Vol. 12 (núm. 2) pp. 73-81
Julio-Diciembre 2021

Ciencia en Desarrollo
Revista de la Facultad de Ciencias
Vicerrectoría en Investigación y Extensión - VIE
Centro de Investigaciones y Extensión de la Facultad de Ciencias - CIEC

https://doi.org/10.19053/01217488.v12.n2.2021.12732

Construcción de conjuntos B_h en varias dimensiones

Constructions of B_h Sets in Various Dimensions

Yadira Caicedo[1], Carlos A. Martos O.[2] y Carlos A. Trujillo S.[3]

Resumen

Un conjunto B_h es un subconjunto A de números enteros con la propiedad que todas las sumas de h elementos son distintas, salvo permutaciones de los sumandos. El problema fundamental consiste en determinar el máximo cardinal de un conjunto B_h contenido en el intervalo entero $[1,n] := \{1,2,3,\ldots,n\}$. Se conocen pocas construcciones de conjuntos B_h enteros, entre ellas se tienen la de Singer [13], Bose-Chowla [3] y Gómez-Trujillo [7].

El concepto de conjunto B_h se puede extender a grupos arbitrarios. En este articulo se presentan las construcciones generalizadas a los grupos que provienen de un cuerpo y se obtiene una nueva construcción de un conjunto B_{h+s} en $h+1$ dimensiones.

***Palabras clave*:** Conjunto B_h, Conjunto B_2, Extensión de cuerpo

Abstract

Let $A \subset \mathbb{Z}^+$ and h be positive integer. We say that A is a B_h set if any integer n can be written in at most one-ways as the sum of h elements of A, The fundamental problem is to determine the cardinal maximum of a set B_h contained in the integer interval $[1,n] := \{1,2,3,\ldots,n\}$. Not many constructions of integer sets B_h are known, among them are Singer [13], Bose-Chowla [3] and Gómez-Trujillo [7]. The B_h set concept can be extended to arbitrary groups. In this article, the generalized constructions on the groups that come from a field are presented and new construction of a set B_{h+s} in $h+1$ dimensions is obtained.

***Keywords*:** B_h Set, B_2 Set, Field extension

Recepción: 05-may-2021
Aceptación: 20-jun-2021

[1]Universidad del Tolima. Correo electrónico: nycaicedob@ut.edu.co
[2]Universidad del Cauca. Correo electrónico: cmartos@unicauca.edu.co
[3]Universidad del Cauca. Correo electrónico: trujillo@unicauca.edu.co

1 Introducción

El estudio de conjuntos de enteros con la propiedad que todas las sumas de dos elementos sean distintas, inicia con Simon Sidon en el año de 1932, cuando quiere determinar el máximo cardinal de un conjunto con esta propiedad contenido en los primeros n enteros positivos; a estos conjuntos se les conoce hoy en día con el nombre de conjuntos Sidon o conjuntos B_2. Aunque estos conjuntos aparecen en los números enteros, el concepto es fácil de extender a cualquier grupo abeliano. También es posible considerar sumas de más de dos elementos para obtener los denominados conjuntos B_h (Conjuntos Sidon de orden h).

En 1938, James Singer [13] en su estudio sobre geometría proyectiva finita, demostró el siguiente resultado relacionado con los conjuntos B_2.

Teorema 1.1. *Si q es una potencia de un primo, entonces existen $q+1$ enteros $a_1, a_2, \ldots, a_{q+1}$ tales que las q^2+q diferencias $a_i - a_j$, distintas de cero representan todos los residuos no cero módulo q^2+q+1.*

Bose [2] probó un análogo del Teorema de Singer, en 1942.

Teorema 1.2. *Si q es una potencia de un primo, entonces existen q enteros $a_1, a_2, \ldots, a_q$ tales que las $q(q-1)$ diferencias $a_i - a_j$, distintas de cero representan todos aquellos residuos no cero módulo q^2-1 que no son múltiplos de $q+1$.*

Como en el anillo de enteros módulo n tener diferencias no cero distintas es equivalente a tener sumas diferentes, los teoremas de Singer y Bose [13, 2] se pueden enunciar en términos de sumas; es decir, se tienen las siguientes consecuencias.

Corolario 1.3. *Si q es una potencia de un primo, entonces existen $q+1$ enteros $a_1, a_2, \ldots, a_{q+1}$ tales que todas las sumas $a_i + a_j$, $1 \leq i \leq j \leq q+1$, son distintas módulo q^2+q+1.*

Corolario 1.4. *Si q es una potencia de un primo, entonces existen q enteros $a_1, a_2, \ldots, a_q$ tales que todas las sumas $a_i + a_j$, $1 \leq i \leq j \leq q$, son distintas módulo q^2-1.*

Más tarde en 1961, Bose y Chowla [3] generalizan los resultados anteriores para sumas de h elementos para todo entero $h \geq 2$.

Teorema 1.5. *Si q es una potencia de un primo y $h \geq 2$ un entero, entonces existen $q+1$ enteros $a_1, a_2, \ldots, a_q, a_{q+1}$ tales que todas las sumas $a_{j_1} + a_{j_2} + \cdots + a_{j_h}$, con $1 \leq j_1 \leq j_2 \leq \cdots \leq j_h \leq q+1$, son distintas módulo $\frac{q^{h+1}-1}{q-1}$.*

Teorema 1.6. *Si q es una potencia de un primo y $h \geq 2$ un entero, entonces existen q enteros $a_1, a_2, \ldots, a_q$ tales que todas las sumas*

$$a_{j_1} + a_{j_2} + \cdots + a_{j_h},$$

con $1 \leq j_1 \leq j_2 \leq \cdots \leq j_h \leq q$, son distintas módulo $q^h - 1$.

El máximo número de elementos de un conjunto B_h contenido en los primeros n enteros positivos se denota mediante $F_h(n)$. De las construcciones mencionadas en los Teoremas 1.5, 1.6 y usando estimaciones de la diferencia entre primos consecutivos se puede deducir que

$$\liminf_{n \longrightarrow \infty} \frac{F_h(n)}{\sqrt[h]{n}} \geq 1,$$

y además Bose y Chowla conjeturan en [3] que

$$\lim_{n \longrightarrow \infty} \frac{F_h(n)}{\sqrt[h]{n}} = 1,$$

resultado que se conoce únicamente para $h = 2$, en [6]. Por otro lado, Jia [10] demostró que

$$F_{2r}(n) \leq (r \cdot r!^2 n)^{1/(2r)}(1 + o(1)),$$

donde o pequeña representa la notación de Landau. Para $h = 2r-1$ con $r \geq 1$, Chen [5], Bravo, Ruiz y Trujillo [1] y Graham [8] demostraron independientemente que

$$F_{2r-1}(n) \leq (r!^2 n)^{1/(2r-1)}(1 + o(1)).$$

En este artículo se estudian las construcciones conocidas de conjuntos B_h definidos sobre grupos finitos que provienen de un cuerpo y se obtiene una nueva construcción de un conjunto B_{h+s} en dimensión $h+1$.

2 Conjuntos B_h: conceptos y notación

En lo que sigue del documento G es un grupo abeliano notado aditivamente, A un subconjunto no vacío de G y $h \geq 2$ un entero. En esta sección se presenta la definición de conjunto B_h, en un grupo abeliano arbitrario, algunas de sus propiedades y problemas fundamentales.

Definición 2.1 ([14]). *Sean $(G,+)$ un grupo abeliano arbitrario, A un subconjunto no vacío de G y $h \leq 2$. A se dice un conjunto B_h en G si para todo $a_1,\ldots,a_h$, $a'_1,\ldots,a'_h \in A$ se tiene que:*

$$a_1+a_2+\cdots+a_h = a'_1+a'_2+\cdots+a'_h,$$

si y solo si $(a'_1,\ldots,a'_h)$ es una permutación de $(a_1,\ldots,a_h)$.

Es decir, un conjunto A es B_h en el grupo aditivo G si todas las sumas de h elementos son distintas.

Las siguientes propiedades de conjuntos B_h se deducen directamente de la definición anterior.

Lema 2.2. *Si G_1, G_2 son grupos abelianos y A un conjunto B_h en G_1, entonces*

- *A es un conjunto B_t en G_1, para todo entero t con $2 \leq t \leq h-1$.*
- *Si $\varphi : G_1 \to G_2$ es un monomorfismo de grupos, entonces $\varphi(A) = \{\varphi(a) : a \in A\}$ es un conjunto B_h en $\varphi(G_2)$.*

Definición 2.3. *Si A es un subconjunto de un grupo aditivo G y h un entero positivo, entonces la suma iterada hA es:*

$$hA := \{a_1+\cdots+a_h : a_1,\ldots,a_h \in A\}.$$

Si A es un conjunto finito con cardinal $|A|$, se tiene el siguiente resultado.

Lema 2.4. *A es un conjunto B_h si y solo si*

$$|hA| = \binom{|A|+h-1}{h}.$$

Uno de los problemas más importantes sobre los conjuntos B_h consiste en investigar el comportamiento asintótico de las siguientes funciones extremas.

Definición 2.5. *Sea f_h una función con dominio el conjunto de todos los grupos abelianos finitos y codominio el conjunto de enteros positivos, definida por*

$$f_h(G) := \max\{|A| : A \subseteq G, A \text{ es conjunto } B_h\},$$

para cada G grupo abeliano finito.

En particular si G es cíclico de orden n ($G \cong \mathbb{Z}_n$) se denota por $f_h(n)$ en lugar de $f_h(\mathbb{Z}_n)$.

Definición 2.6. *Sea $F_h : \mathbb{Z} \longrightarrow \mathbb{Z}^+$ una función definida por*

$$F_h(n) := \max\{|A| : A \subseteq [1,n], A \text{ es conjunto } B_h\},$$

para cada $n \in \mathbb{Z}$.

Si A es un conjunto B_h en un grupo finito G, entonces

$$\binom{|A|+h-1}{h} = |hA| \leq |G|.$$

Esto es,

$$|A| \leq \sqrt[h]{h!|G|},$$

de donde

$$\frac{f_h(G)}{|G|^{1/h}} \leq \sqrt[h]{h!}. \tag{1}$$

En el caso entero, si $A \subset [1,n]$ y A es un conjunto B_h en $\mathbb{Z}$, entonces aparece un factor h adicional puesto que $hA \subset [h,hn]$:

$$\frac{F_h(n)}{n^{1/h}} \leq \sqrt[h]{hh!}. \tag{2}$$

Para los mejores resultados conocidos sobre estas funciones ver [1, 9, 11].

Si $\mathbb{Z}_n$ se identifica con $[1,n]$ entonces no es difícil ver que todo conjunto B_h en $\mathbb{Z}_n$ se puede considerar como un conjunto B_h entero contenido en $[1,n]$. Similarmente, si A es un conjunto B_h en $\mathbb{Z}$ y $A \subset [1,n]$ entonces A se puede identificar con un conjunto B_h en $\mathbb{Z}_{hn}$. Por lo tanto

$$f_h(n) \leq F_h(n) \leq f_h(hn). \tag{3}$$

De las construcciones de Bose y Chowla [3] enunciadas en los Teoremas 1.5 y 1.6 se obtiene como consecuencia las siguientes desigualdades.

Corolario 2.7. *Si q es una potencia de un número primo, entonces*

- $F_h\left(\frac{q^{h+1}-1}{q-1}\right) \geq f_h\left(\frac{q^{h+1}-1}{q-1}\right) \geq q+1.$
- $F_h\left(q^h-1\right) \geq f_h\left(q^h-1\right) \geq q.$

3 Construcciones

En esta sección se presenta la construcción de Bose a partir de un cuerpo arbitrario y en particular se presenta la construcción de Singer generalizada.

Teorema 3.1. *Si $(F,+,\cdot)$ es un cuerpo, α un elemento algebraico sobre F de grado $h \geq 2$ y*

$$\alpha + F := \{\alpha + a : a \in F\},$$

la traslación de F mediante α, entonces $\alpha + F$ es un conjunto B_h en el grupo multiplicativo $F^*(\alpha)$.

Proof. Suponga que existen $a_{i_1},\ldots,a_{i_h},a'_{j_1},\ldots,a'_{j_h}$ en F tales que

$$\prod_{k=1}^{h}(\alpha + a_{i_k}) = \prod_{k=1}^{h}(\alpha + a'_{j_k}),$$

por factorización única y el hecho de que α es de grado h sobre F, esto es equivalente a que $\left(\alpha + a'_{i_1}, \alpha + a'_{i_2},\ldots,\alpha + a'_{i_h}\right)$ es una permutación de $(\alpha + a_{i_1}, \alpha + a_{i_2},\ldots,\alpha + a_{i_h})$.

□

Ejemplo 3.2.

- $\sqrt{2} + \mathbb{Q}$ *es un conjunto B_2 infinito en* $\left(\mathbb{Q}^*(\sqrt{2}),\cdot\right)$.
- $\pi + \mathbb{Q}$ *es un conjunto B_h en $(\mathbb{C}^*(\pi),\cdot)$, para todo h. En este sentido podría llamarse un conjunto B_∞.*

Observación 3.3. *Si F es un cuerpo finito con q elementos, $F = \mathbb{F}_q$, se tiene el isomorfismo $\left(\mathbb{F}^*_{q^h},\cdot\right) \cong \left(\mathbb{Z}_{q^h-1},+\right)$ mediante la función logaritmo discreto base θ, donde θ es una raíz primitiva de $\mathbb{F}_{q^h}$.*

Así:

- $\log_\theta\left(\alpha + \mathbb{F}_q\right)$ *es un conjunto B_h en* $\left(\mathbb{Z}_{q^h-1},+\right)$.
- *Si $\alpha = \theta$ se tiene la construcción de Bose y Chowla del Teorema 1.6.*

Ejemplo 3.4. *Sea $p = 7$, θ un elemento primitivo de $\mathbb{F}_{7^2}$ con polinomio minimal sobre $\mathbb{F}_7$, $min_{\mathbb{F}_7}(\theta) = x^2 + 4x + 5$ y sea $\alpha = \theta$.*

El conjunto

$$\begin{aligned}\theta + \mathbb{F}_7 &= \{\theta, \theta+1, \theta+2, \theta+3, \theta+4, \theta+5, \theta+6\},\\ &= \{\theta, \theta^{46}, \theta^{36}, \theta^{10}, \theta^{31}, \theta^{35}, \theta^{29}\},\end{aligned}$$

es un conjunto B_2 en el grupo multiplicativo $\mathbb{F}^*_{49}$. Usando el logaritmo discreto en la base θ, se tiene que el conjunto

$$A := \log_\theta\left(\theta + \mathbb{F}_7\right) = \{1, 10, 29, 31, 35, 36, 46\},$$

es un conjunto B_2 en el grupo aditivo $\mathbb{Z}_{48}$.

Ahora, se presenta la construcción del conjunto B_h tipo Singer generalizada. Aunque en principio la construcción de Singer apareció primero que la de Bose y Chowla, en esta versión se presenta la construcción de Singer como una consecuencia de la construcción de Bose y Chowla tomando como referencia el artículo [7].

Primero se construye un conjunto B_{h+1} en el grupo aditivo $\mathbb{Z}_{q^{h+1}-1}$ tipo Bose y Chowla con q elementos, luego este conjunto se reduce módulo $(q^h + q^{h-1} + \cdots + q + 1)$, el conjunto resultante es un conjunto B_h en el grupo aditivo $\mathbb{Z}_{q^h+q^{h-1}+\cdots+q+1}$ con q elementos, y por último se agrega el cero al último conjunto para así obtener un conjunto B_h tipo Singer generalizado con $q+1$ elementos en el grupo aditivo $\mathbb{Z}_{q^h+q^{h-1}+\cdots+q+1}$.

Teorema 3.5. *Si $q = p^n$, con p primo, $n \in \mathbb{N}$ y $h \geq 2$ entero, entonces existe un conjunto B_h, con $q+1$ elementos, en el grupo aditivo $\mathbb{Z}_{q^h+q^{h-1}+\cdots+q+1}$.*

Proof. Considere el cuerpo $\mathbb{F}_{q^{h+1}}$ con elemento primitivo θ y $\alpha \in \mathbb{F}^*_{q^{h+1}}$ un elemento de grado $h+1$ sobre $\mathbb{F}_q$. Usando el Teorema 3.1 se construye un conjunto tipo Bose y Chowla $\alpha + \mathbb{F}_q \subseteq \mathbb{F}^*_{q^{h+1}}$ y por el Lema 2.2 se obtiene el conjunto $\mathscr{A} = \log_\theta(\alpha + \mathbb{F}_q)$, que es B_{h+1} en el grupo aditivo $\mathbb{Z}_{q^{h+1}-1}$, con q elementos.

Denote $n_q := q^h + q^{h-1} + \cdots + q + 1$.

Ahora, se modula el conjunto $\mathscr{A}$ módulo n_q, así se obtiene un nuevo conjunto $S = \mathscr{A} \pmod{n_q}$. Se va a

probar que S es un conjunto B_h en el grupo aditivo $\mathbb{Z}_{n_q}$.

Suponga que existe un elemento en el grupo $(\mathbb{Z}_{n_q},+)$ que tiene dos representaciones como suma de h elementos del conjunto S; es decir, existen $a_{i_1},\ldots,a_{i_h},a'_{j_1},\ldots,a'_{j_h}$ en S tales que

$$a_{i_1}+\cdots+a_{i_h}\equiv a'_{j_1}+\cdots+a'_{j_h}(\operatorname{mod} n_q)$$

esto implica que para algún $r\in\mathbb{Z}$,

$$\theta^{a_{i_1}+\cdots+a_{i_h}}=\theta^{a'_{j_1}+\cdots+a'_{j_h}}\theta^{rn_q}$$

y como $v=\theta^{rn_q}\in\mathbb{F}_q^*=\langle\theta^{n_q}\rangle$ se obtiene

$$\theta^{a_{i_1}}\cdots\theta^{a_{i_h}}=v\,\theta^{a'_{j_1}}\cdots\theta^{a'_{j_h}}.$$

Como para cada elemento $\alpha+u_i\in\alpha+\mathbb{F}_q$ existe un único elemento $a_i\in\mathscr{A}$ tal que $\log_\theta(\alpha+u_i)=a_i$, esto implica que

$$(\alpha+u_{i_1})\cdots(\alpha+u_{i_h})=v(\alpha+u'_{j_1})\cdots(\alpha+u'_{j_h}),$$

desarrollando los productos, se observa que α satisface un polinomio de grado h en la variable x con coeficientes en $\mathbb{F}_q^*$,

$$P(x)=(1-v)x^h+(\sigma_1-v\delta_1)x^{h-1}+\cdots+(\sigma_{h-1}-v\delta_{h-1})x+(\sigma_h-v\delta_h),$$

donde $\sigma_k=\sigma_k(u_{i_1},\ldots,u_{i_h})$, $\delta_k=\delta_k(u'_{i_1},\ldots,u'_{i_h})$, $k=1,\ldots,h$, son las funciones simétricas elementales. Luego como α es de grado $h+1$ sobre $\mathbb{F}_q$ el polinomio $P(x)$ debe ser el polinomio nulo y así se tiene que

$$v=1\text{ y }\sigma_k=v\delta_k,$$

para $k=1,\ldots,h$, en consecuencia $v=1$ y $\{u_{i_1},\ldots,u_{i_h}\}=\{u'_{j_1},\ldots,u'_{j_h}\}$.

Por lo tanto,

$$\{a_{i_1},\ldots,a_{i_h}\}=\{a'_{j_1},\ldots,a'_{j_h}\}.$$

Además, S tiene q elementos; en efecto, suponga que existen dos elementos en S que son iguales,

$$a_i\equiv a_j(\operatorname{mod} n_q),$$

con $i\neq j$. Así, existe $w\in\mathbb{Z}$ tal que en $\mathbb{F}_{q^{h+1}}$ se tiene

$$\theta^{a_i}=\theta^{a_j}\theta^{wn_q}$$

y como $y=\theta^{wn_q}\in\mathbb{F}_q^*=\langle\theta^{n_q}\rangle$ entonces

$$\theta^{a_i}=y\theta^{a_j}.$$

Esto implica que

$$(\alpha+u_i)=y(\alpha+u_j),$$

para algún $u_i,u_j\in\mathbb{F}_q$.

Así, α satisface un polinomio de grado 1 con coeficientes en $\mathbb{F}_q$, implicando que $y=1$ y $u_i=u_j$ y así $i=j$, lo cual es una contradicción. Por lo tanto, todos los elementos de S son distintos.

En consecuencia, S es un conjunto B_h en $\mathbb{Z}_{n_q}$, con q elementos.

Por otro lado, se tiene que el conjunto S satisface $S\cap(S\ominus S)=\emptyset$, donde $S\ominus S=(S-S)\setminus\{0\}$. En efecto, suponga que existen $s,r,t\in S$, $r\neq t$, tales que $s\equiv r-t(\operatorname{mod} n_q)$, luego existen $a,b,c\in\mathbb{F}_q$ y $m\in\mathbb{Z}$ tales que $s=\log_\theta(\alpha+a)$, $r=\log_\theta(\alpha+b)$ y $t=\log_\theta(\alpha+c)$, luego

$$\begin{aligned}s-r+t&=\log_\theta(\alpha+a)-\log_\theta(\alpha+b)+\log_\theta(\alpha+c)\\&=mn_q,\end{aligned}$$

lo que implica que

$$(\alpha+a)(\alpha+c)(\alpha+b)^{-1}=\theta^{mn_q},$$

tomando $w=\theta^{mn_q}\in\mathbb{F}_q^*$ se tiene que α satisface el polinomio

$$Q(x)=x^2+(a+c-w)x+ac-bw,$$

con coeficientes en $\mathbb{F}_q$, pero como α es de grado mayor o igual que 3 sobre $\mathbb{F}_q$, entonces $Q(x)$ debe ser el polinomio nulo; lo cual no puede ser posible puesto que el coeficiente de x^2 es 1, de esto se sigue que $S\cap(S\ominus S)=\emptyset$.

En consecuencia, tomando el conjunto

$$S_0:=S\cup\{0\}$$

se obtiene un conjunto B_h en $\mathbb{Z}_{n_q}$ con $q+1$ elementos. □

3.1 Nuevas construcciones

Gómez y Trujillo en [7] encuentran una nueva construcción de conjuntos B_{h+1}, donde realizan el proceso contrario a la construcción de Singer generalizada, ellos a partir de un conjunto B_h obtienen un conjunto B_{h+1}.

En el Teorema 3.6 se presenta una construcción de un conjunto B_{h+s} en el grupo producto $(F^h,+)\times(E^*,\cdot)$, donde E es alguna extensión de F y como consecuencia en el Corolario 3.7 se presenta la generalización a cualquier cuerpo F de la construcción de conjuntos B_{h+1} dada por Gómez y Trujillo [7], a partir de un conjunto B_h tipo Bose y Chowla construido en el Teorema 3.1.

Además, es posible obtener otra construcción de un conjunto B_{h+1} en dimensión dos en el grupo multiplicativo $F^*\times E*$ usando la construcción tipo Bose y Chowla de conjuntos B_h, ver Teorema 3.10. Sin embargo en esta construcción se pierde un elemento, por ejemplo para el caso cuando el cuerpo $F=\mathbb{F}_p$, p primo, el conjunto tiene $p-1$ elementos.

Sea $(F^h,+)$ el grupo producto de h copias del grupo $(F,+)$. A continuación se presenta la construcción de un conjunto B_{h+s} en $h+1$ dimensiones. Dado el conjunto $A_h=\{(x,x^2,\ldots,x^h): x\in F\}$, se conoce por [12] que A_h es un conjunto B_h en el grupo producto $(F^h,+)$, usando la construcción de Bose de un conjunto B_s multiplicativo es posible construir un conjunto B_{h+s} en $h+1$ dimensiones.

Teorema 3.6. *Si F es un cuerpo, α un elemento algebraico de grado $s\geq 2$ sobre F en alguna extensión E de F y $h\geq 1$ un entero. Entonces el conjunto*

$$\mathscr{A}=\{(x,x^2,\ldots,x^h,\alpha+x): x\in F\}$$

es un conjunto B_{h+s} en el grupo producto $(F^h,+)\times(E^*,\cdot)$.

Proof. Se denota por $*$ la operación del grupo producto $(F^h,+)\times(E^*,\cdot)$.

Sean $x=\{x_1,\ldots,x_{h+s}\}$, $y=\{y_1,\ldots,y_{h+s}\}$ subconjuntos de F tales que

$$(x_1,\ldots,x_1^h,\alpha+x_1)*\cdots*(x_{h+s},\ldots,x_{h+s}^h,\alpha+x_{h+s})=$$
$$(y_1,\ldots,y_1^h,\alpha+y_1)*\cdots*(y_{h+s},\ldots,y_{h+s}^h,\alpha+y_{h+s}).$$

Esto implica que

$$x_1+x_2+\cdots+x_{h+s}=y_1+y_2+\cdots+y_{h+s}$$
$$x_1^2+x_2^2+\cdots+x_{h+s}^2=y_1^2+y_2^2+\cdots+y_{h+s}^2$$
$$\vdots$$
$$x_1^h+x_2^h+\cdots+x_{h+s}^h=y_1^h+y_2^h+\cdots+y_{h+s}^h$$
$$(\alpha+x_1)(\alpha+x_2)\cdots(\alpha+x_{h+s})=$$
$$(\alpha+y_1)(\alpha+y_2)\cdots(\alpha+y_{h+s}). \tag{4}$$

Las primeras h igualdades, por las identidades de Newton-Girard, implican la igualdad de las funciones simétricas elementales

$$\sigma_k(x_1,x_2,\ldots,x_{h+s})=\sigma_k(y_1,y_2,\ldots,y_{h+s}), \tag{5}$$

para $1\leq k\leq h$.

Ahora, si se desarrollan los productos de (4) se obtiene

$$\alpha^{h+s}+\sum_{i=1}^{h+s}\sigma_i(x)\alpha^{h+s-i}=\alpha^{h+s}+\sum_{i=1}^{h+s}\sigma_i(y)\alpha^{h+s-i}, \tag{6}$$

luego usando las igualdades de (5) para $1\leq k\leq h$ y simplificando se obtiene que α satisface un polinomio de grado $s-1$, pero como α es algebraico de grado s sobre F entonces el polinomio debe ser el polinomio nulo, esto implica que

$$\sigma_k(x_1,x_2,\ldots,x_{h+s})=\sigma_k(y_1,y_2,\ldots,y_{h+s}), \tag{7}$$

para $h+1\leq k\leq h+s$. En consecuencia, $\{x_1,\ldots,x_{h+s}\}=\{y_1,\ldots,y_{h+s}\}$ y por lo tanto

$$\{(x_i,x_i^2,\ldots,x_i^h,\alpha+x_i): i=1\ldots,h+s\}=$$
$$\{(y_i,y_i^2,\ldots,y_i^h,\alpha+y_i): i=1\ldots,h+s\}.$$

□

Corolario 3.7. *Si $(F,+,\cdot)$ es un cuerpo, α un elemento algebraico de grado $h \geq 2$ sobre F en alguna extensión E de F, entonces el conjunto*

$$A := \{(a, \alpha + a) : a \in F\}$$

es un conjunto B_{h+1} en $(F,+) \times (E^*,\cdot)$.

Observación 3.8. *En particular, si se toma el cuerpo finito $F = \mathbb{F}_p$ con p elementos, p primo, entonces $E = \mathbb{F}_{p^h}$ y $(\mathbb{F}_p,+) \times (\mathbb{F}^*_{p^h},\cdot)$ es isomorfo al grupo $(\mathbb{Z}_p \times \mathbb{Z}_{p^h-1},+)$. Además, como se tiene que $mcd(p, p^h-1) = 1$ entonces por el isomorfismo del Teorema Chino del Residuo se tiene que $\mathbb{Z}_p \times \mathbb{Z}_{p^h-1} \cong \mathbb{Z}_{p(p^h-1)}$. Luego usando el Lema 2.2 se obtiene la construcción de Gómez y Trujillo [7] de un conjunto B_{h+1} dado por*

$$\{p^h \log_\theta(\alpha + a) - (p^h - 1)a : a \in \mathbb{Z}_p\},$$

a partir de un conjunto B_h, donde θ es un elemento primitivo de $\mathbb{Z}_p$.

Ejemplo 3.9. *Del Ejemplo 3.4 se tiene que el conjunto*

$$\theta + \mathbb{F}_7 = \{\theta, \theta+1, \theta+2, \theta+3, \theta+4, \theta+5, \theta+6\}$$

es un conjunto B_2 en el grupo multiplicativo $\mathbb{F}^*_{49}$. Luego el conjunto

$$B = \{(0,\theta), (1,\theta+1), (2,\theta+2), (3,\theta+3), (4,\theta+4), (5,\theta+5), (6,\theta+6)\},$$

es un conjunto B_3 en el grupo $(\mathbb{F}_7,+) \times (\mathbb{F}^*_{49},\cdot)$.

Luego usando la construcción de Gómez y Trujillo se obtiene que el conjunto

$$C = \{10, 49, 125, 131, 190, 319, 324\},$$

es un conjunto B_3 en el grupo aditivo $\mathbb{Z}_{336}$.

Por otro lado, usando la construcción tipo Bose y Chowla de conjuntos B_h se puede obtener otra construcción de un conjunto B_{h+1} en dimensión dos en el grupo multiplicativo $F^* \times E^*$. Sin embargo, cuando F es un cuerpo finito se pierde un elemento.

Teorema 3.10. *Si $(F,+,\cdot)$ es un cuerpo, α un elemento algebraico de grado $h \geq 2$ sobre F en alguna extensión E de F, entonces el conjunto*

$$A := \{(a, \alpha + a) : a \in F^*\}$$

es un conjunto B_{h+1} en $(F^*,\cdot) \times (E^*,\cdot)$.

Ahora se presenta la construcción de un conjunto B_{h+2} en dimensión tres pegando dos conjuntos conocidos, el conjunto de Sidon

$$\mathscr{I} = \{(x,x) : x \in F^*\} \subset (F,+) \times (F^*,\cdot)$$

presentado en [4] y el conjunto B_h tipo Bose y Chowla.

Teorema 3.11. *Si $(F,+,\cdot)$ es un cuerpo, α un elemento algebraico de grado $h \geq 2$ sobre F en alguna extensión E de F, entonces el conjunto*

$$A := \{(a, a, \alpha + a) : a \in F^*\}$$

es un conjunto B_{h+2} en $(F,+) \times (F^*,\cdot) \times (E^*,\cdot)$.

Observación 3.12. *Cuando se tiene el cuerpo finito $F = \mathbb{F}_p$, con p elementos y p primo, entonces $|A| = p-1$. Luego usando el Lema 2.2 se tiene que si $A = \{(a, a, \alpha + a) : a \in \mathbb{F}^*_p\}$ es un conjunto B_{h+2} en $(\mathbb{F}_p,+) \times (\mathbb{F}^*_p,\cdot) \times (\mathbb{F}^*_{p^h},\cdot)$ entonces el conjunto*

$$B = \{(a, \log_{\theta_1} a, \log_{\theta_2}(\alpha + a)) : a \in \mathbb{F}^*_p\}$$

es un conjunto B_{h+2} en $(\mathbb{Z}_p,+) \times (\mathbb{Z}_{p-1},+) \times (\mathbb{Z}_{p^h-1},+)$, donde θ_1 y θ_2 son elementos primitivos de $\mathbb{F}_p$ y $\mathbb{F}_{p^h}$, respectivamente.

Además, como $mcd(p, p^h - 1) = 1$ por el isomorfismo del Teorema Chino del Residuo se tiene que el conjunto

$$C = \{(\log_{\theta_1} a, p^h \log_{\theta_2}(\alpha + a) - (p^h - 1)a) : a \in \mathbb{Z}^*_p\}$$

es un conjunto B_{h+2} en $(\mathbb{Z}_{p-1} \times \mathbb{Z}_{p(p^h-1)},+)$.

Ejemplo 3.13. *Del Ejemplo 3.4 se tiene que*

$$\theta + \mathbb{F}_7 = \{\theta, \theta+1, \theta+2, \theta+3, \theta+4, \theta+5, \theta+6\}$$

es un conjunto B_2 en el grupo multiplicativo $\mathbb{F}^*_{49}$. Además,

$$B = \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6)\}$$

es un conjunto B_2 en $(\mathbb{F}_7,+)\times(\mathbb{F}_7^*,\cdot)$.

Luego

$$C=\{(1,1,\theta+1),(2,2,\theta+2),(3,3,\theta+3),\\(4,4,\theta+4),(5,5,\theta+5),(6,6,\theta+6)\}$$

es un conjunto B_4 en el grupo $(\mathbb{F}_7,+)\times(\mathbb{F}_7^*,\cdot)\times(\mathbb{F}_{49}^*,\cdot)$.

Ahora, usando el Teorema Chino del Residuo se tiene que

$$D=\{(1,190),(2,342),(3,10),(4,319),\\(5,131),(6,125)\}$$

es un conjunto B_4 en el grupo aditivo $\mathbb{Z}_6\times\mathbb{Z}_{336}$.

Por último, como consecuencia del Teorema 3.6 se tiene la construcción de un conjunto B_{h+2} en $h+1$ dimensiones. Como $A_h=\{(x,x^2,\ldots,x^h):x\in F\}$ es un conjunto B_h en el grupo producto $(F^h,+)$, usando la construcción de Bose de un conjunto B_2 multiplicativo es posible construir un conjunto B_{h+2} en $h+1$ dimensiones.

Corolario 3.14. *Si F es un cuerpo, α un elemento algebraico de grado 2 sobre F en alguna extensión E de F y $h\geq 1$ un entero. Entonces el conjunto*

$$\mathscr{A}=\{(x,x^2,\ldots,x^h,\alpha+x):x\in F\}$$

es un conjunto B_{h+2} en el grupo producto $(F^h,+)\times(E^*,\cdot)$.

Como los conjuntos B_h con $h>2$ no se pueden expresar en forma directa como un equivalente en diferencias, como sí se hace en el caso $h=2$, son más difíciles de manipular que los conjuntos de Sidon. Por tal razón, hasta el momento se desconoce el comportamiento asintótico de la función $F_h(n)$ para $h\geq 3$, incluso para el caso de la función $f_h(G)$ donde G es un grupo abeliano de orden n.

4 Conclusiones

Como consecuencia de las construcciones proporcionadas en los Teoremas 3.6 y 3.11 se tiene que:

- Dado el conjunto $A_h=\{(x,x^2,\ldots,x^h):x\in F\}$ que es un conjunto B_h en el grupo producto $(F^h,+)$, usando la construcción de Bose de un conjunto B_s multiplicativo es posible construir un conjunto B_{h+s} en $h+1$ dimensiones.

- Si F es un cuerpo finito y α es un elemento algebraico de grado $h\geq 2$ sobre F en alguna extensión E entonces

$$f_{h+1}\left((F^*,+)\times(E^*,\cdot)\right)\geq|F|-1.$$

- Si F es un cuerpo finito y α es un elemento algebraico de grado $h\geq 2$ sobre F en alguna extensión E entonces

$$f_{h+2}\left((F,+)\times(F^*,\cdot)\times(E^*,\cdot)\right)\geq|F|-1.$$

- La construcción del Corolario 3.14 permite obtener familias de conjuntos B_{h+2} que son óptimamente densos cuando $|G|$ tiende a infinito; es decir, si A es un conjunto B_{h+2} en $G=(F^h,+)\times(E^*,\cdot)$ se tiene que

$$|A|=|F|\gg(|F|^h(|F|^2-1))^{h+2}=|G|^{h+2}.$$

Agradecimientos

Los autores agradecen a los jurados evaluadores por sus comentarios los cuales han mejorado la calidad de este artículo. El segundo autor agradece a MINCIENCIAS por financiar sus estudios de doctorado.

Referencias

[1] J. Bravo, D. Ruiz, and C. Trujillo, "Cardinality of sets associated to B3 and B4 sets", *Revista colombiana de matemáticas* 46, no. 1, pp. 27-37, Ene. 2012. https://revistas.unal.edu.co/index.php/recolma/article/view/31840

[2] R. C. Bose, "An afine analogue of Singer's theorem", *J. Indian Math. Soc. (N.S.)* vol. 6, pp. 1-15, 1942. DOI: 10.18311/jims/1942/17165

[3] R. C. Bose y S. Chowla, "Theorems in the additive theory of numbers", *Comment. Math. Helv.* 37, pp. 141-147, Dec. 1962. DOI: 10.1007/BF02566968

[4] N.Y. Caicedo, "Conjuntos de Sidon en dimensión dos", Tesis doctoral, Departamento de Matemáticas, Universidad del Valle, Santiago de Cali, 2016.

[5] S. Chen, "On the size of finite Sidon sequences", *Proc. Amer. Math. Soc.* vol. 121, no. 2, pp. 353-356, Jun. 1994. DOI: 10.2307/2160407

[6] P. Erdös y P. Turán, "On a problem of Sidon in additive number theory and on some related problems", *Journal of the London Mathematical Society* vol. s1-16 , pp. 212-215. Addendum (by P. Erdös). MR 3, 270e, Oct. 1941. DOI: 10.1112/jlms/s1-16.4.212

[7] A. Gómez and C. Trujillo, "Una nueva construcción de conjuntos B_h modulares", *Matemáticas: Enseñanza Universitaria* vol. XIX, no. 1, pp. 53-62, 2011. https://www.redalyc.org/articulo.oa?id=46818606005

[8] S. W. Graham, "Bh Sequences", *Berndt B.C., Diamond H.G., Hildebrand A.J. (eds) Analytic Number Theory. Progress in Mathematics* vol 138, 1996. DOI: 10.1007/978-1-4612-4086-0_23

[9] B. Green, "The number of squares and $B_h[g]$ sets", *Acta Arithmetica* vol.100, no 4, pp. 365-390, 2001. http://eudml.org/doc/278434

[10] X. D. Jia, "On finite Sidon sequences", *Journal Number Theory* 44, pp. 84-92, May. 1993. DOI: 10.1006/jnth.1993.1037

[11] G. Martin and K. O'Bryant, "Constructions of generalized Sidon sets", *J. Combib. Theory Set* A 113, pp. 591-607, May. 2006. DOI: 10.1016/j.jcta.2005.04.011

[12] D. Ruiz and C. Trujillo, "Constructions of $B_h[g]$ sets in product of groups", *Rev.colomb.mat.* vol. 50, no. 2, pp. 165-174, 2016. DOI: 10.15446/recolma.v50n2.62208

[13] J. Singer, "A theorem infinite projective geometry and some applications to number theory", *Trans. Amer. Math. Soc.* vol. 43, pp. 377-385, 1938. DOI: 10.1090/S0002-9947-1938-1501951-4

[14] T. Tao and V. H. Vu, *Additive Combinatorics*. Cambridge: Cambridge University Press, 2006.