Revista Integración
Escuela de Matemáticas
Universidad Industrial de Santander
Vol. 28, No. 1, 2010, pág. 67–78

Análisis de Fourier sobre $\mathbb{Z}_N$ y conjuntos B_h

Jhon Jairo Bravo G.[a,*], Carlos Alberto Trujillo S.[a]

[a] Universidad del Cauca, Departamento de Matemáticas, Grupo de Investigación: Algebra, Teoría de Números y Aplicaciones, ERM, Cauca, Colombia.

Resumen. Un conjunto $\mathcal{A}$ de enteros positivos se llama un *conjunto* B_h, si todas las sumas de h elementos de $\mathcal{A}$ son diferentes. En este artículo usamos propiedades básicas del análisis de Fourier sobre $\mathbb{Z}_N$ y seguimos el estilo de Ben Green [4] para deducir, con un método diferente, las cotas superiores obtenidas por Jia [6], Chen [2] y Graham [5] respecto al máximo cardinal que puede tener un conjunto B_h contenido en los primeros N enteros positivos.
Palabras claves: Conjuntos de Sidon, conjuntos B_h.
MSC2000: Primaria: 11B50. Secundaria: 11B75, 05B10.

Fourier Analysis on $\mathbb{Z}_N$ and B_h sets

Abstract. A set $\mathcal{A}$ of positive integers is called a B_h set, if all sums of h elements of $\mathcal{A}$ are different. In this paper we use basic properties of Fourier analysis on $\mathbb{Z}_N$ and follow the style of Ben Green [4] to conclude with a different method, the upper bounds obtained by Jia [6], Chen [2] and Graham [5] with respect to the maximum cardinal that can have a B_h set contained in the first N positive integers.
Keywords: Sidon sets, B_h sets.

1. Introducción

Un conjunto $\mathcal{A}$ de enteros positivos se llama un *conjunto* B_h, si todas las sumas de la forma

$$a_1 + a_2 + \cdots + a_h, \quad a_1, a_2, \ldots, a_h \in \mathcal{A}, \quad a_1 \leq a_2 \leq \cdots \leq a_h, \tag{1}$$

son distintas. Los conjuntos B_2 también son conocidos como conjuntos de Sidon, en honor a Simon Sidon, el analista húngaro, quien en 1932 le pregunta a Erdös sobre conjuntos de enteros positivos con todas las sumas de dos elementos distintas.

* Autor para correspondencia: *E-mail*: jbravo@unicauca.edu.co.
Recibido: 12 de mayo de 2010, Aceptado: 17 de noviembre de 2010.

El problema fundamental en el estudio de conjuntos B_h finitos consiste en investigar el máximo cardinal que puede tener un conjunto B_h seleccionado de $[1, N] := \{1, 2, \ldots, N\}$. El paso natural a seguir es estudiar el comportamiento asintótico de la función

$$F_h(N) := \max\big\{|\mathcal{A}| : \mathcal{A} \subseteq [1, N],\ \mathcal{A} \text{ es un conjunto } B_h\big\}, \tag{2}$$

donde $|\mathcal{A}|$ denota el cardinal del conjunto finito $\mathcal{A}$.

Respecto a $F_h(N)$ es bien conocida la *cota superior trivial*

$$F_h(N) \leq (hh!)^{1/h} N^{1/h}. \tag{3}$$

En el caso de los conjuntos de Sidon, los teoremas de Erdös–Turán [3] y Singer [8] demuestran que

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

resultado que constituye la cota asintótica correcta para $F_2(N)$, $F_2(N) \sim N^{1/2}$, $N \to \infty$.

La situación para otros valores de h es bien diferente: de hecho, la asintótica correcta para $F_h(N)$ no se ha obtenido en algún otro caso distinto al de $h = 2$. Mas aún, un problema que aún sigue abierto es decidir si

$$\lim_{N\to\infty} \frac{F_h(N)}{\sqrt[h]{N}},$$

existe, y si existe, determinar su valor. Se conjetura que $F_h(N) \sim N^{1/h}$, $N \to \infty$ para todo $h \geq 2$.

La cota (3) muestra que $F_h(N)$ tiene orden de magnitud $N^{1/h}$, razón por la cual se define

$$\alpha(h) := \limsup_{N\to\infty} \frac{F_h(N)}{N^{1/h}}, \quad \text{para todo } h \geq 2. \tag{4}$$

Los resultados de Erdös y Turán que implican $\alpha(2) = 1$ tienen una generalización natural que proporcionan cotas superiores no triviales para $\alpha(h)$. El primer resultado en este sentido fue obtenido por Lindström [7] en 1969. Él prueba que

$$\alpha(4) \leq 8^{1/4}.$$

Jia [6], Chen [2] y Graham [5] generalizan esta técnica y obtienen las cotas que da el siguiente teorema.

Teorema 1.1.

$$\alpha(2k) \leq \big(k(k!)^2\big)^{1/2k} \qquad y \qquad \alpha(2k-1) \leq (k!)^{2/(2k-1)}.$$

En este artículo se usa la relación existente entre el análisis de Fourier sobre $\mathbb{Z}_N$ y los conjuntos B_h para deducir, con un método diferente, las cotas superiores del Teorema 1.1.

2. *Análisis de Fourier sobre* $\mathbb{Z}_N$

En esta sección se exhiben definiciones y resultados básicos del análisis de Fourier sobre $\mathbb{Z}_N$, los cuales son prerrequisitos para lo siguiente. Es de anotar que los resultados de esta sección se presentan sin demostración. El lector interesado en consultar estas pruebas puede encontrarlas en [9].

El espacio vectorial V de todas las funciones de valor complejo $f : \mathbb{Z}_N \to \mathbb{C}$ puede ser identificado con el espacio euclidiano $N-$dimensional complejo $\mathbb{C}^N$, asignando a cada función f el vector $v_f = (f(0), f(1), \ldots, f(N-1))$. En otras palabras, V y $\mathbb{C}^N$ son espacios isomorfos. V se dota de un producto interno, el hermitiano. En efecto, si $f, g \in V$, se define

$$\langle f, g\rangle = \sum_{x \in \mathbb{Z}_N} f(x)\overline{g(x)},$$

donde $\overline{z}$ indica el complejo conjugado de z. Este producto interno induce a su vez una l^2–norma,

$$\|f\| = \langle f, f\rangle^{1/2}.$$

Para $1 \leq j \leq N$, considere las funciones $e_j : \mathbb{Z}_N \to \mathbb{C}$ definidas por $e_j(k) = w^{-jk}$, donde $w = e^{2\pi i/N}$. Estas funciones se llaman *los caracteres del grupo* $\mathbb{Z}_N$ y forman un conjunto ortogonal del espacio V. Precisamente se tiene

$$\langle e_j, e_k\rangle = \begin{cases} N & \text{si} j = k, \\ 0 & \text{si} j \neq k. \end{cases}$$

Observación 2.1. Nótese que los caracteres del grupo $\mathbb{Z}_N$ son linealmente independientes por ser un conjunto ortogonal, y en consecuencia forman una base para el espacio V, ya que este espacio tiene dimensión N.

Definición 2.2. La **transformada de Fourier discreta** $\hat{f}$, de una función $f \in V$, se define por

$$\hat{f}(r) = \langle f, e_r\rangle = \sum_{x \in \mathbb{Z}_N} f(x)w^{rx}, \quad \text{donde} \quad w = e^{2\pi i/N}.$$

De fundamental importancia son las siguientes propiedades.

Propiedad 2.3. *Si $f, g \in V$, entonces se tiene:*

(*a*) ***Fórmula de Parseval**:*

$$\sum_{x \in \mathbb{Z}_N} f(x)\overline{g(x)} = \frac{1}{N} \sum_{r \in \mathbb{Z}_N} \hat{f}(r)\overline{\hat{g}(r)}.$$

(*b*) ***Fórmula de Plancherel:***

$$\sum_{x \in \mathbb{Z}_N} |f(x)|^2 = \frac{1}{N} \sum_{r \in \mathbb{Z}_N} |\hat{f}(r)|^2.$$

Definición 2.4. Sean $f, g : G \to \mathbb{C}$ funciones sobre un grupo abeliano G. La convolución de f y g, denotada $f * g$, se define por

$$(f * g)(x) = \sum_{y \in G} f(y)\overline{g(y-x)}.$$

Existe una relación entre la transformada de Fourier y la convolución, propiedad que se presenta a continuación.

Propiedad 2.5. *Para $f, g \in V$, se tiene que*

$$\widehat{(f * g)}(r) = \hat{f}(r)\overline{\hat{g}(r)}.$$

Observación 2.6. Nótese que la operación de convolución que se ha definido no es asociativa. Hay situaciones donde es muy tedioso indicar la intensión de la operación por medio de paréntesis, razón por la cual, en este artículo se adopta la siguiente convención:

$$f_1 * f_2 * \cdots * f_k = \Big(f_1 * \cdots * \big(f_{k-2} * (f_{k-1} * f_k)\big)\Big),$$

donde las f_i son funciones definidas sobre un grupo abeliano G. En particular, si $f \in V$, entonces

$$f * f * f = f * (f * f).$$

Notación. Si $f : G \longrightarrow \mathbb{R}$ es una función sobre un grupo abeliano G, se escribe f^{*k} para indicar k–veces la convolución de f con ella misma, esto es

$$f^{*k} = \underbrace{f * f * \cdots * f}_{k-veces}.$$

Ejemplo 2.7. Sean $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}$. En lo que sigue del artículo siempre se identifica un conjunto con su función característica. Así por ejemplo, $\mathcal{A}(x)$ está definida por

$$\mathcal{A}(x) = \begin{cases} 1 & \text{si } x \in \mathcal{A}, \\ 0 & \text{si } x \notin \mathcal{A}. \end{cases}$$

Ahora bien, teniendo en cuenta la Definición 2.4, se tiene que

$$(\mathcal{A} * \mathcal{B})(x) = \sum_{y \in \mathbb{Z}} \mathcal{A}(y)\mathcal{B}(y-x).$$

Nótese que los sumandos de la última expresión toman valores diferentes de cero, solamente si $\mathcal{A}(y) = 1$ y $\mathcal{B}(y-x) = 1$, es decir, si existen elementos $a \in \mathcal{A}$ y $b \in \mathcal{B}$ tales que $y = a$ y $y - x = b$, esto es, si existe $(a, b) \in \mathcal{A} \times \mathcal{B}$ tal que $x = a - b$. En otras palabras, $(\mathcal{A} * \mathcal{B})(x)$ está contando el número de parejas $(a, b) \in \mathcal{A} \times \mathcal{B}$ tales que $x = a - b$. En particular, $(\mathcal{A} * \mathcal{A})(x)$ cuenta el número de soluciones de la ecuación $x = a - a'$, con $a, a' \in \mathcal{A}$. Claramente $(\mathcal{A} * \mathcal{A})(0) = |\mathcal{A}|$.

Como $a + b = c + d \iff a - d = c - b$, los conjuntos de Sidon también se definen como aquellos que tienen la propiedad de que todas las diferencias no nulas de elementos del conjunto son distintas. De esta manera, $\mathcal{A}$ es un conjunto de Sidon si, y sólo si, $(\mathcal{A} * \mathcal{A})(x) \leq 1$ para todo entero $x \neq 0$.

Con un análisis similar al anterior y teniendo en cuenta la Observación 2.6, se puede ver que $A^{*3}(x)$ cuenta las soluciones de la ecuación, $x = a_1 - a_2 + a_3,\ a_1, a_2, a_3 \in A$.

3. Demostración del Teorema 1.1

Para la prueba del Teorema 1.1, necesitamos los siguientes lemas auxiliares.

Lema 3.1. *Sean $h = 2k$ un entero positivo par y $\mathcal{A} \subseteq [1, N]$ un conjunto B_h. Entonces, para todo $x \in \mathbb{Z}$, se tiene*

$$\mathcal{A}^{*2k}(x) \leq (k!)^2 + k^2 |\mathcal{A}| \mathcal{A}^{*(2k-2)}(x).$$

Demostración. Para $x \in \mathbb{Z}$ fijo, $\mathcal{A}^{*2k}(x)$ cuenta las soluciones de la ecuación

$$x = a_1 + \cdots + a_k - b_1 - \cdots - b_k, \quad a_i, b_i \in \mathcal{A}, \quad i, j = 1, \ldots, k. \tag{5}$$

Si la ecuación anterior no tiene solución, el resultado es claro. Demostremos que si (5) tiene una solución $(a_1, \ldots, a_k, b_1, \ldots, b_k) \in \mathcal{A}^h$ en la cual $a_i \neq b_j$ para todo i y todo j, entonces (5) tiene a lo mas $(k!)^2$ soluciones. En efecto, sea $(a_1, \ldots, a_k, b_1, \ldots, b_k)$ una solución con tal característica, y supóngase que $(a'_1, \ldots, a'_k, b'_1, \ldots, b'_k)$ también satisface (5); entonces

$$x = a_1 + \cdots + a_k - b_1 - \cdots - b_k = a'_1 + \cdots + a'_k - b'_1 - \cdots - b'_k,$$

de ahí que

$$a_1 + \cdots + a_k + b'_1 + \cdots + b'_k = a'_1 + \cdots + a'_k + b_1 + \cdots + b_k.$$

Como $\mathcal{A}$ es un conjunto B_h, se deduce que

$$\{a_1, \ldots, a_k, b'_1, \ldots, b'_k\} = \{a'_1, \ldots, a'_k, b_1, \ldots, b_k\}.$$

De la condición de que $a_i \neq b_j$ para todo i y todo j, se desprende que

$$\{a'_1, \ldots, a'_k\} = \{a_1, \ldots, a_k\} \qquad y \qquad \{b'_1, \ldots, b'_k\} = \{b_1, \ldots, b_k\},$$

situación que presenta $(k!)^2$ posibilidades. Así, si (5) tiene una solución en la forma antes mencionada, entonces tendrá a lo más $(k!)^2$ soluciones.

Por otro lado, si (5) no tiene una solución en la forma antes descrita, entonces cualquier solución debe cumplir que $a_i = b_j$ para algún i y algún j. Es claro que para cada una de estas k^2 posibilidades (5) tiene $|\mathcal{A}|\mathcal{A}^{*(2k-2)}(x)$ soluciones. En consecuencia,

$$\mathcal{A}^{*2k}(x) \leq (k!)^2 + k^2|\mathcal{A}|\mathcal{A}^{*(2k-2)}(x).$$

☑

Lema 3.2. *Sean $h = 2k-1$ un entero positivo impar y $\mathcal{A} \subseteq [1, N]$ un conjunto B_h. Entonces, para todo $x \in \mathbb{Z}$ se tiene*

$$\mathcal{A}^{*2k}(x) \leq |\mathcal{A}|\big(k!(k-1)! + k(k-1)\mathcal{A}^{*(2k-2)}(x)\big).$$

Demostración. Para $x \in \mathbb{Z}$ fijo, $\mathcal{A}^{*(2k-1)}(x)$ cuenta las soluciones de la ecuación

$$x = a_1 + \cdots + a_k - b_1 - \cdots - b_{k-1}, \quad a_i, b_i \in \mathcal{A}. \tag{6}$$

Si la ecuación anterior no tiene solución, el resultado es inmediato. Argumentando como antes, sea $(a_1, \ldots, a_k, b_1, \ldots, b_{k-1}) \in \mathcal{A}^h$ una solución de (6) en la cual $a_i \neq b_j$, $i = 1, \ldots, k$, $j = 1, \ldots, k-1$. Supóngase que $(a'_1, \ldots, a'_k, b'_1, \ldots, b'_{k-1})$ es otra solución de (6). Entonces

$$x = a_1 + \cdots + a_k - b_1 - \cdots - b_{k-1} = a'_1 + \cdots + a'_k - b'_1 - \cdots - b'_{k-1},$$

de ahí que

$$a_1 + \cdots + a_k + b'_1 + \cdots + b'_{k-1} = a'_1 + \cdots + a'_k + b_1 + \cdots + b_{k-1}.$$

Como $\mathcal{A}$ es un conjunto B_h, se deduce que

$$\{a_1, \ldots, a_k, b'_1, \ldots, b'_{k-1}\} = \{a'_1, \ldots, a'_k, b_1, \ldots, b_{k-1}\}.$$

Ahora, dado que $a_i \neq b_j$ para $i = 1, \ldots, k$, $j = 1, \ldots, k-1$, se sigue que

$$\{a'_1, \ldots, a'_k\} = \{a_1, \ldots, a_k\} \qquad y \qquad \{b'_1, \ldots, b'_{k-1}\} = \{b_1, \ldots, b_{k-1}\},$$

situación que presenta $(k-1)!\,k!$ posibilidades. En conclusión, si (6) tiene una solución $(a_1, \ldots, a_k, b_1, \ldots, b_{k-1}) \in \mathcal{A}^h$ en la cual $a_i \neq b_j$, $i = 1, \ldots, k$, $j = 1, \ldots, k-1$, entonces (6) tendrá a lo más $(k-1)!\,k!$ soluciones.

Por otro lado, si (6) no tiene una solución en la forma antes descrita, entonces cualquier solución debe cumplir que $a_i = b_j$, para algún $1 \leq i \leq k$ y algún $1 \leq j \leq k-1$. Para cada una de estas $k\,(k-1)$ posibilidades (6) tiene $|\mathcal{A}|\mathcal{A}^{*(2k-3)}(x)$ soluciones. En consecuencia,

$$\mathcal{A}^{*(2k-1)}(x) \leq k!(k-1)! + k(k-1)|\mathcal{A}|\mathcal{A}^{*(2k-3)}(x).$$

De lo anterior y por definición de convolución se tiene que

$$\begin{aligned}\mathcal{A}^{*2k}(x) = (\mathcal{A} * \mathcal{A}^{*(2k-1)}(x)) &= \sum_y \mathcal{A}(y)\mathcal{A}^{*(2k-1)}(y-x) \\ &\leq \sum_y \mathcal{A}(y)\big(k!(k-1)! + k(k-1)|\mathcal{A}|\mathcal{A}^{*(2k-3)}(y-x)\big) \\ &= k!(k-1)!|\mathcal{A}| + k(k-1)|\mathcal{A}|\mathcal{A}^{*(2k-2)}(x). \qquad \boxtimes\end{aligned}$$

Antes de presentar los detalles de la prueba del Teorema 1.1, considérese el siguiente ejemplo.

Ejemplo 3.3. Sea $\mathcal{A} = \{1, 2, 3, 4, 5, 8\}$. En la Tabla 1 se presentan las sumas $(a+a', a \leq a')$ de los elementos del conjunto $\mathcal{A}$.

Tabla 1. Sumas

+	1	2	3	4	5	8
1	2	3	4	5	6	9
2		4	5	6	7	10
3			6	7	8	11
4				8	9	12
5					10	13
8						16

Tabla 2. Versión modular

+	1	2	3	4	5	8
1	2	3	4	5	**6**	9
2		4	5	**6**	7	0
3			**6**	7	8	1
4				8	9	2
5					0	3
8						**6**

Observe que $\mathcal{A}$ es un conjunto B_3. Ahora considere al conjunto $\mathcal{A}$ como subconjunto de $\mathbb{Z}_{10}$ en la forma natural. En este orden de ideas, la Tabla 1 se convierte en la Tabla 2. Nótese que en la nueva versión $\mathcal{A}$ no es un conjunto B_3: de hecho, $\mathcal{A}$ es ahora un conjunto B_4, pues el elemento 6 se repite 4 veces, razón por la cual no hay garantía de que se verifique el Lema 3.2.

En general, en la versión modular de $\mathcal{A}^{*h}$, es decir, considerando al conjunto $\mathcal{A}$ como subconjunto de $\mathbb{Z}_N$ para algún entero positivo N, ya no se verifican los Lemas 3.1 y 3.2, que, sin embargo, son válidos para algunos valores apropiados del entero x, tal como se revela en la siguiente prueba.

Demostración del Teorema 1.1. Sea $\mathcal{A}$ un conjunto B_h, con $h = 2k$ ó $h = 2k-1$, y considérese al conjunto $\mathcal{A}$ como subconjunto de $\mathbb{Z}_{kN+v}$, donde v es un entero positivo

que se escoge posteriormente. En esta prueba se toman como representantes del grupo $\mathbb{Z}_{kN+v}$ los siguientes:

$$\mathbb{Z}_{kN+v} = \{-v, -v+1, \ldots, -1, 0, 1, \ldots, v, v+1, \ldots, kN-1\}.$$

Afirmación. Si $|x| \leq v$, entonces la versión modular de $\mathcal{A}^{*h}$ satisface la cota del Lema 3.1 en el caso $h = 2k$, y la cota del Lema 3.2 en el caso $h = 2k-1$. Por ejemplo, si $h = 2k$, se tiene

$$\mathcal{A}^{*2k}(x) \leq (k!)^2 + k^2|\mathcal{A}|\mathcal{A}^{*(2k-2)}(x), \quad \text{para} \quad |x| \leq v. \tag{7}$$

En efecto, si $(a'_1, \ldots, a'_k, b'_1, \ldots, b'_k)$ es una nueva solución de (5) en la versión modular, entonces $a'_1 + \cdots + a'_k - b'_1 - \cdots - b'_k < -v$ y

$$kN + v + a'_1 + \cdots + a'_k - b'_1 - \cdots - b'_k = x \leq v.$$

Luego

$$kN \leq (b'_1 + \cdots + b'_k) - (a'_1 + \cdots + a'_k),$$

lo cual no es posible pues

$$1 \leq (b'_1 + \cdots + b'_k) - (a'_1 + \cdots + a'_k) < kN.$$

En consecuencia, para $|x| \leq v$, el número de soluciones de (5) en la versión modular, coincide con el número de soluciones en la versión sobre $\mathbb{Z}$. Análogamente se procede en el caso $h = 2k-1$.

Sea $I = \{1, 2, \ldots, u\}$, donde $u \leq v$ es un entero positivo que se propone mas adelante. En lo que sigue, el símbolo sombrero ($\hat{}$) se refiere a la transformada de Fourier sobre $\mathbb{Z}_{kN+v}$.

Definamos E mediante la expresión

$$E = \sum_{x \in \mathbb{Z}_{kN+v}} \mathcal{A}^{*2k}(x)(I * I)(x). \tag{8}$$

De la fórmula de Parseval y la Propiedad 2.5 se tiene

$$\begin{aligned} E &= \frac{1}{kN+v} \sum_{r \in \mathbb{Z}_{kN+v}} \widehat{\mathcal{A}^{*2k}}(r)\overline{\widehat{(I*I)}(r)} \\ &= \frac{1}{kN+v} \sum_{r \in \mathbb{Z}_{kN+v}} |\hat{\mathcal{A}}(r)|^{2k}|\hat{I}(r)|^2. \end{aligned} \tag{9}$$

Por otro lado,

$$\begin{aligned} \sum_{x \in \mathbb{Z}_{kN+v}} (I*I)(x) &= \sum_{-u \leq x \leq u} (I*I)(x) = (I*I)(0) + 2\sum_{1 \leq x \leq u} (I*I)(x) \\ &= u + 2\big((u-1) + (u-2) + \cdots + 1\big) = u + 2\frac{u(u-1)}{2} = u^2. \end{aligned} \tag{10}$$

Adicionalmente, al realizar las diferencias del conjunto I resultan números comprendidos entre $1-u$ y $u-1$, cantidades que al modularlas permanecen igual. Lo cierto es que si $v+1 \leq x \leq kN-1$, entonces la congruencia $x \equiv a - a'$ (mód $kN+v$), con $1 \leq a, a' \leq u$, no tiene solución. En otras palabras, si $v+1 \leq x \leq kN-1$, se tiene que $(I*I)(x) = 0$.

Para el caso $h = 2k$ se usa lo anterior y el Lema 3.1 en la expresión que define a E para obtener

$$\begin{aligned} E &= \sum_{|x| \leq v} \mathcal{A}^{*2k}(x)(I*I)(x) \\ &\leq \sum_{x \in \mathbb{Z}_{kN+v}} \big((k!)^2 + k^2|\mathcal{A}|\mathcal{A}^{*(2k-2)}(x)\big)(I*I)(x) \\ &= (k!)^2u^2 + k^2|\mathcal{A}| \sum_{x \in \mathbb{Z}_{kN+v}} \mathcal{A}^{*(2k-2)}(x)(I*I)(x) \\ &= (k!)^2u^2 + \frac{k^2|\mathcal{A}|}{kN+v} \sum_{r \in \mathbb{Z}_{kN+v}} |\hat{\mathcal{A}}(r)|^{2k-2}|\hat{I}(r)|^2 \\ &\leq (k!)^2u^2 + \frac{k^2|\mathcal{A}|}{kN+v}|\mathcal{A}|^{2k-2} \sum_{r \in \mathbb{Z}_{kN+v}} |\hat{I}(r)|^2 \end{aligned} \tag{11}$$

De la fórmula de Plancherel también se encuentra

$$u = \sum_{x \in \mathbb{Z}_{kN+v}} I(x) = \sum_{x \in \mathbb{Z}_{kN+v}} I^2(x) = \sum_{x \in \mathbb{Z}_{kN+v}} |I(x)|^2 = \frac{1}{kN+v} \sum_{r \in \mathbb{Z}_{kN+v}} |\hat{I}(r)|^2,$$

de donde

$$\sum_{r \in \mathbb{Z}_{kN+v}} |\hat{I}(r)|^2 = (kN+v)u.$$

Del cálculo anterior y de (11) se obtiene

$$\begin{aligned} E &\leq (k!)^2u^2 + \frac{k^2}{kN+v}|\mathcal{A}|^{2k-1}(kN+v)u \\ &\leq (k!)^2u^2 + \frac{k^2(k+1)\big((2k)(2k)!\big)^{1-1/2k}N^{2-1/2k}u}{kN+v} \\ &\leq (k!)^2u^2 + \frac{(2k+4)!N^{2-1/2k}u}{kN+v}, \end{aligned} \tag{12}$$

donde se ha usado el hecho de que $kN+v \leq (k+1)N$ y $|\mathcal{A}| \leq \big((2k)(2k)!\big)^{1/2k}N^{1/2k}$ (cota trivial (3) con $h = 2k$).

Combinando las expresiones (9) y (12) resulta

$$k(k!)^2Nu^2 + (2k+4)!(N^{2-1/2k}u + u^2v) \geq \sum_{r \in \mathbb{Z}_{kN+v}} |\hat{\mathcal{A}}(r)|^{2k}|\hat{I}(r)|^2. \tag{13}$$

Además, trivialmente se tiene que

$$\sum_{r\,\in\,\mathbb{Z}_{kN+v}} |\hat{\mathcal{A}}(r)|^4|\hat{I}(r)|^2 \geq |\hat{\mathcal{A}}(0)|^4|\hat{I}(0)|^2 = |\mathcal{A}|^4u^2.$$

Usando lo anterior en el lado derecho de (13), se encuentra la desigualdad

$$k(k!)^2Nu^2 + (2k+4)!(N^{2-1/2k}u + u^2v) \geq |\mathcal{A}|^{2k}u^2,$$

de ahí que

$$|\mathcal{A}|^{2k} \leq k(k!)^2N + (2k+4)!\left(\frac{N^{2-1/2k}}{u} + v\right). \tag{14}$$

Sean[*] $u = v = \lfloor N^{1-1/4k}\rfloor + 1$. Con estas elecciones de u y v, de (14) se concluye[**] que

$$|\mathcal{A}|^{2k} \leq k(k!)^2N(1+o(1));$$

en consecuencia,

$$\left(\frac{F_{2k}(N)}{N^{1/2k}}\right)^{2k} \leq k(k!)^2(1+o(1)),$$

de donde se deduce la cota de Jia [6]

$$\alpha(2k) \leq \left(k(k!)^2\right)^{1/2k}.$$

En el caso $h = 2k-1$ se usa el Lema 3.2, y se argumenta en forma similar a lo anterior para obtener

$$(k!)^2u^2|\mathcal{A}|N + (2k+4)!|\mathcal{A}|(N^{2-1/(2k-1)}u + u^2v) \geq \sum_{r\,\in\,\mathbb{Z}_{kN+v}} |\hat{\mathcal{A}}(r)|^{2k}|\hat{I}(r)|^2. \tag{15}$$

Esto implica que

$$(k!)^2u^2|\mathcal{A}|N + (2k+4)!|\mathcal{A}|(N^{2-1/(2k-1)}u + u^2v) \geq |\mathcal{A}|^{2k}u^2,$$

luego

$$|\mathcal{A}|^{2k-1} \leq (k!)^2N + (2k+4)!\left(\frac{N^{2-1/(2k-1)}}{u} + v\right).$$

Con $u = v = \lfloor N^{1-1/(4k-2)}\rfloor + 1$, de la última expresión se deduce

$$|\mathcal{A}|^{2k-1} \leq (k!)^2N(1+o(1));$$

[*] Si $x \in \mathbb{Z}$, entonces la parte entera de x, notada $\lfloor x\rfloor$, se define por, $\lfloor x\rfloor := \text{máx}\{n \in \mathbb{Z} : n \leq x\}$.

[**] En este trabajo se usa la notación "*o–pequeña*" para indicar cantidades que varían con N, así que, por ejemplo, $X = o(1)$ significa que $X \to 0$ cuando $N \to \infty$.

por lo tanto,

$$\left(\frac{F_{2k-1}(N)}{N^{1/(2k-1)}}\right)^{2k-1} \leq (k!)^2(1+o(1)),$$

de donde se deduce la cota de Chen [2]–Graham [5],

$$\alpha(2k-1) \leq (k!)^{2/(2k-1)}. \qquad \boxtimes$$

4. Comentarios finales

En este trabajo se usan propiedades básicas del análisis de Fourier sobre $\mathbb{Z}_N$ y se generaliza el argumento de los conjuntos B_4 usado por Ben Green en [4], para deducir en forma alternativa las cotas superiores del Teorema 1.1. Es de anotar que estos resultados fueron obtenidos independientemente por Jia [6], Chen [2] y Graham [5].

Ben Green en [4] presenta una avance importante en el estudio de la función $\alpha(h)$ para h suficientemente grande, y exhibe una técnica muy sofisticada con la que mejora las cotas del Teorema 1.1. Específicamente Greeen prueba que

$$\alpha(2k) \leq \Big(\pi^{1/2}k^{1/2}(k!)^2\big(1+\varepsilon(k)\big)\Big)^{1/2k}$$

y

$$\alpha(2k-1) \leq \Big(\pi^{1/2}k^{-1/2}(k!)^2\big(1+\varepsilon(k)\big)\Big)^{1/(2k-1)},$$

donde $\varepsilon(k)$ es una función que no es calculada explícitamente y tiende a 0 cuando $k \to \infty$.

Además, Ben Green en [4] hace un estudio especial de los conjuntos B_3 y B_4. En este caso prueba que

$$\alpha(3) \leq \left(\frac{7}{2}\right)^{1/3} \quad \text{y} \quad \alpha(4) \leq 7^{1/4},$$

las cuales constituyen las mejores cotas superiores conocidas hasta el momento.

Agradecimientos

Los autores expresan su agradecimiento a la Universidad del Cauca, por el apoyo ofrecido al grupo de investigación: Álgebra, Teoría de Números y Aplicaciones ERM, en la realización de este trabajo.

Referencias

[1] Bravo J., "Análisis de Fourier Finito y Conjuntos $B_h[g]$", Trabajo de grado, Maestría en Ciencias-Matemáticas, Universidad del Valle, 2006.

[2] Chen S., On the Size of Finite Sidon Sequences, *Proc. Amer. Math. Soc*, 121 (1994), 353–356.

[3] Erdös P. and Turán P., On a Problem of Sidon in Additive Number Theory and On Some Related Problems, *Journal of the London Mathematical Society*, 16 (1941), 212–215.

[4] Green B., The number of squares and $B_h[g]$ sets, *Acta Arithmética*, 100 (2001), 365–390.

[5] Graham S. W., B_h Sequences, *Analytic Number Theory*, 1 (Allerton Park, IL, 1995), 431–449, Progress in Mathematics 138, Birkhäuser, Boston MA, 1996.

[6] Jia X., On B_{2k} Sequences, *Journal of Number Theory*, 48 (1994), 183–196.

[7] Lindström B., A Remark on B_4 Sequences, *Journal of Combinatorial Theory*, 7 (1969), 276–277.

[8] Singer J., A Theorem in Finite Projective Geometry and Some Applications to Number Theory, *Transactions of the American Mathematical Society*, 43 (1938), 377–385.

[9] Terras A., "Fourier Analysis on Finite Groups and Aplications," Cambridge University Press, second edition, San Francisco, 1999.