IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 3, 2021, accepted December 20, 2021, date of publication December 23, 2021, date of current version January 5, 2022.

Digital Object Identifier 10.1109/ACCESS.2021.3137996

Almost Difference Sets From Singer Type Golomb Rulers

DAVID FERNANDO DAZA URBANO, CARLOS ANDRES MARTOS OJEDA, AND CARLOS ALBERTO TRUJILLO SOLARTE
Departamento de Matemáticas, Universidad del Cauca, Popayán 190003, Colombia

Corresponding author: David Fernando Daza Urbano (davidaza@unicauca.edu.co)

This work was supported in part by the Ministerio de Ciencia, Tecnología e Innovación (MINCIENCIAS); and in part by the Universidad del Cauca through the Project "g-Golomb rulers and g-congurations" under Grant 5367.

ABSTRACT Let G be an additive group of order v. A k-element subset D of G is called a (v, k, λ, t)-almost difference set if the expressions $g - h$, for g and h in D, represent t of the non-identity elements in G exactly λ times and every other non-identity element $\lambda + 1$ times. Almost difference sets are highly sought after as they can be used to produce functions with optimal nonlinearity, cyclic codes, and sequences with three-level autocorrelation. A set of positive integers A is called a Golomb ruler if the difference between two distinct elements of A are different. In this paper, we use Singer type Golomb rulers to construct new families of almost difference sets. Additionally, we constructed 2-adesigns from these almost difference sets.

INDEX TERMS Almost difference set, difference set, Golomb ruler, t-adesigns.

I. INTRODUCTION

Difference sets are a well-known class of mathematical objects used in the construction of designs and other combinatorial structures. A k-subset D in an additive group G of order v is called a (v, k, λ) *difference set* DS (in G) if $\delta_D(x) = \lambda$ for every nonzero element of G, where $\delta_D(x)$ is the *difference function* defined by

$$\delta_D(x) := |(D + x) \cap D|$$
$$\text{and } D + x = \{d + x : d \in D\}.$$

The difference function counts the number of representations of x in the form $d_i - d_j$ with $d_i, d_j \in D$, that is, $\delta_D(x) = |\{(d_i, d_j) \in D \times D : d_i - d_j = x\}|$.

Many groups do not have DSs for any parameters k and λ, but do have structures that are very close to DSs, which motivates the following definition.

A k-element subset D in an additive group G of order v is said to be a (v, k, λ, t)-*almost difference set* ADS (in G) if $\delta_D(x)$ takes on the value λ altogether t times and $\lambda + 1$ altogether $v - t - 1$ times as x ranges over $G \setminus \{0\}$. This is,

$$\delta_D(x) = |(D + x) \cap D| = \lambda \text{ or } \lambda + 1,$$

for each $x \in G \setminus \{0\}$.

Note that almost difference sets are a generalization of difference sets (when $t = 0$ or $t = v - 1$). Moreover, for an almost difference set D with parameters (v, k, λ, t), its complement $G \setminus D$ is also an almost difference set with parameters $(v, v - k, v - 2k + \lambda, t)$. An almost difference set D is called *abelian* or *cyclic* if the group G is abelian or cyclic, respectively. Almost all difference sets are interesting combinatorial objects that have several applications in many engineering areas. In coding theory, they can be employed, to construct cyclic codes [13]. Additionally, in cryptography, they can be used to construct functions with optimal nonlinearity [8], [11]. Finally, for CDMA communications, some cyclic almost difference sets yield sequences with optimal autocorrelation [1], [15], [16].

Different definitions of an almost difference set were independently developed by Davis and Ding in the early 1990s [9], [11], [12]. Let G be an additive group of order mn and N a subgroup of G of order n. A k-subset D in G is called a $(mn, n, k, \lambda_1, \lambda_2)$ *divisible difference set* DDS (in G) provided that the difference function $\delta_D(x)$ defined above takes on the value λ_1 for each nonzero $x \in N$ and takes on the value λ_2 for each nonzero $x \in G \setminus N$. That is, for each $x \in G \setminus \{0\}$,

$$\delta_D(x) = \begin{cases} \lambda_1, & \text{for } x \in N, \\ \lambda_2, & \text{for } x \in G \setminus N. \end{cases}$$

The associate editor coordinating the review of this manuscript and approving it for publication was Sun-Yuan Hsieh.

If $\lambda_1 = 0$, D is called a *relative difference set* RDS, and N is called the forbidden subgroup. Davis [9] called a divisible difference set an almost difference set in the case where $|\lambda_1 - \lambda_2| = 1$. Davis defined this special class of almost difference sets due to its relationship with symmetric difference sets. Another kind of almost difference sets were defined by Ding [11], [12] for the study of cryptographic functions with optimal nonlinearity. He considered the current definition when $t = \frac{v-1}{2}$.

Number theoretic constraints can be applied to show that some groups cannot contain ADSs with certain parameters [32]. One example is that $(v-1)\lambda + t = k(k-1)$ must hold for any ADS. Other criteria can be discovered by examining the quotient groups of the original group. Despite the effectiveness of these techniques, no general existence criterion is known to determine exactly which groups contain ADSs [7]. Many known construction methods exist for almost difference sets [1], [3], [14], [16]–[18], [32]. These constructions come from: difference sets, cyclotomic classes of finite fields, support of some functions, binary sequences with three-level autocorrelation, or larger product group. For a good survey of almost difference sets, the reader is referred to [24].

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 exists at most 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 $m = 13$ and length $\ell(A) = 176$ is the set

$$A = \{0, 1, 3, 24, 41, 52, 57, 66, 70, 96, 102, 149, 164, 176\}.$$

According to [5], the Golomb rulers were first discovered by W.C. Babcock in 1950 when he investigated the intermodulation distortion. However, Golomb rulers derive their name from Professor Solomon W. Golomb, one of their greatest pioneers.

These sets are important for their applications in different fields, such as communications, fault-tolerant distributed computing, and coding theory, see [2], [19], [21], [22], [27]. They have also been used to study combinatorial problems such as sum product estimates, solvability of some equations, see [6], [31], or in the field of extremal graph theory to study the number $ex(n, C_4)$, see [10], [29], [30].

The concept of the Golomb ruler is invariant under linear applications; if $A = \{a_1, a_2, \ldots, a_m\}$ is a Golomb ruler, then the set

$$x \cdot A + y := \{xa_1 + y, x\, a_2 + y, \ldots, x\, a_m + y\},$$

is a Golomb ruler, for all $x, y \in \mathbb{Z}$, with $x \neq 0$. Thus, 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:

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

A Golomb ruler of order m is optimal if it has the shortest possible length. For example, {0, 4, 20, 30, 57, 59, 62, 76, 100, 111, 123, 136, 144, 145, 151} is an 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], [14] and there is an ongoing search for an optimal 28-marks rule. For more on Golomb rulers, their generalizations, and applications, see [25], [26], and the references in them.

In this paper, we use Singer type Golomb rulers (which are difference sets with $\lambda = 1$, or almost difference set with $\lambda = 0$ and $t = 0$) to construct new families of almost difference sets. These constructions are new, as far as we are aware of. The first construction yields $(N/3, q, 2, 2(q-1))$-ADSs in cyclic groups of order $N/3$, where $N = q^2 + q + 1$ and $q \equiv 1 \bmod 3$ is a prime power greater than 4. This construction uses homomorphic projection. The second construction is obtained by adding a new element to the Golomb ruler and yields $(q^2+q+1, q+2, 1, (q-2)(q+1))$-ADSs in cyclic groups of order q^2+q+1 for all prime power q. The third construction is obtained by removing an element of the Golomb ruler and yields $(q^2+q+1, q, 0, 2q)$-ADSs in cyclic groups of order q^2+q+1 for all prime power q. The latest constructions follow the idea proposed in [1].

Another contribution of this paper is related to t-adesign, which was defined in [14]. Let $D = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure with $v \geq 1$ points and $b \geq 1$ blocks, where every block has size k. If every subset of t points of $\mathcal{P}$ is incident with either λ or $\lambda+1$ blocks of $\mathcal{B}$, then D is called a t-(v, k, λ) adesign, or simply t-adesign. A t-adesign is symmetric if $v = b$. The set $\{D + g : g \in G\}$ of translates of D, denoted by $Dev(D)$, is called the development of D. The following lemma was established in [23] and provides a relationship between almost difference set and t-adesign.

Lemma 1: Let D be a (v, k, λ) almost difference set in an abelian group G. Then, $(G, Dev(D))$ is a 2-(v, k, λ) adesign.

Using the above lemma and the almost difference sets constructed in this paper, we give constructions of 2-adesigns.

The remainder of this paper is organized as follows. In Section 2, we construct $(N/3, q, 2, 2(q-1))$ almost difference sets in groups of order $N/3$, where $N = q^2+q+1$ and $q \equiv 1 \bmod 3$ is a prime power greater than 4. Moreover, we construct $(q^2+q+1, q+2, 1, (q-2)(q+1))$ and $(q^2+q+1, q, 0, 2q)$ almost difference sets in groups of order q^2+q+1 for all prime power q. In Section 3, we present constructions of 2-adesigns. Finally, Section 4 concludes the paper.

II. ALMOST DIFFERENCE SETS VIA SINGER TYPE GOLOMB RULERS

In this section, we describe three new constructions of almost difference sets from Singer type Golomb rulers. These constructions can generate infinitely many almost difference sets in $\mathbb{Z}_n$ for appropriate values of n. First, we present the formal definition of a Golomb ruler.

Definition 1: Let G be an additive abelian group, and A be a subset of G. A is a Golomb ruler in G if

$$\delta_A(x) \leq 1 \quad \textit{for} \quad x \neq 0.$$

If $G = \mathbb{Z}_N$, then A is called a modular Golomb ruler.

From the definition, it is easy to verify that a modular Golomb ruler is a $(v, k, 0, t)$ almost difference set.

If A is a subset of the additive group G and $n \in \mathbb{N}$, then

$$\begin{aligned} A \bmod n &:= \{a \bmod n : a \in A\}; \\ A \ominus A &:= \{a - b : a, b \in A, a \neq b\}; \\ A - x &:= \{a - x : a \in A\}; \\ x - A &:= \{x - a : a \in A\}. \end{aligned}$$

The following construction of modular Golomb ruler is due to Singer [28]. He was not working on number theory but on finite projective geometry when he found this construction. Currently this construction can be described as follows [4], [20].

Proposition 1: Let q be a prime power, θ be a primitive element of the finite field $\mathbb{F}_{q^3}$, $\alpha \in \mathbb{F}_{q^3}$ be an element with cubic minimal polynomial over $\mathbb{F}_q$, and $\mathcal{S} = \{\log_\theta(\alpha + u) : u \in \mathbb{F}_q\}$. Then

$$\mathcal{S}_0 = \mathcal{S} \bmod (q^2 + q + 1) \cup \{0\},$$

is a Golomb ruler in $\mathbb{Z}_{q^2+q+1}$, with $q+1$ elements. Moreover, $\mathcal{S}_0 \ominus \mathcal{S}_0 = \mathbb{Z}_{q^2+q+1} \setminus \{0\}$.

Remark 1: $\mathcal{S}_0$ is a $(q^2 + q + 1, q + 1, 1)$ difference set.

Example 1: Let $q = 7$. If θ is a root of the primitive polynomial $x^3 + 4x^2 + 4x + 4$ over $\mathbb{F}_7$ and $\alpha = \theta$. Then

$$\begin{aligned} A &= \{\theta + u : u \in \mathbb{F}_q\} \\ &= \{\theta, \theta + 1, \theta + 2, \theta + 3, \theta + 4, \theta + 5, \theta + 6\}, \\ &= \{\theta^1, \theta^{274}, \theta^{199}, \theta^{225}, \theta^{329}, \theta^{67}, \theta^{78}\}. \end{aligned}$$

Taking the discrete logarithm of A in base θ yields the set

$$\begin{aligned} \mathcal{S} = \log_\theta A &= \{\log_\theta(\theta + u) : u \in \mathbb{F}_q\}, \\ &= \{1, 274, 199, 225, 329, 67, 78\}. \end{aligned}$$

Reducing the elements of $\mathcal{S}$ modulo 57 gives the set

$$\{1, 46, 28, 54, 44, 6, 21\}.$$

Adding 0 to the above set and ordering its elements yields the Golomb ruler $\{0, 1, 6, 21, 28, 44, 46, 54\}$ in $\mathbb{Z}_{57}$.

Remark 2: The easiest way to work with these examples is to use a computer.

A. CONSTRUCTION 1

The following theorem shows how to construct an almost difference set from a Singer type Golomb ruler using homomorphic projection.

Theorem 1: For all prime power, $q \equiv 1 \bmod 3$ greater than 4, there is a $(\frac{q^2+q+1}{3}, q, 2, 2(q-1))$-ADS.

Proof: According to Singer's construction, for every prime power q, there is a Golomb ruler $\mathcal{S}_0$ in $\mathbb{Z}_{q^2+q+1}$, with $q + 1$ elements, particularly for $q \equiv 1 \bmod 3$.

Let $\varphi : \mathbb{Z}_{q^2+q+1} \to \mathbb{Z}_{\frac{q^2+q+1}{3}}$ be the homomorphism defined by

$$\varphi(a) \equiv a \bmod \left(\frac{q^2 + q + 1}{3}\right),$$

and $D = \varphi(\mathcal{S}_0)$.

Note that, $|D| = q$; indeed, as $\frac{q^2+q+1}{3} \in \mathbb{Z}_{q^2+q+1} \setminus \{0\} = \mathcal{S}_0 \ominus \mathcal{S}_0$ (see Remark 1), then there are two different elements a and b in $\mathcal{S}_0$ such that $a - b \equiv \frac{q^2+q+1}{3} \bmod (q^2 + q + 1)$, hence, $a \equiv b \mod (\frac{q^2+q+1}{3})$, that is, $\varphi(a) = \varphi(b)$. Note that there is no other pair of elements $c, d \in \mathcal{S}_0$ such that $c \equiv d \bmod (\frac{q^2+q+1}{3})$, because this contradicts the fact that $\mathcal{S}_0$ is a Golomb ruler. Therefore, $|D| = q$.

Let $\mathcal{S}_0 = \{s_1, s_2, \ldots, s_{q+1}\}$ with $s_1 \equiv s_2 \bmod \frac{q^2+q+1}{3}$, and let $D = \{d_1, d_2, \ldots, d_q\}$, where $d_1 = \phi(s_1) = \phi(s_2)$ and $d_{i-1} = \varphi(s_i)$, for $3 \leq i \leq q + 1$.

Note that for each $x \in \mathbb{Z}_{\frac{q^2+q+1}{3}} \setminus \{0\}$, there are two distinct elements $x_1 = x + \frac{q^2+q+1}{3}$ and $x_2 = x + 2\left(\frac{q^2+q+1}{3}\right)$ in $\mathbb{Z}_{q^2+q+1}$ for which

$$\varphi(x) = \varphi(x_1) = \varphi(x_2). \tag{1}$$

On the other hand, by (Remark 1) there are unique elements s_i, s_j, s_k, s_l, s_t and s_r in $\mathcal{S}_0$ such that

$$x = s_i - s_j, x_1 = s_k - s_l, \quad \textit{and} \quad x_2 = s_t - s_r,$$

so, by (1)

$$\varphi(x) = \varphi(s_i) - \varphi(s_j) = \varphi(s_k) - \varphi(s_l) = \varphi(s_t) - \varphi(s_r),$$

this is,

$$\varphi(x) = d_i - d_j = d_k - d_l = d_t - d_r.$$

As $\varphi(s_1) = \varphi(s_2) = d_1$ then for $3 \leq j \leq q+1$, the $4(q-1)$ pairwise distinct elements

$$s_1 - s_j, s_2 - s_j, s_j - s_1, s_j - s_2$$

satisfy that

$$\begin{aligned} &\varphi(s_1) - \varphi(s_j) = \varphi(s_2) - \varphi(s_j) = d_1 - d_j, \quad \textit{and} \\ &\varphi(s_j) - \varphi(s_1) = \varphi(s_j) - \varphi(s_2) = d_j - d_1, \end{aligned}$$

therefore, there are $2(q-1)$ distinct elements of $\mathbb{Z}_{\frac{q^2+q+1}{3}}$ that have two different representations as differences of elements in D. The other $\frac{q^2-5q+4}{2}$ elements of $\mathbb{Z}_{\frac{q^2+q+1}{3}}$ can be written in three different ways as differences of elements in D. Thus, D is a $(\frac{q^2+q+1}{3}, q, 2, 2(q-1))$-ADS. □

Example 2: The set $\mathcal{S} = \{0, 1, 6, 21, 28, 44, 46, 54\}$ is a Singer type Golomb ruler in $\mathbb{Z}_{57}$. Reducing the elements of $\mathcal{S}$ modulo $57/3 = 19$ gives the set $\{0, 1, 2, 6, 8, 9, 16\}$, *which is a* $(19, 7, 2, 12)$ *almost difference set in* $\mathbb{Z}_{19}$ *by Theorem 1.*

Example 3: The set $\mathcal{S} = \{0, 1, 3, 24, 41, 52, 57, 66, 70, 96, 102, 149, 164, 176\}$ *is a Singer type Golomb ruler in* $\mathbb{Z}_{183}$*. Reducing the elements of* $\mathcal{S}$ *modulo 183/3 = 61 gives the set* $\{0, 1, 3, 5, 9, 24, 27, 35, 41, 42, 52, 54, 57\}$*, which is a* $(61, 13, 2, 24)$ *almost difference set in* $\mathbb{Z}_{61}$ *by Theorem 1.*

B. CONSTRUCTION 2

The following proposition shows how to construct an almost difference from a difference set by adding an element.

Proposition 2: Let D be a $(v, \frac{v-1}{4}, \frac{v-5}{16})$ *difference set in G, and let* $d \in G \setminus D$*. If* $2d$ *cannot be written as the sum of two distinct elements of D, then* $D \cup \{d\}$ *is a* $(v, \frac{v+3}{4}, \frac{v-5}{16}, \frac{v-1}{2})$ *almost difference set in G, see [1].*

Using the same idea of Proposition 2, we obtain the following result.

Theorem 2: Let D be a (v, k, λ) *difference set in G. If*

1) $g \in G \setminus D$;
2) $(g - D) \cap (D - g) = \emptyset$,

then $D \cup \{g\}$ *is a* $(v, k + 1, \lambda, v - 1 - 2k)$ *almost difference set in G.*

Proof: Let $D = \{d_1, d_2, \ldots, d_k\}$. If $(g - D) \cap (D - g) = \emptyset$, then $2g$ cannot be written as a sum of two distinct elements of D; therefore

$$g - d_1, g - d_2, \ldots, g - d_k$$
$$d_1 - g, d_2 - g, \ldots, d_k - g$$

are $2k$ pairwise distinct elements. Because D is a (v, k, λ) difference set, $D \cup \{g\}$ is a $(v, k + 1, \lambda, v - 1 - 2k)$ almost difference set. □

Corollary 1: There is a $(q^2+q+1, q+2, 1, (q-2)(q+1))$*-ADS in* $\mathbb{Z}_{q^2+q+1}$*, for all prime power q.*

Proof: According to Singer's construction, for every prime power q, there is a Golomb ruler $\mathcal{S}_0$ in $\mathbb{Z}_{q^2+q+1}$. In particular, $\mathcal{S}_0$ is a $(q^2 + q + 1, q + 1, 1)$-DS. Then, the result follows applying Theorem 2 with a suitable element in $\mathbb{Z}_{q^2+q+1} \setminus \mathcal{S}_0$. □

Example 4: The set $D = \{0, 1, 4, 6\}$ *is a Singer type Golomb ruler in* $\mathbb{Z}_{13}$*. Since*

1) $8 \in \mathbb{Z}_{13} \setminus D$;
2) $8 - D = \{2, 4, 7, 8\}$;
3) $D - 8 = \{5, 6, 9, 11\}$;
4) $(8 - D) \cap (D - 8) = \emptyset$.

Then, $D \cup \{8\} = \{0, 1, 4, 6, 8\}$*, is a* $(13, 5, 1, 4)$ *almost difference set in* $\mathbb{Z}_{13}$ *by Theorem 2.*

Example 5: The set $D = \{0, 1, 11, 19, 26, 28\}$ *is a Singer type Golomb ruler in* $\mathbb{Z}_{31}$*. Since*

1) $17 \in \mathbb{Z}_{31} \setminus D$;
2) $17 - D = \{6, 16, 17, 20, 22, 29\}$;
3) $D - 17 = \{2, 9, 11, 14, 15, 25\}$;
4) $(17 - D) \cap (D - 17) = \emptyset$.

Then, $D \cup \{17\} = \{0, 1, 11, 17, 19, 26, 28\}$*, is a* $(31, 7, 1, 18)$ *almost difference set in* $\mathbb{Z}_{31}$ *by Theorem 2.*

Remark 3: Two elements cannot be added to $\mathcal{S}_0$ *in Theorem 2 to obtain a* $(q^2 + q + 1, q + 3, 1, t)$ *almost difference set. Indeed, let* x_1 *and* x_2 *be two distinct elements in* $\mathbb{Z}_{q^2+q+1} \setminus \mathcal{S}_0$ *and* $D = \mathcal{S}_0 \cup \{x_1, x_2\}$*. As* $x_1 \neq x_2$*, then* $x_1 - x_2 \in \mathcal{S}_0 \ominus \mathcal{S}_0$ *(see Remark 1), so*

$$y := x_1 - s_1 = x_2 - s_2$$

for some $s_1, s_2 \in \mathcal{S}_0$ $(s_1 \neq s_2)$*. As* $y \neq 0$*, then* $y \in \mathcal{S}_0 \ominus \mathcal{S}_0$*. Therefore, y can be written in three different ways as differences of elements in D.*

Example 6: The set $\{0, 1, 11, 19, 26, 28\}$ *is a Golomb ruler in* $\mathbb{Z}_{31}$*. By adding 9, and 24, we obtain the set* $D = \{0, 1, 9, 11, 19, 24, 26, 28\}$*. Note that 9 and 24 cannot be written as the sum of two distinct elements of D, but the element 29 in* $\mathbb{Z}_{31}$ *can be written as* $24 - 26 \equiv 9 - 11 \equiv 26 - 18$*. Other elements in* $\mathbb{Z}_{31}$ *can also be written in three different ways as differences of elements in D; for example 8.*

C. CONSTRUCTION 3

The following proposition shows how to construct an almost difference set from a difference set by removing an element.

Proposition 3: Let D be a $(v, \frac{v+3}{4}, \frac{n+3}{16})$ *difference set in G, and let* $d \in D$*. If* $2d$ *cannot be written as the sum of two distinct elements of D, then* $D \setminus \{d\}$ *is a* $(v, \frac{v-1}{4}, \frac{v-13}{16}, \frac{v-1}{2})$ *almost difference set in G, see [1].*

Using the same idea of Proposition 3, we obtain the following result.

Theorem 3: Let D be a (v, k, λ) *difference set in G. If*

1) $d \in D$;
2) $(d - D) \cap (D - d) = \{0\}$,

then $D \setminus \{d\}$ *is a* $(v, k - 1, \lambda - 1, 2(k - 1))$ *almost difference set in G.*

Proof: Let $D = \{d, d_2, \ldots, d_k\}$. If $(d - D) \cap (D - d) = \{0\}$, then $2d$ cannot be written as a sum of two distinct elements of D; therefore

$$d - d_2, d - d_3, \ldots, d - d_k$$
$$d_2 - d, d_3 - d, \ldots, d_k - d$$

are $2(k-1)$ pairwise distinct elements. Because D is a (v, k, λ) difference set, $D \setminus \{d\}$ is a $(v, k - 1, \lambda - 1, 2(k - 1))$ almost difference. □

Corollary 2: There is a $(q^2 + q + 1, q, 0, 2q)$*-ADS in* $\mathbb{Z}_{q^2+q+1}$*, for all prime power q.*

Proof: According to Singer's construction, for every prime power q, there is a Golomb ruler $\mathcal{S}_0$ in $\mathbb{Z}_{q^2+q+1}$. In particular, $\mathcal{S}_0$ is a $(q^2 + q + 1, q + 1, 1)$-DS. Then, the result follows applying Theorem 3 with a suitable element in $\mathbb{Z}_{q^2+q+1} \setminus \mathcal{S}_0$. □

Example 7: The set $D = \{0, 1, 11, 19, 26, 28\}$ *is a Singer type Golomb ruler in* $\mathbb{Z}_{31}$*. Since*

1) $26 \in D$;
2) $26 - D = \{0, 7, 15, 25, 26, 29\}$;
3) $D - 26 = \{0, 2, 5, 6, 16, 24\}$;
4) $(26 - D) \cap (D - 26) = \{0\}$.

Then, $D \setminus \{26\} = \{0, 1, 11, 17, 19, 28\}$*, is a* $(31, 6, 0, 10)$ *almost difference set in* $\mathbb{Z}_{31}$ *by Theorem 3.*

Example 8: The set $D = \{0, 1, 3, 24, 41, 52, 57, 66, 70, 96, 102, 149, 164, 176\}$ *is a Singer type Golomb ruler in* $\mathbb{Z}_{183}$*. Since*

1) $70 \in D$;
2) $70-D = \{0, 4, 13, 18, 29, 46, 67, 69, 70, 77, 89, 104, 151, 157\}$;
3) $D - 70 = \{0, 26, 32, 79, 94, 106, 113, 114, 116, 137, 154, 165, 170, 179\}$;
4) $(70 - D) \cap (D - 70) = \{0\}$.

Then, $D\setminus\{70\} = \{0, 1, 3, 24, 41, 52, 57, 66, 96, 102, 149, 164, 176\}$*, is a* $(183, 12, 0, 26)$ *almost difference set in* $\mathbb{Z}_{183}$ *by Theorem 3.*

Remark 4: The process in Theorem 3 can be continued recursively to obtain an almost difference set with parameters $(q^2 + q + 1, q + 1 - i, 0, 2(iq - \binom{i}{2}))$*, where* $1 \le i < q$ *is the number of elements that are removed.*

Example 9: The set $\{0, 1, 6, 8, 18\}$ *is a Singer type Golomb ruler in* $\mathbb{Z}_{21}$*. By removing 6, we obtain* $\{0, 1, 8, 18\}$*, which is a* $(21, 4, 0, 8)$*-ADS. By removing 1 of this set, we obtain* $\{0, 8, 18\}$*, which is a* $(21, 3, 0, 14)$*-ADS. By removing 18 of the above set, we obtain* $\{0, 8\}$*, which is a* $(21, 2, 0, 18)$*-ADS.*

III. CONSTRUCTIONS OF SYMMETRIC 2-ADESIGNS

From Theorem 1, Theorem 2, and Lemma 1, we obtain corollaries 3 and 4, respectively.

Corollary 3: For all prime power, $q \equiv 1 \bmod 3$ *greater than 4, there is a symmetric* $2\text{-}\left(\frac{q^2+q+1}{3}, q, 2\right)$ *adesign.*

Example 10: The set $D = \{0, 1, 2, 6, 8, 9, 16\}$ *is a* $(19, 7, 2, 12)$ *almost difference set in* $\mathbb{Z}_{19}$ *(see Example 2). By Lemma 1, we obtain a symmetric* $2\text{-}(19, 7, 2)$ *adesign with the following blocks of size 7:*

$\{0, 1, 2, 6, 8, 9, 16\}$ $\{10, 11, 12, 16, 18, 0, 7\}$
$\{1, 2, 3, 7, 9, 10, 17\}$ $\{11, 12, 13, 17, 0, 1, 8\}$
$\{2, 3, 4, 8, 10, 11, 18\}$ $\{12, 13, 14, 18, 1, 2, 9\}$
$\{3, 4, 5, 9, 11, 12, 0\}$ $\{13, 14, 15, 0, 2, 3, 10\}$
$\{4, 5, 6, 10, 12, 13, 1\}$ $\{14, 15, 16, 1, 3, 4, 11\}$
$\{5, 6, 7, 11, 13, 14, 2\}$ $\{15, 16, 17, 2, 4, 5, 12\}$
$\{6, 7, 8, 12, 14, 15, 3\}$ $\{16, 17, 18, 3, 5, 6, 13\}$
$\{7, 8, 9, 13, 15, 16, 4\}$ $\{17, 18, 0, 4, 6, 7, 14\}$
$\{8, 9, 10, 14, 16, 17, 5\}$ $\{18, 0, 1, 5, 7, 8, 15\}$
$\{9, 10, 11, 15, 17, 18, 6\}$

Corollary 4: For all power prime q, there is a symmetric $2\text{-}(q^2 + q + 1, q + 2, 1)$ *adesign.*

Example 11: The set $D = \{0, 1, 4, 6, 8\}$ *is a* $(13, 5, 1, 4)$ *almost difference set in* $\mathbb{Z}_{13}$ *(see Example 4). By Lemma 1, we obtain a symmetric* $2\text{-}(13, 5, 1)$ *adesign with the following blocks of size 5:*

$\{0, 1, 4, 6, 8\}$ $\{5, 6, 9, 11, 0\}$ $\{10, 11, 1, 3, 5\}$
$\{1, 2, 5, 7, 9\}$ $\{6, 7, 10, 12, 1\}$ $\{11, 12, 2, 4, 6\}$
$\{2, 3, 6, 8, 10\}$ $\{7, 8, 11, 0, 2\}$ $\{12, 0, 3, 5, 7\}$
$\{3, 4, 7, 9, 11\}$ $\{8, 9, 12, 1, 3\}$
$\{4, 5, 8, 10, 12\}$ $\{9, 10, 0, 2, 4\}$

IV. CONCLUSION

In this paper, we prove that

1) for every prime power $q \equiv 1 \bmod 3$, there exists a $(N/3, q, 2, 2(q-1))$ almost difference set in $\mathbb{Z}_{N/3}$, where $N = q^2 + q + 1$;
2) There exists a $(q^2 + q + 1, q + 2, 1, (q-2)(q+1))$ almost difference set in $\mathbb{Z}_{q^2+q+1}$, for all prime power q.
3) There exists a $(q^2+q+1, q+1-i, 0, 2(iq-\binom{i}{2}))$ almost difference in $\mathbb{Z}_{q^2+q+1}$, for all prime power q, and for all $1 \le i < q$.

Additionally, we constructed 2-adesigns from these almost difference sets.

On the other hand, there are some questions that can be addressed in future work; we consider it interesting to approach the following problems:

1) To study the structure, properties, and applications of the almost difference sets constructed in this paper.
2) Let $\mathbb{Z}_v$ be the residue class ring module v and t be a divisor of v. Moreover, let S be a difference set in $\mathbb{Z}_v$, $\varphi : \mathbb{Z}_v \to \mathbb{Z}_{\frac{v}{t}}$ be the homomorphism defined by
$$\varphi(a) \equiv a \bmod \left(\frac{v}{t}\right),$$
and $D = \varphi(S)$. For which values of t do the set D form an almost difference set?

3) Is there some infinite family of almost difference sets with parameters $(n, k, 2, t)$, and different from Theorem 1? Is there some infinite family of almost difference sets with parameters $(n, k, 1, t)$?

REFERENCES

[1] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar, and H. M. Martinsen, "Almost difference sets and their sequences with optimal autocorrelation," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2934–2943, Nov. 2001.

[2] E. J. Blum, J. C. Ribes, and F. Biraud, "Some new possibilities of optimal synthetic linear arrays for radioastronomy," *Astron. Astrophys.*, vol. 41, nos. 3–4, pp. 409–411, 1975.

[3] Y. Cai and C. Ding, "Binary sequences with optimal autocorrelation," *Theor. Comput. Sci.*, vol. 410, nos. 24–25, pp. 2316–2322, May 2009.

[4] N. Y. Caicedo, "Conjuntos de Sidon en dos dimensiones," M.S. thesis, Departamento de Matemáticas, Universidad del Valle, Cali, Colombia, 2016.

[5] Y. Caicedo, C. Martos, and C. Trujillo, "G-golomb rulers," *Revista Integración*, vol. 33, no. 2, pp. 161–172, Jul. 2015.

[6] J. Cilleruelo, "Combinatorial problems in finite fields and sidon sets," *Combinatorica*, vol. 32, no. 5, pp. 497–511, May 2012.

[7] D. Clayton, "A note on almost difference sets in nonabelian groups," *Designs, Codes Cryptogr.*, vol. 72, no. 3, pp. 1–6, 2017.

[8] T. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*. Amsterdam, The Netherlands: North-Holland Publishing Co., 1998.

[9] J. A. Davis, "Almost difference sets and reversible difference sets," *Archiv Math.*, vol. 59, no. 6, pp. 595–602, 1992.

[10] D. F. Daza, C. A. Trujillo, and F. A. Benavides, "Sidon sets and C4-saturated graphs," 2019, *arXiv:1810.05262*.

[11] C. Ding, "The differential cryptanalysis and design of natural stream ciphers," in *Proc. Fast Softw. Encryption, Cambridge Secur. Workshop*, in Lecture Notes in Computer Science, vol. 809, R. Anderson, Ed. Springer-Verlag, 1994, pp. 101–115.

[12] C. Ding, "Binary cyclotomic generators," in *Fast Software Encryption* (Lecture Notes in Computer Science), vol. 1008, B. Preneel, Ed. New York, NY, USA: Springer-Verlag, 1995, pp. 29–60.

[13] C. Ding, "Cyclic codes from cyclotomic sequences of order four," *Finite Fields Appl.*, vol. 23, pp. 8–34, Sep. 2013.

[14] C. Ding, *Codes from Difference Sets*. Hackensack, NJ, USA: World Scientific, 2015.

[15] C. Ding, T. Helleseth, and K. Y. Lam, "Several classes of binary sequences with three-level autocorrelation," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2606–2612, Nov. 1999.

[16] C. Ding, T. Helleseth, and H. M. Martinsen, "New families of binary sequences with optimal three-level autocorrelation," *IEEE Trans. Inf. Theory*, vol. 47, no. 1, pp. 428–433, Jan. 2001.

[17] C. Ding, A. Pott, and Q. Wang, "Constructions of almost difference sets from finite fields," *Des. Codes Cryptogr.*, vol. 72, no. 3, pp. 581–592, Sep. 2014.

[18] X. Tang and C. Ding, "New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6398–6405, Dec. 2010.

[19] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[20] C. A. G. Ruiz and C. A. T. Solarte, "A new construction of modular B_h-sequences," in *Matemáticas, Enseñanza Universitaria*, vol. 19, no. 1, pp. 53–62, 2011.

[21] M. Kovacevic and V. Y. F. Tan, "Codes in the space of multisets—Coding for permutation channels with impairments," *IEEE Trans. Inf. Theory*, vol. IT-64, no. 7, pp. 5156–5169, Jul. 1975.

[22] K. Klonowska, L. Lundberg, and H. Lennerstad, "Using Golomb rulers for optimal recovery schemes in fault tolerant distributed computing," in *Proc. Int. Parallel Distrib. Process. Symp.*, 2003, pp. 1–9.

[23] J. Michel and B. Ding, "A generalization of combinatorial designs and related codes," *Des., Codes Cryptogr.*, vol. 82, no. 3, pp. 511–529, Mar. 2017.

[24] K. Nowak, "A survey on almost difference sets," 2014, *arXiv:1409.0114*.

[25] C. A. M. Ojeda, L. M. Delgado, and C. A. Trujillo, "Bh Sets as a generalization of Golomb rulers," in *IEEE Access*, vol. 9, pp. 118042–118050, 2021, doi: 10.1109/ACCESS.2021.3106617.

[26] C. A. M. Ojeda, D. F. D. Urbano, and C. A. T. Solarte, "Near-optimal g-Golomb rulers," *IEEE Access*, vol. 9, pp. 65482–65489, 2021.

[27] H. M. Ruiz, L. M. Delgado, and C. A. Trujillo, "A new construction of optimal optical orthogonal codes from Sidon sets," *IEEE Access*, vol. 8, pp. 100749–100753, 2020.

[28] 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, May 1938.

[29] M. Tait and C. Timmons, "Orthogonal polarity graphs and sidon sets," *J. Graph Theory*, vol. 82, no. 1, pp. 103–116, May 2016.

[30] M. Tait and C. Timmons, "Sidon sets and graphs without 4-cycles," *J. Combinatorics*, vol. 5, no. 2, pp. 155–165, 2014.

[31] L. A. Vinh, "Graphs generated by sidon sets and algebraic equations over finite fields," *J. Combinat. Theory, Ser. B*, vol. 103, no. 6, pp. 651–657, Nov. 2013.

[32] Y. Zhang, J. G. Lei, and S. P. Zhang, "A new family of almost difference sets and some necessary conditions," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2052–2061, May 2006.

DAVID FERNANDO DAZA URBANO received the B.S. degree in mathematics and the M.S. degree in mathematical sciences from the Universidad del Cauca, Colombia, in 2015 and 2018, respectively, where he is currently pursuing the Ph.D. degree. He is also a member of the Algebra, Teoría de Números y Aplicaciones: ERM Research Group (ALTENUA). His research interests include Golomb rulers, Sidon sets, and graphs without four-cycles.

CARLOS ANDRES MARTOS OJEDA received the B.S. degree in mathematics and the M.S. degree in mathematical sciences from the Universidad del Cauca, in 2010 and 2015, respectively, and the Ph.D. degree in mathematics from the Universidad del Valle, in 2020. He is currently a member of the Algebra, Teoría de Números y Aplicaciones: ERM Research Group (ALTENUA). His research interests include additive number theory, Golomb rulers, Sidon sets, and mathematics of communications.

CARLOS ALBERTO TRUJILLO SOLARTE received the B.S. degree in mathematics from the Universidad del Cauca, in 1978, the M.S. degree in mathematical sciences from the Universidad del Valle, in 1987, and the Ph.D. degree in mathematics from the Universidad Politécnica de Madrid, in 1998. He is the Director of the program Doctorado en Ciencias Matemáticas (Universidad del Cauca) and the Director of the Algebra, Teoría de Números y Aplicaciones: ERM Research Group (ALTENUA). His research interests include additive number theory, Sidon sets, Golomb rulers, Costas arrays, sonar sequences, and mathematics of communications.