

# Construction of $B_h[g]$ sets in product of groups

Construcción de conjuntos  $B_h[g]$  en producto de grupos

DIEGO RUIZ<sup>1,✉</sup>, CARLOS TRUJILLO<sup>1</sup>

<sup>1</sup>Universidad del Cauca, Popayán, Colombia

ABSTRACT. A subset  $\mathcal{A}$  of an abelian group  $G$  is a  $B_h[g]$  set on  $G$  if the elements of  $G$  can be written in at most  $g$  ways as sum of  $h$  elements of  $\mathcal{A}$ . Given any field  $\mathbb{F}$ , this work presents constructions of  $B_h[g]$  sets on the abelian groups  $(\mathbb{F}^h, +)$ ,  $(\mathbb{Z}^d, +)$ , and  $(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}, +)$ , for  $d \geq 2$ ,  $h \geq 2$ , and  $g \geq 1$ .

*Key words and phrases.* Sidon sets,  $B_h[g]$  sets.

*2010 Mathematics Subject Classification.* 11B50, 11B75.

RESUMEN. Un subconjunto  $\mathcal{A}$  de un grupo abeliano  $G$  es un conjunto  $B_h[g]$  sobre  $G$  si todo elemento de  $G$  puede escribirse en a lo sumo de  $g$  formas como la suma de  $h$  elementos de  $\mathcal{A}$ . En este trabajo se presentan construcciones de conjuntos  $B_h[g]$  sobre los grupos abelianos  $(\mathbb{F}^h, +)$ ,  $(\mathbb{Z}^d, +)$ , y  $(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}, +)$ , para  $d \geq 2$ ,  $h \geq 2$ , y  $g \geq 1$ , con  $\mathbb{F}$  cualquier campo.

*Palabras y frases clave.* Conjuntos de Sidon, Conjuntos  $B_h$ .

## 1. Introduction

Let  $g$  and  $h$  denote positive integers with  $h \geq 2$ . Let  $G$  be an abelian additive group denoted by  $(G, +)$ . The set  $\mathcal{A} = \{a_1, \dots, a_k\} \subseteq G$  is a  $B_h[g]$  set on  $G$  if every element of  $G$  can be written in at most  $g$  ways as sum of  $h$  elements in  $\mathcal{A}$ , that is, if given  $x \in G$ , the solutions of the equation  $x = a_1 + \cdots + a_h$ , with  $a_1, \dots, a_h \in \mathcal{A}$ , are at most  $g$  (up to rearrangement of summands). If  $g = 1$ ,  $\mathcal{A}$  is a  $B_h$  set, while if  $g = 1$  and  $h = 2$ ,  $\mathcal{A}$  is a Sidon set.

Let  $F_h(G, g)$  denote the largest cardinality of a  $B_h[g]$  on  $G$ . If  $g = 1$  we write  $F_h(G)$ . Furthermore, if  $G$  is the direct product of  $d \geq 2$  abelian groups and  $\mathcal{A}$  is a  $B_h[g]$  set on  $G$ , sometimes we say that  $\mathcal{A}$  is a  $d$ -dimensional  $B_h[g]$  set on  $G$ . For  $N \in \mathbb{N}$ , let  $[0, N - 1] := \{0, 1, \dots, N - 1\}$ . If  $\mathbb{Z}^d$  denotes the set of

all  $d$ -tuples of integer numbers and  $[0, N - 1]^d$  denotes the cartesian product of  $[0, N - 1]$  with itself  $d$  times, we define

$$F_h^d(N, g) := \max\{|\mathcal{A}| : \mathcal{A} \subseteq [0, N - 1]^d, \mathcal{A} \in B_h[g]\}.$$

The main problem on  $B_h[g]$  sets consists on establishing the largest cardinality of a  $B_h[g]$  set on a finite group  $G$ . With analytical constructions it is possible to characterize lower bounds for  $F_h(G, g)$ , while using counting and combinatorial techniques, it is possible to characterize upper bounds. In this work we focus on constructions to obtain known lower bounds for  $F_h(G, g)$  on particular groups  $G$  ( $(\mathbb{F}^h, +)$ ,  $(\mathbb{Z}^d, +)$ , and  $(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}, +)$  for any field  $\mathbb{F}$  and  $d \geq 2$ ,  $h \geq 2$ ,  $g \geq 1$ ), while other works are focused on upper bounds [1], [4], [11].

Different works have introduced constructions of  $B_h[g]$  sets for particular values of  $h$ , and  $g$ . On  $(\mathbb{Z}, +)$ , the most obvious construction of Sidon sets is given by Mian–Chowla using the greedy algorithm [2]. This result is generalized by O’Byrant for any  $h \geq 2$  and any  $g \geq 1$  in [10].

Other constructions of  $B_h$  sets are due to Rusza, Bose, Singer, and Erdős & Turán. Rusza constructs a Sidon set on the group  $(\mathbb{Z}_{(p^2-p)}, +)$  for  $p$  prime. Bose’s construction initially consider  $h = 2$  but could be generalized for any  $h \geq 2$  and any prime power  $q$  on the group  $(\mathbb{Z}_{q^{h-1}}, +)$ . Similarly to Bose, Singer constructs a  $B_h$  set with  $q + 1$  elements on  $(\mathbb{Z}_{(q^{h+1}-1)/(q-1)}, +)$ . Actually this construction can be established using Bose’s construction [8]. Finally, based on quadratic residues modulo a fixed prime  $p$ , Erdős & Turán construct Sidon sets on  $(\mathbb{Z}, +)$  [10].

In dimension  $d = 2$  some constructions are due to Welch, Lempel, Golomb [6], Trujillo [12], and C. Gómez & Trujillo [8]. Welch constructs Sidon sets with  $p - 1$  elements on the groups  $(\mathbb{Z}_{p-1} \times \mathbb{Z}_p, +)$ ,  $(\mathbb{Z}_p \times \mathbb{Z}_{p-1}, +)$ , generalized in [7] to the groups  $(\mathbb{Z}_{q-1} \times \mathbb{F}_q, +)$  and  $(\mathbb{F}_q \times \mathbb{Z}_{q-1}, +)$ , respectively, where  $\mathbb{F}_q$  is the finite field with  $q$  elements. Golomb constructs Sidon sets with  $q - 2$  elements on the group  $(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}, +)$  (Lempel’s construction is a particular case of Golomb). Trujillo in [12] presents an algorithm to construct Sidon sets on  $(\mathbb{Z} \times \mathbb{Z}, +)$  from a given Sidon set on  $(\mathbb{Z}, +)$ . Finally, C. Gómez & Trujillo construct  $B_h$  sets on  $(\mathbb{Z}_p \times \mathbb{Z}_{p^{h-1}-1}, +)$  [8].

In higher dimensions, Cilleruelo in [4] presents a way of mapping Sidon sets in  $\mathbb{N}$  to Sidon sets in  $\mathbb{N}^d$  for  $d \geq 2$ , from which is possible to obtain a relation between the functions  $F_h(N^d)$  and  $F_h^d(N)$ .

In this work we present constructions of  $d$ -dimensional  $B_h[g]$  sets ( $d \geq 2$ ) on special abelian groups. The first construction uses the elementary symmetric polynomials and the Newton’s identities to generalize a construction done initially for  $d = 2$  [3]. In the second construction we generalize Trujillo’s algorithm given in [12] to any dimension  $d$  and all  $h \geq 2$ ,  $g \geq 1$ , obtaining lower bounds for  $F_h^d(N, g)$  from a known lower bounds for  $F_h(N^d, g)$ . Finally, using

a homomorphism between abelian groups, we construct  $d$ -dimensional  $B_h[g']$  sets from  $d$ -dimensional  $B_h[g]$  sets, with  $g$  a divisor of  $g'$ .

The remainder of this work is organized as follows: For any finite field  $\mathbb{F}$ , Section 2 describes a construction of  $B_h$  sets on  $(\mathbb{F}^h, +)$ , where  $\mathbb{F}^h$  denotes the set of all  $h$ -tuples of elements of  $\mathbb{F}$ . Section 3 presents a construction of  $B_h[g]$  sets on  $(\mathbb{Z}^d, +)$ , and in Section 4 we construct  $B_h[g]$  sets on  $(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}, +)$ . Furthermore, we present a generalization of a Golomb Costas array construction. Finally, Section 5 describes the concluding remarks of this work.

**2. Construction of  $B_h$  sets on  $(\mathbb{F}^h, +)$**

Let  $p$  be a prime number. Note that  $\mathcal{A} := \{(x, x^2) : x \in \mathbb{Z}_p\}$  is a  $B_2$  set on  $(\mathbb{Z}_p \times \mathbb{Z}_p, +)$  [3]. In this section we generalize this construction using  $h$ -tuples ( $h > 2$ ). First we introduce the following notations and definitions.

Let  $n$  be a positive integer. The elementary symmetric polynomials in the variables  $x_1, \dots, x_n$ , written by  $\sigma_k(x_1, \dots, x_n)$  for  $k = 1, \dots, n$ , is defined as

$$\sigma_k(x_1, \dots, x_n) := \sum_{1 \leq j_1 < \cdots < j_k \leq n} x_{j_1} \cdots x_{j_n}.$$

If  $k = 0$  we consider  $\sigma_0(x_1, \dots, x_n) = 1$ . For  $n = 3$  we have

$$\begin{aligned} \sigma_0(x_1, x_2, x_3) &= 1, \\ \sigma_1(x_1, x_2, x_3) &= x_1 + x_2 + x_3, \\ \sigma_2(x_1, x_2, x_3) &= x_1x_2 + x_1x_3 + x_2x_3, \\ \sigma_3(x_1, x_2, x_3) &= x_1x_2x_3. \end{aligned}$$

Note that the elementary symmetric polynomials appear in the expansion of a linear factorization of a monic polynomial

$$\prod_{j=1}^n (\lambda - x_j) = \sum_{k=0}^n (-1)^k \sigma_k(x_1, \dots, x_n) \lambda^{n-k}.$$

Note also that if  $p_k(x_1, \dots, x_n) = x_1^k + \cdots + x_n^k$ , the Newton's identities are given by

$$k\sigma_k(x_1, \dots, x_n) = \sum_{i=1}^k (-1)^{i-1} \sigma_{k-i}(x_1, \dots, x_n) p_i(x_1, \dots, x_n), \tag{1}$$

for each  $1 \leq k \leq n$  and for an arbitrary number  $n$  of variables.

**Theorem 2.1.** *Let  $\mathbb{F}$  be a field with characteristic zero or  $p > h$ . The set*

$$\mathcal{A} := \{(x, x^2, \dots, x^h) : x \in \mathbb{F}\},$$

*is a  $B_h$  set on  $(\mathbb{F}^h, +)$ .*

**Proof.** Let  $s \in \mathbb{F}^h$ . Suppose there exist two different representations of  $s$  as sum of  $h$  elements of  $\mathcal{A}$  as follows

$$s = (a_1, \dots, a_1^h) + \dots + (a_h, \dots, a_h^h) = (b_1, \dots, b_1^h) + \dots + (b_h, \dots, b_h^h),$$

$a_i, b_i \in \mathbb{F}$  for  $i = 1, \dots, h$ . Note that for all  $k = 1, \dots, h$ ,  $\sum_{i=1}^h a_i^k = \sum_{i=1}^h b_i^k$ . Because  $p_k(a_1, \dots, a_h) = \sum_{i=1}^h a_i^k$  and  $p_k(b_1, \dots, b_h) = \sum_{i=1}^h b_i^k$ , using (1) recursively we have  $\sigma_i(a_1, \dots, a_h) = \sigma_i(b_1, \dots, b_h)$ , for all  $i = 1, \dots, h$ , that is

$$\begin{aligned} a_1 + \dots + a_h &= b_1 + \dots + b_h, \\ a_1 a_2 + \dots + a_{h-1} a_h &= b_1 b_2 + \dots + b_{h-1} b_h, \\ &\dots \\ a_1 \dots a_h &= b_1 \dots b_h, \end{aligned}$$

which implies that the elements of the sets  $\{a_1, \dots, a_h\}$  and  $\{b_1, \dots, b_h\}$  are roots of the same polynomial  $q(x)$  on  $\mathbb{F}[x]$ , i.e.,

$$q(x) = (x - a_1) \dots (x - a_h) = (x - b_1) \dots (x - b_h).$$

That is,  $\{a_1, \dots, a_h\} = \{b_1, \dots, b_h\}$  ( $\mathbb{F}[x]$  is a unique factorization domain). Thus, cannot be possible to have two different representations of  $s \in \mathbb{F}$  as sum of  $h$  elements of  $\mathbb{F}^h$  and  $\mathcal{A}$  is a  $B_h$  set on  $(\mathbb{F}^h, +)$ .  $\checkmark$

Consider the case when  $\mathbb{F}$  is the finite field  $\mathbb{F}_q$ , with  $q = p^n$  for some  $n \in \mathbb{N}$  and  $p$  prime. Note that the groups  $(\mathbb{F}_{p^n}, +)$  and  $(\mathbb{F}_p^n, +)$  are isomorphic, because if  $\theta$  is a root of an irreducible polynomial of degree  $n$  over  $\mathbb{F}_p$  in an extension field, the function

$$\begin{aligned} \phi : \quad \mathbb{F}_{p^n} &\rightarrow \mathbb{F}_p^n \\ a_0 + \dots + a_{n-1} \theta^{n-1} &\mapsto (a_0, \dots, a_{n-1}) \end{aligned} \tag{2}$$

defines an isomorphism between them.

**Corollary 2.2.** *For all  $p > h$  prime and for all  $n \in \mathbb{N}$  there exists a  $B_h$  set with  $p^n$  elements on  $(\mathbb{Z}_p^{hn}, +)$ .*

**Proof.** It follows immediately from Theorem 2.1 and the isomorphism  $\phi$  given in (2).  $\checkmark$

We illustrate these results in the following example.

**Example 2.3.** Consider  $h = n = 2$  and  $p = 3$ . Let  $p(x) = x^2 + 1$  be an irreducible polynomial on  $\mathbb{Z}_3$ . Suppose that  $\theta$  is a root of  $p(x)$  in an extension field of  $\mathbb{Z}_3$ . The field with 9 elements is given by

$$\begin{aligned} \mathbb{F}_9 &= \{a + b\theta : a, b \in \mathbb{Z}_3\} \\ &= \{0, 1, 2, \theta, \theta + 1, \theta + 2, 2\theta, 2\theta + 1, 2\theta + 2\}. \end{aligned}$$

Using Theorem 2.1 we know that

$$\mathcal{A} = \left\{ \begin{array}{l} (0, 0), (1, 1), (2, 1), (\theta, 2), (\theta + 1, 2\theta), (\theta + 2, \theta), \\ (2\theta, 2), (2\theta + 1, \theta), (2\theta + 2, 2\theta) \end{array} \right\}$$

is a Sidon set on  $(\mathbb{F}_9 \times \mathbb{F}_9, +) = (\mathbb{F}_9^2, +)$ . Furthermore, using Corollary 2.2 we have

$$\mathcal{B} = \left\{ \begin{array}{l} (0, 0, 0, 0), (0, 1, 0, 1), (0, 2, 0, 1), (1, 0, 0, 2), (1, 1, 2, 0), \\ (1, 2, 1, 0), (2, 0, 0, 2), (2, 1, 1, 0), (2, 2, 2, 0) \end{array} \right\}$$

is a Sidon set on  $(\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3, +) = (\mathbb{Z}_3^4, +)$ .

### 3. Construction of $B_h[g]$ sets on $(\mathbb{Z}^d, +)$

In this section we present a construction of  $B_h[g]$  sets for all  $h, g \geq 2$  on  $(\mathbb{Z}^d, +)$ . This construction generalizes a construction introduced by Trujillo in [12] which allows to obtain Sidon sets on  $(\mathbb{Z} \times \mathbb{Z}, +)$  from a Sidon set on  $(\mathbb{Z}, +)$ . Our generalization also allows to construct  $d$ -dimensional  $B_h[g]$  sets for all  $h, g \geq 2$  and any dimension  $d$ , from which it is possible to determine a way to map  $B_h[g]$  sets on  $(\mathbb{Z}, +)$  into  $B_h[g]$  sets on  $(\mathbb{Z}^d, +)$ .

Let  $d, N$  be positive integers greater than 1. Let  $\mathcal{A}$  denote a subset of  $\mathbb{Z}^+$ . If  $a \in \mathcal{A}$ ,  $[a]_N = (n_k, \dots, n_1, n_0)_N$  represents the integer  $a = n_k N^k + \dots + n_1 N + n_0$  in base  $N$  notation, where  $k$  is a nonnegative integer and  $0 \leq n_j \leq N - 1$ , for  $j = 0, 1, \dots, k$ . We denote the set obtained from the representation of each element of  $\mathcal{A}$  in base  $N$  as  $[\mathcal{A}]_N$ . Because every positive integer can be written uniquely in base  $N$ , then

$$|\mathcal{A}| = |[\mathcal{A}]_N|.$$

Note that if  $\mathcal{A} \subseteq [0, N^d - 1]$ , then  $[\mathcal{A}]_N \subseteq [0, N - 1]^d$ .

**Theorem 3.1.** *If  $\mathcal{A}$  is a  $B_h[g]$  set contained in  $[0, N^d - 1]$ , then  $[\mathcal{A}]_N$  is a  $B_h[g]$  set contained in  $[0, N - 1]^d$ .*

**Proof.** Let  $s$  be a  $d$ -tuple in  $\mathbb{Z}^d$  obtained as sum of  $h$  elements in  $[\mathcal{A}]_N$ . Suppose there exist  $g + 1$  representations of  $s$  as follows

$$s = [a_{1,1}]_N + \dots + [a_{1,h}]_N = \dots = [a_{g+1,1}]_N + \dots + [a_{g+1,h}]_N, \quad (3)$$

where  $a_{i,j} \in \mathcal{A}$  for all  $1 \leq i \leq g + 1$ ,  $1 \leq j \leq h$ . Consider the representation of each  $a_{i,j} \in \mathcal{A}$  in base  $N$  as  $[a_{i,j}]_N = (n_{(d-1,i,j)}, \dots, n_{(0,i,j)})$ . Note that for any  $1 \leq i \leq g + 1$

$$\begin{aligned} [a_{i,1}]_N + \dots + [a_{i,h}]_N &= (n_{(d-1,i,1)}, \dots, n_{(0,i,1)}) + \dots + (n_{(d-1,i,h)}, \dots, n_{(0,i,h)}) \\ &= (n_{(d-1,i,1)} + \dots + n_{(d-1,i,h)}, \dots, n_{(0,i,1)} + \dots + n_{(0,i,h)}). \end{aligned}$$

Furthermore

$$(n_{(d-1,i,1)} + \dots + n_{(d-1,i,h)}) N^{d-1} + \dots + (n_{(0,i,1)} + \dots + n_{(0,i,h)}) = a_{i,1} + \dots + a_{i,h}$$

which implies from (3) that

$$a_{1,1} + \dots + a_{1,h} = \dots = a_{g+1,1} + \dots + a_{g+1,h}. \tag{4}$$

Because  $\mathcal{A}$  is a  $B_h[g]$  set, using (4) we know there exist  $\ell, m$  with  $\ell \neq m$  and  $1 \leq \ell, m \leq g + 1$ , such that

$$\{a_{\ell,1}, \dots, a_{\ell,h}\} = \{a_{m,1}, \dots, a_{m,h}\}.$$

Since representation in base  $N$  notation is unique we have

$$\{[a_{\ell,1}]_N, \dots, [a_{\ell,h}]_N\} = \{[a_{m,1}]_N, \dots, [a_{m,h}]_N\},$$

That is, it is not possible to have  $g + 1$  representations of  $s$  as sum of  $h$  elements of  $\mathcal{A}$ . Therefore  $[\mathcal{A}]_N$  is a  $B_h[g]$  set contained in  $[0, N - 1]^d \subset (\mathbb{Z}^d, +)$ .  $\square$

**Example 3.2.** Note that  $\mathcal{A} = \{1, 2, 7\}$  is a Sidon set on  $(\mathbb{Z}_8, +)$ . In [12] Trujillo constructs a  $B_2[2]$  set on  $(\mathbb{Z}, +)$  as follows

$$\mathcal{B} := \mathcal{A} \cup (\mathcal{A} + m) \cup (\mathcal{A} + 3m) = \{1, 2, 7, 9, 10, 15, 25, 26, 31\},$$

with  $m = 8$ . Because  $\mathcal{B} \subseteq [0, 2^5 - 1]$ , using Theorem 3.1 we have that

$$[\mathcal{B}]_2 = \left\{ \begin{array}{l} (0, 0, 0, 0, 1), (0, 0, 0, 1, 0), (0, 0, 1, 1, 1), (0, 1, 0, 0, 1), (0, 1, 0, 1, 0), \\ (0, 1, 1, 1, 1), (1, 1, 0, 0, 1), (1, 1, 0, 1, 0), (1, 1, 1, 1, 1) \end{array} \right\}$$

is a  $B_2[2]$  set contained in  $[0, 1]^5$ . Note also that  $\mathcal{B} \subseteq [0, 6^2 - 1]$ , so

$$[\mathcal{B}]_6 = \{(0, 1), (0, 2), (1, 1), (1, 3), (1, 4), (2, 3), (4, 1), (4, 2), (5, 1)\}$$

is a  $B_2[2]$  set contained in  $[0, 5]^2$ .

#### 4. Construction of $B_h[g]$ sets on $(\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_d}, +)$

This section extend a construction of  $B_h[g]$  sets given in [5] for  $h = 2$  and  $d = 1$ , to all  $h \geq 2$  and any dimension  $d > 1$ . First, we introduce the following result.

**Lemma 4.1.** *Let  $G$  and  $G'$  be two abelian groups and let  $\phi : G \rightarrow G'$  define a homomorphism. If  $\mathcal{A}$  is a  $B_h[g]$  set on  $G$  and  $|Ker(\phi)| = g'$ , then  $\phi(\mathcal{A})$  is a  $B_h[gg']$  set on  $\phi(G)$ , where  $gg'$  denotes the product between  $g$  and  $g'$ .*

The proof is given in [9].

Now, let  $m_1, \dots, m_d$  and  $g_1, \dots, g_d$  be positive integers. Using Lemma 4.1 we have the following result.

**Theorem 4.2.** *Let  $\mathcal{A}$  be a  $B_h[g]$  set on  $(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}, +)$ . If  $g_1, \dots, g_d$  are divisors of  $m_1, \dots, m_d$ , respectively, then*

$$\mathcal{B} := \left\{ \left( a_1 \bmod \frac{m_1}{g_1}, \dots, a_d \bmod \frac{m_d}{g_d} \right) : (a_1, \dots, a_d) \in \mathcal{A} \right\}$$

is a  $B_h[gg_1 \cdots g_d]$  set on  $(\mathbb{Z}_{\frac{m_1}{g_1}} \times \cdots \times \mathbb{Z}_{\frac{m_d}{g_d}}, +)$ .

**Proof.** Using notation used in Lemma 4.1, let  $G = (\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}, +)$  and  $G' = (\mathbb{Z}_{\frac{m_1}{g_1}} \times \cdots \times \mathbb{Z}_{\frac{m_d}{g_d}}, +)$  and define the homomorphism  $\phi : G \rightarrow G'$  as  $\phi(b_1, \dots, b_d) = (b_1 \bmod \frac{m_1}{g_1}, \dots, b_d \bmod \frac{m_d}{g_d})$ . We establish  $\text{Ker}(\phi)$  as follows. Note that  $(b_1, \dots, b_n) \in \text{Ker}(\phi)$  if and only if  $\phi(b_1, \dots, b_n) = (0, \dots, 0)$ , that is, if

$$\left( b_1 \bmod \frac{m_1}{g_1}, \dots, b_d \bmod \frac{m_d}{g_d} \right) = (0, \dots, 0).$$

Note also that  $b_i \bmod \frac{m_i}{g_i} = 0$  if and only if  $b_i = k_i \frac{m_i}{g_i}$ , for  $k_i \in [1, g_i]$  and for all  $i = 1, \dots, d$ , which implies that  $b_i \bmod \frac{m_i}{g_i} = 0$  in exactly  $g_i$  values. Thus,  $|\text{Ker}(\phi)| = \prod_{i=1}^d g_i$ . Finally, using Lemma 4.1 we have that  $\mathcal{B} = \phi(\mathcal{A})$  is a  $B_h[gg_1 \cdots g_d]$  set on  $(\mathbb{Z}_{\frac{m_1}{g_1}} \times \cdots \times \mathbb{Z}_{\frac{m_d}{g_d}}, +)$ .  $\square$

Given  $q$  a prime power and  $\mathbb{F}$  a field, to illustrate Theorem 4.2 we present a construction of Sidon sets on  $(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}, +)$ , which is based on the discrete logarithm<sup>1</sup> on  $\mathbb{F}_q$ .

**Proposition 4.3.** *Let  $q = p^n$  a prime power. If  $\alpha, \beta$  are primitive elements of  $\mathbb{F}_q^*$  and  $a \in \mathbb{F}_q^*$ , then*

$$\mathcal{G}(\alpha, \beta, a) := \{(i, \log_\beta(a - \alpha^i)) : i = 1, \dots, q - 1, \alpha^i \neq a\} \tag{5}$$

is a Sidon set on  $(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}, +)$ .

**Proof.** Suppose there exist  $u, v, w, y \in \mathcal{G}(\alpha, \beta, a)$  such that  $u + v = w + y$ . Using (5) we know that there exist  $i, j, k, \ell \in [1, q - 1]$  such that

$$(i, \log_\beta(a - \alpha^i)) + (j, \log_\beta(a - \alpha^j)) = (k, \log_\beta(a - \alpha^k)) + (\ell, \log_\beta(a - \alpha^\ell)) \tag{6}$$

where  $\alpha^i, \alpha^j, \alpha^k, \alpha^\ell$  are not equal to  $a$ . From (6) we have

$$(i + j) \equiv (k + \ell) \pmod{q - 1},$$

$$\log_\beta(a - \alpha^i) + \log_\beta(a - \alpha^j) \equiv (\log_\beta(a - \alpha^k) + \log_\beta(a - \alpha^\ell)) \pmod{q - 1},$$

<sup>1</sup>If  $\theta$  is a primitive of  $\mathbb{F}_q$ ,  $\log_\theta(x)$  denotes the unique integer  $k \in [1, q - 1]$  such that  $\theta^k = x$  on  $\mathbb{F}_q$ .

what implies that  $(a - \alpha^i)(a - \alpha^j) = (a - \alpha^k)(a - \alpha^\ell)$ . We have in  $\mathbb{F}_q^*$

$$\begin{aligned} \alpha^i \alpha^j &= \alpha^k \alpha^\ell, \\ \alpha^i + \alpha^j &= \alpha^k + \alpha^\ell, \end{aligned}$$

that is,  $\alpha^i, \alpha^j$ , and  $\alpha^k, \alpha^\ell$  are roots of a polynomial  $q(x) \in \mathbb{F}[x]$  of degree 2 (i.e.,  $q(x) = (x + \alpha^i)(x + \alpha^j) = (x + \alpha^k)(x + \alpha^\ell)$ ). Therefore,  $\{\alpha^i, \alpha^j\} = \{\alpha^k, \alpha^\ell\}$  and  $\{i, j\} = \{k, \ell\}$ , which implies that is not possible to have two representations of an element in  $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$  as sum of two elements of  $\mathcal{G}(\alpha, \beta, a)$ . That is,  $\mathcal{G}(\alpha, \beta, a)$  is a Sidon set on  $(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}, +)$ .  $\square$

**Example 4.4.** First we apply Proposition 4.3 to construct a Sidon set on  $(\mathbb{Z}_{16} \times \mathbb{Z}_{16}, +)$ . Let  $q = p = 17$ , and let  $\alpha = 3, \beta = 5$  be primitive elements of  $\mathbb{Z}_{17}^*$ . With  $a = 1$

$$\mathcal{G}(3, 5, 1) = \left\{ \begin{array}{l} (1, 14), (2, 10), (3, 2), (4, 1), (5, 4), (6, 13), (7, 15), (8, 6), \\ (9, 12), (10, 7), (11, 11), (12, 5), (13, 3), (14, 8), (15, 9) \end{array} \right\}$$

is a Sidon set on  $(\mathbb{Z}_{16} \times \mathbb{Z}_{16}, +)$ . Now, if  $g_1 = g_2 = 2$ , using Theorem 4.2,

$$\mathcal{A} = \left\{ \begin{array}{l} (1, 6), (2, 2), (3, 2), (4, 1), (5, 4), (6, 5), (7, 7), (0, 6), \\ (1, 4), (2, 7), (3, 3), (4, 5), (5, 3), (6, 0), (7, 1) \end{array} \right\}$$

is a  $B_2[4]$  set on  $(\mathbb{Z}_8 \times \mathbb{Z}_8, +)$ .

### 5. Concluding remarks

Using the constructions given in this work we can obtain lower bounds and closed formulas for  $F_h^d(G, g)$ , for some abelian group  $G$  and some values of  $d, h$  and  $g$ .

Note from Theorem 2.1 and Corollary 2.2 that  $F_2^h(\mathbb{F}_q^h) \geq q$  for  $q$  a prime power. Particularly if  $h = 2$  and  $q = p$  prime we have  $F_2^2(\mathbb{Z}_p \times \mathbb{Z}_p) \geq p$ , but it is easy to establish that  $F_2^2(\mathbb{Z}_p \times \mathbb{Z}_p) = p$  [7]. A natural question to state is the following: Can we obtain a similar result, as the last one, on the group  $(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p, +)$ ? That is,

$$F_2^3(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p) \sim p^{3/2}?$$

Now, using Theorem 3.1, for integers  $d, g, N \geq 1$  and  $h \geq 2$  we know that

$$F_h(N^d, g) \leq F_h^d(N, g)$$

Particularly, if  $d = 2, h = 2$ , and  $g = 1$  we have that  $F_2^1(N^2) \leq F_2^2(N)$ , which implies that good constructions of Sidon sets on  $\mathbb{Z}$  give good lower bounds for Sidon sets on  $\mathbb{Z} \times \mathbb{Z}$ . Furthermore, an interesting work consists in to analyze the behavior of the difference  $F_2^2(N) - F_2^1(N^2)$  when  $N$  grows.



Finally, from Proposition 4.3 we can establish that  $F_2^2(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}) \geq q-2$ , which lead us to wonder if is it possible to state that  $F_2^2(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}) = q-1$ ?

**Acknowledgment.** We thank to COLCIENCIAS and Universidad del Cauca for the support to our research group “Algebra, Teoría de Números y Aplicaciones–ALTENUA ERM” under the projects 110356935047 and VRI–3744. We also thank to the anonymous referee for their helpful comments. This work is dedicated to the memory of Javier Cilleruelo (1961-2016).

### References

- [1] J. Bravo, D. Ruiz, and C. Trujillo, *Cardinality of sets associated to  $B_3$  and  $B_4$  sets*, Revista colombiana de matemáticas **46** (2012), no. 1, 27–37.
- [2] S. Chowla and A. Mian, *Solution of a problem of Erdős and Turán in additive–number theory*, Proc. Nat. Acad. Sci. India Series A **14** (1944), 3–4.
- [3] J. Cilleruelo, *Conjuntos de enteros con todas las diferencias distintas*, La Gaceta de la RSME **11** (2008), no. 1, 151–170.
- [4] ———, *Sidon sets in  $\mathbb{N}^d$* , Journal of Combinatorial Theory Series A **117** (2010), no. 7, 857–871.
- [5] G. Garcia, C. Trujillo, and J. Velasquez,  *$B_2^\pm[g]$  finite sets*, Journal Of Algebra, Number Theory And Applications **4** (2004), no. 3, 593–604.
- [6] S. Golomb and G. Gong, *The status of Costas arrays*, IEEE Transactions on Information Theory **53** (2007), no. 11, 4260–4265.
- [7] A. Gómez, D. Ruiz, and C. Trujillo, *Construcción de conjuntos de Sidon en dimensión dos*, XVIII Congreso Colombiano de Matemáticas, Universidad Industrial de Santander (Colombia), Julio 2011.
- [8] C. Gómez and C. Trujillo, *Una nueva construcción de conjuntos  $B_h$  modulares*, Matemáticas: Enseñanza Universitaria **19** (2011), no. 1, 53–62.
- [9] J. Gómez, *Construcción de conjuntos  $B_h[g]$* , Master thesis, Universidad del Valle, Colombia, 2011.
- [10] K. O’Bryant, *A complete annotated bibliography of work related to sidon sequences*, The electronic Journal of Combinatorics–Dynamic Surveys **11** (2004), 39.
- [11] L. Rackham and P. Šarka,  *$B_h$  sequences in higher dimensions*, The Electronic Journal of Combinatorics **17** (2010), no. 1, R35 (electronic), 15.

- [12] C. Trujillo, *Sucesiones de sidon*, Ph.D. thesis, Universidad Politécnica de Madrid, España, 1998.

(Recibido en abril de 2016. Aceptado en julio de 2016)

DEPARTAMENTO DE MATEMÁTICAS  
UNIVERSIDAD DEL CAUCA  
CALLE 5 No. 4-70  
POPAYÁN, COLOMBIA  
*e-mail:* [dfruiz@unicauca.edu.co](mailto:dfruiz@unicauca.edu.co)  
*e-mail:* [trujillo@unicauca.edu.co](mailto:trujillo@unicauca.edu.co)