Received April 15, 2020, accepted May 8, 2020, date of publication May 22, 2020, date of current version June 9, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2996813

A New Construction of Optimal Optical Orthogonal Codes From Sidon Sets

HAMILTON M. RUIZ, LUIS M. DELGADO, AND CARLOS A. TRUJILLO

Departamento de Matemáticas, Universidad del Cauca, 190001 Popayán, Colombia

Corresponding author: Hamilton M. Ruiz (mauruiz@unicauca.edu.co)

This work was supported in part by the Departamento Administrativo de Ciencia, Tecnología e Innovación COLCIENCIAS, and in part by the University of Cauca through the project ''Aplicaciones a la teoría de la información y comunicación de los Conjuntos de Sidon y sus generalizaciones'' under Grant Código 110371250560.

ABSTRACT Two new constructions for families of optical orthogonal codes are presented. The first is a generalization of the well-known construction of Sidon sets given by I. Z. Ruzsa. The second construction is optimal with respect to the Johnson bound, and its parameters (n, w, λ) are respectively $(p^{h+1} - p, p, 1)$, where p is any prime, h is an integer greater than 1 and the family size is $p^{h-1} + p^{h-2} + \cdots + p^2 + p$.

INDEX TERMS Optical code-division multiple access (OCDMA), optical orthogonal code (OOC), optical CDMA, Sidon set.

I. INTRODUCTION

An (n, w, λ) optical orthogonal code (OOC) [2] $\mathcal{C}$, $n > 1$, $1 \le w \le n$, $1 \le \lambda \le w$, is a family of (0, 1) sequences of length n and constant Hamming weight w which satisfy the following two properties:

- The Autocorrelation Property:
$$\sum_{k=0}^{n-1} x_k x_{k\oplus\tau} \le \lambda, \tag{1}$$
for any $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathcal{C}$ and any integer $\tau \not\equiv 0 \bmod n$.
- The Cross-Correlation Property:
$$\sum_{k=0}^{n-1} x_k y_{k\oplus\tau} \le \lambda, \tag{2}$$
for any $x = (x_0, x_1, \ldots, x_{n-1})$, $y = (y_0, y_1, \ldots, y_{n-1})$ in $\mathcal{C}$, such that $x \neq y$ and any integer τ, where $\oplus$ denotes addition modulo n. We will refer to λ as the maximum correlation parameter.

Codes with these properties have been called optical orthogonal codes in [1] and [2] in connection with applications in optical code-division multiple-access communication systems (OCDMA). OOC was first suggested in 1989 [2], in particular, OOCs with $\lambda = 1$ have been more extensively studied in [2]–[11].

The associate editor coordinating the review of this manuscript and approving it for publication was Xueqin Jiang.

For a given set of values of n, w and λ, the largest possible size of an (n, w, λ) optical orthogonal code is denoted by $\Phi(n, w, \lambda)$. A code achieving this maximum size is called *optimal*. The Johnson upper bound [2] on the cardinality of a constant-weight binary code can be adapted to yield the following upper bound

$$\Phi(n, w, \lambda) \le \left\lfloor \frac{1}{w} \left\lfloor \frac{n-1}{w-1} \left\lfloor \frac{n-2}{w-2} \left\lfloor \cdots \left\lfloor \frac{n-\lambda}{w-\lambda} \right\rfloor \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor.$$

This correspondence is concerned only with OOCs families having parameter $\lambda = 1$. In this case, the Johnson bound takes on the form

$$\Phi(n, w, 1) \le \left\lfloor \frac{n-1}{w(w-1)} \right\rfloor.$$

Some know algebraic constructions for families of OOCs are presented in Table 1. The new constructions introduced in this paper are shown in Table 2.

We may also view optical orthogonal codes from a set-theoretical perspective. An (n, w, λ)-OOC $\mathcal{C}$ can be alternatively considered as a family of w-sets of integers modulo n, in which each w-set corresponds to a codeword and the integers within each w-set specify the nonzero bits of the codeword. In this setting, the correlation properties can be reformulated as follow.

The Autocorrelation Property:

$$|\,(a + X) \cap X\,| \le \lambda, \tag{3}$$

TABLE 1. Parameters of optical orthogonal codes with $\lambda = 1$, here p denote a prime, and q is a power prime of p.

Construction name	Parameters	Code Size	Constraints
Singer Construction* [16] [2]	$(q^2+q+1, q+1, 1)$	1	
Projective Geometry* [2]	$(\frac{q^{d+1}-1}{q-1}, q+1, 1)$	$\begin{cases} \frac{q^d-1}{q^2-1}, & d \text{ even}, \\ \frac{q^d-q}{q^2-1}, & d \text{ odd}. \end{cases}$	
Combinatorial Method* [2]	$(n, 3, 1)$	$\lfloor \frac{n-1}{6} \rfloor$	$n \not\equiv 2 \bmod 6$
Generalized Bose-Chowla* [4]	$(q^m-1, q, 1)$	$\frac{q^{m-1}-1}{q-1}$	All positive integer m
Chu-Golomb* [8]	$(m(q^2+q+1), q+1, 1)$	m	Every prime divisor of m is greater than q and $m < q^2+q+1$
Chu-Golomb [8]	$((q^2+q+1)^t, q+1, 1)$	$(q^2+q+1)^{t-1}$	All prime divisors of q^2+q+1 are bigger than q
JK construction $\mathcal{A}$ [11]	$(Mp^n, M, 1)$	$\frac{p^n-1}{M}$	$p-1 = MT$
JK construction* $\mathcal{B}1$ [11]	$(Mp, M, 1)$	T	$p-1 = MT$, $(M-1)^2 > p-1$
JK construction $\mathcal{B}2$ [11]	$(Mp_1\cdots p_k, M, 1)$	$\frac{p_1\cdots p_k - 1}{M}$	$M \mid (p_i - 1)$ for $i = 1, \ldots, k$
Conics on Finite [17] Projective Plane	$(q^3+q^2+q+1, q+1, 2)$	q^3-q^2+q	
Chung-Kumar* [3]	$(p^{2m}-1, p^m+1, 2)$	p^m-2	All positive integer m
Chung-Kumar* [3] (via Wilson difference sets)	$(p, w, 1)$	r	$p = w(w-1)r+1$ $w = 2t+1$, or $w = 2t$
Alderson-Mellinger* [15]	$(q^k+1, q+1, 2)$	$q^{k-1}(q^{k-2}+q^{k-4}+\cdots+q^2+1)$	k is even
MZKZ Family $\mathcal{A}$ [9]	(pm, m, t)	$\frac{1}{mp}\sum_{d\mid p-1} p^{\lceil (t+1)/d \rceil}\mu(d)$	$m \mid (p-1)$, $1 \le t \le m$
MZKZ Family $\mathcal{B}$ [9]	$((q-1)p, p-t, t)$	$\frac{q}{p}(\frac{q^t-1}{q-1})$	$1 \le t \le (p-t)$
MZKZ Family $\mathcal{C}$ [9]	$(m(q+1), m, 2t)$	$\frac{1}{(q+1)m}\sum_{d\mid(q-1)}\mu(d)c([t/d])$ where $c(t) = \begin{cases} q^{2t+1}-q, & 1 \le t \le 6 \\ \ge q^{2t+1}-q^{2t-6}/7, & t \ge 7 \end{cases}$	$m\mid(q-1)$, $(m, q+1) = 1$, $1 \le t \le m/2$

An $*$ in the table indicates that the corresponding construction is optimal with respect to the Johnson bound.

TABLE 2. New family of optical orthogonal codes from this correspondence.

Construction name	Parameters	Code Size	Constraints
Ruiz, Delgado, Trujillo Construction	$(p^{h+1}-p, p, 1)$	$p^{h-1}-1$	p is prime, $h \ge 2$
Ruiz, Delgado, Trujillo Construction*	$(p^{h+1}-p, p, 1)$	$\frac{p(p^{h-1}-1)}{p-1}$	p is prime, $h \ge 2$

An $*$ in the table indicates that the corresponding construction is optimal with respect to the Johnson bound.

for any $X \in \mathcal{C}$ and any integer $a \not\equiv 0 \bmod n$.

The Correlation Property:

$$| (a+X) \cap Y | \le \lambda, \tag{4}$$

for any $X, Y \in \mathcal{C}$, such that $X \neq Y$ and any integer a, where $a+X = \{a+x : x \in X\}$, and all integers under consideration are taken modulo n.

Using this fact, we can derive the following interpretation of the correlation properties.

Let $\mathcal{C}$ be an (n, w, λ)-OOC, then the following two conditions hold:

1) for each $X \in \mathcal{C}$, any nonzero integer a can be represented as a difference $x - x'$, with $x, x' \in X$ in at most λ ways;
2) for each $X \in \mathcal{C}$ and $Y \in \mathcal{C}$ with $X \neq Y$, any integer a can be represented as a difference $x - y$, with $x \in X$ and $y \in Y$ in at most λ ways.

The following notation will be useful later.

Notation 1: For a subset X of an additive group G, we will denote by $\Delta(X)$ the set of all the nonzero differences in X:

$$\Delta(X) := \{a - b : a, b \in X, a \neq b\}.$$

We will use the following elementary proposition about $(n, w, 1)$-OOCs.

Lemma 1: Let $\mathcal{C}$ be an $(n, w, 1)$-OOC then

1) $|\Delta(X)| = w(w-1)$ for any $X \in \mathcal{C}$.
2) $\Delta(X) \cap \Delta(Y) = \emptyset$ for any $X, Y \in \mathcal{C}$, with $X \neq Y$.

In Section II, we present two new families of optical orthogonal codes with $\lambda = 1$. One of these is optimal with respect to the Johnson bound. We will show that these have a nice algebraic structure. Our constructions use the Sidon set given by Ruzsa [14] and the construction of OOC by Moreno *et al.* [4]. Finally, we give some concluding remarks in Section III.

II. CONSTRUCTIONS

Definition 1: Let $(G, +)$ be an abelian additive group with identity e and $A \subset G$. A is called a Sidon set in G, if for any $x \not\equiv e \bmod G$, we have

$$|(x + A) \cap A| \leq 1.$$

Lemma 2: Let $(G_1, +)$, $(G_2, *)$ be abelian groups and $\varphi : G_1 \longrightarrow G_2$ an injective homomorphism. If A is a Sidon set in G_1, then $\varphi(A)$ is a Sidon set in G_2.

Example 1: Let p be a prime number, α a primitive root modulo p, and $\mathcal{R} = \{(i, \alpha^i) : 1 \leq i \leq p-1\} \subset (\mathbb{Z}_{p-1} \times \mathbb{Z}_p, +)$. $\mathcal{R}$ is a Sidon set in $(\mathbb{Z}_{p-1}, +) \times (\mathbb{Z}_p, +)$ with $p-1$ elements. Define $\varphi : (\mathbb{Z}_{p-1}, +) \times (\mathbb{Z}_p, +) \longrightarrow \mathbb{Z}_{p(p-1)}$ by $\varphi(i, \alpha^i) = x$, where x is a solution to the system of congruences

$$x \equiv i \bmod (p-1),$$
$$x \equiv \alpha^i \bmod p.$$

By the Chinese remainder theorem, φ is an injective homomorphism and so

$$\varphi(\mathcal{R}) = \mathcal{R}(p, \alpha) = \{pi - (p-1)\alpha^i : 1 \leq i \leq p-1\}$$

is a Sidon set in $\mathbb{Z}_{p(p-1)}$ with $p-1$ elements.

The set $\mathcal{R}(p, \alpha)$ is know as Ruzsa's construction [14].

A. CONSTRUCTION A

Let p be a prime number, $h \geq 2$ integer, $\mathbb{F}_{p^h}$ the finite field with p^h elements, and θ a primitive element in $\mathbb{F}_{p^h}$. Let

$$\mathcal{P} = \{p(x) \in \mathbb{F}_p[x] : 1 \leq \deg(p(x)) \leq h-1 \text{ and } p(0) = 0\}, \tag{5}$$

then $|\mathcal{P}| = p^{h-1} - 1$. We will prove that

$$\mathcal{C} = \{\{p^h \log_\theta(p(\theta) + a) - (p^h - 1)a : a \in \mathbb{F}_p\} : p(x) \in \mathcal{P}\}$$

is a $(p(p^h - 1), p, 1)$-OOC with $p^{h-1} - 1$ elements.

Proof 1: We consider the family of subsets

$$R = \{\{(a, \log_\theta(p(\theta) + a)) : a \in \mathbb{F}_p\} : p(x) \in \mathcal{P}\}, \tag{6}$$

of the group $(\mathbb{Z}_p, +) \times (\mathbb{Z}_{p^h - 1}, +)$.

Cross Correlation Property: we need to show that each element $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_{p^h - 1}$ can be represented as a difference $(x, y) - (x', y')$ with $(x, y) \in X$ and $(x', y') \in Y$ in at most one way, for any $X, Y \in R$ with $X \neq Y$. By contradiction, suppose that there exist $a_1, a_2, a_3, a_4 \in \mathbb{Z}_p$, with $a_1 \neq a_2$, $a_3 \neq a_4$, and $p(x)$, $q(x)$ in $\mathcal{P}$, $p(x) \neq q(x)$ with $\deg p = i$ and $\deg q = j$, such that

$$\begin{aligned}(a_1, \log_\theta(p(\theta) + a_1)) &- (a_2, \log_\theta(p(\theta) + a_2)) \\ &= (a_3, \log_\theta(q(\theta) + a_3)) - (a_4, \log_\theta(q(\theta) + a_4)).\end{aligned}$$

Then

$$a_1 - a_2 = a_3 - a_4 \bmod p, \tag{7}$$

$$(p(\theta) + a_1)(p(\theta) + a_4) = (q(\theta) + a_3)(q(\theta) + a_2) \bmod p^h.$$

Therefore

$$(a_1 - a_2)q(\theta) + a_1 a_4 = (a_3 - a_4)p(\theta) + a_3 a_2 \tag{8}$$

in $\mathbb{F}_{p^h}$. The equation (8) can be seen as a polynomial in θ with degree less than h, and therefore must be equal to zero.

If $j > i$, then $a_1 = a_2$, which is a contradiction then $i = j$ and since $\deg(p(x)), \deg(q(x)) > 0$ we have

$$(a_1 - a_2)q(\theta) = (a_3 - a_4)p(\theta), \tag{9}$$
$$a_1 a_4 = a_3 a_2. \tag{10}$$

By (9)

$$a_1 - a_2 = (a_3 - a_4)u, \tag{11}$$

for some unit $u \in \mathbb{Z}_p$. By (7) and (11) we have

$$(a_3 - a_4)(u - 1) \equiv 0 \bmod p.$$

If $u \not\equiv 1 \bmod p$, then $a_3 - a_4 \equiv 0 \bmod p$ which is a contradiction. Therefore $u = 1$ and then $q(\theta) = p(\theta)$ which contradicts the fact that $\deg(\theta, \mathbb{F}_p) = h$.

This concludes the proof of the cross-correlation property.

Autocorrelation Property: in this case, we can set $p(x) = q(x)$ in the previous proof. From (9) and (10) we have that a_1, a_2, a_3, a_4 are roots of the equation $x^2 - (a_1 + a_4)x + a_1 a_4 = 0$ over $\mathbb{F}_p$. Thus

$$\{a_1, a_4\} = \{a_2, a_3\}.$$

Since $a_1 \neq a_2$ and $a_3 \neq a_4$, then $a_1 = a_3$ and $a_2 = a_4$, which corresponds to autocorrelation at the shift zero.

Finally, by the Chinese remainder theorem and Lemma 2, the set

$$\mathcal{C} = \{\{p^h \log_\theta(p(\theta) + a) - (p^h - 1)a : a \in \mathbb{Z}_p\} : p(x) \in \mathcal{P}\}$$

is a $(p(p^h - 1), p, 1)$-OOC with $p^{h-1} - 1$ elements.

Theorem 1: For any prime p and any integer $h \geq 2$, the set $\mathcal{C}$ defined as above is a $(p(p^h - 1), p, 1)$-OOC with $p^{h-1} - 1$ codewords.

Example 2: For $p = 3$ and $h = 3$, consider $p(x) = x^3 + 2x + 1$ as the generator polynomial for $\mathbb{F}_{27}$ and let θ be a root of $p(x)$. We can construct the following (78, 3, 1)-OOC $\mathcal{C}_1$ consisting of the following codewords.

$$c_1 = \{27\log_\theta(p_1(\theta)+a) - 26a : a \in \mathbb{Z}_3\} = \{27, 29, 61\},$$
$$c_2 = \{27\log_\theta(p_2(\theta)+a) - 26a : a \in \mathbb{Z}_3\} = \{16, 66, 74\},$$
$$c_3 = \{27\log_\theta(p_3(\theta)+a) - 26a : a \in \mathbb{Z}_3\} = \{38, 54, 73\},$$
$$c_4 = \{27\log_\theta(p_4(\theta)+a) - 26a : a \in \mathbb{Z}_3\} = \{71, 75, 76\},$$
$$c_5 = \{27\log_\theta(p_5(\theta)+a) - 26a : a \in \mathbb{Z}_3\} = \{11, 36, 58\},$$
$$c_6 = \{27\log_\theta(p_6(\theta)+a) - 26a : a \in \mathbb{Z}_3\} = \{8, 15, 25\},$$
$$c_7 = \{27\log_\theta(p_7(\theta)+a) - 26a : a \in \mathbb{Z}_3\} = \{30, 59, 70\},$$
$$c_8 = \{27\log_\theta(p_8(\theta)+a) - 26a : a \in \mathbb{Z}_3\} = \{5, 46, 69\},$$

where $p_1(x) = x$, $p_2(x) = 2x$, $p_3(x) = x^2$, $p_4(x) = 2x^2$, $p_5(x) = x^2 + x$, $p_6(x) = 2x^2 + x$, $p_7(x) = x^2 + 2x$, and $p_8(x) = 2x^2 + 2x$.

B. CONSTRUCTION B

The previous construction is not optimal with respect to the Johnson bound. However, it is possible to generate an optimal optical orthogonal code by adding to it a suitable number of codewords.

For this purpose, we analyze the set of nonzero elements that can be represented as a difference $x - x'$ with $x, x' \in X$, $X \in \mathcal{C}$. We consider the sets

$$\Delta(X) = \{(a-b) \bmod (p(p^h-1)) : a, b \in X, a \neq b\},$$
$$D = \bigcup_{X\in\mathcal{C}} \Delta(X).$$

By Lemma 1 we have that $|D| = (p-1)(p^h - p)$.

Denote by M_p the set of nonzero multiples of p modulo $p(p^h - 1)$. Let $M = M_p \cup M_q$, where $q = \frac{p^h-1}{p-1}$. We will prove that $D \cap M = \emptyset$.

1) Let $z = pt$ for some $1 \le t \le p^h - 2$. Suppose that $z = x - y$, for some $x, y \in X$ and $X \in C$. Then

$$z = [\log_\theta(p(\theta)+a)(p(\theta)+b)^{-1}] \bmod (p^h-1),$$
$$z = (a-b) \bmod p,$$

for some $a, b \in \mathbb{Z}_p$ and $p(x) \in \mathcal{P}$. Since $z = pt$, then $a = b \bmod p$, therefore $a = b$. Accordingly $z = 0 \bmod (p^h - 1)$ and also $z = 0 \bmod p$, implying $z = 0 \bmod p(p^h - 1)$ which is a contradiction.

2) Let $z = qt$ for some $1 \le t < p^2 - p$. Suppose that $z = x - y$ for some $x, y \in X$ and $X \in C$. Then

$$z = [\log_\theta(p(\theta)+a)(p(\theta)+b)^{-1}] \bmod (p^h-1),$$
$$z = (a-b) \bmod p,$$

for some $a, b \in \mathbb{Z}_p$ and $p(x) \in \mathcal{P}$. Therefore $\theta^z(p(\theta) + b) = p(\theta) + a$ in $\mathbb{F}_{p^h}$.

We consider two cases.

Case 1. If $\theta^z = 1$, then $a = b \bmod p$ and thereby $z = 0 \bmod p$. Thus $t = pk$ for some $1 \le k < p - 1$. Since $\theta^z = 1$, then $z = 0 \bmod (p^h - 1)$ and therefore $z = 0 \bmod (p - 1)$. By the above, we have $p = 0 \bmod p(p - 1)$ which is a contradiction.

Case 2. If $\theta^z \neq 1$, since $\theta^z \in \mathbb{F}_p$ then $q(x) = p(x)(\theta^z - 1) + (b - a)$ is a polynomial in $\mathbb{F}_p[x]$ of degree less than h that such $q(\theta) = 0$, which is a contradiction.

Thus

$$D = \mathbb{Z}_{p(p^h-1)} \setminus (M \cup \{0\}).$$

Now we will use the following construction of OOC given by Moreno *et al.* [4].

Lemma 3: Let $h \ge 2$ be an integer, θ a primitive element of $\mathbb{F}_{p^h}$, $\mathcal{P}$ as in (5) and $\mathcal{Q} = \{p(x) \in \mathcal{P} : p \text{ is monic}\}$. Then

$$\mathcal{C} = \{\{\log_\theta(p(\theta)+a) : a \in \mathbb{F}_p\} : p(x) \in \mathcal{Q}\}$$

is an optimal $(p^h - 1, p, 1)$-OOC with $\frac{p^{h-1}-1}{p-1}$ codewords.

Now, let $\varphi : \mathbb{Z}_{p^h-1} \to \mathbb{Z}_{p(p^h-1)}$ given by $\varphi(x) = px$. It is not hard to see that φ is an injective homomorphism. Applying φ to each element of C, by Lemma 2 we have that

$$\bigcup_{X\in C} \varphi(X) = \{\{p\log_\theta(p(\theta)+a) : a \in \mathbb{Z}_p\}$$

is a $(p^{h+1} - p, p, 1)$-OOC with $\frac{p^{h-1}-1}{p-1}$ codewords.

Finallly, we prove that $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ where

$$\mathcal{C}_1 = \{\{p^h\log_\theta(p(\theta)+a) - (p^h-1)a : a \in \mathbb{Z}_p\} : p(x) \in \mathcal{P}\}$$
$$\mathcal{C}_2 = \{\{p\log_\theta(p(\theta)+a) : a \in \mathbb{Z}_p\} : p(x) \in \mathcal{Q}\}\}$$

is a $(p(p^h - 1), p, 1)$-OOC.

It is sufficient to prove the cross-correlation property for any $X \in \mathcal{C}_1$ and any $Y \in \mathcal{C}_2$. We will prove that

$$|(a + X) \cap Y| \le 1$$

for any integer a.

Suppose that there exists an integer a such that

$$a = x - y = x' - y',$$

for some $x, x' \in X$, $y, y' \in Y$ with $x \neq x'$ and $y \neq y'$. Then $x - x' = y' - y$, which is a contradiction because $x - x' \notin M_p$, while that $y' - y \in M_p$. Also, since $\mathcal{C}_1 \cap \mathcal{C}_2 = \emptyset$, we have $|\mathcal{C}| = p^{h-1} + p^{h-2} + \cdots + p^2 + p$.

Theorem 2: For any prime p and any integer $h \ge 2$, the set $\mathcal{C}$ defined as above is a $(p(p^h - 1), p, 1)$-OOC with $p^{h-1} + p^{h-2} + \cdots + p^2 + p$ codewords.

Corollary 1: The construction of Theorem 2 is optimal with respect to the Johnson bound.

Proof 2:

$$\Phi(p^{h+1} - p, p, 1) = \left\lfloor \frac{p^{h+1} - p^2}{p^2 - p} + \frac{p^2 - p - 1}{p^2 - p} \right\rfloor = |\,C\,|.$$

Remark 1: For $h = 1$ the set given in (6) can be expressed in the form

$$R = \{(a, \log_\theta(\theta + a) : \theta + a \neq 0\} \subset \mathbb{Z}_p \times \mathbb{Z}_{p-1},$$

which coincides with the Sidon set shown in Example 2.

Example 3: Continuing with Example 2, by Lemma 3 we can construct the following $(26, 3, 1)$-OOC $\mathcal{C}'$ consisting of the following codewords.

$$c_9 = \{\log_\theta(p_1(\theta) + a) : a \in \mathbb{F}_3\} = \{1, 3, 9\},$$
$$c_{10} = \{\log_\theta(p_3(\theta) + a) : a \in \mathbb{F}_3\} = \{2, 12, 21\},$$
$$c_{11} = \{\log_\theta(p_5(\theta) + a) : a \in \mathbb{F}_3\} = \{6, 10, 11\},$$
$$c_{12} = \{\log_\theta(p_7(\theta) + a) : a \in \mathbb{F}_3\} = \{4, 7, 18\}.$$

Then $\mathcal{C}_2 = \{\{3, 9, 27\}, \{6, 36, 63\}, \{18, 30, 33\}, \{12, 21, 54\}\}$ is a $(78, 3, 1)$-OOC, and so $\mathcal{C}_1 \cup \mathcal{C}_2$ is an optimal $(78, 3, 1)-$OOC.

Remark 2: Constructions $\mathcal{A}$ and $\mathcal{B}$ in this paper have the same length of the Family $\mathcal{B}$ in [9] for $t = 1$ (see the MZKZ Family $\mathcal{B}$ in Table 1). However, our constructions have weight one unit more. Our approach seems to be more natural and as a consequence, our second code has optimal cardinality, which is an advantage if it is applied to OCDMA systems. In this scenario, construction $\mathcal{B}$ is better than MZKZ Family $\mathcal{B}$.

III. CONCLUSION

We presented two new constructions of optical orthogonal codes with $\lambda = 1$. One of these is optimal with respect to the Johnson bound and its parameters are $(p(p^h - 1), p, 1)$, where p is a prime number and h is an integer greater than 1. The code size is $p^{h-1} + \cdots + p^2 + p$.

For $\lambda > 1$ the combinatorial problem involving the concept of OOC is more difficult. We can apply a procedure similar to that seen in this document, however, the size of the obtained code is far from reaching the Johnson bound. The current method under certain circumstances can be applied to optimize the families of asymptotically optimal OOCs presented in [11] and [12]. This is a subject for future work.

ACKNOWLEDGMENT

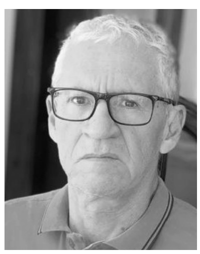
The authors would like to thank the Universidad del Cauca. H. M. Ruiz and L. M. Delgado would like to thank COLCIENCIAS for supporting their doctoral studies.

REFERENCES

[1] E. F. Brickell and V. K. Wei, "Optical orthogonal codes and cyclic block designs," *Congr. Numer*, vol. 58, pp. 175–192, Jan. 1987.
[2] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: Design, analysis and applications," *IEEE Trans. Inf. Theory*, vol. 35, no. 3, pp. 595–604, May 1989.
[3] H. Chung and P. V. Kumar, "Optical orthogonal codes-new bounds and an optimal construction," *IEEE Trans. Inf. Theory*, vol. 36, no. 4, pp. 866–873, Jul. 1990.
[4] O. Moreno, R. Omrani, P. V. Kumar, and H.-F. Lu, "A generalized Bose–Chowla family of optical orthogonal codes and distinct difference sets," *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1907–1910, May 2007.
[5] G.-C. Yang, "Some new families of optical orthogonal codes for code-division multiple-access fibre-optic networks," *IEE Proc.-Commun.*, vol. 142, no. 6, pp. 363–368, Dec. 1995.
[6] J. Yin, "Some combinatorial constructions for optical orthogonal codes," *Discrete Math.*, vol. 185, nos. 1–3, pp. 201–219, Apr. 1998.
[7] Y. Miao and R. Fuji-Hara, "Optical orthogonal codes: Their bounds and new optimal constructions," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2396–2406, Nov. 2000.
[8] W. Chu and S. W. Golomb, "A new recursive construction for optical orthogonal codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 3072–3076, Nov. 2003.
[9] O. Moreno, Z. Zhang, P. V. Kumar, and V. A. Zinoviev, "New constructions of optimal cyclically permutable constant weight codes," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 448–455, Mar. 1995.
[10] R. M. Wilson, "Cyclotomy and difference families in elementary abelian groups," *J. Number Theory*, vol. 4, no. 1, pp. 17–47, Feb. 1972.
[11] J.-H. Chung and K. Yang, "Asymptotically optimal optical orthogonal codes with new parameters," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3999–4005, Jun. 2013.
[12] J.-H. Chung and K. Yang, "New construction of asymptotically optimal optical orthogonal codes," in *Proc. IEEE Inf. Theory Workshop Fall (ITW)*, Oct. 2015, vol. 59, no. 6, pp. 129–132.
[13] C. Gomez and C. Trujillo, "Una nueva construccion de conjuntos B_h modulares," *Matematicas, Ensenanza Universitaria*, vol. 19, no. 1, pp. 53–62, 2011.
[14] I. Ruzsa, "Solving a linear equation in a set of integers i," *Acta Arithmetica*, vol. 65, no. 3, pp. 259–282, 1993.
[15] T. L. Alderson and K. E. Mellinger, "Geometric constructions of optimal optical orthogonal codes," *Adv. Math. Commun.*, vol. 2, no. 4, pp. 451–467, 2008.
[16] 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, 1938.
[17] N. Miyamoto, H. Mizuno, and S. Shinohara, "Optical orthogonal codes obtained from conics on finite projective planes," *Finite Fields Appl.*, vol. 10, no. 3, pp. 405–411, Jul. 2004.

HAMILTON M. RUIZ received the B.S. degree in mathematics from the Universidad de Nariño, Colombia, in 2013, and the M.S. degree in mathematical sciences from the Universidad del Cauca, Colombia, in 2018, where he is currently pursuing the Ph.D. degree. He is a member of the research group ALTENUA (Algebra, Teoria de Números y Aplicaciones). His research interests include coding theory, design theory, and Sidon sets.

LUIS M. DELGADO received the B.S. degree in mathematics from the Universidad de Nariño, Colombia, in 2009, and the M.S. degree in mathematical sciences from the Universidad del Cauca, Colombia, in 2018, where he is currently pursuing the Ph.D. degree. He is a member of the research group ALTENUA (Algebra, Teoria de Números y Aplicaciones). His research interests include Golomb rulers and Sonar sequences.



CARLOS A. TRUJILLO 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 1986, and the Ph.D. degree in mathematics from the Universidad Politécnica de Madrid, in 1998. He is currently the Director of the Ph.D. program in mathematical sciences with the Universidad del Cauca, and the Director of the research group ALTENUA (Algebra, Teoria de Números y Aplicaciones). His research interests include coding theory, Golomb rulers, Sonar sequences, and Sidon sets.