}{h}$$

Definición general de conjuntos B_h

Sea $A = \{a_1, \ldots, a_k\}$, se tiene

$$A \in B_h \text{ sii } |hA| = \binom{k+h-1}{h}$$

Todo $x \in hA$ tiene representación única como suma de h elementos de A (salvo permutaciones de sumandos).

Definición general de conjuntos B_h

Sea $A = \{a_1, \ldots, a_k\}$, se tiene

$$A \in B_h \text{ sii } |hA| = \binom{k+h-1}{h}$$

Todo $x \in hA$ tiene representación única como suma de h elementos de A (salvo permutaciones de sumandos).

Todas las sumas $a_{i_1} + \cdots + a_{i_h}$, $1 \leq i_1 \leq \cdots \leq i_h \leq k$, son diferentes.

Problema fundamental (G es fnito)

¿Máximo número de elementos que puede tener un conjunto B_h en G?

$$f_h(G) := \max\{|A| : A \in B_h \text{ (en } G)\}.$$

¿Máximo número de elementos que puede tener un conjunto B_h en G?

$$f_h(G) := \max\{|A| : A \in B_h \text{ (en } G)\}.$$

Sea $A \in B_h$, $|A| = k$, $|G| = N$:

$$\frac{k^h}{h!} \leq \binom{k+h-1}{h} = |hA| \leq N$$

$$k \leq (h!N)^{1/h}$$

$$\limsup \frac{f_n(G)}{|G|^{1/h}} \leq (h!)^{1/h}$$

Para $h = 2$, se conocen algunos grupos G en los cuales se tienen valores exactos,

$f_2(\mathbb{Z}_{q^2+q+1}) = q + 1,$

$f_2(\mathbb{Z}_{q^2-1}) = q,$

$f_2(\mathbb{Z}_p \times \mathbb{Z}_{p-1}) = p - 1,$

$f_2(\mathbb{Z}_p \times \mathbb{Z}_p) = p,$

$f_2(\mathbb{F}_q \times \mathbb{F}_q) = q,$

$f_2(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}) \in \{q - 2, q - 1\}.$

Para $h = 2$, se conocen algunos grupos G en los cuales se tienen valores exactos,

$f_2(\mathbb{Z}_{q^2+q+1}) = q + 1,$

$f_2(\mathbb{Z}_{q^2-1}) = q,$

$f_2(\mathbb{Z}_p \times \mathbb{Z}_{p-1}) = p - 1,$

$f_2(\mathbb{Z}_p \times \mathbb{Z}_p) = p,$

$f_2(\mathbb{F}_q \times \mathbb{F}_q) = q,$

$f_2(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}) \in \{q - 2, q - 1\}.$

Para $h \geq 3$ nada similar.

Sea $A \in B_h$ (en G), $|A| = k$, $|G| = N$.

- $h = 2$: $k(k-1) \leq N - 1$

$$\lim_{N \to \infty} \sup \frac{f_2(G)}{N^{1/2}} \leq 1 \qquad (\text{ trivial: } \sqrt{2})$$

Sea $A \in B_h$ (en G), $|A| = k$, $|G| = N$.

- $h = 2$: $k(k-1) \leq N - 1$

$$\lim_{N \to \infty} \sup \frac{f_2(G)}{N^{1/2}} \leq 1 \qquad (\text{ trivial: } \sqrt{2})$$

- $h = 3$: $k(k^2 - k + 2) \leq 2N$

$$\lim_{N \to \infty} \sup \frac{f_3(G)}{N^{1/3}} \leq \sqrt[3]{2} \qquad (\text{ trivial: } \sqrt[3]{6})$$

Sea $A \in B_h$ (en G), $|A| = k$, $|G| = N$.

- $h = 2$: $k(k-1) \leq N - 1$

$$\lim_{N\to\infty} \sup \frac{f_2(G)}{N^{1/2}} \leq 1 \qquad (\text{ trivial: } \sqrt{2})$$

- $h = 3$: $k(k^2 - k + 2) \leq 2N$

$$\lim_{N\to\infty} \sup \frac{f_3(G)}{N^{1/3}} \leq \sqrt[3]{2} \qquad (\text{ trivial: } \sqrt[3]{6})$$

- $h = 4$: $k(k-1)(k^2 - k + 6) \leq 4(N-1)$

$$\lim_{N\to\infty} \sup \frac{f_4(G)}{N^{1/4}} \leq \sqrt[4]{4} = \sqrt{2} \qquad (\text{ trivial: } \sqrt[4]{24} = \sqrt{2\sqrt{6}})$$

- $h = 2s - 1$: $(k - 2s + 2)^{2s-1} \leq s!(s-1)!N$

$$f_{2s-1}(G) \leq (s!(s-1)!N)^{1/(2s-1)} + 2s - 2$$

- $h = 2s - 1$: $(k - 2s + 2)^{2s-1} \leq s!(s-1)!N$

$$f_{2s-1}(G) \leq \left(s!(s-1)!N\right)^{1/(2s-1)} + 2s - 2$$

- $h = 2s$: $(k - 2s + 1)^{2s} \leq (s!)^2 N$

$$f_{2s}(G) \leq \left((s!)^2!N\right)^{1/(2s)} + 2s - 1$$

- $h = 2s - 1$: $(k - 2s + 2)^{2s-1} \leq s!(s-1)!N$

$$f_{2s-1}(G) \leq (s!(s-1)!N)^{1/(2s-1)} + 2s - 2$$

- $h = 2s$: $(k - 2s + 1)^{2s} \leq (s!)^2 N$

$$f_{2s}(G) \leq \left((s!)^2!N\right)^{1/(2s)} + 2s - 1$$

J. Jia, H. Chen, sin constantes explícitas.

Códigos binarios

- Un subconjunto $\mathcal{C}$ de $\mathbb{F}_2^n$ se llama un código binario de longitud n.

Códigos binarios

- Un subconjunto $\mathcal{C}$ de $\mathbb{F}_2^n$ se llama un código binario de longitud n.
- Para $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ en $\mathcal{C}$, la distancia Hamming es

$$\delta(x, y) := |\{i : x_i \neq y_i\}|$$

Códigos binarios

- Un subconjunto $\mathcal{C}$ de $\mathbb{F}_2^n$ se llama un código binario de longitud n.
- Para $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ en $\mathcal{C}$, la distancia Hamming es

$$\delta(x, y) := |\{i : x_i \neq y_i\}|$$

- El peso de x es:

$$\omega(x) := d(x, 0) = |\{i : x_i \neq 0\}|$$

Códigos binarios

- Un subconjunto $\mathcal{C}$ de $\mathbb{F}_2^n$ se llama un código binario de longitud n.
- Para $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ en $\mathcal{C}$, la distancia Hamming es

$$\delta(x, y) := |\{i : x_i \neq y_i\}|$$

- El peso de x es:

$$\omega(x) := d(x, 0) = |\{i : x_i \neq 0\}|$$

- Distancia Mínima de $\mathcal{C}$:

$$\delta_{\mathcal{C}} := \min\{\delta(x, y) : x, y \in \mathcal{C}, x \neq y\}$$

Códigos binarios

- Un subconjunto $\mathcal{C}$ de $\mathbb{F}_2^n$ se llama un código binario de longitud n.
- Para $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ en $\mathcal{C}$, la distancia Hamming es

$$\delta(x, y) := |\{i : x_i \neq y_i\}|$$

- El peso de x es:

$$\omega(x) := d(x, 0) = |\{i : x_i \neq 0\}|$$

- Distancia Mínima de $\mathcal{C}$:

$$\delta_{\mathcal{C}} := \min\{\delta(x, y) : x, y \in \mathcal{C}, x \neq y\}$$

- Un Problema Fundamental. Para n, d, w dados

$$A(n, d) := \max\{|\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_2^n,\ \delta_{\mathcal{C}} \geq d\}$$

$$A(n, d, w) := \max\{|\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_2^n,\ \delta_{\mathcal{C}} \geq d,\quad \underbrace{\omega(\mathcal{C}) = w}_{\text{peso constante } w}\quad\}$$

R. L. Graham, N. J. A. Sloane (1980). Lower bounds for constant weight codes. IEEE Transactions on Information Theory, Vol. 11, No. 1, January 1980, 37-43 ($\oint$ III).

Un subconjunto $S = \{s_1, \ldots, s_n\}$ de $\mathbb{Z}_m$ se llama un conjunto B_h débil (Conjunto S_h) de tamaño n y módulo m si todas las sumas $s_{i_1} + s_{i_2} + \cdots + s_{i_h}$, para $i_1 < i_2 < \cdots < i_n$ son distintas en $\mathbb{Z}_m$.

R. L. Graham, N. J. A. Sloane (1980). Lower bounds for constant weight codes. IEEE Transactions on Information Theory, Vol. 11, No. 1, January 1980, 37-43 ($\oint$ III).

Un subconjunto $S = \{s_1, \ldots, s_n\}$ de $\mathbb{Z}_m$ se llama un conjunto B_h débil (Conjunto S_h) de tamaño n y módulo m si todas las sumas $s_{i_1} + s_{i_2} + \cdots + s_{i_h}$, para $i_1 < i_2 < \cdots < i_n$ son distintas en $\mathbb{Z}_m$.

$$\widehat{h}S = \underbrace{S \oplus \cdots \oplus S}_{h-\text{copias}} := \{s_1 + \cdots + s_h : s_1, \ldots, s_h \in S, \text{ todos distintos}\}$$

h- suma débil de S.

$$S \text{ es } B_h \text{ débil sii } |\widehat{h}S| = \binom{n}{h}.$$

Claramente, S es $B_h \Rightarrow S$ es B_h débil.

Teorema

(Teorema Graham y Sloane, 1980)
Si existe un conjunto $B_{\delta-1}$ débil de tamaño n y módulo m entonces

$$A(n, 2\delta, \omega) \geq \frac{1}{m}\binom{n}{\omega}$$

Teorema

(Teorema Graham y Sloane, 1980)
Si existe un conjunto $B_{\delta-1}$ débil de tamaño n y módulo m entonces

$$A(n, 2\delta, \omega) \geq \frac{1}{m}\binom{n}{\omega}$$

Utilizando la construcción de Singer, extendida por Bose & Chowla (1968).

Teorema

(Teorema Graham y Sloane, 1980)
Si existe un conjunto $B_{\delta-1}$ débil de tamaño n y módulo m entonces

$$A(n, 2\delta, \omega) \geq \frac{1}{m}\binom{n}{\omega}$$

Utilizando la construcción de Singer, extendida por Bose & Chowla (1968).

Teorema

(Teorema Graham y Sloane, 1980)
Sea q la menor potencia prima tal que $q+1 \geq n$. Entonces para $\delta \geq 3$,

$$A(n, 2\delta, \omega) \geq \frac{q-1}{q^{\delta}-1}\binom{n}{\omega}.$$

Construir conjunto B_h débil módulo m con cardinal máximo.

- $\widehat{f}_h(\mathbb{Z}_m) := \max\{|A| : A \in \widehat{B}_h \text{ en } \mathbb{Z}_m\}$
- $\upsilon(h, m) := \min\{m \in \mathbb{Z}^+ : \exists A \in \widehat{B}_h (\mathrm{mod} m),\ |A| = n\}$

Construir conjunto B_h débil módulo m con cardinal máximo.

- $\widehat{f}_h(\mathbb{Z}_m) := \max\{|A| : A \in \widehat{B}_h \text{ en } \mathbb{Z}_m\}$
- $\upsilon(h, m) := \min\{m \in \mathbb{Z}^+ : \exists A \in \widehat{B}_h (\mathrm{mod} m),\ |A| = n\}$

Construcción de conjuntos B_h módulo m (maximales) conocidos.

- Bose & Chowla (1944,1968).
- Singer (1932, 1968).
- A. Gómez & C. T. (2010).

- $\mathcal{C} \subseteq \mathbb{F}_2^n$, $\mathcal{C}$ subespacio de dimensión k.

  $\mathcal{C}$ es un $[n, k]$-código (binario, lineal).

  Si además, $\delta_{\mathcal{C}} = d$,

  $[n, k, d]$- código binario (longitud n, dimensión k, distancia d).

- $\mathcal{C} \subseteq \mathbb{F}_2^n$, $\mathcal{C}$ subespacio de dimensión k.

  $\mathcal{C}$ es un $[n, k]$-código (binario, lineal).

  Si además, $\delta_{\mathcal{C}} = d$,

  $[n, k, d]$- código binario (longitud n, dimensión k, distancia d).

- Un problema básico:

$$B(n, d) := \max\{|\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_2^n, \mathcal{C} \text{ lineal}, \delta_{\mathcal{C}} \leq d\}$$

- $\mathcal{C} \subseteq \mathbb{F}_2^n$, $\mathcal{C}$ subespacio de dimensión k.

  $\mathcal{C}$ es un $[n, k]$-código (binario, lineal).

  Si además, $\delta_{\mathcal{C}} = d$,

  $[n, k, d]$- código binario (longitud n, dimensión k, distancia d).

- Un problema básico:

$$B(n, d) := \max\{|\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_2^n, \mathcal{C} \text{ lineal}, \delta_{\mathcal{C}} \leq d\}$$

- Claramente:

$$B(n, d) \leq A(n, d).$$

H. Haanpää & P. Ostergárd. Sets in Abelian Groups with Distinct Sums of Pairs. Journal of Number Theory 123(2007), 144-153.

Teorema

Existe un $[n, n-r, 5]$-código binario (lineal) si y sólo si existe un conjunto B_2 débil (Sidon débil) en $\mathbb{F}_2^r$ con $n+1$ elementos.

Generalizamos:

Teorema

Existe un $[n, k, d]$-código binario (lineal), con $d \geq 2n + 1$, si y sólo si existe un conjunto B_h débil con $n + 1$ elementos en $\mathbb{F}_2^{n-k}$, donde $n - k \geq 2h$.

($\Rightarrow$)

$\{\text{Columnas matriz chequeo de paridad}\} \cup \{\overrightarrow{0}\} = A$,

donde A es un conjunto B_h-débil.

($\Leftarrow$)

$r = n - k$, A_1 conjunto B_h-débil con $n + 1$ elementos en $\mathbb{F}_2^r$ $(n > r \geq 2h)$.

($\Leftarrow$)

$r = n - k$, A_1 conjunto B_h-débil con $n + 1$ elementos en $\mathbb{F}_2^r$ $(n > r \geq 2h)$.

- Extenderlo a un $\overline{A}$ con un número maximal de elementos (manteniendo B_h-débil)

($\Leftarrow$)

$r = n - k$, A_1 conjunto B_h-débil con $n+1$ elementos en $\mathbb{F}_2^r$ $(n > r \geq 2h)$.

- Extenderlo a un $\overline{A}$ con un número maximal de elementos (manteniendo B_h-débil)
- Para $b \in \overline{A}$, sea $A = b + \overline{A}$.

  $0 \in A$, A contiene una base de $\mathbb{F}_2^r$ sobre $\mathbb{F}_2$.

($\Leftarrow$)

$r = n - k$, A_1 conjunto B_h-débil con $n+1$ elementos en $\mathbb{F}_2^r$ $(n > r \geq 2h)$.

- Extenderlo a un $\overline{A}$ con un número maximal de elementos (manteniendo B_h-débil)
- Para $b \in \overline{A}$, sea $A = b + \overline{A}$.

  $0 \in A$, A contiene una base de $\mathbb{F}_2^r$ sobre $\mathbb{F}_2$.
- Sea H matriz $r \times n$: columnas son n elementos no cero de A (incluyendo una base de $\mathbb{F}_2^r$).

($\Leftarrow$)

$r = n - k$, A_1 conjunto B_h-débil con $n+1$ elementos en $\mathbb{F}_2^r$ $(n > r \geq 2h)$.

- Extenderlo a un $\overline{A}$ con un número maximal de elementos (manteniendo B_h-débil)
- Para $b \in \overline{A}$, sea $A = b + \overline{A}$.

  $0 \in A$, A contiene una base de $\mathbb{F}_2^r$ sobre $\mathbb{F}_2$.
- Sea H matriz $r \times n$: columnas son n elementos no cero de A (incluyendo una base de $\mathbb{F}_2^r$).
- Código cuya matriz chequeo de paridad es H tiene parámetros deseados: $d \geq 2h+1$, $k = n - r$.

$$F_h(N) := \max\{|A| : A \subseteq [1, N],\ A \in B_h\}$$

$$F_h(N) := \max\{|A| : A \subseteq [1, N],\ A \in B_h\}$$

$$¿ \lim_{N\to\infty} \frac{F_h(N)}{N^{1/h}} ?$$

$$F_h(N) := \max\{|A| : A \subseteq [1, N],\ A \in B_h\}$$

$$¿ \lim_{N\to\infty} \frac{F_h(N)}{N^{1/h}} ?$$

1. Mejorar la estimación

$$F_2(N) < N^{1/2} + N^{1/4} + 1/2.$$

$$F_h(N) := \max\{|A| : A \subseteq [1, N],\ A \in B_h\}$$

$$¿ \lim_{N\to\infty} \frac{F_h(N)}{N^{1/h}} ?$$

1. Mejorar la estimación

$$F_2(N) < N^{1/2} + N^{1/4} + 1/2.$$

2. Construir conjuntos B_2 "propiamente" enteros suficientemente densos.

$$F_h(N) := \max\{|A| : A \subseteq [1,N],\ A \in B_h\}$$

$$\text{¿}\lim_{N\to\infty} \frac{F_h(N)}{N^{1/h}}?$$

1. Mejorar la estimación
$$F_2(N) < N^{1/2} + N^{1/4} + 1/2.$$
2. Construir conjuntos B_2 "propiamente" enteros suficientemente densos.
3. Mejorar cotas superiores conocidas para $F_h(N)$, $h \geq 3$:
$$F_3(N) \leq \left(\frac{7}{2}N\right)^{1/3}(1+o(1)) \quad \text{(Ben Green)}$$
$$F_4(N) \leq (7N)^{1/4}(1+o(1))$$

4.

$$f_h(N) := F_h(\mathbb{Z}_N) := \max\{|A| : A \in B_h \text{ en } \mathbb{Z}_N\}$$

$$¿ \lim_{N\to\infty} \frac{f_h(N)}{N^{1/h}} ?$$

$h = 2$:

$$\frac{\sqrt{2}}{2} \leq \liminf \frac{f_2(N)}{\sqrt{N}} \leq \limsup \frac{f_2(N)}{\sqrt{N}} \leq 1$$

4.

$$f_h(N) := F_h(\mathbb{Z}_N) := \max\{|A| : A \in B_h \text{ en } \mathbb{Z}_N\}$$

$$\text{¿} \lim_{N\to\infty} \frac{f_h(N)}{N^{1/h}} ?$$

$h = 2$:

$$\frac{\sqrt{2}}{2} \leq \liminf \frac{f_2(N)}{\sqrt{N}} \leq \limsup \frac{f_2(N)}{\sqrt{N}} \leq 1$$

5. Construcción de conjuntos B_2 (B_h) en otros grupos.

4.

$$f_h(N) := F_h(\mathbb{Z}_N) := \max\{|A| : A \in B_h \text{ en } \mathbb{Z}_N\}$$

$$¿ \lim_{N\to\infty} \frac{f_h(N)}{N^{1/h}} ?$$

$h = 2$:

$$\frac{\sqrt{2}}{2} \leq \liminf \frac{f_2(N)}{\sqrt{N}} \leq \limsup \frac{f_2(N)}{\sqrt{N}} \leq 1$$

5. Construcción de conjuntos B_2 (B_h) en otros grupos.

Hoy:

$f_2(\mathbb{Z}_{q^2+q+1}) = q+1$

$f_2(\mathbb{Z}_{q^2-1}) = q$

$f_2(\mathbb{Z}_p \times \mathbb{Z}_{p-1}) = f_2(\mathbb{Z}_{p^2-p}) = p-1$

$f_2(\mathbb{F}_q \times \mathbb{F}_q) = q$

$f_2(\mathbb{Z}_{q-1} \times \mathbb{F}_q^*) = q-1$

- B_2/ Sidon / Golomb / Enteros: Radio comunicación (Interferencias, Antenas)

- B_2/ Sidon / Golomb / Enteros: Radio comunicación (Interferencias, Antenas)
- B_2/ Sidon / Costas / $\mathbb{Z} \times \mathbb{Z}$: Radar, Sonar (Efecto Dopler), Arreglos Costas, Secuencias Sonar.

  (Tesis Doctoral Yadira Caicedo- Universidad del Valle)

- B_2/ Sidon / Golomb / Enteros: Radio comunicación (Interferencias, Antenas)
- B_2/ Sidon / Costas / $\mathbb{Z} \times \mathbb{Z}$: Radar, Sonar (Efecto Dopler), Arreglos Costas, Secuencias Sonar.

  (Tesis Doctoral Yadira Caicedo- Universidad del Valle)
- Criptografía

- B_2/ Sidon / Golomb / Enteros: Radio comunicación (Interferencias, Antenas)
- B_2/ Sidon / Costas / $\mathbb{Z} \times \mathbb{Z}$: Radar, Sonar (Efecto Dopler), Arreglos Costas, Secuencias Sonar.

  (Tesis Doctoral Yadira Caicedo- Universidad del Valle)
- Criptografía
- Rotulamiento de Grafos

- B_2/ Sidon / Golomb / Enteros: Radio comunicación (Interferencias, Antenas)
- B_2/ Sidon / Costas / $\mathbb{Z} \times \mathbb{Z}$: Radar, Sonar (Efecto Dopler), Arreglos Costas, Secuencias Sonar.

  (Tesis Doctoral Yadira Caicedo- Universidad del Valle)
- Criptografía
- Rotulamiento de Grafos
- Combinatoria (Diseños...)

- B_2/ Sidon / Golomb / Enteros: Radio comunicación (Interferencias, Antenas)
- B_2/ Sidon / Costas / $\mathbb{Z} \times \mathbb{Z}$: Radar, Sonar (Efecto Dopler), Arreglos Costas, Secuencias Sonar.

  (Tesis Doctoral Yadira Caicedo- Universidad del Valle)
- Criptografía
- Rotulamiento de Grafos
- Combinatoria (Diseños...)
- Teoría de Códigos: Lineales, COO

- Reglas Golomb Óptimas (cortas).

- Reglas Golomb Óptimas (cortas).
- Existencia de Arreglos Costas para todo orden.

NUEVOS PROBLEMAS

- Reglas Golomb Óptimas (cortas).
- Existencia de Arreglos Costas para todo orden.
- Problema Secuencias Sonar.

- Reglas Golomb Óptimas (cortas).
- Existencia de Arreglos Costas para todo orden.
- Problema Secuencias Sonar.
- Estimar función

$$\upsilon(h,n) := \min_{2h \le r < n} \left\{ r : \exists A \in \widehat{B}_h \text{ en } \mathbb{F}_2^r,\ |A| = n+1 \right\}$$

Importante porque: (A. Gómez y C. T., 2011)

$$\log_2 B(n, 2h+1) = n - \upsilon(h,n).$$

- Reglas Golomb Óptimas (cortas).
- Existencia de Arreglos Costas para todo orden.
- Problema Secuencias Sonar.
- Estimar función

$$\upsilon(h,n) := \min_{2h \le r < n} \left\{ r : \exists A \in \widehat{B}_h \text{ en } \mathbb{F}_2^r, \, |A| = n+1 \right\}$$

  Importante porque: (A. Gómez y C. T., 2011)

$$\log_2 B(n, 2h+1) = n - \upsilon(h,n).$$

- Conjuntos B_h débiles asociados a códigos lineales especiales: BCH, cíclicos, MDS, etc...

Determinar el mínimo orden de un grupo G que contiene un conjunto B_h con n elementos:

$$c(n,h) := \min_{\text{grupos}} \{|G| : \text{ existe } A \in B_h \text{ en } G, \, |A| = n\}$$

GRACIAS