Revista Integración
Escuela de Matemáticas
Universidad Industrial de Santander
Vol. 33, No. 2, 2015, pág. 161–172

g-Golomb Rulers

Yadira Caicedo[a*], Carlos A. Martos[b], Carlos A. Trujillo[b]

[a]Universidad del Tolima, Departamento de Matemáticas y Estadística, Ibagué, Colombia.

[b]Universidad del Cauca, Departamento de Matemáticas, Popayán, Colombia.

Abstract. A set of positive integers A is called a g-Golomb ruler if the difference between two distinct elements of A is repeated at most g times. This definition is a generalization of the Golomb ruler ($g = 1$). In this paper we construct g-Golomb ruler from Golomb ruler and we prove two theorems about extremal functions associated with this sets.
Keywords: Sidon sets, B_2 sets, Golomb ruler.
MSC2010: 11B50, 12E20, 20K01, 20K30.

Reglas g-Golomb

Resumen. Se dice que un conjunto de enteros positivos A satisface la regla g-Golomb si la diferencia entre dos elementos distintos de A se repite a lo más g veces. Esta definición es una generalización de las reglas de Golomb ($g = 1$). En este artículo construimos reglas g-Golomb a partir de reglas Golomb y demostramos dos teoremas sobre las funciones extremas asociadas con estos conjuntos.
Palabras clave: Conjuntos de Sidon, conjuntos B_2, reglas Golomb.

1. Introduction

A Golomb ruler is a set of non-negative integers with the property that all the non-zero differences of two elements in the set are distinct. The elements of the ruler are called marks.

The Golomb rulers were first discovered by W.C. Babcock in 1950 when he was investigating the intermodulation distortion, while he analyzed the positioning of radio channels in the frequency spectrum seeking to eliminate the third and fifth order interferences. However, the Golomb rulers derive their name from Professor Solomon W. Golomb, one of their greatest pioneers, who studied their construction at relation to combinatorics, coding theory and communications, by using finite field theory.

[*] E-mail: nycaicedob@ut.edu.co
Received: 31 July 2015, Accepted: 10 November 2015.
To cite this article: Y. Caicedo, C.A. Martos, C.A. Trujillo, g-Golomb, *Rev. Integr. Temas Mat.* 33 (2015), No. 2, 161–172.

Definition 1.1. A Golomb ruler is a set of integers $A = \{a_1, a_2, \cdots, a_m\}$, with the property that for each positive integer d there exists at most one solution of the equation $d = a_i - a_j$, for $i > j$.

Given a Golomb ruler A, its number of elements is called *order* and the largest distance between two elements of the ruler is called *length*, denoted $\ell(A)$; this is:

$$\ell(A) = \max A - \min A,$$

where $\max A := \max\{a_1, \dots, a_m\}$ and $\min A := \min\{a_1, \dots, a_m\}$.

An example of a Golomb ruler A with order $m = 15$ and length $\ell(A) = 151$ is the set

$$A = \{0, 4, 20, 30, 57, 59, 62, 76, 100, 111, 123, 136, 144, 145, 151\}. \tag{1}$$

As the concept of Golomb ruler is invariant under translations, it is possible to consider the first element or minimum value of the ruler equal to zero. The following result, which proof is based on the former definition, shows that the concept of Golomb ruler is invariant under linear applications.

Proposition 1.2 (Linearity). *Let $A = \{a_1, a_2, \cdots a_n\}$ be a Golomb ruler; then, the set $x \cdot A + y = \{xa_1 + y, xa_2 + y, \cdots xa_n + y\}$ is also a Golomb ruler, for all $x, y \in \mathbb{Z}$, with $x \neq 0$.*

1.1. Optimal Golomb rulers

We say that a Golomb ruler is optimal of order m if it has the shortest possible length for a given number of marks m (optimally short). For example, the ruler given in (1) for $m = 15$ is a optimal Golomb ruler with length 151.

Currently, we know optimal rulers up to 27 marks (February 2014) and there is an ongoing search for an optimal 28-marks ruler.

The fundamental problem in the study of the Golomb rulers is to find the shortest rulers for a certain number of marks; that is, to investigate the following function:

$$G(m) := \min\{\ell(A) : A \text{ is a Golomb ruler}, |A| = m\}.$$

As mentioned above, so far we know the exact values of $G(m)$ for $1 \leq m \leq 27$ marks, and we also have some prospects for optimal rulers to values from m up to 150.

A. Dimitromanolakis [4] proved computationally in 2002 that $G(m) \leq m^2$, for all $m \leq 65000$, and he conjectured that that this is true for every integer m.

We can find a trivial lower bound by counting the number of distinct differences of a Golomb ruler with m elements; so, $G(m) \geq \frac{1}{2}m(m-1)$.

Some researchers succeeded in improving the trivial lower bound, having the following results.

- $G(m) \geq m^2 - 2m\sqrt{m}$ (M.D. Atkinson, N. Santoro y J. Urrutia [1]).
- $G(m) \geq m^2 - 2m\sqrt{m} + \sqrt{m} - 2$ (A. Dimitromanolakis [4]).

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

1.2. g-Golomb Rulers

It is important to consider a generalization of the Golomb ruler concept, on account of a comment made in the article [1] by M.D. Atkinson and others, in which distances between each pair of marks of the ruler can be repeated up to g times.

In order to define these new rulers, we will mention some concepts before.

Definition 1.3. Let G be an additive abelian group, A, B subsets of G. The functions of representation with domain the group G and co-domain the non-negative integers, are defined by

$$R_{A-B}(x) := |\{(a,b) \in A \times B : \, a - b = x\}|, \tag{2}$$

$$R_{A+B}(x) := |\{(a,b) \in A \times B : \, a + b = x\}|, \tag{3}$$

for all $x \in G$.

Let us note that the function representation counts the number of times in which x can be represented as a difference of an element of A with an element of B. When $B = A$, we have the concept of a g-Golomb ruler as follows.

Definition 1.4. A g-Golomb ruler or $B_2^- \, [g]$ set is a set A of integers such that

$$R_{A-A}(x) \leq g, \text{ for all } x \in \mathbb{Z}, \, x \neq 0.$$

Thus, if $g = 1$ a 1-Golomb ruler or $B_2^- \, [1]$ set is a Golomb ruler, also called Sidon set.

The following examples show 2-Golomb and 3-Golomb rulers, respectively:

$$A_1 = \{0, 1, 3, 8, 10, 14, 20, 25, 28, 29\},$$

$$A_2 = \{0, 1, 2, 5, 8, 11, 13, 15, 19, 20\}.$$

The corresponding extension of the function $G(m)$ related to a g-Golomb ruler is the following:

$$G(g, m) := \min \{\ell\,(A) : |A| = m \text{ and } A \text{ is a } g\text{-Golomb ruler}\}.$$

The descriptions below are two problems related to the behavior of this function.

Problem 1. Optimally short g-Golomb rulers: The main problem of the optimally short g-Golomb rulers is to estimate the function $G(g, m)$ and study the $\lim\limits_{m \to \infty} \frac{G(g,m)}{m^2}$.

Problem 2. Optimally dense g- Golomb rulers: The main problem of the optimally dense g-Golomb rulers is to estimate the function

$$F_2^-(g, n) := \max \{|A| : A \subseteq [1, n] \, , \text{ A is a } g\text{-Golomb ruler}\},$$

where $[1, n] := \{1, 2, \ldots, n\}$ and study the $\lim\limits_{m \to \infty} \frac{F_2^-(g,n)}{(gn)^{1/2}}$.

When we consider the case $g = 1$, $G(1, m) = G(m)$, and for this function we know exact values up to $m = 27$; we also know $G(m) \leq m^2$ up to $m = 65000$ and $G(m) \geq m^2 + 2m\sqrt{m-1} - \frac{m}{\sqrt{m-1}} + \sqrt{m} - 1$ (Corollary 2.9). Also, we know that $F_2^-(1, n) = F_2(n)$, and we know that $F_2(n) \leq n^{\frac{1}{2}} + n^{\frac{1}{4}} + \frac{1}{2}$, [3].

2. Additive energy

In this section we present the concept of additive energy between two sets and some properties which allow us to estimate the functions $G(g,m)$ and $F_2^-(g,n)$. We obtain a lower bound for the function $G(g,m)$, so when $g=1$ this bound is better than the lower bound given by A. Dimitromanolakis [4] to the function $G(m)$. In the case of the function $F_2^-(g,n)$, we prove through a different method the upper bound given in [11], which generalizes the bound of Lindström [6], who uses other arguments in order to demonstrate that $F_2^-(g,n) \leq (gn)^{1/2} + (gn)^{1/4} + 1$.

Definition 2.1. Let G be a finite Abelian group, A, B subsets of G. The *additive energy* between A and B, denoted $E(A,B)$, is defined as

$$E(A,B) := |\{(a,a',b,b') \in A \times A \times B \times B : \ a+b = a'+b'\}|.$$

When $A=B$, we write $E(A)$ instead of $E(A,A)$.

From the definition of additive energy, it is easy to see that

$$E(A,B) = |\{(a,a',b,b') \in A \times A \times B \times B : \ a-b' = a'-b\}|,$$

$$E(A,B) = |\{(a,a',b,b') \in A \times A \times B \times B : \ a-a' = b'-b\}|.$$

The following lemma show the relationship between additive energy and the representative functions [10].

Lemma 2.2. *Let G be an additive Abelian group, A, B subsets of G. We have the following identities*

$$E(A,B) = \sum_{x \in A+B} R_{A+B}^2(x), \tag{4}$$

$$E(A,B) = \sum_{y \in A-B} R_{A-B}^2(y), \tag{5}$$

$$E(A,B) = \sum_{z \in (A-A)\cap(B-B)} R_{A-A}(z)\, R_{B-B}(z). \tag{6}$$

On the other hand, as a consequence of Lemma 2.2, we have the followings inequalities [10].

Corollary 2.3. *Let A and B be subsets of an additive Abelian group G; then, there are $x \in A+B$, $y \in A-B$ such that*

$$\frac{|A|\,|B|}{|A \pm B|} \leq \frac{E(A,B)}{|A|\,|B|} \leq |R_{A+B}(x)|, |R_{A-B}(y)|. \tag{7}$$

The next lemma is due to J. Cilleruelo [3], which allows us to delimit the cardinality of a g-Golomb ruler.

Lemma 2.4. *Let G be an additive group and A,B subsets of G. If $R_{A-A}(x) \leq g$, for all $x \neq 0$ in G, then*

$$|A|^2 \leq |A+B| \left(g + \frac{|A|-g}{|B|} \right). \tag{8}$$

Proof. Since $R_{A-A}(x) \leq g$ for all $x \neq 0$ in G, using (6) we have

$$\begin{aligned}
E(A,B) &= \sum_{x \in (A-A)\cap(B-B)} R_{A-A}(x)R_{B-B}(x) \\
&= R_{A-A}(0)R_{B-B}(0) + \sum_{\substack{x \in (A-A)\cap(B-B) \\ x \neq 0}} R_{A-A}(x)R_{B-B}(x) \\
&= |A||B| + \sum_{\substack{x \in (A-A)\cap(B-B) \\ x \neq 0}} R_{A-A}(x)R_{B-B}(x) \\
&\leq |A||B| + \sum_{\substack{x \in (A-A)\cap(B-B) \\ x \neq 0}} gR_{B-B}(x) \\
&\leq |A||B| + g \sum_{\substack{x \in (B-B) \\ x \neq 0}} R_{B-B}(x) \\
&= |A||B| + g(|B|^2 - |B|);
\end{aligned}$$

then using (7) and the above inequality we obtain

$$\begin{aligned}
|A|^2 &\leq \frac{|A+B|}{|B|^2} E(A,B) \\
&\leq \frac{|A+B|}{|B|^2} \left[|A||B| + g(|B|^2 - |B|) \right] \\
&= |A+B| \left(\frac{|A|}{|B|} + g - \frac{g}{|B|} \right) \\
&= |A+B| \left(g + \frac{|A| - g}{|B|} \right).
\end{aligned}$$

☑

Using the Lemma 2.4 we obtain the following result.

Theorem 2.5. *For all $g, n \in \mathbb{N}$ we have*

$$F_2^-(g,n) \leq (gn)^{1/2} + (gn)^{1/4} + 1. \tag{9}$$

Proof. Let $A \subset [1,n]$ be a g-Golomb ruler and B the set of integers $B = [0,u]$, for which $|B| = u+1$. Since $R_{A-A}(x) \leq g$ for all $x \neq 0$, $A + B \subseteq [1, u+n]$, from Lemma 2.4 we have

$$\begin{aligned}
|A|^2 &\leq |A+B| \left(g + \frac{|A| - g}{|B|} \right) \\
&\leq (u+n) \left(g + \frac{|A| - g}{u+1} \right) \\
&= \frac{(u+n)(gu + |A|)}{u+1}.
\end{aligned}$$

If we make $u = \left\lfloor \sqrt[4]{\frac{n^3}{g}} \right\rfloor$, where $\lfloor x \rfloor$ denotes the integer part of the real number x, we obtain

$$\begin{aligned}|A|^2 &\leq \frac{\left[\left(\frac{n^3}{g}\right)^{1/4} + n\right]\left[g\left(\frac{n^3}{g}\right)^{1/4} + |A|\right]}{\left(\frac{n^3}{g}\right)^{1/4}} \\ &= [(gn)^{1/4} + 1]|A| + gn + (gn)^{3/4};\end{aligned}$$

then,

$$|A|^2 - [(gn)^{1/4} + 1]|A| \leq gn + (gn)^{3/4};$$

now, if we complete squares in the left side we have

$$\left(|A| - \frac{(gn)^{1/4}+1}{2}\right)^2 \leq gn + (gn)^{3/4} + \left(\frac{(gn)^{1/4}+1}{2}\right)^2,$$

and by completing the squares in the right side we obtain

$$\begin{aligned}\left(|A| - \frac{(gn)^{1/4}+1}{2}\right)^2 &\leq \left((gn)^{1/2} + \frac{(gn)^{1/4}+1}{2}\right)^2 + (gn)^{3/4} - (gn)^{1/2}((gn)^{1/4}+1) \\ &= \left((gn)^{1/2} + \frac{(gn)^{1/4}+1}{2}\right)^2 - (gn)^{1/2} \\ &\leq \left((gn)^{1/2} + \frac{(gn)^{1/4}+1}{2}\right)^2,\end{aligned}$$

implying that

$$|A| - \frac{(gn)^{1/4}+1}{2} \leq (gn)^{1/2} + \frac{(gn)^{1/4}+1}{2},$$

and so,

$$|A| \leq (gn)^{1/2} + (gn)^{1/4} + 1.$$

As the g- Golomb ruler A was chosen arbitrarily, we have

$$F_2^-(g,n) \leq (gn)^{1/2} + (gn)^{1/4} + 1,$$

for all g and n positive integers. ☑

As a consequence of the Theorem 2.5, we have the following results for the case of optimally dense Golomb rulers.

Corollary 2.6. *For all natural number n we have*

$$F_2(n) \leq n^{1/2} + n^{1/4} + 1.$$

Corollary 2.7.

$$\limsup_{n\to\infty} \frac{F_2^-(g,n)}{\sqrt{n}} \leq \sqrt{g}. \tag{10}$$

Now, by using the Lemma 2.4, we present a lower bound to the function $G(g,m)$.

Theorem 2.8. *If $A = \{a_i : 1 \leq i \leq m\}$ is a g-Golomb ruler with m marks such that $0 = a_1 < \ a_2 < \cdots < a_m = \ell(A)$, then*

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

Proof. Let us consider the set $B = [0,u]$, for which $|B| = u+1$; since A is a g-Golomb ruler with $|A| = m$ and $\ell(A) = a_m$, then $R_{A-A}(x) \leq g$ for all non-zero integer x. Furthermore, since $A + B \subset [0, a_m + u]$, then $|A+B| \leq a_m + u + 1$, and from Lemma 2.4 we obtain

$$|A|^2 \leq |A+B| \left(g + \frac{|A|-g}{|B|} \right).$$

Then,

$$\begin{aligned} m^2 &\leq (a_m + u + 1) \left(g + \frac{m-g}{u+1} \right) \\ &= \frac{(a_m + u + 1)(gu + m)}{u+1}; \end{aligned}$$

it follows that

$$\begin{aligned} a_m &\geq \frac{m^2(u+1)}{gu+m} - u - 1, \\ &= (u+1) \left[\frac{m^2}{gu+m} - 1 \right]. \end{aligned}$$

Choosing $u = \lfloor \frac{m\sqrt{m-g}}{g} - \frac{m}{g} \rfloor$, we have $u \leq \frac{m\sqrt{m-g}}{g} - \frac{m}{g} \leq u+1$; therefore,

$$\begin{aligned} a_m &\geq \frac{m^2(\frac{m\sqrt{m-g}}{g} - \frac{m}{g})}{m\sqrt{m-g}} - \left(\frac{m\sqrt{m-g}}{g} - \frac{m}{g} \right) - 1 \\ &= \frac{m^2}{g} - \frac{m^2}{g\sqrt{m-g}} - \frac{m\sqrt{m-g}}{g} + \frac{m}{g} - 1. \\ &= \frac{m^2}{g} - \left(\frac{2m^2 - gm}{g\sqrt{m-g}} \right) + \frac{m}{g} - 1 \\ &= \frac{m^2}{g} - m \left(\frac{2(m-g)}{g\sqrt{m-g}} + \frac{gm}{g\sqrt{m-g}} \right) + \frac{m}{g} - 1 \\ &= \frac{m^2}{g} - \frac{2m\sqrt{m-g}}{g} - \frac{m}{\sqrt{m-g}} + \frac{m}{g} - 1. \end{aligned}$$

That is,

$$a_m \geq \frac{m^2}{g} - \frac{2m\sqrt{m-g}}{g} - \frac{m}{\sqrt{m-g}} + \frac{m}{g} - 1.$$

As the previous inequality is valid for any g-Golomb ruler of length a_m (in particular it holds for the shorter g-Golomb ruler), then

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

In the case where $g = 1$ we obtain a better lower bound than the one previously known in the literature, at the function $G(m)$ defined for Golomb rulers; that is,

Corollary 2.9. *For all positive integer m*

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

Corollary 2.10. *For all integer $g \geq 1$,*

$$\lim_{n\to\infty} \inf \frac{G(g,m)}{m^2} \geq \frac{1}{g}. \tag{11}$$

3. Constructions of g-Golomb rulers

Now we will prove a lower bound for the function $F_2^-(g,n)$ and a upper bound for the function $G(g,m)$. For this, we use a result that allows us to transform a Golomb ruler or B_2 set into a $B_2^-[g]$ set through a groups' homomorphism [5].

Theorem 3.1. *Let $g \in \mathbb{N}$ and let $\varphi : G \to G'$ be a groups' homomorphism with $|ker(\varphi)| = g$. If A is a Golomb ruler in G, then $\varphi(A)$ is a g-Golomb ruler in $\varphi(G)$.*

Proof. Let $b_i, b_i' \in \varphi(A)$, $i = 1, 2, \dots, g+1$, there are $a_i, a_i' \in A$ such that $b_i = \varphi(a_i)$ and $b_i' = \varphi(a_i')$, for $i = 1, 2, \dots, g+1$, and suppose that

$$b_1 - b_1' = b_2 - b_2' = \cdots = b_g - b_g = b_{g+1} - b_{g+1}. \tag{12}$$

Then

$$\varphi(a_1) - \varphi(a_1') = \varphi(a_2) - \varphi(a_2') = \cdots = \varphi(a_g) - \varphi(a_g) = \varphi(a_{g+1}) - \varphi(a_{g+1}), \tag{13}$$

and, as φ is a homomorphism of groups, we have

$$\varphi(a_1 - a_1') = \varphi(a_2 - a_2') = \cdots = \varphi(a_g - a_g) = \varphi(a_{g+1} - a_{g+1}). \tag{14}$$

Hence it follows that

$$\varphi((a_1 - a_1') - (a_j - a_j')) = 0, \text{ for all } j = 2 \dots, g+1,$$

implying that $\beta_j = (a_1 - a_1') - (a_j - a_j') \in ker(\varphi)$, $j = 2 \dots, g+1$.

As by hypothesis $|ker(\varphi)| = g$, by the pigeonhole principle two cases can happen:

CASE I.

There exist a $j \in \{2 \dots, g+1\}$ such that $\beta_j = 0$.

This implies that $a_1 - a'_1 = a_j - a'_j$, and since $a_1, a'_1, a_j, a'_j \in A$, being A a Golomb ruler, then $\{a_1, a'_1\} = \{a_j, a'_j\}$; therefore, $\{b_1, b'_1\} = \{b_j, b'_j\}$.

CASE II.

There are $i, j \in \{2 \ldots, g+1\}$ such that $\beta_i = \beta_j = t$, $t \neq 0$.

This means that $(a_1 - a'_1) - (a_i - a'_i) = (a_1 - a'_1) - (a_j - a'_j)$; then $a_i - a'_i = a_j - a'_j$, and since $a_i, a'_i, a_j, a'_j \in A$, being A a Golomb ruler, then $\{a_i, a'_i\} = \{a_j, a'_j\}$; thus, $\{b_i, b'_i\} = \{b_j, b'_j\}$. ☑

Furthermore, we know that there are three constructions of Golomb rulers or B_2 sets very well-know; these are:

- Singer's construction [9] that provides a Golomb ruler with $q+1$ elements, modulo q^2+q+1.
- Bose's construction [2] that provides a Golomb ruler with q elements, modulo q^2-1.
- Ruzsa's construction [8] that provides a Golomb ruler with $p-1$ elements, modulo p^2-p.

Here, q is a prime power and p is a prime. Therefore, since there are infinitely many Golomb rulers or infinitely many B_2 sets, then by the homomorphism of Theorem 3.1 it is possible to obtain infinitely many g-Golomb rulers or infinitely many $B_2^-[g]$ sets, for all $g \in \mathbb{N}$. Although the definition of $B_2^-[g]$ set is at first given for subsets of positive integers, this can be extended for subsets of any additive group. In particular, the construction of Bose type B_2 sets is given for the case of a subset from the additive group $\mathbb{Z}_{q^2-1}$, and since all B_2 sets in $\mathbb{Z}_n$ are integer B_2 sets contained in $[1, n]$, by Bose's construction we obtain integer B_2 sets in $[1, q^2-1]$, for all prime powers q.

First of all, we will state the Bose Theorem and the a lemma that allows us to determine the appropriate homomorphism.

Theorem 3.2 (Bose, 1942). *For every prime power q, there exists a set $A \subseteq [1, q^2-1]$ with q elements such that $A \in B_2$ in $\mathbb{Z}_{q^2-1}$. Also, $A \ominus A = \mathbb{Z}_{q^2-1} \setminus M_{q+1}$, where M_{q+1} indicates the set of multiples set of $q+1$ in $\mathbb{Z}_{q^2-1}$.*

Remark 3.3. Notation: Let A and B be subsets of any group $(G, +)$; then, we define the set

$$A \ominus B = \{a + b : \, a \in A, b \in B, \, a \neq b\}.$$

Lemma 3.4. *For every integer $g \geq 2$ and every prime power $q \equiv 1 (\bmod g)$, there exists a $B \in B_2^-[g]$ set such that $|B| = q$ and $B \subseteq \left[1, \frac{q^2-1}{g}\right]$.*

Proof. By Bose's construction there is a Sidon set A with q elements in $\mathbb{Z}_{q^2-1}$, for every prime power q; in particular, for every prime power $q \equiv 1 (\bmod g)$.

By the Corollary 3.1, there exists a homomorphism

$$\varphi : \mathbb{Z}_{q^2-1} \to \mathbb{Z}_{\frac{q^2-1}{g}}$$

defined as

$$\varphi(a) \equiv a(\text{mod}\frac{q^2-1}{g}), \text{ for all } a \in \mathbb{Z}_{q^2-1},$$

where $|ker(\varphi)| = g$.

Then, $B = \varphi(A) \in B_2^-[g]$ in $\mathbb{Z}_{\frac{q^2-1}{g}}$ and $|B| = q$.

Indeed, since $A \ominus A = \mathbb{Z}_{q^2-1} \setminus M_{q+1}$, this implies that for $r, s \in A$ such that $r \neq s$, we have that $r \not\equiv s(\text{mod} q+1)$; then, as for all prime power q, $q \equiv 1(\text{mod} g)$,

$$r \not\equiv s \left(\text{mod } \frac{(q+1)(q-1)}{g} \right);$$

then $|B| = |A| = q$.

And since every modular $B_2^-[g]$ set is an integer $B_2^-[g]$ set, we have that $B \subseteq \left[1, \frac{q^2-1}{g}\right]$ is an integer $B_2^-[g]$ set. ☑

In particular, in the previous lemma the existence of $B_2^-[g]$ sets for the case $q = p$ prime is guaranteed.

The following result also guarantees the lower bound for the function $F_2^-(n, g)$, $g \geq 2$.

Theorem 3.5. *Let $g \geq 2$ be an integer. For infinitely many values n, there exists a $A \subseteq [1, n]$ set, $A \in B_2^-[g]$, with $|A| \geq (gn)^{1/2}$.*

Proof. For any $g \geq 2$ integer, according to the Dirichlet Theorem on primes in arithmetic progressions, there are infinitely many primes p meeting $p \equiv 1(\text{mod} g)$.

For each of these primes p , let $n = \frac{p^2-1}{g}$; by Lemma 3.4 there exists a $B \subseteq [1, n]$ set, that is, a $B_2^-[g]$ set with

$$|B| = p \geq \sqrt{p^2-1} = \sqrt{gn}.$$ ☑

For $g = 1$ the existence of Golomb rulers or B_2 sets is guaranteed by Bose's construction.

Theorem 3.6. *For infinitely many positive integers n, there exists a Golomb ruler $A \subseteq [1, n]$ with $|A| \geq \sqrt{n}$.*

Proof. Since there are infinitely many primes, we have infinitely many prime powers q. Let $n = q^2 - 1$; by Bose's construction, for every q there exists a Golomb ruler $A \subseteq [1, n]$ such that $|A| = q = \sqrt{q^2} \geq \sqrt{q^2-1} = \sqrt{n}$. ☑

Accordingly, we have the next corollary.

Corollary 3.7. *For all $g \in \mathbb{N}$, all prime power q and all prime p, we have*

$$F_2^-\left(g, \frac{q^2-1}{g}\right) \geq q. \tag{15}$$

From Theorems 3.5 and 3.6, we can conclude that

$$F_2^-(g,n) \geq (gn)^{1/2},$$

for all $g \in \mathbb{N}$ and infinites n.

Corollary 3.8.

$$\liminf_{n\to\infty} \frac{F_2^-(g,n)}{\sqrt{n}} \geq \sqrt{g}. \tag{16}$$

Also, by using the Bose's construction we can obtain an upper bound for the function $G(g,m)$. By Lemma 3.4 we know that for all $g \geq 2$ integers and all $p \equiv 1(\bmod g)$ primes, there is a g-Golomb ruler contained in $[1, \frac{p^2-1}{g}]$ with p marks. Therefore, $G(g,p) \leq \frac{p^2-1}{g}$. If $g = 1$ we obtain the same conclusion as Bose's Theorem 3.2. So, we have the following result.

Corollary 3.9. *For all integer $g \geq 1$, we have*

$$\lim_{m\to\infty} \sup \frac{G(g,m)}{m^2} \leq \frac{1}{g}.$$

3.1. General theorems

Theorem 3.10. *For every $g \geq 1$ integer, we have*

$$\lim_{n\to\infty} \frac{F_2^-(g,n)}{\sqrt{n}} = \sqrt{g}.$$

Proof. It follows from (10) and (16). ☑

Theorem 3.11. *For every $g \geq 1$ integer, we have*

$$\lim_{m\to\infty} \frac{G(g,m)}{m^2} = \frac{1}{g}.$$

Acknowledgments

The authors are grateful for the financial support provided by COLCIENCIAS, Universidad del Cauca and Universidad del Valle. Also, the authors thank to “Patrimonio Autónomo Fondo Nacional de Financiamiento para la Ciencia, la Tecnología y la Innovación - Francisco José de Caldas”, Universidad del Cauca and COLCIENCIAS for financial support under reseach project 110356935047 titled “Construcciones de conjuntos $B_h[g]$, propiedad de Midy, y algunas aplicaciones”.

In addition, we thank the reviewers of this article for suggesting by a comparison with known results $B_2[g]$ sets of article [7]; but this study will be done in a later work.

References

[1] Atkinson M.D., Santoro N. and Urrutia J., "Integer Sets with Distinct Sums and Differences and Carrier Frequency Assignments for Nonlinear Repeaters", *IEEE Transactions on Communications* 34 (1986), No. 6, 614–617.

[2] Bose R.C., "An affine analogue of Singer's theorem", *J. Indian Math. Soc. (N.S.)* 6 (1942), 1–15.

[3] Cilleruelo J., "Sidon sets in $\mathbb{N}^d$", *J. Combin. Theory Ser. A* 117 (2010), No. 7, 857–871.

[4] Dimitromanolakis A., "Analysis of the Golomb Ruler and the Sidon set Problems, and Determination of Large, near-optimal Golomb rulers". Thesis (Master), Technical University of Crete, 2002, 118 p.

[5] Gómez J., "Construcción de conjuntos $B_h[g]$", Tesis (Maestría), Universidad del Valle, Cali, 2011, 69 p.

[6] Lindström B., "An inequality for B_2-sequences", *J. Combinatorial Theory* 6 (1969), 211–212.

[7] Martin G. and O'Bryant K., "Constructions of generalized Sidon sets", *J. Combin. Theory Ser. A* 113 (2006), No. 4, 591–607.

[8] Ruzsa I., "Solving a linear equation in a set of integers I", *Acta Arith.* 65 (1993), No. 3, 259–282.

[9] Singer J., "A theorem infinite projective geometry and some applications to number theory", *Trans. Amer. Math. Soc.* 43 (1938), No. 3, 377–385.

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

[11] Trujillo C.A., García G. and Velásquez J.M., "$B_2^{\pm}[g]$ finite sets", *JP J. Algebra Number Theory Appl.* 4 (2004), No. 3, 593–604.