Spectral Classification and Multiplicative Partitioning of Constant-Weight Sequences Based on Circulant Matrix Representation of Optical Orthogonal Codes

Mohammad M. Alem-Karladani and Jawad A. Salehi, *Senior Member, IEEE*

***Abstract*—Considering the space of constant-weight sequences as the reference set for every optical orthogonal code (OOC) design algorithm, we propose a classification method that preserves the correlation properties of sequences. First, we introduce the circulant matrix representation of optical orthogonal codes and, based on the spectrum of circulant matrices, we define the spectral classification of the set $S_{n,w}$ of all (0, 1) -sequences with length n, weight w, and the first chip "1". Then, as a method for spectrally classifying the set $S_{n,w}$, we discuss an algebraic structure called multiplicative group action. Using the above multiplicative group action, we define an equivalence relation on $S_{n,w}$ in order to classify it into equivalence classes called multiplicative partitions which are the same as the spectral classes. The algebraic properties of the proposed partitioning such as the number of classes and the size of each class are investigated and in the case of prime n, a novel formula for the number of classes is derived. Finally, we present and prove the autocorrelation, intraclass and interclass cross-correlation properties of our proposed classification of the space $S_{n,w}$ that decrease the computational complexity of search algorithms in designing and constructing $(n, w, \lambda_a, \lambda_c)$-OOC.**

***Index Terms*—Autocorrelation, circulant matrix, cross correlation, group action, multiplicative partitioning, optical orthogonal code (OOC), spectral classification.**

I. Introduction

An OPTICAL orthogonal code (OOC) is a family of (0, 1)-sequences with desired auto- and cross-correlation properties providing asynchronous multi-access communications with easy synchronization and good performance in OCDMA communication networks [1]–[3]. Ever since the introduction of optical orthogonal codes, there has been continuous and extensive efforts for devising efficient algorithms to construct these codes. The algorithms based on mathematical structures such as finite projective geometry [1], [4], block design [5]–[8], finite Möbius geometry [9], combinatorics [1], [10], Galois fields [11], [12], etc., are applicable for particular numbers of code-length n, code-weight w, auto- and cross-correlation constraints λ_a and λ_c that may not be suitable for real and practical systems. For example, to the best of our knowledge, there is not any mathematical algorithm for constructing OOCs of length $n = 2^k$ which is appropriate for implementation in digital systems such as Field Programmable Gate Array (FPGA) [13]. Hence, it seems that the only available method for designing optical orthogonal codes with rather arbitrary values of length, weight and correlation constraints is the use of search algorithms. One of the major drawbacks of the search methods such as greedy, accelerated greedy, and outer-product matrix algorithms is their lack of optimality from the number of codewords viewpoint [1], [14]. In other words, in these algorithms there is a substantial gap between the number of constructed codewords and that of potentially available ones. Furthermore, this gap increases as the code length and weight increase [14]. In order to find optimal codes via search algorithms, it is necessary to run a complete search on the set of all possible sequences which is almost impossible due to its excessive computational complexity. However, in this paper, we show that by establishing an algebraic structure on the reference set of available sequences and using its properties, it is possible to confine the search space and decrease the complexity of the search algorithms.

Definition 1: An $(n, w, \lambda_a, \lambda_c)$ optical orthogonal code is a family C of (0, 1)-sequences of length n with constant Hamming-weight w satisfying the following two properties:

The autocorrelation property: For any codeword $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in C$, the inequality $R_{\mathbf{xx}}(\tau) = \sum_{i=0}^{n-1} x_i x_{i\oplus\tau} \leq \lambda_a$ holds for any integer $\tau \neq 0 (\mathrm{mod}\ n)$.

The cross-correlation property: For any two distinct codewords $\mathbf{x}$ and $\mathbf{y}$ in C, the inequality $R_{\mathbf{xy}}(\tau) = \sum_{i=0}^{n-1} x_i y_{i\oplus\tau} \leq \lambda_c$ holds for any integer τ.

$\oplus$ denotes the modulo-n addition and λ_a and λ_c are respectively called autocorrelation and cross-correlation constraints.

When $\lambda_a = \lambda_c = \lambda$, we denote (n, w, λ)-OOC for simplicity. The number of codewords is called the size of optical orthogonal code. From a practical point of view, a code with large size is required [2], [3]. To find the best possible codes, we need to determine an upper bound on the size of an OOC with the given parameters. Let $\Phi(n, w, \lambda_a, \lambda_c)$ be the largest possible size of an $(n, w, \lambda_a, \lambda_c)$-OOC. An OOC achieving this maximum size is said to be optimal [1]. It is easily shown that if $w(w-1) > \lambda_a(n-1)$ then $\Phi(n, w, \lambda_a, \lambda_c) = 0$ and if $w^2 > \lambda_c n$ then $\Phi(n, w, \lambda_a, \lambda_c) \leq 1$ [12]. The Johnson bound is the most general upper bound for $\Phi(n, w, \lambda)$[1], [12]

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

where $\lfloor\ \rfloor$ denotes the integer floor function. As an example, the set $\{1100100000000, 1010000100000\}$ is a (13, 3, 1)-OOC

Manuscript received October 07, 2009; revised April 25, 2010. Date of current version August 18, 2010. This work was supported in part by the Iran National Science Foundation (INSF).

The authors are with the Optical Networks Research Laboratory (ONRL), Advanced Communications Research Institute (ACRI), Electrical Engineering Department, Sharif University of Technology, Tehran, Iran (e-mail: malem@alum.sharif.edu, jasalehi@sharif.edu).

Communicated by N. Yu, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2010.2054570

with two codewords. This code is optimal since $\Phi(13,3,1) \leq \left\lfloor \frac{1}{3}\left\lfloor \frac{13-1}{3-1} \right\rfloor \right\rfloor = 2$.

A useful depiction for OOC is the set-theoretical representation $X = \{k \in Z_n; x_k = 1\}$ for each codeword $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$, where $Z_n = \{0, 1, \ldots, n-1\}$ denotes the modulo-n integers [1]. As an instance, $\{\{0,1,4\},\{0,2,7\}\} \pmod{13}$ is the representation of the above (13,3,1)-OOC. For another example, the following set is the set-theoretical representation of an optimal (40,4,1)-OOC [4]

$$C = \Big\{\{0,1,28,37\},\{0,2,18,25\},\{0,5,11,19\}\Big\} \pmod{40}. \tag{2}$$

Based on this representation, the correlation properties for any codewords X and Y and any modulo-n integers a and b can be reformulated as follows [1].

The autocorrelation property: $|(a \oplus X) \cap (b \oplus X)| \leq \lambda_a, a \neq b \pmod{n}$.

The cross-correlation property: $|(a \oplus X) \cap (b \oplus Y)| \leq \lambda_c, X \neq Y$.

$a \oplus X$ is defined as $\{a \oplus x; x \in X\}$ and $|X|$ denotes the cardinal number of the set X.

Similar to low-density parity-check (LDPC) codes, the density of marked chips in optical orthogonal codes is very low and it has motivated some research on the relation of OOCs and LDPC codes [15], [16]. There are several OOC design methods based on mathematical structures such as projective geometry [1], [4] and finite field theory [11], [12], [17], as well as search algorithms such as greedy [1] and outer-product matrix [14]. A comprehensive study of the OOC construction algorithms has been given in [18].

The codewords of an $(n, w, \lambda_a, \lambda_c)$-OOC are in the space of (0,1)-sequences with length n and weight w which contains $\binom{n}{w}$ members. It is clear from the correlation properties of OOC that no cyclic shift of a codeword of an optical orthogonal code can make a new codeword. In other words, all cyclic shifts of a codeword are different representations of that single codeword. So, by cyclic shifting we can always select a codeword such that its first chip is equal to "1". Accordingly, the universal discourse on every design algorithm for an $(n, w, \lambda_a, \lambda_c)$-OOC is the set $S_{n,w}$ of all (0,1)-sequences of length n, weight w and the first chip "1" which is defined as follows:

$$S_{n,w} = \left\{1x_1x_2\ldots x_{n-1}; x_i \in \{0,1\}, \sum_{i=1}^{n-1} x_i = w-1\right\}. \tag{3}$$

The set-theoretical representation of $S_{n,w}$ is the collection of all w-subsets of modulo-n integers Z_n which contain "0" as a fixed element, so the cardinal number of $S_{n,w}$ is $|S_{n,w}| = \binom{n-1}{w-1}$. As an example, the set-theoretical representation of reference set for the construction of (7,3,1)-OOC that contains $|S_{7,3}| = \binom{7-1}{3-1} = 15$ sequences is as follows:

$$\begin{aligned} S_{7,3} = \{&\{0,1,2\},\{0,1,3\},\{0,1,4\},\{0,1,5\},\{0,1,6\} \\ &\{0,2,3\},\{0,2,4\},\{0,2,5\},\{0,2,6\},\{0,3,4\} \\ &\{0,3,5\},\{0,3,6\},\{0,4,5\},\{0,4,6\},\{0,5,6\}\}. \end{aligned} \tag{4}$$

Hereafter, when we refer to the set $S_{n,w}$, we consider it interchangeably both as the sequence space and as its set-theoretical representation proportionate to the context. The rest of the paper is organized as follows. In Section II, we introduce the circulant matrix representation of optical orthogonal codes and present the spectral classification of constant-weight sequences. The establishment of multiplicative group action on the reference set of sequences and its algebraic properties are investigated in Section III. Section IV is devoted to the autocorrelation, intraclass and interclass cross-correlation properties of spectral classes obtained from the multiplicative group action and their use in decreasing the computational complexity of the OOC design algorithms. Finally, Section V concludes the paper and proposes some research problems for future work.

II. Circulant Matrix Representation of Optical Orthogonal Codes

In [14], corresponding to every OOC codeword $\mathbf{x}$, displayed as a row vector, the outer-product matrix $D_{\mathbf{xx}} = \mathbf{x}^{\mathcal{T}}\mathbf{x}$ is defined where $\mathcal{T}$ denotes the matrix transpose operation and based on the properties of this definition, a search algorithm for designing a subclass of optical orthogonal codes, namely, $(n, w, \lambda_a, 1)$-OOC is developed. Outer-product matrix representation of optical orthogonal codes initiates the use of matrix algebra in the analysis and design of these codes. The proper selection of appropriate types of matrices corresponding to optical orthogonal codes is of great importance to be suitably effective in developing OOC construction algorithms. Because of the cyclic structure of OOC codewords and the cyclic nature of its correlation properties, in the following definition we introduce the circulant matrix representation of optical orthogonal codes displaying all possible cyclic shifts of a codeword in a circulant matrix.

Definition 2: The circulant matrix representation of every codeword $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ in an $(n, w, \lambda_a, \lambda_c)$-OOC is defined as follows:

$$C_{\mathbf{x}} = Circ\{\mathbf{x}\} = \begin{bmatrix} x_0 & x_1 & \ldots & x_{n-1} \\ x_{n-1} & x_0 & \ldots & x_{n-2} \\ \vdots & \vdots & \ldots & \vdots \\ x_1 & x_2 & \ldots & x_0 \end{bmatrix}. \tag{5}$$

As an example, the circulant matrix representation of (5,2,1)-OOC with two codewords $\mathbf{x} = 10100$ and $\mathbf{y} = 11000$ is obtained as follows:

$$C_{\mathbf{x}} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} C_{\mathbf{y}} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{6}$$

It can be easily seen that the autocorrelation vector $\mathbf{R_{xx}} = (R_{\mathbf{xx}}(0), R_{\mathbf{xx}}(1), \ldots, R_{\mathbf{xx}}(n-1))$ and the cross-correlation vector $\mathbf{R_{xy}} = (R_{\mathbf{xy}}(0), R_{\mathbf{xy}}(1), \ldots, R_{\mathbf{xy}}(n-1))$ can be obtained from circulant matrices as $\mathbf{R_{xx}} = \mathbf{x}C_{\mathbf{x}}^{\mathcal{T}}$ and $\mathbf{R_{xy}} = \mathbf{y}C_{\mathbf{x}}^{\mathcal{T}}$. Acording to these equations, for (5,2,1)-OOC,

we have $\mathbf{R_{xx}} = (2,0,1,1,0)$, $\mathbf{R_{yy}} = (2,1,0,0,1)$, and $\mathbf{R_{xy}} = (1,1,0,1,1)$.

Since all circulant matrices of order n have the same n distinct eigenvectors, they form a simultaneously diagonalizable collection of matrices, and, therefore, their matrix multiplication commutes [19], [20]. Accordingly, the space of all circulant matrices of order n which is denoted by $Circ\{n\}$ [20], is a commutative linear algebra [19]. We use this convention that the inequality $A \leq B$ for matrices $A = [a_{i,j}]$ and $B = [b_{i,j}]$ means that for every i and j we have $a_{i,j} \leq b_{i,j}$. Now, we present a new definition of optical orthogonal codes on the space of circulant matrices as an algebraically commutative space.

Definition 3: An $(n, w, \lambda_a, \lambda_c)$-OOC is a family $\mathcal{C}$ of $n \times n$ circulant (0,1)-matrices with w "1s" in each row satisfying the following two conditions:

The autocorrelation property: for any matrix $A \in \mathcal{C}$, $AA^{\mathcal{T}} \leq \lambda_a U_n + (w - \lambda_a) I_n$.

The cross-correlation property: for any two distinct matrices $A, B \in \mathcal{C}$, $AB^{\mathcal{T}} \leq \lambda_c U_n$.

U_n denotes the $n \times n$ all-"1" matrix and I_n represents the identity matrix of order n.

Now, we obtain the spectrum of circulant matrix representation of constant-weight sequences for establishing a classification on the space $S_{n,w}$. First, we define a basic circulant matrix of order n as $T_n = Circ\{(\overset{0}{\downarrow}\!0, 1, 0, \ldots, \overset{n-1}{\downarrow}\!0)\}$, so, we have $T_n^k = \overbrace{T_n \times T_n \times \ldots \times T_n}^{k \text{ factors}} = Circ\{(0, \ldots, 0, \overset{k}{\downarrow}\!1, 0, \ldots, 0)\}$ and $T_n^0 = T_n^n = I_n$. Therefore, every circulant matrix $C_{\mathbf{x}} = Circ\{(x_0, x_1, \ldots, x_{n-1})\}$ can be written in terms of basic circulant matrices as $C_{\mathbf{x}} = x_0 I_n + x_1 T_n + x_2 T_n^2 + \ldots + x_{n-1} T_n^{n-1}$. As an example, for (5,2,1)-OOC in (6) we have $C_{\mathbf{x}} = I_5 + T_5^2$ and $C_{\mathbf{y}} = I_5 + T_5$. It can be easily computed that the characteristic polynomial of the basic circulant matrix T_n is equal to $det(zI_n - T_n) = z^n - 1$, and, therefore, its eigenvalues are the roots of characteristic equation $z^n = 1$, namely, the nth roots of unit which are denoted by $\theta_n^k = e^{i\frac{2\pi k}{n}}$ for $k = 0, 1, \ldots, n-1$. As we know from matrix algebra, if z is an eigenvalue of matrix M and $P(M) = a_0 + a_1 M + \ldots + a_n M^n$, then $P(z)$ is an eigenvalue of $P(M)$ [19]. So, the spectrum of matrix $C_{\mathbf{x}}$ which is defined as the set of its eigenvalues [20], is as follows:

$$Spec(C_{\mathbf{x}}) = \left\{ x_0 + x_1\theta_n^k + x_2\theta_n^{2k} + \ldots + x_{n-1}\theta_n^{(n-1)k} \right. \\ \left. k = 0, 1, \ldots, n-1 \right\}. \quad (7)$$

It is clear that the spectrum of every circulant matrix $C_{\mathbf{x}} = Circ\{(x_0, x_1, \ldots, x_{n-1})\}$ is the set of all discrete Fourier transform (DFT) values of vector $(x_0, x_1, \ldots, x_{n-1})$. Also, for any constant-weight sequence $\mathbf{x} \in S_{n,w}$, we have $w = \sum_{k=0}^{n-1} x_k \in Spec(C_{\mathbf{x}})$.

Definition 4: Two sequences $\mathbf{x}$ and $\mathbf{y}$ in $S_{n,w}$ are said to be equivalent if their corresponding circulant matrices have the same spectrum. In other words, $\mathbf{x} \sim \mathbf{y} \Leftrightarrow Spec(C_{\mathbf{x}}) = Spec(C_{\mathbf{y}})$.

Based on this equivalence relation, every equivalence class $[\mathbf{x}] = \{\mathbf{y} \,;\, Spec(C_{\mathbf{y}}) = Spec(C_{\mathbf{x}})\}$ contains all sequences of the same spectrum and the collection of all classes forms a partition on the set $S_{n,w}$ which we call the spectral classification of constant-weight sequences. For example, the set $S_{5,3}$ that contains $\binom{5-1}{3-1} = 6$ sequences can be spectrally partitioned into two classes $\{11100, 11010, 10101, 10011\}$ with spectrum $\{3, 1+\theta+\theta^2, 1+\theta+\theta^3, 1+\theta^2+\theta^4, 1+\theta^3+\theta^4\}$ and $\{11001, 10110\}$ with spectrum $\{3, 1+\theta+\theta^4, 1+\theta^2+\theta^3\}$ where $\theta = e^{i\frac{2\pi}{5}}$.

As we shall see in Section IV, the spectral classification of $S_{n,w}$ preserves the correlation properties of constant-weight sequences that can be very effective in designing and developing OOC construction algorithms. However, it is a difficult and time-consuming process to compute all eigenvalues of the circulant matrices corresponding to the constant-weight sequences for establishing the spectral classification on $S_{n,w}$. Therefore, in Section III, based on the multiplicative group action we propose a method of partitioning $S_{n,w}$ which is equivalent to its spectral classification.

III. Multiplicative Partitioning in Lieu of Spectral Classification

In mathematics, it is a common approach to establish an algebraic or geometric structure on a raw set to equip it with powerful tools for future uses [21], [22]. In this section, the algebraic structure we intend to establish on the set $S_{n,w}$ is a group action which devises a method for spectral classification of $S_{n,w}$. The set Π_n of all positive integers not greater than n, which are prime with respect to n, and the binary operation of modulo-n multiplication $\odot$ form a multiplicative group $(\Pi_n, \odot)$ of order $\phi(n)$ in which ϕ is the Euler function and if n has a prime factorization $p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$ for prime numbers p_i's and positive integers m_i's, then we have [21]

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right). \quad (8)$$

If n is a prime number, then $\Pi_n = \{1, 2, \ldots, n-1\}$ and $\phi(n) = n - 1$

Definition 5: A group action of a group G on a set S is a map $f : G \times S \to S$ satisfying the following two properties:

1. $f(e, s) = s$ for all $s \in S$.
2. $f(g_1 g_2, s) = f(g_1, f(g_2, s))$ for all $g_1, g_2 \in G$ and $s \in S$, where e is the identity of G [21].

Proposition 1: The following map is the group action of the multiplicative group Π_n on the reference set $S_{n,w}$

$$f : \Pi_n \times S_{n,w} \to S_{n,w}$$
$$f(g, X) = g \odot X \triangleq \left\{ g \odot 0, g \odot k_1, \ldots, g \odot k_{w-1} \right\} \quad (9)$$

where $g \in \Pi_n$ and $X = \{0, k_1, \ldots, k_{w-1}\} \in S_{n,w}$.

Proof: First, we show that for all $X \in S_{n,w}$ the set $g \odot X$ is in $S_{n,w}$. For $k_i \neq k_j$ in Z_n, if $g \odot k_i = g \odot k_j$, then $g \odot (k_i - k_j) = 0 \pmod n$, so $n | g(k_i - k_j)$, namely, n is a factor of $g(k_i - k_j)$, and since $gcd^{1}(n, g) = 1$, according to Euclid's lemma $n | (k_i - k_j)$ which is a contradiction to $k_i, k_j \in Z_n$. Also

[1]Greatest common divisor.

TABLE I
CLASSIFICATION PARAMETERS OF $S_{n,w}$

n	w	$\lvert S_{n,w}\rvert$	$\phi(n)$	$\lvert S_{n,w}/\Pi_n\rvert$	$L \times N_L$
5	3	6	4	2	$4\times 1,\ 2\times 1$
6	3	10	2	6	$2\times 4,\ 1\times 2$
7	4	20	6	4	$6\times 3,\ 2\times 1$
8	5	35	4	12	$4\times 6,\ 2\times 5,\ 1\times 1$
9	4	56	6	10	$6\times 9,\ 2\times 1$
10	7	84	4	22	$4\times 20,\ 2\times 2$
11	4	120	10	12	10×12
11	6	252	10	26	$10\times 25,\ 2\times 1$
12	4	165	4	52	$4\times 32,\ 2\times 17,\ 1\times 3$
12	7	462	4	135	$4\times 98,\ 2\times 33,\ 1\times 4$

$0 = g\odot 0 \in g\odot X$, so $g\odot X$ is a w-subset of Z_n which contains "0", therefore, $g \odot X \in S_{n,w}$. Now we verify the properties of group action.

1. $f(1,X) = 1 \odot X = \{1\odot 0, 1\odot k_1, \ldots, 1\odot k_{w-1}\} = \{0, k_1, \ldots, k_{w-1}\} = X$.
2. $f(g_1 \odot g_2, X) = (g_1 \odot g_2) \odot X = \{0, (g_1 \odot g_2) \odot k_1, \ldots, (g_1 \odot g_2) \odot k_{w-1}\} = \{0, g_1 \odot (g_2 \odot k_1), \ldots, g_1 \odot (g_2 \odot k_{w-1})\} = g_1 \odot (g_2 \odot X) = f(g_1, f(g_2, X))$. □

Definition 6: For the group action of the multiplicative group Π_n on the set $S_{n,w}$, we say that two sequences X and Y in $S_{n,w}$ are related and we write $X \sim Y$, when there is a $g \in \Pi_n$ so that $X = g \odot Y$.

It can be easily seen that the relation $X \sim Y$ is an equivalence relation that decomposes the set $S_{n,w}$ into the equivalence classes where every class is defined as $[X] = \{Y \in S_{n,w}; Y \sim X\}$ and X is called the representative of the class $[X]$. In group theory context, the class $[X]$ is called the orbit of X and is equal to $\{g \odot X; g \in \Pi_n\}$ [22]. Furthermore, the collection of all classes of $S_{n,w}$ is called the orbit space or the quotient of group action and is denoted by $S_{n,w}/\Pi_n$ [21]. Accordingly, the number of sequences in the class $[X]$ is equal to the index of the stabilizer of X in Π_n[21]. So, if $|[X]|$ is the number of sequences in the class $[X]$ and $|S_X|$ is the order of the stabilizer subgroup $S_X = \{g \in \Pi_n; g \odot X = X\}$, then we have $|[X]||S_X| = |\Pi_n| = \phi(n)$; thus, the number of sequences in every class is a factor of $\phi(n)$. We refer to the class with $\phi(n)$ sequences as complete class and otherwise incomplete. For instance, the set $S_{7,3}$ in (4) has two complete classes with $\phi(7) = 6$ sequences and one incomplete class with three members. It can be partitioned as $S_{7,3} = [\{0,1,2\}] \cup [\{0,1,3\}] \cup [\{0,1,6\}]$ where

$$\begin{aligned}
[\{0,1,2\}] &= \Big\{\{0,1,2\}, \{0,1,4\}, \{0,2,4\}, \\
&\qquad \{0,3,6\}, \{0,3,5\}, \{0,5,6\}\Big\} \\
[\{0,1,3\}] &= \Big\{\{0,1,3\}, \{0,1,5\}, \{0,2,3\}, \\
&\qquad \{0,2,6\}, \{0,4,5\}, \{0,4,6\}\Big\} \\
[\{0,1,6\}] &= \Big\{\{0,1,6\}, \{0,2,5\}, \{0,3,4\}\Big\}. \qquad (10)
\end{aligned}$$

There are some major questions on the orbit space $S_{n,w}/\Pi_n$ that are about the number of complete and incomplete classes and the size of every incomplete class. For prime n, we present an equation for the number of classes in the following theorem which is proved in the appendix using Burnside's lemma. The general case is remained as an open problem for future work.

Theorem 1: If n is prime, the number of classes in the orbit space $S_{n,w}/\Pi_n$ will be

$$|S_{n,w}/\Pi_n| = \sum_{\substack{d|(n-1)\\ d|(w-1)}} \binom{\frac{n-1}{d}}{\frac{w-1}{d}} \frac{\phi(d)}{n-1}. \qquad (11)$$

Proof: For proof see Appendix A.

In the following tables, we present some classification parameters of the space $S_{n,w}$ which is useful for verification of any proposed formula. The last column of each table displays $L \times N_L$ in which L denotes the size of each class and N_L represents the number of classes with size L; therefore, we have $\sum_L N_L L = |S_{n,w}|$. All details of Tables I–III such as number of complete and incomplete classes, and size of incomplete classes have been obtained via a computer search program on the space $S_{n,w}$. Theorem 1 is only useful for enumerating all multiplicative classes on the set $S_{n,w}$ when n is a prime number, however, it is not valid for nonprime n.

From Table I, we can see that when n is prime, i.e., $\phi(n) = n-1$, the complete class has the largest size $n-1$ and so the number of classes is the lowest amount in contrast with composite n. For example, $S_{11,4}$ has 12 classes with size 10 while $S_{12,4}$ has 52 classes of sizes 4, 2, and 1.

Tables II and III depict the classification parameters of $S_{n,w}$ for all possible values of w and for prime $n = 13$ and composite $n = 14$, respectively. In these tables N_{CC} is the number of complete classes and N_{IC} is the number of incomplete classes, so $N_{CC} + N_{IC} = |S_{n,w}/\Pi_n|$.

It can be seen from Table II and Table III that the behavior of S_{n,w_1} classification is similar to that of S_{n,w_2} when $w_1 + w_2 = n+1$. Also, for both prime and composite sequence lengths, most classes are complete and there are few classes of incomplete size.

Theorem 2: The spectral classification of $S_{n,w}$ is equivalent to its multiplicative partitioning.

Proof: Assume that the set-theoretical representation of sequence $\mathbf{x} \in S_{n,w}$ is $X = \{0, k_1, \ldots, k_{w-1}\}$ and its multiplicative permutation $\mathbf{y}$ has the representation $Y = k \odot X =$

TABLE II
CLASSIFICATION PARAMETERS OF $S_{13,w}$

w	$\lvert S_{n,w}\rvert$	$\lvert S_{n,w}/\Pi_n\rvert$	N_{CC}	N_{IC}	$L \times N_L$
2	12	1	1	0	12×1
3	66	6	5	1	$12 \times 5,\ 6 \times 1$
4	220	19	18	1	$12 \times 18,\ 4 \times 1$
5	495	43	40	3	$12 \times 40,\ 6 \times 2,\ 3 \times 1$
6	792	66	66	0	12×66
7	924	80	75	5	$12 \times 75,\ 6 \times 3,\ 4 \times 1,\ 2 \times 1$
8	792	66	66	0	12×66
9	495	43	40	3	$12 \times 40,\ 6 \times 2,\ 3 \times 1$
10	220	19	18	1	$12 \times 18,\ 4 \times 1$
11	66	6	5	1	$12 \times 5,\ 6 \times 1$
12	12	1	1	0	12×1

TABLE III
CLASSIFICATION PARAMETERS OF $S_{14,w}$

w	$\lvert S_{n,w}\rvert$	$\lvert S_{n,w}/\Pi_n\rvert$	N_{CC}	N_{IC}	$L \times N_L$
2	13	3	2	1	$6 \times 2,\ 1 \times 1$
3	78	14	12	2	$6 \times 12,\ 3 \times 2$
4	286	50	46	4	$6 \times 46,\ 3 \times 2,\ 2 \times 2$
5	715	123	116	7	$6 \times 116,\ 3 \times 5,\ 2 \times 2$
6	1297	217	212	5	$6 \times 212,\ 3 \times 5$
7	1716	292	282	10	$6 \times 282,\ 3 \times 6,\ 2 \times 2,\ 1 \times 2$
8	1716	292	282	10	$6 \times 282,\ 3 \times 6,\ 2 \times 2,\ 1 \times 2$
9	1297	217	212	5	$6 \times 212,\ 3 \times 5$
10	715	123	116	7	$6 \times 116,\ 3 \times 5,\ 2 \times 2$
11	286	50	46	4	$6 \times 46,\ 3 \times 2,\ 2 \times 2$
12	78	14	12	2	$6 \times 12,\ 3 \times 2$
13	13	3	2	1	$6 \times 2,\ 1 \times 1$

$\{0, k \odot k_1, \ldots, k \odot k_{w-1}\}$, where $k \in \Pi_n$. So, the spectra of their corresponding circulant matrices are

$$Spec(C_{\mathbf{x}}) = \Big\{1 + \theta_n^{k_1 \odot t} + \theta_n^{k_2 \odot t} + \ldots + \theta_n^{k_{w-1} \odot t} \quad t = 0, 1, \ldots, n-1\Big\}$$

$$Spec(C_{\mathbf{y}}) = \Big\{1 + \theta_n^{k_1 \odot k \odot s} + \theta_n^{k_2 \odot k \odot s} + \ldots + \theta_n^{k_{w-1} \odot k \odot s} \quad s = 0, 1, \ldots, n-1\Big\}.$$

Since $k \in \Pi_n$, there is $k' \in \Pi_n$ such that $k \odot k' = 1$. Therefore, the eigenvalue of $C_{\mathbf{x}}$ for $t \in Z_n$ is equal to that of $C_{\mathbf{y}}$ for $s = k' \odot t \in Z_n$, and so we have $Spec(C_{\mathbf{x}}) = Spec(C_{\mathbf{y}})$. Conversely, if the circulant matrices $C_{\mathbf{x}}$ and $C_{\mathbf{y}}$ corresponding to two sequences $\mathbf{x}$ and $\mathbf{y}$ in $S_{n,w}$ have the same spectrum, it is necessary that the sets of the powers of $\theta_n = e^{i\frac{2\pi}{n}}$ in their spectrum are multiplicative permutation of each other, and, therefore, there is a $k \in \Pi_n$, such that $Y = k \odot X$. □

According to the aforementioned theorem, we can spectrally classify $S_{n,w}$ by establishing the multiplicative partitioning on it without any need for computing the spectrum of sequences. There are a lot of pure mathematical questions about the structure of the proposed multiplicative group action of Π_n on the set $S_{n,w}$ that can be attractive to mathematicians. However, our goal is to use the proposed classification in the construction algorithms of optical orthogonal codes which is dealt with in Section IV.

IV. CORRELATION PROPERTIES OF MULTIPLICATIVE PARTITIONS

Definition 7: The sequence $\mathbf{y} = y_0 y_1 \ldots y_{n-1}$ is called the multiplicative permutation of the sequence $\mathbf{x} = x_0 x_1 \ldots x_{n-1}$, if there is a $g \in \Pi_n$ so that $y_k = x_{k \odot g}$ for $k = 0, 1, \ldots, n-1$ and it is denoted by $\mathbf{y} = \mathbf{x} \odot g$.

The following proposition shows the relation between the set-theoretical representations of the sequences that are multiplicative permutations of each other.

Proposition 2: If X and Y are the set-theoretical representations of $\mathbf{x}$ and $\mathbf{y} = \mathbf{x} \odot g$, respectively, then we have $Y = g' \odot X$ where g' is the inverse of $g \in \Pi_n$, namely, $g \odot g' = 1$.

Proof: Suppose that $\mathbf{y} = \mathbf{x} \odot g$ for some $g \in \Pi_n$ and consider $k \in Y$, so we have $y_k = x_{k \odot g} = 1$ then $k \odot g \in X$. Since g is in the multiplicative group Π_n, there is a $g' \in \Pi_n$ so that $g \odot g' = 1$ and then $k = (k \odot g) \odot g' \in g' \odot X$ and vice versa. □

As we see from the previous proposition, there is a bijection between multiplicative permutations of sequences and multiplicative action on their set-theoretical representations. So, the orbit $[X] = \{g \odot X; g \in \Pi_n\}$ is in one-to-one correspondence with the set $\{\mathbf{x} \odot g; g \in \Pi_n\}$ containing all multiplicative permutations of sequence $\mathbf{x}$. Now we have the sufficient tools for investigating the correlation properties of multiplicative classes for using in OOC design algorithms.

Autocorrelation: As an example, consider the sequence $\mathbf{x} = 1101000010$ in the space $S_{10,4}$. Its autocorrelation vector is equal to $\mathbf{R_{xx}} = (4, 1, 2, 2, 0, 2, 0, 2, 2, 1)$. Now suppose that $\mathbf{y} = \mathbf{x} \odot 3 = 1100001100$, and then $\mathbf{R_{yy}} = (4, 2, 0, 1, 2, 2, 2, 1, 0, 2)$. We easily see that

$\mathbf{R_{yy}} = \mathbf{R_{xx}} \odot 3$. This is a general result and it is proved in the following theorem.

Theorem 3: If $\mathbf{x} \in S_{n,w}$ and $\mathbf{y} = \mathbf{x} \odot g$ for some $g \in \Pi_n$, then we have $\mathbf{R_{yy}} = \mathbf{R_{xx}} \odot g$.

Proof: According to the definition of autocorrelation, we have

$$\begin{aligned} R_{\mathbf{yy}}(m) &= \sum_{k=0}^{n-1} y_k y_{k\oplus m} = \sum_{k=0}^{n-1} x_{k\odot g} x_{(k\oplus m)\odot g} \\ &= \sum_{k=0}^{n-1} x_{k\odot g} x_{(k\odot g)\oplus(m\odot g)} = \sum_{l=0}^{n-1} x_l x_{l\oplus(m\odot g)} \\ &= R_{\mathbf{xx}}(m \odot g). \end{aligned}$$

□

As an application for the above theorem, we see that all the sequences of a class have the same autocorrelation pattern. In other words, their autocorrelation vectors are the multiplicative permutations of each other. Therefore, if for a sequence $\mathbf{x}$, the autocorrelation property in the OOC definition is established, then it is satisfied for all sequences of its class $\{\mathbf{x} \odot g; g \in \Pi_n\}$ and if it is not held for a sequence, it is satisfied for none of its multiplicative permutations. Therefore, by computing the autocorrelation of the representative of each class we decide to hold the corresponding class in the search space or not. For instance, consider the classification of $S_{7,3}$ in (10). It can be easily computed that the autocorrelation pattern for classes $[\{0,1,2\}]$ and $[\{0,1,6\}]$ is (3,2,1,0,0,1,2) and for class $[\{0,1,3\}]$ is (3,1,1,1,1,1,1). Therefore, to design a (7,3,1,λ_c)-OOC, our search space is the class $[\{0,1,3\}]$ with 6 sequences not the set $S_{7,3}$ with 15 sequences.

Cross correlation: In the case of cross correlation, we have two categories, the cross correlation between different sequences of a same class, which is called intraclass cross correlation, and the cross correlation between the sequences of distinct classes, which is referred to as interclass cross correlation. First, we deal with the case of intraclass cross correlation by the following theorem.

Theorem 4: The cross correlation between the sequences $\mathbf{y} = \mathbf{x} \odot r$ and $\mathbf{z} = \mathbf{x} \odot s$ has the same pattern with the cross correlation between the sequences $\mathbf{x}$ and $\mathbf{x} \odot s \odot r'$ where r' is the inverse of r in group Π_n.

Proof: From the definition of cross correlation and by substituting the variable $k \odot r$ by l, and thus, the variable $k \odot s$ by $l \odot s \odot r'$, we have

$$\begin{aligned} R_{\mathbf{yz}}(m) &= \sum_{k=0}^{n-1} y_k z_{k\oplus m} = \sum_{k=0}^{n-1} x_{k\odot r} x_{(k\oplus m)\odot s} \\ &= \sum_{k=0}^{n-1} x_{k\odot r} x_{(k\odot s)\oplus(m\odot s)} \\ &= \sum_{l=0}^{n-1} x_l x_{(l\odot s\odot r')\oplus(m\odot s)} \\ &= R_{\mathbf{xx}\odot s\odot r'}(m \odot s). \end{aligned}$$

So, the cross correlation of $\mathbf{y}$ and $\mathbf{z}$ and that of $\mathbf{x}$ and $\mathbf{x} \odot s \odot r'$ have the same pattern. □

TABLE IV
CROSS CORRELATIONS BETWEEN $X = \{0, 1, 4\}$ AND ITS CLASS MEMBERS

g	$g \odot X$	$\mathbf{R}_{Xg\odot X}$
2	$\{0,2,8\}$	(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)
3	$\{0,3,12\}$	(1, 3, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)
4	$\{0,3,4\}$	(2, 2, 0, 0, 1, 0, 0, 0, 0, 1, 2, 1, 0)
5	$\{0,5,7\}$	(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)
6	$\{0,6,11\}$	(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)
7	$\{0,2,7\}$	(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)
8	$\{0,6,8\}$	(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)
9	$\{0,9,10\}$	(1, 1, 0, 1, 3, 1, 0, 1, 1, 0, 0, 0, 0)
10	$\{0,1,10\}$	(2, 1, 0, 2, 2, 0, 0, 1, 0, 0, 0, 0, 1)
11	$\{0,5,11\}$	(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)
12	$\{0,9,12\}$	(1, 2, 1, 0, 2, 2, 0, 0, 1, 0, 0, 0, 0)

The application of this theorem is in the computation of cross correlation between sequences in a class. Suppose that class $[X]$ has K sequences. Therefore, we have $\binom{K}{2} = \frac{K(K-1)}{2}$ cross-correlation sequences between all distinct members of the class. But many of these cross-correlation sequences have the same pattern and actually we need to know $K-1$ cross correlations between the representative X and other $K-1$ members of the class in the cross-correlation property of OOC definition. As an example, consider the complete class $[\{0,1,4\}]$ in the space $S_{13,3}$ with $\phi(13) = 12$ sequences. Table IV shows all 11 necessary cross-correlation patterns needed for OOC design from all 66 possible cross-correlation vectors.

Suppose that we want to examine the cross-correlation property of two sequences $5 \odot X = [0,5,7]$ and $8 \odot X = [0,6,8]$. According to Theorem 4, their cross-correlation pattern is the same as one between sequences X and $(8\odot 5')\odot X = 12 \odot X = \{0,9,12\}$ which is equal to (1, 2, 1,0, 2, 2, 0, 0, 1, 0, 0, 0, 0). Therefore, these sequences are not appropriate for any (13, 3, λ_a, 1)-OOC.

In the case of interclass cross correlation, we want to compute the cross correlations between the sequences of different classes. The following theorem facilitates the examination of cross-correlation property in the OOC definition.

Theorem 5: Consider the sequences $\mathbf{u} = \mathbf{x} \odot r$ and $\mathbf{v} = \mathbf{y} \odot s$ in the classes $[X]$ and $[Y]$, respectively. The cross correlation between $\mathbf{u}$ and $\mathbf{v}$ has the same pattern with one between $\mathbf{x}$ and $\mathbf{y} \odot s \odot r'$ where r' is the inverse of r in Π_n

Proof: Similar to the proof of Theorem 4, we have

$$\begin{aligned} R_{\mathbf{uv}}(m) &= \sum_{k=0}^{n-1} u_k v_{k\oplus m} = \sum_{k=0}^{n-1} x_{k\odot r} y_{(k\oplus m)\odot s} \\ &= \sum_{k=0}^{n-1} x_{k\odot r} y_{(k\odot s)\oplus(m\odot s)} \\ &= \sum_{l=0}^{n-1} x_l y_{(l\odot s\odot r')\oplus(m\odot s)} \\ &= R_{\mathbf{xy}\odot s\odot r'}(m \odot s). \end{aligned}$$

□

Suppose that we have two classes with K_1 and K_2 sequences. There are K_1K_2 cross correlations between the sequences of these classes which are necessary for the examination of cross-correlation property in the OOC definition. But, from the above theorem we can deduce that it is sufficient to compute $\min\{K_1, K_2\}$ cross-correlation vectors because the others

TABLE V
CROSS-CORRELATIONS BETWEEN $\{0,1,6\}$ AND THE MEMBERS OF $[\{0,1,12\}]$

$g \odot \{0,1,12\}$	$\mathbf{R}_{Xg\odot Y}$
$\{0,1,12\}$	$(2,2,1,0,0,1,1,1,0,0,0,0,1)$
$\{0,2,11\}$	$(1,1,1,1,1,0,1,0,1,0,0,1,1)$
$\{0,3,10\}$	$(1,1,0,2,1,0,1,0,0,1,1,1,0)$
$\{0,4,9\}$	$(1,1,1,0,1,1,1,0,0,1,2,0,0)$
$\{0,5,8\}$	$(1,2,0,0,0,1,2,0,1,1,0,1,0)$
$\{0,6,7\}$	$(2,1,0,0,0,0,2,2,1,0,0,0,1)$

have the same patterns with these computed cross correlations. For example, consider the complete class $[\{0,1,6\}]$ with 12 sequences and the incomplete class $[\{0,1,12\}]$ with 6 sequences in the space $S_{13,3}$. From all $6 \times 12 = 72$ cross correlations we only need to compute 6 ones between $\{0,1,6\}$ and 6 members of multiplicative class of sequence $Y = \{0,1,12\}$ which are depicted in the following table.

So, if we need to examine the cross correlation between two sequences $\{0,8,9\} = 8 \odot \{0,1,6\}$ and $\{0,3,10\} = 3 \odot \{0,1,12\}$, from Theorem 5 we know that it has the same pattern with the cross correlation between $\{0,1,6\}$ and $(8' \odot 3) \odot \{0,1,12\} = \{0,2,11\}$ which is equal to (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) from Table V. Therefore, these two sequences are suitable for (13, 3, λ_a, 1)-OOC.

Now, we summarize the results of the previous theorems. Consider the set $S_{n,w}$ as the reference set for $(n,w,\lambda_a,\lambda_c)$-OOC construction. If we apply the multiplicative group action of Π_n on this set, we obtain the spectral classification of $S_{n,w}$ called multiplicative partitioning $S_{n,w}/\Pi_n$. Suppose that there are N mutually disjoint classes $C_1, C_2, \ldots, C_N$ in this partitioning with sizes $K_1, K_2, \ldots, K_N$, respectively, so that $\cup_{i=1}^{N} C_i = S_{n,w}$ and $\sum_{i=1}^{N} K_i = \binom{n-1}{w-1}$. First, we compute the autocorrelation of each class representative and examine whether it satisfies the autocorrelation property of OOC or not. If a class representative is satisfactory we hold the class in the space and if not we eliminate the whole class from the desired space. In this manner, we make a smaller reference set for search algorithms. To examine the cross-correlation property of OOC, what we need is the computation of cross correlations between class representatives and other sequences, not the cross correlations between any two arbitrary sequences. Since most classes are complete and have $\phi(n)$ sequences, we can claim that the multiplicative partitioning of reference set $S_{n,w}$ decreases the correlation computations of order $\phi(n)$. For prime n we have $\phi(n) = n-1$, so the order of decreasing is n. But, generally we have $\phi(n) > \sqrt{n}$ for $n > 6$[22], and we can say that this classification decreases the correlation computations of order at least $\sqrt{n}$ for composite n.

As an example, we construct (16, 4, 1, 2)-OOC using the proposed classification method. First, the sequence space $S_{16,4}$ with $\binom{16-1}{4-1} = 455$ members is classified to $|S_{16,4}/\Pi_{16}| = 69$ classes including $N_{CC} = 48$ complete classes with size $\phi(16) = 8$ and $N_{IC} = 21$ incomplete classes including 15 partitions with size 4, 5 partitions with size 2, and 1 partition with size 1. Then, we check the autocorrelation constraint $\lambda_a = 1$ for all 69 class representatives and eliminate all those classes not satisfying the autocorrelation constraint. It can be easily computed that there are only 6 survived classes with representatives $\{0,1,3,7\}$, $\{0,1,3,12\}$, $\{0,1,4,6\}$, $\{0,1,5,14\}$, $\{0,1,10,12\}$, and $\{0,1,10,14\}$. Since the survived classes are all complete, we have only $6 \times 8 = 48$ sequences out of 455 in the search space. Now, we form the corresponding graph of (16, 4, 1, 2)-OOC construction by considering every sequence as a vertex and connecting two vertices if their cross correlation satisfies the constraint $\lambda_c = 2$. According to the correlation properties of spectral classes, the examination of cross-correlation condition only needs the computation of $6 \times (8-1) + \binom{6}{2} \times 8 = 162$ out of $\binom{48}{2} = 1128$ cross correlations. The optimal (16, 4, 1, 2)-OOC is equivalent to a clique (a complete subgraph of a graph) with maximum order. By running a simple maximum clique algorithm we find the largest complete subgraph of order 4 and, therefore, the optimal (16, 4, 1, 2)-OOC as follows:

$$(16,4,1,2)-\text{OOC} = \Big\{\{0,3,5,9\},\{0,7,11,13\} \{0,1,3,12\},\{0,9,11,12\}\Big\}. \quad (12)$$

Since the proposed algorithm is a complete search method, the constructed OOC is optimal, namely, $\Phi(16,4,1,2) = 4$.

Similar to the previous example, (19, 5, 2)-OOC is constructed using the classification of $S_{19,5}$ which has $\binom{19-1}{5-1} = 3060$ sequences. $S_{19,5}/\Pi_{19}$ consists of 168 complete classes with size 18 and 4 incomplete classes with size 9. There are 109 complete classes and 2 incomplete classes containing 1980 out of 3060 sequences that satisfy the autocorrelation criterion $\lambda_a = 2$. The corresponding graph is formed so as to satisfy the cross-correlation criterion $\lambda_c = 2$. The number of both intraclass and interclass cross-correlation computations needed to form the graph matrix is $109 \times (18-1) + 2 \times (9-1) + \binom{109}{2} \times 18 + \binom{2}{2} \times 9 + 109 \times 2 \times \min\{9,18\} = 109788$ out of $\binom{1980}{2} = 1959210$ cross correlations. After running a max clique algorithm on the graph matrix we have the following optical orthogonal code with four codewords:

$$(19,5,2)-\text{OOC} = \Big\{\{0,1,2,5,7\},\{0,3,6,10,15\} \{0,7,9,11,18\},\{0,5,10,11,13\}\Big\}. \quad (13)$$

From the Johnson bound in (1), we have $\Phi(19,5,2) \leq \left\lfloor \frac{1}{5} \left\lfloor \frac{19-1}{5-1} \left\lfloor \frac{19-2}{5-2} \right\rfloor \right\rfloor \right\rfloor = 4$, so, our construction is optimal.

V. CONCLUSION AND FUTURE WORK

The circulant matrix representation of optical orthogonal codes was introduced and based on this representation a new definition of OOC on the commutative linear algebra of circulant matrices was presented. Using the spectrum of the circulant matrices corresponding to the constant-weight sequences, we proposed the spectral classification of $S_{n,w}$ preserving the correlation properties of constant-weight sequences. As a method for spectrally classifying $S_{n,w}$, we suggested the multiplicative group action on it. Therefore, the reference set of $(n,w,\lambda_a,\lambda_c)$-OOC design algorithms was equipped with the multiplicative group action thus was classified to multiplicative orbits. This group action crystalized some mathematical problems about the algebraic structure of the multiplicative partitioning such as the number and the size of its orbits.

Furthermore, we proposed a novel equation for the number of orbits when the code-length is prime and in the case of composite numbers it remained as an open problem for future work. Correlation properties of multiplicative partitions including autocorrelation, intraclass and interclass cross correlations were derived and their use in the examination of correlation conditions of optical orthogonal codes was investigated. Generally, the multiplicative partitioning of the set $S_{n,w}$ reduced the correlation computations of order $\phi(n)$. Another advantage for this classification is in its independence from code-length n, code-weight w, and correlation constraints λ_a and λ_c that makes it suitable for construction of optical orthogonal codes with any arbitrary parameters.

APPENDIX

In this Appendix, we prove Theorem 1 presented in Section III that enumerates the number of multiplicative classes when n is a prime number. The key point in this proof is the use of Burnside's lemma that we first mention it.

Burnside's Lemma: Let $f : G\times S \rightarrow S$ be the group action of the group G on the finite set S. Its number of orbits is

$$|S/G| = \frac{1}{|G|}\sum_{g\in G}|S_g| \tag{A.1}$$

where $S_g = \{s \in S; f(g,s) = s\}$ contains all fixed points of the map f for some $g \in G$ [21], [22].

Now we apply this lemma to the multiplicative group action to find the size of the orbit space $S_{n,w}/\Pi_n$. It is clear that $|G| = |\Pi_n| = n-1$ and we must obtain the size of $S_g = \{X \in S_{n,w}; g \odot X = X\}$. First, we show that if S_g is a nonempty set then the order of element g is a factor of $w-1$. Suppose that $ord(g) = d$ and $X = \{0, a_1, a_2, \ldots, a_{w-1}\} \in S_g$, then we have $\{0, a_1, \ldots, a_{w-1}\} = \{0, g\odot a_1, \ldots, g\odot a_{w-1}\}$. Consider $a_{i_1} \in I = \{a_1, \ldots, a_{w-1}\}$, so we have $I_1 = \{a_{i_1}, g\odot a_{i_1}, \ldots, g^{d-1}\odot a_{i_1}\} \subseteq I$. If $I_1 \neq I$, we choose $a_{i_2} \in I - I_1$ and form I_2 like as I_1. In this manner we continue to the set I_k so that $\cup_{i=1}^{k} I_k = I$ and $I_i \neq I_j$ for $i \neq j$. Therefore, we have $w-1 = d\times k$ and then $ord(g)|(w-1)$. Accordingly, for $g \in \Pi_n$ that $ord(g)$ is not a factor of $w-1$, the set S_g is empty and $|S_g| = 0$. However, if $ord(g)|(w-1)$, we should enumerate the number of ways for choosing $\frac{w-1}{ord(g)}$ cosets from $\frac{n-1}{ord(g)}$ cosets of the cyclic subgroup $\langle g\rangle = \{1, g, , g^2, \ldots, g^{ord(g)-1}\}$ in the group Π_n which is equal to $\binom{\frac{n-1}{ord(g)}}{\frac{w-1}{ord(g)}}$. According to (A.1), we have

$$|S_{n,w}/\Pi_n| = \frac{1}{n-1}\sum_{\substack{g\in\Pi_n \\ ord(g)|(w-1)}} \binom{\frac{n-1}{ord(g)}}{\frac{w-1}{ord(g)}}. \tag{A.2}$$

In order to obtain the desired equation, we compute the summation in terms of $d = ord(g)$ instead of $g \in \Pi_n$. Since Π_n is a cyclic group, for any $d|(n-1)$ there are $\phi(d)$ elements of order d in Π_n so that $\sum_{d|(n-1)}\phi(d) = n-1$. Applying this fact to (A.2), we have

$$|S_{n,w}/\Pi_n| = \frac{1}{n-1}\sum_{\substack{d|(n-1) \\ d|(w-1)}} \phi(d)\binom{\frac{n-1}{d}}{\frac{w-1}{d}}. \tag{A.3}$$

Therefore, the proof is complete and we obtain an equation to enumerate the number of orbits when the length n is a prime number. □

ACKNOWLEDGMENT

The authors would like to thank M. J. Saberian for his valuable comments on Group Theory.

REFERENCES

[1] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: Design, analysis, and applications," *IEEE Trans. Inf. Theory*, vol. 35, pp. 593–604, May 1989.
[2] J. A. Salehi, "Code division multiple-access techniques in optical fiber networks—Part I: Fundamental principles," *IEEE Trans. Commun.*, vol. 37, pp. 824–833, Aug. 1989.
[3] J. A. Salehi and C. A. Brackett, "Code division multiple-access techniques in optical fiber networks—Part II: System performance analysis," *IEEE Trans. Commun.*, vol. 37, pp. 834–842, Aug. 1989.
[4] N. Miyamoto, H. Mizuno, and S. Shinohara, "Optical orthogonal codes obtained from conics on finite projective planes," *Finite Fields Appl.*, vol. 10, pp. 405–411, 2004.
[5] W. Chu and C. J. Colbourn, "Optimal $(n, 4, 2)$ -OOC of small orders," *Discrete Math.*, vol. 729, pp. 163–172, 2004.
[6] S. Bitan and T. Etzion, "Constructions for optimal constant weight cyclically permutable codes and difference families," *IEEE Trans. Inf. Theory*, vol. 41, no. 1, pp. 77–87, Jan. 1995.
[7] G. C. Yang and T. E. Fuja, "Optical orthogonal codes with unequal auto- and cross-correlation constraints," *IEEE Trans. Inf. Theory*, vol. 41, pp. 96–106, Dec. 2001.
[8] R. Fuji-Hara and Y. Miao, "Optical orthogonal codes: Their bounds and new optimal constructions," *IEEE Trans. Inf. Theory*, vol. 46, pp. 2396–2406, Nov. 2000.
[9] C. S. Weng and J. Wu, "Optical orthogonal code with nonideal cross correlation," *J. Lightw. Technol.*, vol. 19, pp. 1856–1863, Dec. 2001.
[10] I. B. Djordjevic and B. Vasic, "Combinatorial constructions of optical orthogonal codes for OCDMA systems," *IEEE Commun. Lett.*, vol. 8, pp. 391–393, Jun. 2004.
[11] C. Ding and C. Xing, "Cyclotomic optical orthogonal codes of composite lengths," *IEEE Trans. Commun.*, vol. 52, pp. 263–268, Feb. 2004.
[12] H. Chung and P. V. Kumar, "Optical orthogonal codes—New bounds and an optimal construction," *IEEE Trans. Inf. Theory*, vol. 36, pp. 866–873, Jul. 1990.
[13] B. M. Ghaffari, M. D. Matinfar, and J. A. Salehi, "Wireless optical CDMA LAN: Digital design concepts," *IEEE Trans. Commun.*, vol. 56, pp. 2145–2155, Dec. 2008.
[14] H. Charmchi and J. A. Salehi, "Outer-product matrix representation of optical orthogonal codes," *IEEE Trans. Commun.*, vol. 54, pp. 983–989, Jun. 2006.
[15] R. Omrani, H. Lu, O. Moreno, and P. V. Kumar, "Construction of low-density parity-check codes from optical orthogonal codes," in *Proc. Int. Symp. Inf. Theory*, 2003, pp. 60–60.
[16] H. Wen, F. Hu, J. Li, and F. Jin, "A new family of irregular LDPC codes," in *Proc. IEEE 6th CAS Symp. Emerging Technologies: Frontiers of Mobile and Wireless Communication*, 2004, vol. 1, pp. 285–288.
[17] K. Momihara and M. Buratti, "Bounds and constructions of optimal $(n,4, 2, 1)$ optical orthogonal codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 514–523, Feb. 2009.
[18] J. A. Salehi, "Emerging OCDMA communication systems and data networks [invited]," *J. Opt. Netw.*, vol. 6, pp. 1138–1178, Sep. 2007.
[19] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1985.
[20] P. J. Davis, *Circulant Matrices*. Hoboken, NY: Wiley, 1979.
[21] D. S. Dummit and R. M. Foote, *Abstract Algebra*. Upper Saddle River, NJ: Prentice-Hall, 1991.
[22] J. J. Rotman, *A First Course in Abstract Algebra*, 3rd ed. Upper Saddle River, NJ: Prentice-Hall, 2005.

Mohammad M. Alem-Karladani was born in Isfahan, Iran, on January 7, 1982. He received the B.S. degree from Isfahan University of Technology (IUT), Isfahan, Iran, in 2004, and the M.S. degree from the Sharif University of Technology (SUT), Tehran, in 2006, both in electrical engineering.

Since September 2006, he has been with the Optical Networks Research Laboratory (ONRL), Advanced Communications Research Institute (ACRI), EE Department, SUT. His research interests include optical communications, nonlinear optics, and information theory.

Jawad A. Salehi (M'84–SM'07) was born in Kazemain, Iraq, on December 22, 1956. He received the B.S. degree from the University of California, Irvine, in 1979, and the M.S. and Ph.D. degrees from the University of Southern California (USC), Los Angeles, in 1980 and 1984, respectively, all in electrical engineering.

He is currently a Full Professor at the Optical Networks Research Laboratory (ONRL), Department of Electrical Engineering, Sharif University of Technology (SUT), Tehran, Iran, where he is also the Co-Founder of the Advanced Communications Research Institute (ACRI). From 1981 to 1984, he was a Full-Time Research Assistant at the Communication Sciences Institute, USC. From 1984 to 1993, he was a Member of Technical Staff of the Applied Research Area, Bell Communications Research (Bellcore), Morristown, NJ. During 1990, he was with the Laboratory of Information and Decision Systems, MIT, Cambridge, as a Visiting Research Scientist. He holds 12 U.S. patents on optical CDMA.

Prof. Salehi has been an Associate Editor for Optical CDMA for the IEEE TRANSACTIONS ON COMMUNICATIONS since May 2001. In September 2005, he was elected as the Chair of the IEEE Iran Section. He is the recipient of several awards, including the Bellcore's Award of Excellence, the Nationwide Outstanding Research Award from the Ministry of Science, Research, and Technology in 2003, and the Nation's Highly Cited Researcher Award in 2004. He is among the 250 preeminent and most influential researchers worldwide in the ISI Highly Cited in the Computer Science Category. In 2009, he was elected as a member of Iran Academy of Sciences and also as a Fellow of Islamic World Academy of Sciences.