**B**\(_h\) Sets as a Generalization of Golomb Rulers

CARLOS ANDRES MARTOS OJEDA\(^1\), LUIS MIGUEL DELGADO ORDOÑEZ\(^2\),
AND CARLOS ALBERTO TRUJILLO SOLARTE\(^2\)

\(^1\)Departamento de Matemáticas, Universidad del Cauca, Popayán 190003, Colombia
\(^2\)Doctorado en Ciencias Matemáticas, Universidad del Cauca, Popayán 190003, Colombia

Corresponding author: Carlos Andres Martos Ojeda (cmartos@unicauca.edu.co)

ABSTRACT A set of positive integers \(A\) is called a Golomb ruler if the difference between two distinct elements of \(A\) are different, equivalently if the sums of two elements are different (\(B_2\) set, Sidon set). An extension of this concept is to consider that the sum of \(h\) elements in \(A\) are all different, except for permutation of the summands, with \(h \geq 2\), in this case it is said that \(A\) is a set \(B_h\), the length of \(A\) is given by \(\ell(A) = \max A - \min A\). One problem associated with this type of set is that of the optimal dense \(B_h\) sets, that is, determining the greatest cardinal of a set \(B_h\) contained in the integer interval \([1,N]\), for this defines the function \(F_h(N)\). Another problem that can be associated is the optimally short \(B_h\) sets, that is, finding a shorter \(B_h\) set with \(m\) elements, for which the \(G_h(m)\) function is defined. In this paper we are going to prove that these two problems are inverse, that is, that the functions \(G_h(m)\) and \(F_h(N)\) have inverse relationships. Furthermore, the asymptotic behavior of the \(G_h(m)\) function is studied, obtaining some upper and lower bounds, we also obtain tables of \(B_3\) and \(B_4\) near-optimal up to \(m = 31\).

INDEX TERMS Golomb rulers, \(B_h\) set, intermodulation interference.

I. INTRODUCTION

Intermodulation interference is the combining of several signals in a nonlinear device, producing new, unwanted frequencies. The intermodulation between frequency components will form additional components such as harmonic signals in a nonlinear device, producing new, unwanted interference, formulated the following problems.

1) For any given \(m\), find integers \(a_1 < a_2 < \cdots < a_m\) so as to the equation \(a_r + a_i - a_j = a_u\) does not have different solutions from the trivial one.

2) For any given \(m\), find integers \(a_1 < a_2 < \cdots < a_m\) so as to the equation \(a_r + a_i - a_j = a_u\) doesn’t have different solutions from the trivial one.

Hence the need to study sets with the property that all the sums of two elements are different and sets with the property that all sums of three elements are different (\(B_3\) set).

A set of non-negative integers in which all the differences of two elements different or equivalently sums of two elements are distinct is called Golomb ruler; the elements of this ruler are called marks.

The Golomb rulers are important by their applications in different fields of engineering and communications, see [1], [3], [9]. Another application of Golomb Rulers is in the field of coding theory for find to optimal optical orthogonal Codes [19]. Sets of rulers are used to generate self-orthogonal codes that play an important role in communications [17], the optimal Golomb Rulers are used for the FWM Crosstalk Elimination in WDM Systems [20].

Definition 1: A Golomb ruler is a set of integers \(A = \{a_1, a_2, \ldots, a_m\}\) with \(a_1 < a_2 < \cdots < a_m\) in which for each positive integer \(d\) there are not more than one solution of the equation \(d = a_i - a_j\), where \(i > j\), its number of elements is called order and the largest distance between two elements...
of the ruler is called length, denoted \( \ell(A) \). So,
\[
\ell(A) = \max A - \min A = a_m - a_1.
\]

An example of a Golomb ruler \( A \) with order \( m = 15 \) and length \( \ell(A) = 151 \) is the set
\[
A = \{0, 4, 20, 30, 57, 59, 62, 76, 100, 111, 123, 136, 144, 145, 151\}.
\]

The concept of the Golomb ruler is invariant under linear applications.

**Proposition 2** (Linearity): If \( A = \{a_1, a_2, \ldots, a_m\} \) is a Golomb ruler, then the set
\[
x \cdot A + y := \{xa_1 + y, xa_2 + y, \ldots, xa_m + y\},
\]
is a Golomb ruler, for all \( x, y \in \mathbb{Z} \), with \( x \neq 0 \).

Since the concept of the Golomb ruler is invariant under translations, it is possible to assume that the minimum value is \( a_1 = 0 \) and the length is \( a_m \).

The fundamental problem in the study of the Golomb rulers is to find the shortest rulers for a certain number of marks; equivalently investigate the following function:
\[
G(m) := \min \{ \ell(A) : A \text{ is a Golomb ruler, } |A| = m \}.
\]

We say that a Golomb ruler of order \( m \) is optimal if it has the shortest length possible (optimally short). For example, the ruler given in (1) where \( m = 15 \) is a optimal Golomb ruler with length 151 and \( G(15) = 151 \). Currently, there are also optimal Golomb rulers where \( 2 \leq m \leq 27 \) marks \([8],[16]\) and there is an ongoing search for an optimal 28-marks rule. Dimitromanolakis \([7]\) proved computationally in 2002 that \( G(m) \leq m^2 \), for every \( m \leq 65000 \), and he conjectured that this is true for all integer \( m \).

In \([18]\), Rokicki and Dogon obtain near-optimally Golomb rules for values for \( m \) up to 40000, they use some new ideas and improve the existing algorithms.

We can find a trivial lower bound counting the number of distinct differences of a Golomb ruler with \( m \) elements, so
\[
G(m) \geq m(m - 1)/2.
\]

Some researchers achieved best the trivial lower bound, their results are the followings
- \( G(m + 1) \geq m^2 - 2m\sqrt{m} \), \([1]\).
- \( G(m) \geq m^2 - 2m\sqrt{m} + \sqrt{m} - 2 \), \([7]\).
- \( G(m) \geq m^2 - 2m\sqrt{m} - 1 - m\sqrt{m - 1} + \sqrt{m} - 1 \), \([4]\).

Atkinson et al. \([1]\) it is conjectured that for all \( m \) is possible that
\[
G(m) \geq m^2 - m\sqrt{m}.
\]

On the other hand in \([1]\) Atkinson et al. studied a generalization of Golomb ruler (when the sum of 3 elements in \( A \) are all different), these are called \( B_3 \) sets (for another generalization see \([13]-[15]\)), furthermore, this concept can be generalized for sums of \( h \) elements i.e. an integers set \( A = \{a_1, a_2, \ldots, a_m\} \), is called a \( B_h \) set, if the sum of \( h \) elements in \( A \) are all different, except for permutation of the summads, with \( h \geq 2 \). One problem associated with this type of sets is optimally dense \( B_h \) sets, that is, determining the greatest cardinal of a set \( B_h \) contained in the integer interval \([1, N]\), for this defines the function \( F_h(N) \). Another problem that can be associated is the optimally short \( B_h \) sets, that is, finding a shorter \( B_h \) set with \( m \) elements, for which the \( G_h(m) \) function is defined, in \([1]\) Atkinson et al. presented near-optimally short \( B_3 \) sets with \( m \leq 18 \) marks and in \([12]\) Lam and Duan presented optimal \( B_3 \) sets with \( m \leq 7 \) and \( B_4 \) with \( m \leq 6 \). In this paper we are going to prove a generalization of the results given \([7]\), i.e. that the functions \( G_h(m) \) and \( F_h(N) \) have inverse relationships. Furthermore, the asymptotic behavior of the \( G_h(m) \) function is studied, obtaining some upper and lower bounds.

In Section II, we introduce the concept of \( B_h \) set, we considered two fundamental problems about these sets and we present some properties, constructions, and known results. In section III we show that the maximal functions \( F_h(N) \) and \( G_h(m) \) have inverse relationships, generalizing the results of \([7]\). In Section IV, we present upper and lower bounds for the function \( G_h(m) \) and we generalize the results presented in \([22]\) for \( B_h \) sets and arbitrary module.

**II. GENERALIZED GOLOMB RULERS**

Now we present the formal definition of a \( B_h \) set.

**Definition 3**: Let \((G, +)\) be an abelian group, \( A \) be a subset of \( G \) and \( h \geq 2 \) an integer. \( A \) is a \( B_h \) set in \( G \) if the sums of \( h \) elements of \( A \) are all different i.e. for all \( x \in G \), the equation
\[
x = a_1 + a_2 + \cdots + a_h,
\]
with \( a_i \in A \), it has at most a single solution in \( A \), except for permutations of the summads.

If \( G = \mathbb{Z}_N \) the set of integers modulo \( N \), then \( A \) is called a modular \( B_h \) set. Notice that a modular \( B_h \) set is also a \( B_h \) set in \( \mathbb{Z} \), analogously we can define length, marks, order and the \( G_h(m) \) function.

**Lemma 4**: Let \( A = \{a_1, a_2, \ldots, a_m\} \) be a \( B_h \) set.
- If \( A \subset \mathbb{Z} \), then
  \[
x \cdot A + y := \{xa_1 + y, xa_2 + y, \ldots, xa_m + y\},
  \]
is a \( B_h \) set, for all \( x, y \in \mathbb{Z} \), with \( x \neq 0 \).
- If \( A \) is a modular \( B_h \) set in \( \mathbb{Z}_N \) then for \( x, y \in \mathbb{Z}_N \) with \( \gcd(x, N) = 1 \) the set
  \[
x \cdot A + y := \{xa_1 + y, xa_2 + y, \ldots, xa_m + y\},
  \]
is a \( B_h \) set in \( \mathbb{Z}_N \).
- If \( A \subset \mathbb{Z} \) with \( \ell(A) = a_m \), then \( A \) is a modular \( B_h \) set in \( \mathbb{Z}_N \), where \( N = ha_m + 1 \).

**A. TWO FUNDAMENTAL PROBLEMS**

The main problem is to find optimally dense and optimally short \( B_h \) set, i.e. finding answers to the following two optimization questions.

Let \( A \subset \mathbb{Z} \) be a \( B_h \) set and \( m, n \in \mathbb{Z}^+ \).
• What can we say about the shortest length of $B_h$ set $A$ such that $|A| = m$? In this case, $A$ is called optimally short.

• What can we say about the maximum number of elements that a $B_h$ set $A$ can have, with $A$ contained in the set of integers $[0, N - 1]$, where $[0, N - 1] := \{0, 1, \ldots, N - 1\}$? In this case $A$ is called optimally dense.

Now we present some descriptions of these two problems.

Problem 1 (Optimally Short $B_h$ sets): The main problem of the optimally short $B_h$ set is to estimate the function $G_h(m)$, where

$$G_h(m) := \min \{\ell(A) : |A| = m \text{ and } A \text{ is a } B_h \text{ set}\}.$$  

If $h = 2$, then $G_2(m) = G(m)$ and exact values for $1 < m < 27$ are known for this function. On the other hand, Caicedo, Martos and Trujillo proved in [4] that:

Theorem 5: If $A = \{a_i : 1 \leq i \leq m\}$ is a $B_h$ set such that

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

For $h = 3$, Atkinson, Santoro and Urrutia proved in [1] that:

Theorem 6: If $A = \{a_i : 1 \leq i \leq m\}$ is a $B_h$ set such that

$$G_3(m + 1) > \frac{10}{57}m^3.$$  

Furthermore, in [12] Lam and Duan find optimal $B_3$ sets with $m$ marks for $m \leq 7$ and $B_4$ for $m \leq 6$.

Problem 2 (Optimally Dense $B_h$ sets): This problem is related to the estimation of the following function:

$$F_h(N) := \max \{|A| : A \subseteq [1, N], A \text{ is a } B_h \text{ set}\}.$$  

For $h = 2$ Cilleruelo proved in [4], [5] that:

$$F_2(N) \leq N^{\frac{2}{3}} + N^{\frac{1}{2}} + 1.$$  

There is a trivial upper bound, it is given by:

$$F_h(N) < (h \cdot h!)^{\frac{1}{2}}.$$  

Bose and Chowla [2] conjecture that

$$\lim_{N \to \infty} \frac{F_3(N)}{\sqrt{N}} = 1.$$  

In the case of $h = 3$ and $h = 4$, in [11] it is proved that:

$$F_3(N) \leq \sqrt[3]{\frac{24}{5}}N + 2,$$

$$F_4(N) \leq \sqrt[4]{12N} + 3.$$  

In [11] it is mentioned that it has been Green proved that:

$$F_3(N) \leq \sqrt[3]{\frac{7}{2}}N(1 + o(1)),$$

$$F_4(N) \leq \sqrt[4]{7N}N(1 + o(1)).$$  

From where it can be deduced

$$\lim_{N \to \infty} \frac{F_3(N)}{\sqrt{N}} \leq \sqrt[3]{\frac{7}{2}}.$$  

B. CONSTRUCTIONS

Three optimal constructions for $B_h$ sets are known, these are the Bose-Chowla type, generalized Singer type, and Gómez-Trujillo type, we are going to quickly describe each one of them after they provide us with bounds for the extreme functions.

Let $F$ be a field, $E$ be an algebraic extension of degree $h$ on $F$, and $\alpha$ an algebraic element of degree $h$ on $F$, if $E^*$ is the multiplicative group of $E$, then, the set

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

is a $B_h$ set in $E^*$ see [10]. Now if $F$ is a finite field then $F = \mathbb{F}_q$, with $q$ prime power, $\alpha$ an algebraic element of degree $h$ on $\mathbb{F}_q$ and $\theta$ a primitive element of the extension field $\mathbb{F}_{q^h}$ on $\mathbb{F}_q$, the set

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

is a $B_h$ set in $(\mathbb{F}_{q^h}^*, *)$ with $q$ elements, see [10].

On the other hand, as $(\mathbb{F}_{q^h}^*, *)$ is a cyclic group of order $q^h - 1$ then

$$(\mathbb{F}_{q^h}^*, *) \cong (\mathbb{Z}_{q^h - 1}, +),$$  

considering the isomorphism

$$\log_\theta : (\mathbb{F}_{q^h}^*, *) \to (\mathbb{Z}_{q^h - 1}, +)$$

$$\theta^k \to \log_\theta(\theta^k) = k,$$

from where Bose and Chowla [2] proved that.

Theorem 7 (Bose-Chowla): The set

$$A(\alpha, \theta, q) = \log_\theta(\alpha + \mathbb{F}_q) := (\log_\theta(\alpha + a) : a \in \mathbb{F}_q),$$

is a $B_h$ set modulo $(q^h - 1)$ with $q$ elements.

Example 8: Let $\mathbb{F}_5$ be finite field, and $\theta = \alpha$ be a primitive root of the polynomial $x^3 + 3x + 2$ on $\mathbb{F}_5$. Then $\mathbb{F}_{5^3}$ is an extension field with degree 3 on $\mathbb{F}_5$ and the elements of $\mathbb{F}_{5^3}$ can be written as powers of $\theta$.

The set

$$\theta + \mathbb{F}_5 = \{\theta + 0, \theta + 1, \theta + 2, \theta + 3, \theta + 4\} = \{\theta, \theta^{103}, \theta^{119}, \theta^{14}, \theta^{34}\},$$

is a $B_3$ set in $\mathbb{F}_{5^3}$. Furthermore, by means of the isomorphism of the discrete logarithm, we have to

$$\log(\theta + \mathbb{F}_5) = \{1, 14, 34, 103, 119\},$$

is a $B_3$ set modulo 124 $= 5^3 - 1$.

The generalized Singer-type $B_h$ set construction [2] can be seen as a consequence of the Bose-Chowla-type construction.

Let $q$ be a prime power, $\mathbb{F}_{q^{h+1}}$ be a finite field with primitive element $\theta$ and $\alpha$ an algebraic element of degree $h + 1$ on $\mathbb{F}_q$. If $\alpha = \theta$, the set $\theta + \mathbb{F}_q$ is a set $B_{h+1}$ with $q$ elements in the multiplicative group of $\mathbb{F}_{q^{h+1}}$. By Theorem 7, we can obtain a
set $A(q, \alpha, \theta) = \log_\theta (\alpha + F_q)$ which is $B_{h+1}$ in $\mathbb{Z}_{q^{h+1} - 1}$ with $q$ elements.

Now, let $N_q = \frac{q^{h+1} - 1}{q - 1}$, and $B(q, \alpha, \theta) = A(q, \alpha, \theta)$ let’s consider the set

$$S := B(q, \theta) \mod N_q = \{a \mod N_q : a \in B(q, \theta)\},$$

in [2] Bose and Chowla proved that $S \cup \{0\}$ is a $B_h$ set in $(\mathbb{Z}_{N_q} + 1)$ with $q + 1$ elements.

**Theorem 9 (Singer generalized):** Let $q$ be a power prime and $h \geq 2$ an integer, there are $q + 1$ integers $a_1, a_2, \ldots, a_q, a_{q+1}$ such that all sums

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

with $1 \leq j_1 \leq j_2 \leq \cdots \leq j_h \leq q + 1$, are different modulus $\frac{q^{h+1} - 1}{q - 1}$.

**Example 10:** Let $\mathbb{F}_5$ be finite field, and $\theta = \alpha$ be a primitive root of the polynomial $x^3 + 3x + 2$ on $\mathbb{F}_5$.

The set $\log(\theta + \mathbb{F}) = \{1, 14, 34, 103, 119\}$ is a $B_3$ set modulus $124 = 5^2 - 1$ Bose type. Now let’s consider $S_0 = (B \bmod 124/4) \cup \{0\}$, then

$$S_0 = \{0, 1, 3, 10, 14, 26\},$$

is a $B_2$ set in $\mathbb{Z}_{31}$.

The Gómez-Trujillo construction presented in 2011 [10] can be seen as a generalization of the Ruzsa-type construction for the case $h = 2$. This construction consists of obtaining a set $B_h$ from a set $B_{h-1}$ of the Bose type.

**Theorem 11 (Gómez-Trujillo):** Let $(\mathbb{F}, +, \ast)$ be a field, $\alpha$ be an algebraic element of degree $h - 1$ on $\mathbb{F}$ and $\mathbb{F}(\alpha) = \mathbb{E}$ be a degree extension $h - 1$ on $\mathbb{F}$. The set

$$A := \{(a, \alpha + a) : a \in \mathbb{F} \text{ y } \alpha + a \in \mathbb{E}^\ast\},$$

is a $B_h$ set in $(\mathbb{F}, +) \times (\mathbb{E}, \ast)$.

If $\mathbb{F}$ is a finite field, i.e., $\mathbb{F} = \mathbb{F}_p$ with $p$ a prime number and $\mathbb{E} = \mathbb{F}_p^{\alpha}$ a extension field of degree $h - 1$, then

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

is a $B_h$ set in $\mathbb{Z}_p \times \mathbb{Z}_{p^h - 1}$ by Theorem 11. Furthermore, by the Chinese remainder Theorem we obtain a $B_h$ set modulo $p^h - p$ with $p$ elements, given by

$$\left(p^{h-1} \log_\alpha(\theta + a) - (p^{h-1} - 1)a : a \in \mathbb{Z}_p\right) \subset \mathbb{Z}_{p^h - p}.$$

**Example 12:** Let $p = 7$, $\theta$ be a primitive element on $\mathbb{F}_7$ with minimal polynomial $p(x) = 2x^2 + x + 3$, then by Theorem 9, the set

$$\theta + \mathbb{F}_7 = \{\theta, \theta + 1, \theta + 2, \ldots, \theta + 6\},$$

is a $B_2$ set in $\mathbb{F}_7^\ast$, then the set

$$B = \{(0, \theta), (1, \theta + 1), \ldots, (6, \theta + 6)\},$$

is a $B_3$ set in $(\mathbb{F}_7, +) \times (\mathbb{F}_7^\ast, \ast)$. Furthermore, the set

$$R = \{(0, \log_\theta(\theta)), (1, \log_\theta(\theta + 1)), \ldots, (6, \log_\theta(\theta + 6))\},$$

is a $B_3$ set in $(\mathbb{Z}_7, +) \times (\mathbb{Z}_{7 - 1}, +)$, then using the Chinese remainder theorem we obtain that

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

is $B_3$ set Gómez-Trujillo type, in $\mathbb{Z}_{336}$.

**III. RELATIONSHIPS BETWEEN MAXIMAL FUNCTIONS**

For the sets $B_2$ there is an inverse relationship between the functions $G(m)$ and $F_2(N)$, which were proved in 2002 by Dimitromanolakis [7]. In this section we prove a generalization of the results of [7] for the case of the sets $B_h$.

To find equality relations between the functions, let us assume that the exact value of $F_h(N)$ or $G_h(m)$ is known, from these values we will find some relations between them.

**Lemma 13:** If $n, m \in \mathbb{Z}$, then,

$$F_h(n) = m \Leftrightarrow \begin{cases} G_h(m) \leq n - 1 \\ G_h(m + 1) > n - 1 \end{cases}$$

**Proof:** If $F_h(n) = m$, then, the cardinal greatest of a $B_h$ set contained in $[1, n]$ is $m$, let $A$ with $|A| = m$ be the said set, then $\ell(A) \leq n - 1$, that is to say that $G_h(m) \leq n - 1$. Also, since $A \subset [0, n - 1]$ and this is the set $B_h$, greatest cardinal content in that interval, then $G_h(m+1) > n - 1$. The converse follows from the definition of the respective functions.

**Corollary 14:** If $m, n \in \mathbb{Z}$, then,

$$G_h(m) = n \Leftrightarrow \begin{cases} F_h(n) = m - 1 \\ F_h(n+1) = m \end{cases}$$

**Proof:** It follows easily from definitions and Lemma 13.

From the previous corollary we can deduce some exact values for the function $F_3(N)$ and $F_4(N)$ from the known ones for $G_3(m)$ and $G_4(m)$ given in [12] see Table 1.

**TABLE 1. Values for the functions $F_3(N)$ and $F_4(N)$.**

| $G_3(3)$ | $G_3(4)$ | $G_3(5)$ | $G_3(6)$ | $G_3(7)$ | $G_3(8)$ | $G_3(9)$ | $G_3(10)$ | $G_3(11)$ | $G_3(12)$ | $G_3(13)$ | $G_3(14)$ | $G_3(15)$ | $G_3(16)$ | $G_3(17)$ | $G_3(18)$ | $G_3(19)$ | $G_3(20)$ |
|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| 4         | 4        | 23       | 43       | 82       | 7         | 15       | 41       | 100      | 5        | 6         | 2        | 46       | 6         | 14       | 26       | 44       | 64       |
| $P_3(4)$  | $P_3(5)$  | $P_3(6)$  | $P_3(7)$  | $P_3(8)$  | $P_3(9)$  | $P_3(10)$ | $P_3(11)$ | $P_3(12)$ | $P_3(13)$ | $P_3(14)$ | $P_3(15)$ | $P_3(16)$ | $P_3(17)$ | $P_3(18)$ | $P_3(19)$ | $P_3(20)$ |
| 2         | 15       | 5        | 6        | 7        | 82       | 9        | 100      | 14       | 26       | 44       | 64       | 2         | 5        | 6         | 26       | 44       | 64       |
| $P_4(5)$  | $P_4(6)$  | $P_4(7)$  | $P_4(8)$  | $P_4(9)$  | $P_4(10)$ | $P_4(11)$ | $P_4(12)$ | $P_4(13)$ | $P_4(14)$ | $P_4(15)$ | $P_4(16)$ | $P_4(17)$ | $P_4(18)$ | $P_4(19)$ | $P_4(20)$ |
| 3         | 2        | 4        | 5        | 6        | 7        | 82       | 9        | 100      | 14       | 26       | 44       | 64       | 2         | 5        | 6         | 26       | 44       | 64       |

On the other hand, in case of knowing exact values of either of the two functions, the two previous results give us information about the other function, although in some sense it is better to know exact values of $G_h(m)$ as it provides exact information about $F_h(n)$. Whereas if the exact value of $F_h(n)$ is known, it provides a bound for $G_h(m)$.

**Lemma 15:** Let $n, m$ be positive integers, if $F_h(n) > m$, then, $G_h(m) \leq n - 1$.

**Proof:** If $F_h(n) > m$, suppose that $F_h(n) = m'$ for some $m' > m$, therefore

$$G_h(m') \leq n - 1.$$
by Lemma 13. On the other hand we know that $G_h(m)$ is increasing, it follows that $G_h(m') \geq G_h(m)$ and by (5) we must have $G_h(m) \leq n - 1$.

**Lemma 16:** Let $n, m$ be positive integers, if $F_h(n) < m$, then $G_h(m) \geq n - 1$.

**Proof:** Analogous to Lemma 15.

Using this lemmas, we prove that.

**Theorem 17:** Suppose $l(n)$ and $u(n)$ are well-defined and there are inverse functions $l^{-1}(n)$ and $u^{-1}(n)$ inside an integer interval $I \subset \mathbb{N}$. If

$$l(n) < F_h(n) < u(n),$$

then

$$u^{-1}(m) \leq G_h(m) + 1 \leq l^{-1}(m).$$

**Proof:** Suppose that $F_h(n) > l(n)$, by Lemma 15 $G_h(l(n)) \leq n - 1$ therefore:

$$G_h(l(n)) \leq l^{-1}(l(n)) - 1,$$

from where $G_h(m) + 1 \leq l^{-1}(m)$.

On the other hand, if $F_h(n) < u(n)$ then $G_h(u(n)) \geq n - 1$ by Corollary 16, so we have

$$G_h(u(n)) \geq u^{-1}(u(n)) - 1,$$

from where $G_h(m) + 1 \geq u^{-1}(m)$. In consequence

$$u^{-1}(m) \leq G_h(m) + 1 \leq l^{-1}(m).$$

Let us now consider the case in which we know some bound for $G_h(m)$ and see what results can be obtained for $F_h(n)$.

**Lemma 18:** Let $n, m$ be positive integers, if $G_h(m) < n$, then, $F_h(n) \geq m$.

**Proof:** If $G_h(m) < n$, there is a $B_h$ set $A = \{a_1, \ldots, a_m\}$ with $|A| = m$ and $A \subset [0, n]$, then, by definition $F_h(n) \geq m$.

**Lemma 19:** Let $m, n$ be positive integers, if $G_h(m) > n$, then, $F_h(n) \leq m$.

**Proof:** If $G_h(m) > n$ then the maximum number of integers that can be selected to form a $B_h$ set contained in $[1, n + 1]$ is less than $m$. Hence $F_h(n + 1) < m$ and since $F_h(n)$ is increasing function, then $F_h(n) \leq m$.

Now suppose that $G_h(m)$ has upper and lower bounds.

**Theorem 20:** Suppose $l(n)$ and $u(n)$ are well-defined and there are inverse functions $l^{-1}(n)$ and $u^{-1}(n)$ inside an integer interval $I \subset \mathbb{N}$. If

$$l(m) < G_h(m) < u(m),$$

then

$$u^{-1}(n) \leq F_h(n) \leq l^{-1}(n).$$

**Proof:** If $G_h(m) > l(m)$, then $F_h(l(m)) \leq m$ by Lemma 19, hence:

$$F_h(l(m)) \leq l^{-1}(l(m)),$$

from where it follows that $F_h(n) \leq l^{-1}(n)$.

On the other hand, if $G_h(m) < u(m)$, then $F_2(u(m)) \geq m$ by Lemma 18, hence:

$$F_h(u(m)) \geq u^{-1}(u(m)),$$

from where it follows that $F_h(n) \geq u^{-1}(n)$. Therefore

$$u^{-1}(n) \leq F_h(n) \leq l^{-1}(n).$$

The theorems 17 and 20 are important because, in addition to proving the inverse relationship between the two problems, it allows finding upper and lower bounds for the function $G_h(m)$ from the known bounds for $F_h(n)$ , this is done in the next section.

**IV. UPPER AND LOWER BOUNDS**

In this section, we are going to properly construct a short $B_h$ set with $p$ elements and thus find an upper bound for $G_h(p)$ with $p$ prime. On the other hand, to find a lower bound we are going to make use of the inverse relationship that exists between the functions $G_h(m)$ and $F_h(n)$ presented in Theorem 20.

With the constructions of the Theorems 9, 7 and 11 we can obtain upper and lower bounds for the functions $G_h(m)$ if $m$ is a prime number and $F_h(N)$ see Table 2.

**TABLE 2. Bounds for the functions $G_h(m)$ and $F_h(N)$ from known constructions.**

| Singer generalized | $F_h\left(\frac{q^{n+1} - 1}{q - 1}\right) \geq q + 1.$ | $G(q + 1) \leq \frac{q^{n+1} - 1}{q - 1}$. |
|--------------------|--------------------------------------------------|---------------------------------------------|
| Bose-Chowla | $F_h(q^{n} - 1) \geq q$ | $G(q) < q^n - 1$. |
| Gómez-Trujillo | $F_h(p^{h} - p) \geq p$ for $h \geq 3$. | $G(p^{h} - 1) \leq p^{h} - p$ for $h \geq 3$. |

**A. AN UPPER BOUND**

Using a technique initially presented by Zhang [22], where it is allowed to construct Golomb rulers with a suitable length from modular rulers, we can improve the upper bound for the function $G_h(m)$ presented in Theorem 27. In his paper, Zhang only considers Golomb rulers obtained from Bose construction. In this paper, we generalize the results presented in [22] for $B_h$ sets and arbitrary modules.

To find an upper bound of the function $G_h(m)$ we must build a $B_h$ set with $m$ marks and $\ell(A) = w$. In this case, $G_h(m) \leq w$.

**Definition 21:** Let $A = \{a_1, a_2, \ldots, a_m, a_{m+1}\}$ be a $B_h$ set with $m + 1$ marks and $1 = a_1 < a_2 < \cdots < a_{m+1}$. We define $D(m)$ by

$$D(m) := \max\{a_{i+1} - a_i : 1 \leq i \leq m\}.$$

Note that there are, at least $m$ distinct consecutive differences because $A$ is a $B_h$ set, so

$$D(m) \geq m.$$
Lemma 22: If \( m \) is a positive integer and \( A = \{a_1, \ldots, a_m\} \) is a \( B_h \) set modulo \( N \), with \( a_1 = 1 \), then
\[
\overline{A} = A \cup \{N + 1\},
\]
is a \( B_h \) set in \( \mathbb{Z} \).

**Proof:** Let
\[
\overline{A} = A \cup \{N + 1\} = \{1, a_2, \ldots, a_m, N + 1\},
\]
without loss of generality suppose that two sums of \( h \) elements coincide, i.e.
\[
\sum_{j=1}^{h} a_{i_j} = \left( \sum_{k=1}^{h-1} a_{i_k} \right) + (N + 1),
\]
with \( \{a_{i_j}\}_{j=1}^{h} \neq \{a_{i_k}\}_{k=1}^{h-1} \) \( \forall 1 \leq j, k \leq h \), then
\[
\sum_{j=1}^{h} a_{i_j} \equiv \left( \sum_{k=1}^{h-1} a_{i_k} \right) + 1 \mod N,
\]
that is
\[
\sum_{j=1}^{h} a_{i_j} \equiv \left( \sum_{k=1}^{h-1} a_{i_k} \right) + a_1 \mod N,
\]
which is not possible because \( A \) is supposed to be a \( B_h \) set modulo \( N \), therefore \( \overline{A} \) is a \( B_h \) set in \( \mathbb{Z} \).

Lemma 23: If \( m \) is a positive integer,
\[
A = \{1, a_2, \ldots, a_m\}
\]
is a \( B_h \) set modulo \( N \) and
\[
\overline{A} = \{1, a_2, \ldots, a_m, a_{m+1} = N + 1\}
\]
then for all \( i \) with \( 1 \leq i \leq m \),
\[
B = \{a_{m+1} = a_1 + N, a_2 + N, \ldots, a_i + N, a_{i+1}, \ldots, a_m\},
\]
is a \( B_h \) set in \( \mathbb{Z} \).

**Proof:** Reasoning by contradiction, without loss of generality, suppose that there are two sums of \( h \) elements that coincide as follows:
\[
\left( \sum_{j=1}^{h} a_{i_j} \right) = \left( \sum_{k=1}^{h-1} a_{i_k} \right) + (a_i + N),
\]
con \( \{a_{i_j}\}_{j=1}^{h} \neq \{a_{i_k}\}_{k=1}^{h-1} \) \( \forall 1 \leq j, k \leq h \), then
\[
\left( \sum_{j=1}^{h} a_{i_j} \right) \equiv \left( \sum_{k=1}^{h-1} a_{i_k} \right) + a_i \mod N,
\]
which cannot be since by hypothesis \( A \) is a \( B_h \) modulo \( N \), therefore \( B \) is a \( B_h \) set in \( \mathbb{Z} \).

Lemma 24: If \( m \) is a positive integer and \( A = \{a_1, \ldots, a_m\} \) is a \( B_h \) set with \( m \) marks, then \( A - w = \{a_i - w : a_i \in A\} \) is a \( B_h \) set, with \( w \leq a_1 \).

**Proof:** It follows from the translation properties of the \( B_h \) sets.

With these lemmas, a \( B_h \) set of length \( N - D(m) - 1 \) can be constructed as shown in the following result.

**Theorem 25:** If \( A = \{1, a_2, \ldots, a_m\} \) is a \( B_h \) set modulo \( N \) and
\[
\overline{A} = \{1, a_2, \ldots, a_m, a_{m+1} = N + 1\},
\]
then for some \( t, 1 \leq t \leq m \) and \( w = a_{t+1} - 1 \),
\[
B = \{1, b_2, \ldots, b_m = N + 1 - (a_{t+1} - a_1)\},
\]
is a \( B_h \) set, where
\[
b_i = \left\{ \begin{array}{ll}
a_{i+t} - w, & 1 \leq i \leq m - t, \\
a_{i+t-m} + N - w, & m - t < i \leq m.
\end{array} \right.
\]

**Proof:** It follows from Lemmas 22, 23 and 24.

**Example 26:** Let \( A = \{1, 70, 72, 88, 195, 224, 306\} \) a \( B_3 \) set in \( \mathbb{Z}_{342} \) and \( \overline{A} = \{1, 70, 72, 88, 195, 224, 306, 343\} \).

The greatest difference of consecutive elements of \( \overline{A} \) is \( a_5 - a_4 = 195 - 88 = 107 \), from where \( a_{t+1} = a_5 = 195 \) and \( w = a_{t+1} - 1 = 194 \), then by Theorem 25, The set
\[
b_i = \left\{ \begin{array}{ll}
a_{i+4} - 194, & 1 \leq i \leq 3, \\
a_{i+4} + 342 - 195, & 3 < i \leq 7.
\end{array} \right.
\]
is a \( B_3 \) set, i.e. \( B = \{1, 30, 112, 148, 217, 219, 235\} \) is a \( B_3 \) set, where \( \ell(B) = 234 = N = (a_5 - a_4) - 1 = 342 - 107 \).

Notice that, the set \( B \), constructed in the previous theorem, has length
\[
\ell(B) = N - (a_{t+1} - a_t) - 1,
\]
also if we take the maximum of the consecutive differences \( (a_{t+1} - a_t) \) in \( \overline{A} \), that is
\[
D(m) := \max\{a_{i+1} - a_i : 1 \leq i \leq m\},
\]
where \( A = \{1, a_2, \ldots, a_m\} \) is a \( B_h \) set modulo \( N \), with the previous theorem we can find a set \( B \) which is \( B_h \) set and has length
\[
\ell(B) = N - D(m) - 1.
\]
But counting the consecutive differences of a set \( \overline{A} \) of \( m + 1 \) elements we can see that \( D(m) \geq m \), so
\[
\ell(B) = N - m - 1
\]
would therefore have a higher bound for \( G_h(m) \) given by:
\[
G_h(m) \leq N - m - 1. \quad (6)
\]

As a consequence of (6) and the constructions of \( B_h \) sets, we have.

**Theorem 27:** Let \( p \) be a prime number, \( q \) be a prime power, we have:
1) \( G_h(p) \leq p^h - 2p, \) \( \text{con} \ h \geq 3, \)
2) \( G_h(q + 1) \leq \frac{q^{h+1} - q}{q - 1} - q, \)
3) \( G_h(q) \leq q^h - q - 1. \)
Proof: By Gómez-Trujillo construction, we have a $B_h$ set with $q$ marks, modulo $q^h - q$, from Theorem 25 we have a set $B$, where $B$ is a $B_h$ set and $\ell(B) = q^h - q - D(q)$, therefore

$$G_g(q, q) \leq q^h - 2q.$$  

Analogously we can now prove 2 and 3, with Singer generalized an Bose-Chowla constructions.

We can now rephrase this theorem for $h = 3$.

**Corollary 28:** Let $p$ be a prime number, $q$ be a prime power, then we have:

1. $G_3(p) \leq p^3 - 2p$,
2. $G_3(q) \leq q^3 - q - 1$,
3. $G_3(u) \leq u^3 - 2u^2 + u + 1$, if $u = q + 1$.

And for $h = 4$ we can have.

**Corollary 29:** Let $p$ be a prime number, $q$ be a prime power, then we have:

1. $G_4(p) \leq p^4 - 2p$,
2. $G_4(q) \leq q^4 - q - 1$,
3. $G_4(u) \leq u^4 - 3u^3 + 4u^2 - 3u + 1$, if $u = q + 1$.

Remark: The upper bound given in Theorem 27, improves the known upper bounds for the function $G_{3}(m)$ . To obtain a new upper bound different from the one given in (6) it is necessary to construct a $B_h$ sets with $m$ elements in a suitable module, the smaller the modulo is the better the upper bound will be. An interesting question arises here, what is the smallest modulo $N$ in which a $B_h$ set with $m$ elements may be contained?

**Definition 30:** $v_{y,h}(m)$ is defined by the smallest $N$, where there is a $B_h$ set $A$ with $m$ marks and $A \subseteq \mathbb{Z}_N$, i.e.

$$v_{y,h}(m):=\min\{N\in\mathbb{N} : A \text{ is a } B_h \text{ set in } \mathbb{Z}_N \text{ and } |A|=m\}.$$  

If $h \geq 3$, exact values are not known for this function, for $h = 2$ values are known in The Online Encyclopedia of Integer Sequences sequence A004136. So it is important to study its asymptotic behavior and/or it is upper and lower bounds. On the other hand, note that the upper bound given in (6), can be expressed as

$$G_{h}(m) \leq v_{y,h}(m) - m.$$  

In Lemma 4 we proved that every $B_h$ set in $\mathbb{Z}$ with $m$ elements is a $B_h$ sets in $\mathbb{Z}_N$, where $N = ha_0 + 1$. So we can prove that

$$v_{y,h}(m) \leq hG_{h}(m) + 1.$$  

**B. A LOWER BOUND**

To find a lower bound of the function $G_{h}(m)$, we are going to use the inverse relationship between the functions $F_h(n)$ and $G_{h}(m)$ given in Theorem 20. In the following theorem, we obtain a lower bound for $G_{h}(m)$ using a known upper bound for $F_h(N)$.

**Theorem 31:** Let $m$ be a positive integer, then

$$G_{h}(m) \geq \frac{m^h}{hh!} - 1.$$  

**Proof:** We know that $F_h(n) < (h \cdot h!n)^{\frac{1}{2}}$, if

$$u(n) = (h \cdot h!n)^{\frac{1}{2}},$$

then $u^{-1}(n) = \frac{n}{hh!}$, therefore by Theorem 17 we have the result

Now for the case $h = 3$ we are going to use an upper bound given in [11] for the function $F_3(n)$.

**Theorem 32:** Let $m$ be a positive integer, then

$$G_3(m) \geq \frac{5}{24}m^3 - \frac{15}{12}m^2 + \frac{5}{2}m - \frac{8}{3}.$$  

**Proof:** We know by 3 that $F_3(n) \leq \frac{3\sqrt{24}}{5}n + 2$, Let

$$u(n) = \frac{n}{\sqrt{24}} \geq \frac{n}{\sqrt{5}},$$

then there is $u^{-1}(n)$ and its given by

$$u^{-1}(n) = \frac{5}{24}(n - 2)^3,$$

then by the Theorem 17 we have

$$G_3(m) \geq \frac{5}{24}(m - 2)^3 - 1,$$

from which the desired result is obtained.

The lower bound obtained in Theorem 32 represents an improvement for large values of $m$, with respect to the bound given by Atkinson et al. [1], which is given by $G_3(m + 1) \geq \frac{10}{57}m^3$. Indeed, it can be observed that starting from $m = 37$, the bound of the previous theorem is better than that given by Atkinson, Santoro and Urrutia.

For $h = 4$ we have.

**Theorem 33:** Let $m$ be a positive integer, then

$$G_4(m) \geq \frac{1}{12}m^4 - m^3 + \frac{9}{2}m^2 - 9m + \frac{5}{4}.$$  

**Proof:** We know by 4 that $F_4(n) \leq \sqrt[3]{12n} + 3$, let

$$u(n) = \sqrt[3]{12n} + 3,$$

then there is $u^{-1}(n)$ and is given by

$$u^{-1}(n) = \frac{1}{12}(n - 3)^4,$$

then by Theorem 17 we have

$$G_4(m) \geq \frac{1}{12}(m - 3)^4 - 1,$$

from where the desired result is obtained.

**V. CONCLUSION**

In this paper we find inverse relationships between the functions $F_h(N)$ and $G_{h}(m)$ generalizing the results of [7]. Additionally, in this paper, we make a study of the asymptotic behavior of the function $G_{h}(m)$ obtaining an upper and lower bound. On the other hand, some questions that can be addressed in future work, which we consider interesting to approach the following problems.
An inverse relationship is demonstrated between the functions \( F_h(n) \) and \( G_h(m) \), results that generalize those given by Dimitromanolakis in [7]. Can these results be used to improve the existing bounds? Can the bounds of the functions be improved?

\[
\lim_{N \to \infty} \frac{F_h(N)}{N^{1/h}}
\]

- To study the asymptotic behavior of the function \( v_{\delta,g}(m) \) with \( g > 1 \) and obtain new optimal bounds.
- To consider analogous problems for the modular case and for sums sets.
APPENDIX

ANOTHER NUMERICAL RESULTS

In [1] Atkinson et al. obtained the suboptimal $B_3$ sets to $m = 18$ and in [12] Lam and Duan presented optimal $B_3$ sets to $m = 7$ and $B_4$ sets to $m = 6$. Using the constructions of $B_6$ sets Singer Generalized(SG), Bose-Chowla(BC) and Gómez-Trujillo(GT), truncating and the Lemma 4, we have found, as shown in Table 3 and Table 4, the suboptimal $B_3$ and $B_4$ sets for $m < 31$. In these tables we present the construction used and the prime number or prime power used.

ACKNOWLEDGMENT

The authors would like to thank the Universidad del Cauca.

REFERENCES

[1] M. Atkinson, N. Santoro, and J. Urrutia, “Integer sets with distinct sums and differences and carrier frequency assignments for nonlinear repeaters,” IEEE Trans. Commun., vol. COM-34, no. 6, pp. 614–617, Jun. 1986.

[2] R. C. Bose and S. Chowla, “Theorems in the additive theory of numbers,” Commentarii Math. Helvetici, vol. 37, no. 1, pp. 141–147, Dec. 1962.

[3] W. C. Babcock, “Intermodulation interference in radio systems,” Bell Syst. Tech. J., vol. 32, no. 1, pp. 63–73, Jan. 1953.

[4] Y. Caicedo, C. A. Martos, and C. A. Trujillo, “g4g-Golomb rulers,” Revista Integración, vol. 33, no. 2, pp. 161–172, 2015.

[5] J. Cilleruelo, “Sidon sets in $\mathbb{Z}_n$,” J. Combination Theory A, vol. 117, no. 7, pp. 857–871, 2010.

[6] D. F. Daza, C. A. Trujillo, and F. A. Benavides, “Sidon sets and $C_3$-saturated graphs,” 2019. arXiv:1810.05262. [Online]. Available: https://arxiv.org/abs/1810.05262

[7] A. Dimitromanolakis, “Analysis of the Golomb ruler and the Sidon set problems, and determination of large, near-optimal Golomb rulers,” M.S. thesis, Dept. Electron. Comput. Eng., Tech. Univ. Crete, Chania, Greece, Jun. 2002.

[8] A. Dollas, W. T. Rankin, and D. McCracken, “A new algorithm for Golomb ruler derivation and proof of the 19 mark ruler,” IEEE Trans. Inf. Theory, vol. 44, no. 1, pp. 374–382, Jan. 1998.

[9] R. J. F. Fang and W. A. Sandrin, “Carrier frequency assignment for non-linear repeaters,” Comsat Tech. Rev., vol. 7, no. 1, pp. 227–245, 1977.

[10] A. Dimitromanolakis, “Analysis of the Golomb ruler and the Sidon set problems, and determination of large, near-optimal Golomb rulers,” M.S. thesis, Dept. Electron. Comput. Eng., Tech. Univ. Crete, Chania, Greece, Jun. 2002.

[11] J. P. Robinson, “Optimum Golomb rulers,” IEEE Trans. Comput., vol. C-28, no. 12, pp. 943–949, Dec. 1979.

[12] T. Rokicki and G. Dogon, “Larger Golomb rulers,” to be published. [Online]. Available: https://www.gathering4garden.org/g4g12gift/Rokicki_Dogon_Larger_Golomb_Rulers.pdf

[13] S. Bansal, “A comparative study of nature-inspired metaheuristic algorithms in search of near-to-optimal Golomb rulers for the FWM crosstalk elimination in WDM systems,” Appl. Artif. Intell., vol. 33, no. 14, pp. 1199–1265, Dec. 2019.

[14] J. Singer, “A theorem in finite projective geometry and some applications to number theory,” Trans. Amer. Math. Soc., vol. 43, no. 3, pp. 377–385, 1948.

[15] Z. Zhang, “Finding finite $B_2$-sequences with larger $m - a_2$, Math. Comput., vol. 53, no. 207, pp. 403–414, 1994.