Large Families of Asymptotically Optimal Two-Dimensional Optical Orthogonal Codes

Reza Omrani, Gagan Garg, P. Vijay Kumar, Petros Elia, and Pankaj Bhambhani

***Abstract*—Nine new 2-D OOCs are presented here, all sharing the common feature of a code size that is much larger in relation to the number of time slots than those of constructions appearing previously in the literature. Each of these constructions is either optimal or asymptotically optimal with respect to either the original Johnson bound or else a non-binary version of the Johnson bound introduced in this paper.**

The first 5 codes are constructed using polynomials over finite fields - the first construction is optimal while the remaining 4 are asymptotically optimal. The next two codes are constructed using rational functions in place of polynomials and these are asymptotically optimal. The last two codes, also asymptotically optimal, are constructed by composing two of the above codes with a constant weight binary code.

Also presented, is a three-dimensional OOC that exploits the polarization dimension.

Finally, phase-encoded optical CDMA is considered and construction of two efficient codes are provided.

***Index Terms*—Optical orthogonal codes, optical CDMA, OCDMA, two-dimensional codes, 2-D OOC, wavelength-time hopping codes, Johnson bound, phase-encoded OCDMA.**

I. Introduction

There has been an upsurge of interest in applying code division multiple access (CDMA) techniques to optical networks - optical CDMA (OCDMA) [1]. This is partly due to the increase in security [2] afforded by OCDMA (as measured, for instance, by the increased effort needed to intercept an OCDMA signal) and partly due to the flexibility and simplicity [3] of network control afforded by OCDMA.

There are two main approaches to data modulation and spreading in optical CDMA (OCDMA). The first approach, known as direct-sequence encoding [1], makes use of on-off-keying (OOK) data modulation and unipolar spreading sequences with good correlation properties. Traditionally, as in the case of wireless communication, the spreading has been carried out in the time domain and we will refer to this class of OOCs as one-dimensional OOCs (1-D OOCs) [3]–[26]. A drawback of 1-D OOCs is the requirement of a large chip rate. By employing two-dimensional optical orthogonal codes (2-D OOCs) that spread in both time and wavelength domain, it turns out that the large-chip-rate requirement can be substantially reduced [27]. There is a considerable literature on 2-D OOC constructions. However, in this paper, we focus our attention only on optimal and asymptotically optimal constructions. A quick overview of optimal (or asymptotically optimal) constructions of 2-D codes in the literature is presented in Table I. The code constructions presented here came about as a result of a DARPA-funded project [28], a subgoal of which was coming up with constructions that would give the experimentalist the maximum possible flexibility in choosing the parameters Λ and T. In this context, Fig. 2 provides a visual depiction of the parameter sets for small Λ, T in the range, $2 \leq \Lambda \leq 17$, $2 \leq T \leq 33$ for which constructions are now available as a result of the 9 constructions presented here.

The second OCDMA approach uses spectral encoding. In this method, spreading is achieved by encoding of amplitude or phase of the data spectrum [29], [30].

This paper is organized as follows: Section II provides background material along with an overview of the results of this paper. In Section III, we propose two new bounds on the size of 2-D OOCs - we use these bounds to prove optimality of some of the constructions presented in the current paper as well as of two constructions previously known in the literature, but which were not known to be optimal. In the next section, we propose five families of 2-D OOCs constructed using polynomials over finite fields. In Section V, we present two families of asymptotically optimal codes constructed using rational functions over finite fields. We show in Section VI how one can generate two asymptotically optimal families by composing two of the previous constructions with a constant weight binary code. In Section VII, we present a three-dimensional OOC using polarization as the third dimension. In Sections VIII and IX, we use generalized bent functions to construct two families of efficient asynchronous phase-encoding sequences for Optical CDMA. The last section concludes the paper. New results are presented as Propositions, known results appear as Theorems. Most of the proofs have been moved to the Appendices to ensure smooth reading of the paper.

Reza Omrani is with Telegent Systems, 470 Porrero Avenue, Sunnyvale, CA 94085, USA. omrani@usc.edu

Gagan Garg is with Indian Institute of Technology, Mandi 175001, Himachal Pradesh, India. Part of this work was carried out while he was at Indian Institute of Science. gagan.garg@gmail.com

P. Vijay Kumar is currently with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore 560012, India. Part of this work was carried out while he was at University of Southern California. vijayk@usc.edu

Petros Elia is with the Department of Mobile Communications, EURECOM, BP 193, F-06904, Sophia Antipolis cedex, France. petros.elia@eurecom.fr

Pankaj Bhambhani is with Cisco Systems India Pvt. Ltd., Cessna Business Park, Sarjapur, Bangalore 560087, India. pankaj.ani2000@gmail.com

This research was supported in part by DARPA OCDMA Program Grant No. N66001-02-1-8939.

The results of this paper have been presented in part at ISIT 2005, 2006 and SETA 2004, 2006.

TABLE I

OPTIMAL AND ASYMPTOTICALLY OPTIMAL 2-D OPTICAL ORTHOGONAL CODES IN THE LITERATURE

Construction Name	Parameters	Code Size	Constraint Satisfied	Optimality
Lee, Seo [31]	$(\Lambda \times T, 3, 1)$	$6\Lambda st + \Lambda s + \Lambda t$, where s and t are the sizes of the optimal OOCs $(\Lambda, 3, 1)$ and $(T, 3, 1)$ respectively. (O) when $\Lambda, T \equiv 1 \pmod 6$; (AO) otherwise	None	(O)
Shurong et. al. [32]	$(\Lambda \times T, \omega, 1)$, $\Lambda = p^k$	$\frac{\Lambda(\Lambda T-1)}{\omega(\omega-1)}$	None	(O)
Kwong, Yang [33]	$(\Lambda \times T, \omega, 1)$, $\Lambda = p_1 p_2 \cdots p_k$, $T = p_1$, $p_k \geq p_{k-1} \geq \ldots \geq p_1 \geq \omega$	$\frac{\Lambda^2}{p_k} + \frac{\Lambda^2}{p_k p_{k-1}} + \frac{\Lambda^2}{p_k p_{k-1} p_{k-2}} + \ldots + \Lambda$	AM-OPPTS	(AO)
Yang, Kwong [34]	$(\Lambda \times T, \omega, 1)$, $\Lambda = T = \omega t(\omega - 1) + 1$, Λ is prime, t is some integer	$\frac{\Lambda(\Lambda^2-1)}{\omega(\omega-1)}$	None	(O)
Yang, Kwong [34]	$(\Lambda \times T, \omega, 1)$, $\omega = \Lambda$, $T = p_1 p_2 \cdots p_k$, $p_k \geq p_{k-1} \geq \ldots \geq p_1 \geq \Lambda$	T	OPPW	(O)*
Yang, Kwong [34]	$(\Lambda \times T, \omega, 1), \omega = \Lambda - 1$, $\Lambda = p_1, T = (p_1 - 1)p_2 \cdots p_k$, $p_k \geq p_{k-1} \geq \ldots \geq p_1$	$\frac{\Lambda T}{\Lambda - 1}$	AM-OPPW	(AO)
Kwong et. al. [35]	$(\Lambda \times T, \omega, 1)$, $\Lambda = p_1 p_2 \cdots p_k$, $p_k \geq p_{k-1} \geq \ldots \geq p_1 \geq \omega$	$\Lambda^2 \cdot \Phi_{OOC}$, where Φ_{OOC} is the cardinality of the optimal $(T, \omega, 1)$ OOC	AM-OPPTS	(AO)
Shivaleela et. al. [36]	$(\Lambda \times T, \omega, 1)$, $\Lambda = T = \omega$, T is prime	T	OPPW	(O)*

Here,

- (O) denotes Optimal,
- (AO) denotes Asymptotically Optimal,
- p or p_i denotes a prime.

* These constructions are shown to be optimal using the bounds proposed in this paper.

II. BACKGROUND AND RESULTS

The focus of the entire paper (except for Sections VIII and IX) is on direct-sequence encoding. Phase-encoding is restricted to Sections VIII and IX only.

The advent of Wavelength-Division-Multiplexing (WDM) and dense-WDM (D-WDM) technology has made it possible to spread in both wavelength and time [34]. The corresponding codes are variously called wavelength-time hopping codes and multiple-wavelength codes. Here, we will simply refer to these codes as two-dimensional OOCs (2-D OOCs).

A 2-D $(\Lambda \times T, \omega, \kappa)$ OOC $\mathcal{C}$ is a family of $\{0,1\}$ $\Lambda \times T$ arrays of constant weight ω. Every pair $\{A, B\}$ of arrays in $\mathcal{C}$ is required to satisfy:

$$\sum_{\lambda=1}^{\Lambda} \sum_{t=0}^{T-1} A(\lambda, t) B(\lambda, (t \oplus_T \tau)) \leq \kappa, \tag{1}$$

where either $A \neq B$ or $\tau \neq 0$. We will refer to κ as the maximum collision parameter (MCP) when in addition to (1) holding for all τ, we have that equality holds in (1) for some pair A, B and for some τ. Note that the asynchronism is present only along the time axis.

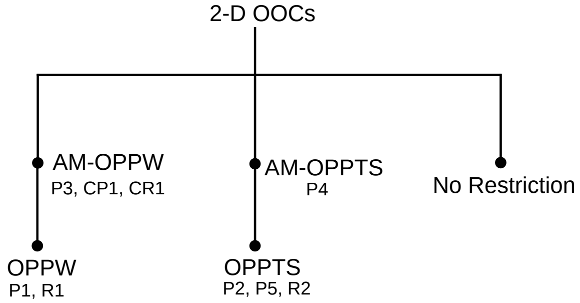

Fig. 1. Various types of 2-D OOCs. The symbols P3, CP1 etc. are reference to specific constructions appearing in Table II.

Practical considerations often place restrictions on the placement of pulses within an array. With this in mind, we introduce the following terminology (see Fig. 1):

TABLE II
NEW 2-D OPTICAL ORTHOGONAL CODES PROPOSED IN THIS PAPER

Construction Name	Parameters	Code Size	Constraint Satisfied	Optimality
P1	$(\Lambda \times T, \omega, \kappa)$, $\kappa < \omega = \Lambda \leq T$, T is prime	T^{κ}	OPPW	(O)
P2	$(\Lambda \times T, \omega, \kappa)$, $\Lambda = p$, $\omega = T$, $\kappa < \omega$, $T \mid p-1$	$\frac{1}{T} \sum_{d \mid (\Lambda-1)} \left(\Lambda^{\left\lceil \frac{\kappa+1}{d} \right\rceil} - 1 \right) \mu(d)$	OPPTS	(AO)
P3	$(\Lambda \times T, \omega, \kappa)$, $1 \leq \Lambda \leq p^m$, $T = p^m - 1$, $\omega = \Lambda - \kappa$, $\kappa < \omega$	$\frac{(T+1)^{\kappa+1}-1}{T}$	AM-OPPW	(AO)
P4	$(\Lambda \times T, \omega, \kappa)$, $\omega = T - \kappa$, $T \mid p^m - 1$, $\Lambda = p^m - 1$, $\kappa < \omega$	$\frac{1}{T} \sum_{d \mid \Lambda} \left((\Lambda+1)^{\left\lceil \frac{\kappa+1}{d} \right\rceil} - 1 \right) \mu(d)$	AM-OPPTS	(AO)
P5	$(\Lambda \times T, \omega, \kappa)$, $\omega = T$, $\Lambda = p^m$, $\kappa < \omega$, $T \mid p^m - 1$	$\frac{1}{T} \sum_{d \mid (\Lambda-1)} \left(\Lambda^{\left\lceil \frac{\kappa+1}{d} \right\rceil} - 1 \right) \mu(d)$	OPPTS	(AO)
R1	$(\Lambda \times T, \omega, \kappa)$, $\omega = \Lambda$, $\Lambda \leq T - 1$, $T = p^m + 1$, $\kappa < \omega$ is even	$\frac{c\left(\frac{\kappa}{2}\right)}{T} + 1$	OPPW	(AO)
R2	$(\Lambda \times T, \omega, \kappa)$, $T \vert p^m - 1$, $\Lambda = p^m + 1$, $\omega = T$, $\kappa < \omega$ is even	$\frac{1}{T(q-1)} \sum_{h(x)} u(d - deg(h(x)), T, 1)\hat{\mu}(h(x))$ where the sum is over monic $h(x) \in \mathbb{F}_q[x]$ of deg $\leq d$	OPPTS	(AO)
CP1	$(\Lambda \times T, \omega, \kappa)$, $\kappa < \omega \leq \Lambda$, T is prime	$T^{\kappa} \left\lfloor \frac{\Lambda}{\omega} \left\lfloor \frac{\Lambda-1}{\omega-1} \left\lfloor \frac{\Lambda-2}{\omega-2} \cdots \left\lfloor \frac{\Lambda-\kappa}{\omega-\kappa} \right\rfloor \right\rfloor \right\rfloor \right\rfloor$	AM-OPPW	(AO)
CR1	$(\Lambda \times T, \omega, \kappa)$, $\omega \leq \Lambda$, $\kappa < \omega$ is even, $T = p^m + 1$	$\left(\frac{c\left(\frac{\kappa}{2}\right)}{T} + 1 \right) \left\lfloor \frac{\Lambda}{\omega} \left\lfloor \frac{\Lambda-1}{\omega-1} \left\lfloor \frac{\Lambda-2}{\omega-2} \cdots \left\lfloor \frac{\Lambda-\kappa}{\omega-\kappa} \right\rfloor \right\rfloor \right\rfloor \right\rfloor$	AM-OPPW	(AO)

Here,

- (O) denotes Optimal and (AO) denotes Asymptotically Optimal,
- p denotes a prime, $q = p^m$
- $\mu(\cdot)$ is the Mobius function,
- $\hat{\mu}(\cdot)$ and $u(\cdot)$ are defined in equations (6) and (22) respectively, and
- $c(t) = \begin{cases} q^{2t+1} - q, & t = 1,2,3,4,5,6 \\ \geq q^{2t+1} - \frac{q^{2t-6}}{7}, & t \geq 7. \end{cases}$

- arrays with one-pulse per wavelength (OPPW): each row of every $(\Lambda \times T)$ code array in $\mathcal{C}$ is required to have Hamming weight $= 1$.
- arrays with at most one-pulse per wavelength (AM-OPPW): each row of any $(\Lambda \times T)$ code in $\mathcal{C}$ is required to have Hamming weight ≤ 1.
- arrays with one-pulse per time slot (OPPTS): each column of every $(\Lambda \times T)$ code array in $\mathcal{C}$ is required to have Hamming weight $= 1$.
- arrays with at most one-pulse per time slot (AM-OPPTS): each column of any $(\Lambda \times T)$ array in $\mathcal{C}$ is required to have Hamming weight ≤ 1 .

The constructions mentioned in Fig. 1 are proposed in this paper and have been summarized in Table II.

Remark 1: Note that for codes that are AM-OPPW or OPPW, the autocorrelation for non-zero values of the time shift is zero. This is obvious since there is (at most) one 1 in each row; hence, the time-shifted code matrix cannot have any overlap with the original code matrix. We shall use this fact later while proving the correlation properties of our constructions.

A. Johnson Bound

For a given set of values of $\Lambda, T, \omega, \kappa$, let $\Phi(\Lambda \times T, \omega, \kappa)$ denote the largest possible cardinality of a $(\Lambda \times T, \omega, \kappa)$ 2-D OOC. The following adaptation of the Johnson's bound for constant weight codes to 2-D OOCs was first noted by Yang and Kwong in [34]:

Theorem 1: [Johnson Bound]

$$\Phi(\Lambda \times T, \omega, \kappa) \leq \left\lfloor \frac{\Lambda}{\omega} \left\lfloor \frac{\Lambda T - 1}{\omega - 1} \cdots \left\lfloor \frac{\Lambda T - \kappa}{\omega - \kappa} \right\rfloor \right\rfloor \right\rfloor . \qquad (2)$$

A construction method with $\Phi(\Lambda \times T, \omega, \kappa)$ codewords is called optimal and therefore, a construction meeting the Johnson bound is optimal. A construction that meets this bound asymptotically (i.e., when Λ or T (or both) tend to infinity) is called an asymptotically optimal construction.

B. Literature Review

In this subsection, we focus primarily on prior constructions of optimal or asymptotically optimal constructions of 2-D OOCs in the literature. A summary of these appears in Table I. Note that all these constructions are optimal (or asymptotically optimal) only for MCP $= 1$. However, the constructions that we propose in this paper are optimal (or asymptotically optimal) for all values of the MCP, i.e., MCP ≥ 1 thereby leading to larger size (this is explained in detail in the next subsection).

The construction by Lee and Seo [31] spreads in the wavelength and the time domain by using two different 1-D OOCs. Shurong et. al [32] construct a 2-D OOC by employing a frequency hopping code to spread in the wavelength domain and a 1-D OOC to spread along the time axis. The construction by Kwong and Yang [33] interchanges the time and wavelength components of a frequency-hopping code and then applies specific cyclic shifts to control the value of the MCP. The first construction by Yang and Kwong [34] uses a 1-D OOC to achieve spreading in the wavelength and time domains. The remaining two constructions in [34] modify frequency-hopping codes to construct 2-D OOCs. The construction by Kwong et. al [35] spreads in the wavelength domain using a frequency-hopping code and in the time domain using a 1-D OOC. The OPPW construction by Shivaleela et. al [36] places a 1 in the first time slot of the first wavelength. By cyclically shifting the position of the 1 in the subsequent wavelengths by k, the entire 2-D code is generated. The k for different codewords varies from 0 to $T-1$, where T is the number of time slots.

Additional papers in the literature dealing with the design of 2-D OOCs include [2], [37]–[61]. However, since the focus of the current paper is on optimal or asymptotically optimal constructions, we do not discuss these further here. A paper relating to 3-D code construction is [62].

C. Overview of Results

We propose a version of non-binary Johnson bound and derive two other bounds from it - these bounds provide upper bounds on the size of 2-D OOCs for the case of AM-OPPW 2-D OOCs and OPPW 2-D OOCs. A special instance is shown to lead to the Singleton bound.

We then propose 9 new families of 2-D OOCs of large size. All the codes proposed in this paper are optimal (or asymptotically optimal) with respect to the original Johnson bound [34] or the new bounds proposed in this paper. We obtain codes with large size by constructing optimal families for large values of the MCP. Consider MCP $= \kappa = 1$, for example. The 2-D Johnson bound gives

$$\begin{aligned} \Phi(\Lambda \times T, \omega, \kappa) &\leq \left\lfloor \frac{\Lambda}{\omega} \left\lfloor \frac{\Lambda T - 1}{\omega - 1} \right\rfloor \right\rfloor \\ &\approx \frac{\Lambda}{\omega} \left(\frac{\Lambda T - 1}{\omega - 1} \right) \\ &\approx \frac{\Lambda^2 T}{\omega^2} \\ &= \frac{1}{T} \left(\frac{\Lambda T}{\omega} \right)^2 . \end{aligned}$$

Similarly, for large values of κ, we get

$$\Phi(\Lambda \times T, \omega, \kappa) \lesssim \frac{1}{T} \left(\frac{\Lambda T}{\omega} \right)^{\kappa+1} .$$

This shows that, for fixed values of Λ, T and ω, the upper bound on the maximum number of codewords increases exponentially in the MCP. Note that all the constructions in Table I have MCP $= 1$ thereby restricting the size to $\frac{\Lambda^2 T}{\omega^2}$. Hence, by constructing optimal (or asymptotically optimal) constructions for larger values of the MCP, we are proposing 2-D OOCs with size larger than has been previously constructed.

All the 9 constructions presented in this paper have been summarized in Table II. Additionally, Fig. 2 provides a visual depiction of the parameter sets for small Λ, T in the range, $2 \leq \Lambda \leq 17$, $2 \leq T \leq 33$ for which constructions are now available as a result of the 9 constructions presented here. All constructions are either optimal or else drawn from a family of asymptotically optimal constructions and correspond in every case to a code whose size is large in relation to the number T of time slots. This table brings out the need for proposing different constructions since these 9 constructions are applicable to different values of Λ and T. For ease of representation, we use the following legend:

Construction Name	Name in the Table	Construction Name	Name in the Table
P1	A	R1	F
P2	B	R2	G
P3	C	CP1	H
P4	D	CR1	I
P5	E		

For example, consider the entry in the table corresponding to $T = 5, \Lambda = 3$. The entry reads AFHI. This means that for $T = 5$ and $\Lambda = 3$, we are proposing four optimal (or asymptotically optimal) constructions in this paper, viz., construction P1, R1, CP1 and CR1.

Remark 2: Note that the rows corresponding to $T = 21, 25$ and 27 are empty. However, this does imply that there are no constructions for these values of T - it simply means that there are no constructions for $2 \leq \Lambda \leq 17$. For example, for $T = 21$, we have construction P2 (or B) for $\Lambda = 43, 127, 211$ etc. Similarly, we have construction P2 for $T = 25, \Lambda = 101, 151, 251$; and for $T = 27, \Lambda = 109, 163, 271$ and so on.

The seven constructions (P1 to P5, R1 and R2) are generated by regarding a codeword in the 2-D code as the graph of a function. For example, a codeword in a 2-D AM-OPPW code can be regarded as the graph of a function $t = f(\lambda)$, $0 \le t \le T-1$, $0 \le \lambda \le \Lambda - 1$ mapping wavelength to time. Analogously, a codeword in a 2-D AM-OPPTS OOC can be regarded as the graph of a function $\lambda = f(t)$, $0 \le t \le T-1$, $0 \le \lambda \le \Lambda - 1$ mapping time to wavelength.

The first 5 of these codes (P1 to P5) are constructed using polynomials over finite fields. Code P1 is optimal while codes P2 to P5 are asymptotically optimal.

The next two codes (R1 and R2) are constructed using rational functions over finite fields. Both these codes are defined for even values of the MCP and are asymptotically optimal.

Next, we compose P1 with a constant weight binary code and generate the concatenated code CP1. This code is asymptotically optimal and is AM-OPPW. We do a similar composition of R1 and a constant weight binary code to generate CR1, which is also asymptotically optimal.

We present a 3-D code construction using polarization as the third dimension. This code is constructed using the Chinese Remainder Theorem.

Finally, we use generalized bent functions to construct a family of efficient asynchronous phase-encoding sequences for optical CDMA.

III. New Bounds on the Code Size

In this section, we begin by proposing a one-dimensional Johnson bound on constant weight codes over a non-binary alphabet. The bound will establish the optimality of some of the constructions that we propose in the sections that follow.

The codes under consideration are over an alphabet $\mathcal{A}$ of size $(T+1)$ containing a distinguished element, which we shall call 0. For codes over such an alphabet, we define the Hamming correlation between two codewords to be the number of symbol locations in which the two codewords contain the same *non-zero* symbol.

Let $A_T(\Lambda, \omega, \kappa)$ denote the maximum possible size of a constant-weight code $\mathcal{C}$ over the alphabet $\mathcal{A}$ of size $T+1$ of length Λ, Hamming weight ω, and Hamming correlation $\le \kappa$.

Proposition 2 (Nonbinary Johnson Bound):

$$A_T(\Lambda, \omega, \kappa) \le \left\lfloor \frac{T\Lambda}{\omega} \left\lfloor \frac{T(\Lambda-1)}{\omega-1} \cdots \left\lfloor \frac{T(\Lambda-\kappa)}{\omega-\kappa} \right\rfloor \right\rfloor \right\rfloor .$$

For the proof, we refer the reader to Appendix A.

Remark 3 (Recovering the Binary Johnson Bound): In the binary case, i.e., when $T+1 = 2$, the above inequality reduces to the Johnson bound for constant-weight binary codes.

Remark 4 (Singleton Bound): For the special case when $\Lambda = \omega$, the above bound reduces to

$$A_T(\Lambda, \omega, \kappa) \ \le \ T^{\kappa+1}$$

and we have, in fact, recovered the Singleton bound of coding theory.

We now proceed to apply the non-binary Johnson bound to derive bounds on AM-OPPW 2-D OOCs.

Proposition 3 (Bound on AM-OPPW Code Size): The maximum possible size $\Phi(\Lambda \times T, \omega, \kappa)$ of an AM-OPPW 2-D OOC with parameters $(\Lambda \times T, \omega, \kappa)$ satisfies:

$$\Phi(\Lambda \times T, \omega, \kappa) \le \left\lfloor \frac{\Lambda}{\omega} \left\lfloor \frac{T(\Lambda-1)}{\omega-1} \cdots \left\lfloor \frac{T(\Lambda-\kappa)}{\omega-\kappa} \right\rfloor \right\rfloor \right\rfloor .$$

For the proof, we refer the reader to Appendix B.

Corollary 4 (Bound on OPPW Code Size): The maximum possible size $\Phi(\Lambda \times T, \omega, \kappa)$ of an OPPW 2-D OOC with parameters $(\Lambda \times T, \omega, \kappa)$ satisfies:

$$\Phi(\Lambda \times T, \omega, \kappa) \ \le \ T^{\kappa}.$$

It follows from the above that the following constructions are optimal (note that $\kappa = 1$ here) although this was unknown to the authors (see Table I):

- the second construction by Yang and Kwong [34] and
- the construction by Shivaleela et. al [36].

The next few sections will each introduce new constructions of optimal (or asymptotically optimal) 2-D OOCs.

IV. New Constructions Based on Polynomial Functions

A codeword in a 2-D AM-OPPW OOC can be regarded as the graph of a function $t = f(\lambda)$, $0 \le t \le T-1$, $0 \le \lambda \le \Lambda - 1$ mapping wavelength to time. Analogously, a codeword in a 2-D AM-OPPTS OOC can be regarded as the graph of a function $\lambda = f(t)$, $0 \le t \le T-1$, $0 \le \lambda \le \Lambda - 1$ mapping time to wavelength.

Without loss of generality, in the constructions below, we will identify the T time slots with the set $\mathbb{Z}_T$, which we label as $\mathcal{T}$. This will allow us to identify cyclic shifts in the time domain with $\pmod T$ additions in $\mathbb{Z}_T$. We will identify the Λ wavelengths with subsets $\mathcal{L}$ of algebraic structures. Thus, $\mid \mathcal{T} \mid = T$ and $\mid \mathcal{L} \mid = \Lambda$.

All of the constructions in this section employ polynomial functions whose degree is bounded above by the desired value of the MCP κ. In the next section, we use rational functions to construct 2-D OOCs.

While the constructions below have some elements in common, they also have their differences. The reason for providing the set of constructions is to provide constructions for as many (Λ, T) parameter sets as possible. The impact of the different constructions given here can be seen in Fig. 2, where we identify constructions with the entries in the table.

A. Construction P1: Mapping Wavelength to Time, OPPW, $\omega = \Lambda, \ \Lambda \le T, \ \kappa < \omega, \ T$ prime

Here $T = p$, $\mathcal{T} = \mathbb{Z}_p$, $\mathcal{L} \subseteq \mathbb{Z}_p$ and we consider polynomials $f(\lambda)$ over $\mathbb{Z}_p$ of degree $\le \kappa$ mapping $\mathcal{L} \to \mathcal{T}$, where p is a prime. Let φ be a mapping from the set of all such functions to the code matrices, where the $\Lambda \times T$ code

		Value of Λ															
	T \ Λ	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
T	2	ACDH	BCEH	DGH	BEH	DGH	BEH	DGH	EH	DGH	BEH	DGH	BEH	GH	H	DH	BEH
	3	ACEFHI	ACDGHI	CHI	EHI	DGHI	BHI	EHI	GHI	HI	EHI	DGHI	BHI	HI	DHI	HI	EHI
	4	CFI	CEFI	CDGI	BCI	I	EI	DGI	I	I	EI	DGI	BI	I	I	DI	BI
	5	AFHI	AFHI	AEFHI	AGHI	HI	HI	HI	EHI	DGHI	BHI	HI	HI	HI	DHI	HI	HI
	6	CFI	CFI	CFI	CEFI	CDGI	BCI	I	I	I	EI	DGI	BI	I	I	I	EI
	7	ACH	ACH	ACH	ACH	ACH	ACDH	CH	H	H	H	H	EH	GH	H	H	H
	8	CFI	CFI	CFI	CFI	CFI	CEFI	CDGI	CI	I	I	I	I	I	I	DI	BI
	9	FI	FI	FI	FI	FI	FI	EFI	GI	I	I	I	I	I	I	I	EI
	10	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CEFI	CDGI	BCI	I	I	I	I	I	I
	11	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	H	H	H	H	H	H
	12	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CEFI	CDGI	BCI	I	I	I	I
	13	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	H	H	H	H
	14	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	EFI	GI	I	I	I
	15	C	C	C	C	C	C	C	C	C	C	C	C	C	CD	C	
	16	C	C	C	C	C	C	C	C	C	C	C	C	C	C	CD	BC
	17	AFHI	AFHI	AFHI	AFHI	AFHI	AFHI	AFHI	AFHI	AFHI	AFHI	AFHI	AFHI	AFHI	AFHI	AEFHI	AGHI
	18	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CEFI
	19	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH
	20	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI
	21																
	22	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
	23	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH
	24	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI
	25																
	26	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI
	27																
	28	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI
	29	A	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH
	30	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI	CFI
	31	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH	AH
	32	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI
	33	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI	FI

Fig. 2. Representative table showing constructions for (Λ, T), $\Lambda \in [2, 17]$, $T \in [2, 33]$

matrix C associated to function f is given by $C(\lambda, t) = 1$ iff $f(\lambda) = t$, where $\lambda \in \mathcal{L}$.

We first show that φ is an injective mapping, i.e., the code matrices C_1 and C_2, corresponding to polynomials f_1 and f_2 respectively, are equal iff $f_1 = f_2$. This is true since $C_1(\lambda, t) = C_2(\lambda, t) \Leftrightarrow f_1(\lambda) = f_2(\lambda)$. Since $f_1(\lambda) - f_2(\lambda)$ is a non-zero polynomial of degree $\leq \kappa$, this equation can have a maximum of κ zeroes. Hence, as $\omega > \kappa$, these two functions cannot coincide in all the ω positions.

Since this code is OPPW, the autocorrelation function for each of these matrices for non-zero cyclic shifts is 0 by Remark 1.

We next declare two polynomials $f(\lambda)$ and $f(\lambda) + \delta$, where $\delta \in \mathbb{Z}_p$, to be equivalent. This causes the set of all the code matrices to be partitioned into equivalence classes, each of size T. This results in $\frac{T^{\kappa+1}}{T} = T^{\kappa}$ code matrices.

Note first that $C_a(\lambda, t + \tau) = 1 = C_b(\lambda, t)$ iff $f_a(\lambda) - \tau = f_b(\lambda)$. For cross-correlation, consider $C_a(\lambda, t + \tau)$ and $C_b(\lambda, t)$ from different equivalence classes corresponding to functions f_a and f_b respectively. Next, the polynomial $f_a(\lambda) - \tau - f_b(\lambda)$ is non-zero since f_a and f_b belong to different equivalence classes. Since the polynomial is non-zero, it can have a maximum of κ zeroes (the degree of the polynomial); hence, the two code matrices C_a and C_b can have a maximum of κ collisions.

This results in a $(\Lambda \times T, \Lambda, \kappa)$ 2-D OOC of size T^{κ}. This construction can be seen to be optimal by Corollary 4.

Remark 5: The elements of this 2D-OOC can also be regarded as corresponding to codewords in a Reed-Solomon code under an appropriate equivalence relation between the codewords. Let Λ, κ, T be as above. In particular $T = p$, where p is a prime. The $[\Lambda, \kappa]$ Reed-Solomon code $\mathcal{C}_{RS}$ may be constructed as follows: let $\{\alpha_1, \alpha_2, \ldots, \alpha_\Lambda\}$ denote a set of Λ distinct elements drawn from $\mathbb{F}_p$. Let $\mathcal{P}_\kappa$ denote the set of all polynomials over $\mathbb{F}_p$ of degree $\leq \kappa$. Set

$$\mathcal{C}_{RS} \quad = \quad \{(f(\alpha_1), \ldots, f(\alpha_\Lambda)) \mid f \in \mathcal{P}_\kappa\}. \tag{3}$$

Next, partition the set of all the codewords into p^κ equivalence classes by declaring $\underline{c}_1 \sim \underline{c}_2$ if $\underline{c}_1 - \underline{c}_2 = \eta \underline{1}$, $\eta \in \mathbb{F}_p^* = \mathbb{F}_p \backslash \{0\}$ (where $\underline{1}$ denotes the all 1 vector). Finally, we form a set $\mathcal{S}$ by picking precisely one element from each equivalence class and by associating a $(\Lambda \times T)$ matrix $A(\lambda, t)$ to each vector $\underline{a} \in \mathcal{S}$ by setting

$$A(\lambda, t) = 1 \quad \text{iff } a_\lambda \; = \; t, \quad 1 \leq \lambda \leq \Lambda.$$

B. Construction P2: Mapping Time to Wavelength, OPPTS, $\Lambda = p,\ p$ prime$,\ T \mid p - 1,\ \omega = T,\ \kappa < \omega$

Here $\mathcal{L} = \mathbb{Z}_p$. Let α be an element of $\mathbb{Z}_p$ of multiplicative order T and let H be the subgroup of order T generated by α in $\mathbb{Z}_p$. We will identify $\mathbb{Z}_T$ with H by associating t with α^t. Consider polynomials $f(x)$ over $\mathbb{Z}_p$ of degree $\leq \kappa$ mapping $H \rightarrow \mathcal{L}$. Let φ be a mapping from the set of all such functions to the code matrices, where the $\Lambda \times T$ code array C is obtained by setting $C(\lambda, t) = 1$ iff $f(\alpha^t) = \lambda$, where $t \in \mathcal{T}$ and $\lambda \in \mathbb{Z}_p$.

We first prove that φ is injective, i.e., the code matrices C_1 and C_2, corresponding to polynomials f_1 and f_2 respectively, are equal iff $f_1 = f_2$. This is true since $C_1(\lambda, t) = C_2(\lambda, t) \Leftrightarrow f_1(\alpha^t) = f_2(\alpha^t)$. Since $f_1(\alpha^t) - f_2(\alpha^t)$ is a non-zero polynomial of degree $\leq \kappa$, this equation can have a maximum of κ zeroes. Hence, as $\omega > \kappa$, these two polynomials cannot coincide in all the ω positions.

We next discard all sub-period polynomials, i.e., polynomials $f(x)$ that satisfy $f(\alpha^i x) = f(x)$ for some $i \in \mathbb{Z}_T^*$. This ensures good autocorrelation. Since $f(\alpha^i x) - f(x)$ is not the zero polynomial, we know that it has a maximum of κ zeroes (the degree of the polynomial). Hence, the autocorrelation is bounded above by κ.

We now define two polynomials $f(x), g(x)$ to be equivalent if $f(\alpha^i x) = g(x)$ for some $i \in \mathbb{Z}_T$. We pick a code matrix corresponding to each equivalence class to form a code of size $\frac{1}{T} \sum_{d|(\Lambda-1)} \left(\Lambda^{\lceil \frac{\kappa+1}{d} \rceil} - 1\right) \mu(d)$, where $\mu(\cdot)$ is the Mobius function (see [6] for code size computation).

Now, consider two polynomials f_a and f_b drawn from different equivalence classes. Consider the corresponding code matrices C_a and C_b. We know that $C_a(\lambda, t + \tau) = C_b(\lambda, t) \Leftrightarrow f_a(\alpha^{t+\tau}) = f_b(\alpha^t)$. Since these two polynomials have been drawn from distinct equivalence classes, the difference polynomial $f_a(\alpha^\tau x) - f_b(x)$ is non-zero. This implies that $f_a(\alpha^\tau x) - f_b(x)$ has $\leq \kappa$ zeroes. This proves that the crosscorrelation is bounded above by κ.

This construction is shown to be asymptotically optimal in Appendix C.

C. Construction P3: Mapping Wavelength to Time, AM-OPPW, $\omega = \Lambda - \kappa,\ \kappa < \omega,\ 1 \leq \Lambda \leq p^m,\ T = p^m - 1,\ p$ prime

Let p be prime and α a primitive element of $\mathbb{F}_{p^m}$. Let $T = p^m - 1$, $\mathcal{T} = \mathbb{Z}_T$ and $\mathcal{L} \subseteq \mathbb{F}_{p^m}$. Consider polynomials $f(x)$ over $\mathbb{F}_{p^m}$ of degree $\leq \kappa$ mapping $\mathcal{L} \rightarrow \mathbb{F}_{p^m}$. Let φ be a mapping from the set of all such functions to the code matrices, where the $\Lambda \times T$ code array C is obtained by setting $C(\lambda, t) = 1$ iff $f(\lambda) = \alpha^t$, where $t \in \mathcal{T}$ and $\lambda \in \mathcal{L}$. For those values of λ such that $f(\lambda) = 0$, the entire row is left blank. Clearly, at most κ rows in any matrix can be blank. To restore the constant weight property, we arbitrarily delete appropriate number of 1's to keep the weight equal to $\Lambda - \kappa$ for all the codewords.

We first prove that φ is injective, i.e., the code matrices C_1 and C_2, corresponding to polynomials f_1 and f_2 respectively, are equal iff $f_1 = f_2$. This is true since $C_1(\lambda, t) = C_2(\lambda, t) \Leftrightarrow f_1(\lambda) = f_2(\lambda)$. Since $f_1(\lambda) - f_2(\lambda)$ is a non-zero polynomial of degree $\leq \kappa$, this equation can have a maximum of κ zeroes. Hence, as $\omega > \kappa$, these two polynomials cannot coincide in all the ω positions.

Since this code is AM-OPPW, the autocorrelation function for each of these matrices for non-zero cyclic shifts is 0 by Remark 1.

We define two polynomials $f(x), g(x)$ of degree $\leq \kappa$ to be equivalent if $\alpha^i f(x) = g(x)$ for some $i \in \mathbb{Z}_T$. In our construction, we choose one polynomial from each equivalence class. This gives us a code of size $\frac{(T+1)^{\kappa+1}-1}{T}$.

Now, consider two polynomials f_a and f_b drawn from different equivalence classes. Consider the corresponding code matrices C_a and C_b. We know that $C_a(\lambda, t+\tau) = C_b(\lambda, t) \Leftrightarrow \alpha^{-\tau} f_a(x) = f_b(x)$. Since these two polynomials have been drawn from distinct equivalence classes, the difference polynomial $\alpha^{-\tau} f_a(x) - f_b(x)$ is non-zero. This implies that $\alpha^{-\tau} f_a(x) - f_b(x)$ has $\leq \kappa$ zeroes. This proves that the crosscorrelation is bounded above by κ.

This construction is proved to be asymptotically optimal in Appendix D.

D. Construction P4: Mapping Time to Wavelength, AM-OPPTS, $\Lambda = p^m - 1,\ p\, prime,\ \omega = T - \kappa,\ \kappa < \omega,\ T \mid p^m - 1$

Let p be prime. Let α be a primitive element of $\mathbb{F}_{p^m}$ and let β be a non-zero element in $\mathbb{F}_{p^m}$ of multiplicative order T. Let H be the subgroup of $\mathbb{F}_{p^m}$ generated by β. We will identify $\mathbb{Z}_T$ with H by associating t with β^t. Let $\mathcal{L} = \mathbb{F}_{p^m}^* = \{1, \alpha, \ldots, \alpha^{p^m-2}\}$ and $\mathcal{T} = \mathbb{Z}_T$. Consider polynomials $f(x)$ over $\mathbb{F}_{p^m}$ of degree $\leq \kappa$ mapping $H \rightarrow \mathcal{L}$. Let φ be a mapping from the set of all such functions to the code matrices, where the $\Lambda \times T$ code array C is obtained by setting $C(\lambda, t) = 1$ iff $f(\beta^t) = \lambda$. For those values of λ such that $f(\beta^t) = 0$, the entire column is left blank. Clearly, at most κ columns in any matrix can be blank. To restore the constant weight property, we arbitrarily delete an appropriate number of 1's to keep the weight equal to $T - \kappa$ for all the codewords.

We first prove that φ is injective, i.e., the code matrices C_1 and C_2, corresponding to polynomials f_1 and f_2 respectively, are equal iff $f_1 = f_2$. This is true since $C_1(\lambda, t) = C_2(\lambda, t) \Leftrightarrow f_1(\beta^t) = f_2(\beta^t)$. Since $f_1(\beta^t) - f_2(\beta^t)$ is a non-zero polynomial of degree $\leq \kappa$, this equation can have a maximum of κ zeroes. Hence, as $\omega > \kappa$, these two polynomials cannot coincide in all the ω positions.

We next discard all sub-period polynomials, i.e., polynomials $f(x)$ that satisfy $f(\beta^i x) = f(x)$ for some $i \in \mathbb{Z}_T^*$. This ensures good autocorrelation. Since $f(\beta^i x) - f(x)$ is not the zero polynomial, we know that it has a maximum of κ zeroes (the degree of the polynomial). Hence, the autocorrelation is bounded above by κ.

We now define two polynomials $f(x), g(x)$ to be equivalent if $f(\beta^i x) = g(x)$ for some $i \in \mathbb{Z}_T$. We pick a code matrix corresponding to each equivalence class to form a code of size $\frac{1}{T} \sum_{d|\Lambda} \left((\Lambda+1)^{\lceil \frac{\kappa+1}{d} \rceil} - 1 \right) \mu(d)$ (see [6] for code size computation).

Now, consider two polynomials f_a and f_b drawn from different equivalence classes. Consider the corresponding code matrices C_a and C_b. We know that $C_a(\lambda, t+\tau) = C_b(\lambda, t) \Leftrightarrow f_a(\beta^{t+\tau}) = f_b(\beta^t)$. Since these two polynomials have been drawn from distinct equivalence classes, the difference polynomial $f_a(\beta^\tau x) - f_b(x)$ is non-zero. This implies that $f_a(\beta^\tau x) - f_b(x)$ has $\leq \kappa$ zeroes. This proves that the crosscorrelation is bounded above by κ.

Since the number of codewords is similar to the number of codewords for construction P2, the proof for asymptotic optimality is along the same lines - see Appendix C.

E. Construction P5: Mapping Time to Wavelength, OPPTS, $\Lambda = p^m,\ p\ prime,\ \omega = T,\ \kappa < \omega,\ T \mid p^m - 1$

Let p be prime. Let α be a primitive element of $\mathbb{F}_{p^m}$ and let β be a non-zero element in $\mathbb{F}_{p^m}$ of multiplicative order T. Let H be the subgroup of $\mathbb{F}_{p^m}$ generated by β. We will identify $\mathbb{Z}_T$ with H by associating t with β^t. Let $\mathcal{L} = \mathbb{F}_{p^m} = \{0, 1, \alpha, \ldots, \alpha^{p^m-2}\}$ and $\mathcal{T} = \mathbb{Z}_T$. Consider polynomials $f(x)$ over $\mathbb{F}_{p^m}$ of degree $\leq \kappa$ mapping $H \rightarrow \mathcal{L}$. Let φ be a mapping from the set of all such functions to the code matrices, where the $\Lambda \times T$ code array C is obtained by setting $C(\lambda, t) = 1$ iff $f(\beta^t) = \lambda$. Thus, the construction here is along the lines of the previous construction except that the wavelengths are in 1-1 correspondence with *all* of $\mathbb{F}_{p^m}$.

We first prove that φ is injective, i.e., the code matrices C_1 and C_2, corresponding to polynomials f_1 and f_2 respectively, are equal iff $f_1 = f_2$. This is true since $C_1(\lambda, t) = C_2(\lambda, t) \Leftrightarrow f_1(\beta^t) = f_2(\beta^t)$. Since $f_1(\beta^t) - f_2(\beta^t)$ is a non-zero polynomial of degree $\leq \kappa$, this equation can have a maximum of κ zeroes. Hence, as $\omega > \kappa$, these two polynomials cannot coincide in all the ω positions.

We next discard all sub-period polynomials, i.e., polynomials $f(x)$ that satisfy $f(\beta^i x) = f(x)$ for some $i \in \mathbb{Z}_T^*$. This ensures good autocorrelation. Since $f(\beta^i x) - f(x)$ is not the zero polynomial, we know that it has a maximum of κ zeroes (the degree of the polynomial). Hence, the autocorrelation is bounded above by κ.

We now define two polynomials $f(x), g(x)$ to be equivalent if $f(\beta^i x) = g(x)$ for some $i \in \mathbb{Z}_T$. We pick a code matrix corresponding to each equivalence class to form a code of size $\frac{1}{T} \sum_{d|(\Lambda-1)} \left(\Lambda^{\lceil \frac{\kappa+1}{d} \rceil} - 1 \right) \mu(d)$ (see [6] for code size computation).

Now, consider two polynomials f_a and f_b drawn from different equivalence classes. Consider the corresponding code matrices C_a and C_b. We know that $C_a(\lambda, t+\tau) = C_b(\lambda, t) \Leftrightarrow f_a(\beta^{t+\tau}) = f_b(\beta^t)$. Since these two polynomials have been drawn from distinct equivalence classes, the difference polynomial $f_a(\beta^\tau x) - f_b(x)$ is non-zero. This implies that $f_a(\beta^\tau x) - f_b(x)$ has $\leq \kappa$ zeroes. This proves that the crosscorrelation is bounded above by κ.

The proof for asymptotic optimality of construction P5 is similar to the proof for construction P2 - see Appendix C.

V. New Asymptotically Optimal Constructions Based on Rational Functions

We now use rational functions over $\mathbb{F}_q$ to construct two 2-D OOCs. Some properties of rational functions that we use are summarized in the first subsection; the following two subsections deal with the two constructions.

A. Cyclic Ordering for the Projective Line

Consider all elements of $\mathbb{F}_q^2$ other than the element $[0 \quad 0]^T$. We define an equivalence relation amongst these elements as follows:

$$[a \quad b]^T \quad \sim \quad [c \quad d]^T, \tag{4}$$

if for some $\eta \in \mathbb{F}_q^*$, we have $[c \quad d]^T = [\eta a \quad \eta b]^T$. This partitions $\mathbb{F}_q^2$ into $(q+1)$ equivalence classes, with each class containing $(q-1)$ elements. The projective line is obtained by taking precisely one element from each equivalence class.

We denote this by $\mathbb{P}^1(\mathbb{F}_q)$. Thus, there are $(q+1)$ "points" on the projective line. We will use

$$\begin{bmatrix}a\\b\end{bmatrix}_{\text{eq}}$$

to denote the equivalence class containing

$$\begin{bmatrix}a\\b\end{bmatrix}.$$

We next present a cyclic ordering of the elements of $\mathbb{P}^1(\mathbb{F}_q)$.

Let $h(x) = x^2 + h_1 x + h_0$ with $h_1, h_0 \in \mathbb{F}_q$ be a primitive polynomial over $\mathbb{F}_q$. Let α be a zero of this polynomial and

$$H = \left[\begin{array}{cc} 0 & -h_0 \\ 1 & -h_1 \end{array}\right]$$

be the associated companion matrix.

Theorem 5: We claim that

$$\left\{ \left[H^i \begin{bmatrix}1\\0\end{bmatrix} \right]_{\text{eq}} \;\middle|\; 0 \le i \le q \right\} = \mathbb{P}^1(\mathbb{F}_q). \tag{5}$$

Proof: Note from the definition of the companion matrix that

$$H^i \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}a\\b\end{bmatrix}$$

is equivalent to saying that

$$\alpha^i \cdot 1 = a + b\alpha.$$

Thus

$$H^i \begin{bmatrix}1\\0\end{bmatrix} \sim H^j \begin{bmatrix}1\\0\end{bmatrix},$$

with $j > i$ iff

$$\alpha^i = \theta \alpha^j$$

for some $\theta \in \mathbb{F}_q^*$, i.e., iff

$$(q+1) \mid (j-i).$$

Hence, the equivalence classes

$$\left[H^i \begin{bmatrix}1\\0\end{bmatrix} \right]_{\text{eq}} \;\middle|\; 0 \le i \le q$$

are all distinct, thus proving the theorem. ■

Example 1: We present a cyclic ordering of $\mathbb{P}^1(\mathbb{F}_3)$. The polynomial $f(x) = x^2 + x + 2$ is a primitive polynomial over $\mathbb{F}_3$. Thus

$$H = \left[\begin{array}{cc} 0 & -2 \\ 1 & -1 \end{array}\right] = \left[\begin{array}{cc} 0 & 1 \\ 1 & 2 \end{array}\right] \Rightarrow$$

$$H \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix},\; H^2 \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\2\end{bmatrix},\; H^3 \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}2\\2\end{bmatrix} \Rightarrow$$

$$\mathbb{P}^1(\mathbb{F}_3) = \left\{ \begin{bmatrix}1\\0\end{bmatrix}_{\text{eq}}, \begin{bmatrix}0\\1\end{bmatrix}_{\text{eq}}, \begin{bmatrix}1\\2\end{bmatrix}_{\text{eq}}, \begin{bmatrix}2\\2\end{bmatrix}_{\text{eq}} \right\}.$$

It can easily be checked that

$$H^4 \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}2\\0\end{bmatrix} \sim \begin{bmatrix}1\\0\end{bmatrix},$$

which shows that the ordering is cyclic.

B. Construction R1: Mapping Wavelength to Time, OPPW, $T = q+1$, for $q = p^m$, $\;p$ prime, $\Lambda \le q$, $\omega = \Lambda$, $\kappa < \omega$, $\kappa = 2\kappa' = 2d$

Set $\mathcal{T} = \mathbb{P}^1(\mathbb{F}_q)$ and $\mathcal{L} = \{\alpha_1, \alpha_2, \ldots, \alpha_\lambda, \ldots, \alpha_\Lambda\} \subseteq \mathbb{F}_q$.

Let f, g be polynomials over $\mathbb{F}_q$ and let ϕ denote the mapping given by:

$$\phi(\alpha_i) = \begin{bmatrix}f(\alpha_i)\\g(\alpha_i)\end{bmatrix}_{\text{eq}}, \quad 1 \le i \le \Lambda.$$

We will regard ϕ as a rational function map because when $g(\alpha_i) \neq 0$ for any i, we equivalently have:

$$\phi(\alpha_i) = \begin{bmatrix}\frac{f(\alpha_i)}{g(\alpha_i)}\\1\end{bmatrix}_{\text{eq}}.$$

Let $\mathcal{F}_d$ denote the class of rational functions

$$\begin{bmatrix}f(x)\\g(x)\end{bmatrix}$$

over $\mathbb{F}_q$ (and hence over $\mathcal{L}$ by restriction) where f and g are polynomials over $\mathbb{F}_q$ satisfying:

1) f and g are both non-zero and both of degree $\le d$,
2) f and g are relatively prime, i.e., $(f, g) = 1$,
3) f is monic, and
4) either f or g must be a non-constant function; equivalently, $\frac{f(x)}{g(x)}$ is not the constant function.

The last condition has been included here since it is mathematically convenient to exclude the constant functions at this stage and bring them back later. Let $\hat{\mu}(\cdot),\; \hat{\mu}(\cdot) : \mathbb{F}_q[x] \to \mathbb{Z}$ be the function defined by

$$\hat{\mu}(b(x)) = \begin{cases} 1, & b(x) = 1, \\ (-1)^r, & b(x) \text{ is the product of } r \text{ monic,} \\ & \text{irreducible polynomials over } \mathbb{F}_q, \\ 0, & \text{else.} \end{cases} \tag{6}$$

Then the number $c_d = \mid \mathcal{F}_d \mid$ of rational functions in $\mathcal{F}_d$ can be computed from the results in [6] and is given by:

$$\mid \mathcal{F}_d \mid = \sum_{h(x)} \frac{(q^{d-s+1} - 1)^2}{(q-1)} \hat{\mu}(h(x)) \;-\; (q-1)$$

where the sum is over all monic polynomials $h(x) \in \mathbb{F}_q[x]$ of degree $s \le d$ and where the last term accounts for the disallowed constant functions. It can be shown [6] that

$$c(d) = \begin{cases} q^{2d+1} - q, & d = 1,2,3,4,5,6 \\ \ge q^{2d+1} - \frac{q^{2d-6}}{7}, & d \ge 7. \end{cases} \tag{7}$$

Let φ be a mapping from $\mathcal{F}_d$ to the code matrices, where the $\Lambda \times T$ code array is obtained by setting $C(\lambda, t) = 1$ iff

$$\begin{bmatrix}f(\alpha_\lambda)\\g(\alpha_\lambda)\end{bmatrix} \sim H^t \begin{bmatrix}1\\0\end{bmatrix}.$$

We first prove that φ is injective, i.e., the code matrices C_a and C_b, corresponding to rational functions $\left[\begin{smallmatrix}f_a(\alpha_\lambda)\\g_a(\alpha_\lambda)\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}f_b(\alpha_\lambda)\\g_b(\alpha_\lambda)\end{smallmatrix}\right]$ respectively, are equal iff $f_a(x) = f_b(x)$ and $g_a(x) =$

$g_b(x)$. Clearly, the code matrices C_a and C_b are equal iff for every $1 \leq \lambda \leq \Lambda$,

$$\begin{bmatrix} f_a(\alpha_\lambda) \\ g_a(\alpha_\lambda) \end{bmatrix} = \theta_\lambda \begin{bmatrix} f_b(\alpha_\lambda) \\ g_b(\alpha_\lambda) \end{bmatrix} \text{ for some } \theta_\lambda \in \mathbb{F}_q^*, \tag{8}$$

i.e., iff

$$\begin{aligned} \Leftrightarrow f_a(\alpha_\lambda) = \theta_\lambda f_b(\alpha_\lambda) \text{ and } g_a(\alpha_\lambda) &= \theta_\lambda g_b(\alpha_\lambda) \ \forall\ \lambda \\ \Leftrightarrow \theta_\lambda \left[f_a(\alpha_\lambda) g_b(\alpha_\lambda) - f_b(\alpha_\lambda) g_a(\alpha_\lambda) \right] &= 0 \ \forall\ \lambda \\ \Leftrightarrow f_a(\alpha_\lambda) g_b(\alpha_\lambda) - f_b(\alpha_\lambda) g_a(\alpha_\lambda) &= 0 \ \forall\ \lambda \\ \Leftrightarrow f_a(x) g_b(x) - f_b(x) g_a(x) &= 0 \text{ as polynomials} \\ \Leftrightarrow f_a(x) g_b(x) &= f_b(x) g_a(x). \end{aligned}$$

Since $f_a(x)$ is coprime to $g_a(x)$, it must be that $f_a(x) | f_b(x)$. Similarly, $f_b(x) | f_a(x)$. Since both $f_a(x)$ and $f_b(x)$ are monic, it implies that $f_a(x) = f_b(x)$ which forces $g_a(x) = g_b(x)$ and hence proves that φ is injective.

Since this code is OPPW, the autocorrelation function for each of these matrices for non-zero cyclic shifts is 0 by Remark 1.

Next, we would like to establish that the collection of matrices $\varphi(\mathcal{F}_d)$ is closed under cyclic shifts along the time axis. To show this, it is sufficient to show that if $C(\lambda, t)$ is the code matrix associated to element $\left[\begin{smallmatrix} f(x) \\ g(x) \end{smallmatrix}\right] \in \mathcal{F}_d$, then there exists $\left[\begin{smallmatrix} f'(x) \\ g'(x) \end{smallmatrix}\right] \in \mathcal{F}_d$ whose associated code matrix is $C(\lambda, t{+}1 \pmod{T})$. Such an element $\left[\begin{smallmatrix} f'(x) \\ g'(x) \end{smallmatrix}\right] \in \mathcal{F}_d$ is easily found by setting

$$\begin{bmatrix} f'(x) \\ g'(x) \end{bmatrix} = \mu_0 \begin{bmatrix} 0 & -h_0 \\ 1 & -h_1 \end{bmatrix} \begin{bmatrix} f(x) \\ g(x) \end{bmatrix} = \mu_0 \begin{bmatrix} -h_0 g(x) \\ f(x) - h_1 g(x) \end{bmatrix}$$

where μ_0 is chosen to ensure that $(\mu_0)(-h_0)g(x)$ is monic.

Let us define two elements $\left[\begin{smallmatrix} f_a(x) \\ g_a(x) \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} f_b(x) \\ g_b(x) \end{smallmatrix}\right]$ to be equivalent, i.e.,

$$\begin{bmatrix} f_a(x) \\ g_a(x) \end{bmatrix} \sim \begin{bmatrix} f_b(x) \\ g_b(x) \end{bmatrix}$$

if the corresponding code matrices C_a and C_b obtained via the mapping φ, are cyclic shifts of each other. Since φ is a $1-1$ mapping and since every code matrix $C(\lambda, t)$ in the image of φ has T distinct cyclic shifts, it follows that there are T elements within each such equivalence class. Our 2D-OCDMA code $\mathcal{C}$ is then the code obtained by selecting one element of $\mathcal{F}_d$ from each equivalence class and then applying the mapping φ. It follows then that this code is of size $\frac{c(d)}{T}+1$, where the 1 arises from the inclusion of the constant function and where $c(\cdot)$ is as defined in (7).

It remains to establish the cross-correlation bound for the code $\mathcal{C}$. Consider two rational functions $\left[\begin{smallmatrix} f_a(x) \\ g_a(x) \end{smallmatrix}\right], \left[\begin{smallmatrix} f_b(x) \\ g_b(x) \end{smallmatrix}\right]$ and their corresponding code matrices C_a and C_b. Let $\left[\begin{smallmatrix} f_c(x) \\ g_c(x) \end{smallmatrix}\right]$ be the element of $\mathcal{F}_d$ associated to a cyclic shift of $C_a(\lambda, t)$ by τ. Let the value of the cross-correlation be ν and let $\mathcal{V}$ denote the collection of $(t, \lambda) \in \{1, 2, \cdots, \Lambda\} \times \{1, 2, \cdots, T\}$ such that

$$C_a(\lambda, t + \tau \pmod{T}) \;=\; C_b(\lambda, t) \;=\; 1.$$

This implies that for every λ such that $(\lambda, t) \in \mathcal{V}$,

$$\begin{bmatrix} f_c(\alpha_\lambda) \\ g_c(\alpha_\lambda) \end{bmatrix} = \theta_\lambda \begin{bmatrix} f_b(\alpha_\lambda) \\ g_b(\alpha_\lambda) \end{bmatrix} \text{ for some } \theta_\lambda \in \mathbb{F}_q^*, \tag{9}$$

i.e.,

$$\begin{aligned} f_c(\alpha_\lambda) = \theta_\lambda f_b(\alpha_\lambda) \text{ and } g_c(\alpha_\lambda) &= \theta_\lambda g_b(\alpha_\lambda) \\ \Leftrightarrow \theta_\lambda \left[f_c(\alpha_\lambda) g_b(\alpha_\lambda) - f_b(\alpha_\lambda) g_c(\alpha_\lambda) \right] &= 0, \\ \Leftrightarrow f_c(\alpha_\lambda) g_b(\alpha_\lambda) - f_b(\alpha_\lambda) g_c(\alpha_\lambda) &= 0. \end{aligned}$$

But since the product polynomials $f_c(x)g_b(x)$ and $f_b(x)g_c(x)$ both have degree that is bounded above by $2d = \kappa$, it follows that $\mid \mathcal{V} \mid \leq \kappa$, thereby establishing that all cross-correlations for any cyclic shift are bounded above by κ, i.e., that the MCP $\leq \kappa$ and we are done. This construction is proved to be asymptotically optimal in Appendix E.

C. Construction R2: Mapping Time to Wavelength, OPPTS, $\omega = T,\ T \mid q-1,\ \Lambda = q+1$, for $q = p^m$, p prime, $\kappa = 2\kappa' = 2d < \omega$

We associate with each wavelength a distinct element of $\mathbb{P}^1(\mathbb{F}_q)$. Unlike in the case of Construction R1, the ordering of elements of $\mathbb{P}^1(\mathbb{F}_q)$ is immaterial here. We associate β^t with the t-th time slot, $0 \leq t \leq T-1$, where $\beta \in \mathbb{F}_q$ has multiplicative order T, $T|(q-1)$. As before, we associate elements along the time axis with elements of $\mathbb{Z}_T$.

We restrict our rational functions to once again belong to the set $\mathcal{F}_d$ for $d = \frac{\kappa}{2}$, where $\mathcal{F}_d$ is as defined in the previous subsection. In this case, we need to necessarily exclude the constant functions since they lead to constant autocorrelation function equal to ω for all time shifts and $\omega > \kappa$. Thus unlike the case of Construction R1, the last condition in the definition of $\mathcal{F}_d$ is needed here.

Let φ be a mapping from $\mathcal{F}_d$ to the code matrices, where the $\Lambda \times T$ code array associated to $\left[\begin{smallmatrix} f(x) \\ g(x) \end{smallmatrix}\right]$ is obtained by setting $C(\lambda, t) = 1$ iff

$$\begin{bmatrix} f(\beta^t) \\ g(\beta^t) \end{bmatrix} \sim \lambda,$$

where $t \in \mathbb{Z}_T$ and $\lambda \in \mathbb{P}^1(\mathbb{F}_q)$.

Once again, the first objective is to prove that φ is injective, i.e., that the code matrices C_a and C_b, corresponding to rational functions $\left[\begin{smallmatrix} f_a(x) \\ g_a(x) \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} f_b(x) \\ g_b(x) \end{smallmatrix}\right]$ respectively, are equal iff $f_a(x) = f_b(x)$ and $g_a(x) = g_b(x)$. Clearly, C_a and C_b are equal iff

$$\begin{bmatrix} f_a(\beta^t) \\ g_a(\beta^t) \end{bmatrix} = \theta_t \begin{bmatrix} f_b(\beta^t) \\ g_b(\beta^t) \end{bmatrix} \text{ where } \theta_t \in \mathbb{F}_q^* \text{ all } 0 \leq t \leq T-1.$$

This equation is similar to equation (8) obtained in the previous subsection and hence by arguing in similar fashion, we conclude that φ is injective.

If $C(\lambda, t)$ is the code matrix corresponding to rational function $\left[\begin{smallmatrix} f(x) \\ g(x) \end{smallmatrix}\right]$, and μ_f is the coefficient of the highest degree term in $f(\beta^\tau x)$, then it is clear that $C(\lambda, t + \tau \pmod{T})$ is uniquely associated to $\frac{1}{\mu_f}\left[\begin{smallmatrix} f(\beta^\tau x) \\ g(\beta^\tau x) \end{smallmatrix}\right]$. Next, note that if the autocorrelation function of $C(\lambda, t)$ is equal to ω for some nonzero time shift τ, this must mean that the matrices $C(\lambda, t)$ and $C(\lambda, t{+}\tau \pmod{T})$ are identical, which in turn can only happen by the $1-1$ nature of φ, if and only if the functions $\left[\begin{smallmatrix} f(x) \\ g(x) \end{smallmatrix}\right]$ and $\frac{1}{\mu_f}\left[\begin{smallmatrix} f(\beta^\tau x) \\ g(\beta^\tau x) \end{smallmatrix}\right]$ are identical. It follows then that to avoid constructing code matrices $C(\lambda, t)$ with autocorrelation function equal to ω for some nonzero time shift τ, we need to discard sub-period functions, i.e., functions that satisfy

$$\begin{bmatrix} f(\beta^\tau x) \\ g(\beta^\tau x) \end{bmatrix} = \theta \begin{bmatrix} f(x) \\ g(x) \end{bmatrix}, \quad \theta \in \mathbb{F}_q^* \tag{10}$$

for any $1 \leq \tau \leq T-1$. Accordingly, our next objective is to calculate the size of the set resulting from discarding the sub-period functions belonging to $\mathcal{F}_d$. Let us first calculate the number of polynomial pairs $(f(x), g(x))$ satisfying

1) f and g are both non-zero and both of degree $\leq d$,
2) $f(x)$ is monic and
3) the pair $(f(x), g(x))$ is not sub-periodic, i.e., that $\left[\begin{smallmatrix} f(x) \\ g(x) \end{smallmatrix}\right]$ does not satisfy (10) for any value of time-shift parameter τ (this condition subsumes the requirement of elements of $\mathcal{F}_d$, that either $f(x)$ or $g(x)$ be a non-constant polynomial).

We will subsequently modify this count to ensure that $\left[\begin{smallmatrix} f(x) \\ g(x) \end{smallmatrix}\right]$ satisfies the remaining requirement that will cause $\left[\begin{smallmatrix} f(x) \\ g(x) \end{smallmatrix}\right]$ to belong to $\mathcal{F}_d$, namely that

4) $(f, g) = 1$.

Let

$$f(x) = \sum_{i=1}^{r} f_i x^{e_i},$$

where without loss of generality $0 \leq e_1 < e_2 < \ldots < e_r \leq d$ and $f_r = 1$. Similarly, let

$$g(x) = \sum_{j=1}^{s} g_j x^{a_j}$$

where $0 \leq a_1 < a_2 < \ldots < a_s \leq d$. It is straightforward to show that (10) holds iff for some $1 \leq \tau \leq (T-1)$:

$$\begin{aligned} \beta^{\tau(e_i - e_1)} &= 1 \text{ for } 2 \leq i \leq r, \\ \beta^{\tau(a_j - a_1)} &= 1 \text{ for } 2 \leq j \leq s, \quad \text{and} \\ \beta^{\tau(e_1 - a_1)} &= 1. \end{aligned} \tag{11}$$

It will be found convenient to partition the different ways in which this can happen as follows:

- **Case (A)** $e_1 = a_1$ and $r = s = 1$.
- **Case (B)** $e_1 = a_1$, either $r > 1$ or $s > 1$ and
$$\begin{aligned} \gcd\left(\{e_i - e_1\}_{i=2}^{r}, \{a_j - a_1\}_{j=2}^{s},\ T\right) \\ = l \text{ for some } l > 1. \end{aligned} \tag{12}$$
- **Case (C)** $e_1 > a_1$ and
$$\begin{aligned} \gcd\left(\{e_i - e_1\}_{i=2}^{r}, \{a_j - a_1\}_{j=2}^{s}, (e_1 - a_1),\ T\right) \\ = l \text{ for some } l > 1. \end{aligned} \tag{13}$$
- **Case (D)** $a_1 > e_1$ and
$$\begin{aligned} \gcd\left(\{e_i - e_1\}_{i=2}^{r}, \{a_j - a_1\}_{j=2}^{s}, (a_1 - e_1),\ T\right) \\ = l \text{ for some } l > 1. \end{aligned} \tag{14}$$

Our interest is in counting the number of rational functions $\left[\begin{smallmatrix} f(x) \\ g(x) \end{smallmatrix}\right]$ corresponding to Cases B, C, D where $l = 1$ in each case and will carry out the count for the different cases separately. Clearly the count for Case C and Case D is the same, so it suffices to obtain a count for Cases B and C. We begin with the count for Case C.

Case C Count For $l|T$, let us define $u_C(l)$ to be the number of integer sets corresponding to Case C, i.e., the number of integer sets, $\{e_i \mid 0 \leq e_i \leq d, 1 \leq i \leq r\}$, $\{a_j \mid 0 \leq a_j \leq d, 1 \leq j \leq s\}$ where $e_1 > a_1$ and where in addition,

$$\begin{aligned} \gcd\left(\{e_i - e_1\}_{i=2}^{r}, \{a_j - a_1\}_{j=2}^{s}, |e_1 - a_1|,\ T\right) \\ = l. \end{aligned} \tag{16}$$

Our interest lies in computing $u_C(1)$ and we will do this using Mobius inversion [6].

Let $y_C(l)$ be the number of integer sets $\{e_i \mid 0 \leq e_i \leq d, 1 \leq i \leq r\}$, $\{a_j \mid 0 \leq a_j \leq d, 1 \leq j \leq s\}$ where $e_1 > a_1$ and where in addition,

- $l|T$,
- $l|(e_i - e_1)\ \forall\ 2 \leq i \leq r$,
- $l|(a_j - a_1)\ \forall\ 2 \leq j \leq s$ and
- $l|(e_1 - a_1)$.

It follows that

$$y_C(l) = \sum_{l':\ l|l'|T} u_C(l'). \tag{17}$$

Set

$$\begin{aligned} \tilde{y}_C(l) &= y_C(\frac{T}{l}), \\ \tilde{u}_C(l) &= u_C(\frac{T}{l}). \end{aligned}$$

Then we can rewrite (17) in the form

$$\begin{aligned} \tilde{y}_C(\frac{T}{l}) &= \sum_{l':\ l|l'|T} \tilde{u}_C(\frac{T}{l'}), \\ &= \sum_{l':l'|T \text{ and } \frac{T}{l'}|\frac{T}{l}} \tilde{u}_C(\frac{T}{l'}), \end{aligned}$$

i.e., for any divisor l of T,

$$\tilde{y}_C(l) = \sum_{l'|l} \tilde{u}_C(l').$$

Our goal is to compute $u_C(1) = \tilde{u}_C(T)$. Using Mobius inversion allows us to write

$$\begin{aligned} u_C(1) = \tilde{u}_C(T) &= \sum_{l|T} \tilde{y}_C\left(\frac{T}{l}\right)\mu(l), \\ &= \sum_{l|T} y_C(l)\mu(l), \end{aligned} \tag{18}$$

where $\mu(\cdot)$ is the Mobius function. The value of $y_C(l)$ can be shown to be given by

$$\begin{aligned} y_C(l) &= \\ \sum_{e_1=0}^{d} &\left\{q^{\lfloor \frac{d-e_1}{l} \rfloor + 1} - 1\right\} \sum_{c=1}^{\lfloor \frac{e_1}{l} \rfloor} \left\{q^{\lfloor \frac{d-e_1+cl}{l} \rfloor + 1} - 1\right\}. \end{aligned} \tag{19}$$

The count is really a count of the number of polynomials with exponents given by the $\{e_i, a_j\}$. This follows from

$$|C| = \frac{1}{T(q-1)} \sum_{h(x)} \left[\sum_{l|T} \left\{ 2 \sum_{e_1=0}^{d-deg(h(x))} \left\{ q^{\lfloor \frac{d-deg(h(x))-e_1}{l} \rfloor + 1} - 1 \right\} \sum_{c=1}^{\lfloor \frac{e_1}{l} \rfloor} \left\{ q^{\lfloor \frac{d-deg(h(x))-e_1+cl}{l} \rfloor + 1} - 1 \right\} + \sum_{e_1=0}^{d-deg(h(x))} \left\{ q^{\lfloor \frac{d-deg(h(x))-e_1}{l} \rfloor + 1} - 1 \right\}^2 - (q-1)^2 \left(d - deg(h(x)) + 1 \right) \right\} \mu(l) \right] \hat{\mu}(h(x)). \quad (15)$$

writing

$$\begin{aligned} f(x) &= \sum_{i=1}^{r} f_i x^{e_i} \\ &= x^{e_1} \left\{ \sum_{i=1}^{r} f_i x^{(e_i - e_1)} \right\} \\ &= x^{e_1} \left\{ \sum_{i=1}^{r} f_i y^{\frac{(e_i - e_1)}{l}} \right\} \\ &\quad (\text{where } \; y = x^l) \\ &= x^{e_1} f'(x) \end{aligned}$$

where $f'(x)$ is a polynomial of degree $\lfloor \frac{(d-e_1)}{l} \rfloor$ in y. This explains the count on the left. The inside summation in (19) above, does the same for the polynomials whose exponents are the $\{a_j\}$ with $a_1 = (e_1 - cl)$.

Since we are interested in counting the number of polynomials $\begin{bmatrix} f(x) \\ g(x) \end{bmatrix}$ where $f(x)$ is monic, we are interested in the quantity $\frac{u_C(1)}{(q-1)}$ which can be computed by substituting for y_C from (19) into (18) and then dividing by $(q-1)$.

Case B Count An analogous argument can be used to show that the corresponding expressions for $y_B(l)$, $u_B(1)$ in Case B are given by

$$\begin{aligned} y_B(l) &= \sum_{e_1=0}^{d} \left\{ q^{\lfloor \frac{d-e_1}{l} \rfloor + 1} - 1 \right\}^2 - (q-1)^2 \left(d+1 \right), \\ u_B(1) &= \sum_{l|T} y_B(l) \mu(l) \end{aligned} \quad (20)$$

in which the subtracted second term in the expression for $y_B(l)$ ensures that the instances when both $f(x)$ and $g(x)$ are monomials of the same degree are not counted.

Overall Count Putting together Cases B, C, D, we see that the analogous expressions for $y(l)$ and $u(1)$ for the desired overall count $u(1)$ are given by

$$\begin{aligned} y(l) &= \\ & 2 \sum_{e_1=0}^{d} \left\{ q^{\lfloor \frac{d-e_1}{l} \rfloor + 1} - 1 \right\} \sum_{c=1}^{\lfloor \frac{e_1}{l} \rfloor} \left\{ q^{\lfloor \frac{d-e_1+cl}{l} \rfloor + 1} - 1 \right\} \\ & + \sum_{e_1=0}^{d} \left\{ q^{\lfloor \frac{d-e_1}{l} \rfloor + 1} - 1 \right\}^2 - (q-1)^2 \left(d+1 \right), \quad (21) \\ u(1) &= \sum_{l|T} y(l) \mu(l). \quad (22) \end{aligned}$$

The overall count is computed by substituting for y from (21) into (22) and then dividing by $(q-1)$.

We next proceed to modify this count to ensure that $f(x)$ and $g(x)$ are co-prime.

Let us set

$$N(d,T) = \frac{u(d,T,1)}{(q-1)}$$

where we have written $u(d,T,1)$ in place of $u(1)$ to emphasize that u is a function of both d, T as well. In the ensuing, it will be found convenient to keep in mind that for any polynomial $h(x)$, the function $\begin{bmatrix} f(x)h(x) \\ g(x)h(x) \end{bmatrix}$ is sub-periodic iff the function $\begin{bmatrix} f(x) \\ g(x) \end{bmatrix}$ is sub-periodic. Let $h(x)$ be a fixed, monic polynomial over $\mathbb{F}_q$ of degree s and let $M(d,T,h(x))$ denote the number of polynomials satisfying

1) f and g are both non-zero and both of degree $\leq d$,
2) $f(x)$ is monic
3) $f(x) = h(x)f^{'}(x)$, $g(x) = h(x)g^{'}(x)$, for some $f^{'}(x)$, $g^{'}(x)$,
4) $(f^{'}(x), g^{'}(x))$ are not sub-periodic, i.e., that $\begin{bmatrix} f^{'}(x) \\ g^{'}(x) \end{bmatrix}$ does not satisfy (10) for any value of time shift parameter τ.

It is not hard to show that $M(d,T,h(x))$ is a function of the polynomial $h(x)$ only through its degree s and that moreover,

$$M(d,T,h(x)) = N(d-s,T).$$

Let us also define $M(d,T)$ to be the set of all polynomials $\begin{bmatrix} f(x) \\ g(x) \end{bmatrix}$ satisfying

1) f and g are both non-zero and both of degree $\leq d$,
2) $f(x)$ is monic
3) $(f(x), g(x))$ are not sub-periodic, i.e., that $\begin{bmatrix} f(x) \\ g(x) \end{bmatrix}$ does not satisfy (10) for any value of time shift parameter τ and in addition
4) $(f,g) = 1$.

Then we can show that $M(d,T)$ is given by

$$\begin{aligned} M(d,T) &= \sum_{h(x)} M(d,T,h(x)) \hat{\mu}(h(x)), \\ &= \sum_{h(x)} N(d - \text{deg}(h(x)), T) \hat{\mu}(h(x)), \end{aligned}$$

where the function $\hat{\mu}$ is as defined in (6) and where the sum is over all monic polynomials $h(x) \in \mathbb{F}_q[x]$ of degree $\leq d$. We can now define equivalence classes on the $M(d,T)$ functions that remain as before by defining the functions $\begin{bmatrix} f(x) \\ g(x) \end{bmatrix}$ and $\frac{1}{\mu_f} \begin{bmatrix} f(\beta^\tau x) \\ g(\beta^\tau x) \end{bmatrix}$ to be equivalent and choosing precisely one function from each equivalence class. Since there are no sub-period functions, there are precisely T elements in each equivalence class and thus the total number of code matrices is then finally given by

$$\frac{M(d,T)}{T} \quad (23)$$

and we have completed our count. This overall count is given in (15).

It is relatively easy to verify that the autocorrelation function is bounded above by $2d = \kappa$ for all nonzero time shifts and that the crosscorrelation function is uniformly bounded above by κ as well. The proof for asymptotic optimality for construction R2 is given in Appendix F.

VI. New Asymptotically Optimal Constructions based on Concatenation

Consider a $(\Lambda \times T,\ \omega,\ \kappa)$ 2-D OOC $\mathcal{C}$ under the requirement that there is at most one pulse per wavelength (AM-OPPW). We present two asymptotically optimal constructions that are, in a sense, concatenation of a constant-weight binary code and an OPPW code. We use this method to construct two new AM-OPPW codes by composing a constant weight binary code with code P1 (or R1).

Let $\mathcal{C}_{cw}$ be a constant weight binary $\{0,1\}$ code of maximum possible size having the following parameters: length$=\Lambda$, weight$=\omega$, and maximum inner product between any two codewords $\leq \kappa$. The size of $\mathcal{C}_{cw}$ is upper bounded by the one-dimensional Johnson Bound:

$$\mid \mathcal{C}_{cw} \mid \leq \left\lfloor \frac{\Lambda}{\omega} \left\lfloor \frac{\Lambda-1}{\omega-1} \left\lfloor \frac{\Lambda-2}{\omega-2} \cdots \left\lfloor \frac{\Lambda-\kappa}{\omega-\kappa} \right\rfloor \right\rfloor \right\rfloor \right\rfloor .$$

The idea is to construct a 2-D OOC whose code arrays are partitioned into $\mid \mathcal{C}_{cw} \mid$ subsets with each subset associated to a distinct codeword in $\mathcal{C}_{cw}$. Consider a codeword in $\mathcal{C}_{cw}$ where the 1's in this binary codeword, appear in the ω symbol locations $\lambda_1, \lambda_2, \cdots, \lambda_w$. We associate with this codeword, a maximal collection of 2-D code arrays with MCP κ which are such that only the wavelengths associated to rows $\lambda_1, \cdots, \lambda_w$ contain a pulse. No pulse is sent along any of the other wavelengths. For any of the $\mid \mathcal{C}_{cw} \mid$ choices of ω wavelengths, let us use a 2-D OOC $\mathcal{C}_{oppw}$ with exactly one pulse per wavelength.

It is easy to see that the composition of these two codes forms a 2-D OOC code with parameters $(\Lambda \times T, \omega, \kappa)$ of size $\mid \mathcal{C}_{cw} \mid \cdot \mid \mathcal{C}_{oppw} \mid$.

Since the new code is AM-OPPW, the autocorrelation is 0 by Remark 1.

For crosscorrelation, consider two codewords C_a and C_b from the new code. There are two possibilities: either both C_a and C_b have originated from the same codeword (of the constant weight binary code), or from different codewords. If C_a and C_b correspond to the same codeword in the constant weight binary code, then they have the same selection of rows and hence, their crosscorrelation is the same as that of the corresponding codewords from the 2-D OPPW code, which we know is $\leq \kappa$. If, on the other hand, C_a and C_b have originated from two different codewords in the constant weight binary code, then the maximum number of rows that can overlap in these two codewords is bounded above by κ, and each row can contribute a maximum of 1 collisions; hence, the crosscorrelation is bounded above by κ.

Remark 6: One might think of using a Steiner system instead of a constant weight binary code. The size of a $S(\kappa+1, \omega, \Lambda)$ Steiner system (which is the same as a $(\kappa+1)$-$(\Lambda, \omega, 1)$ t-design) is

$$\frac{\left(\begin{array}{c} \Lambda \\ \kappa+1 \end{array} \right)}{\left(\begin{array}{c} \omega \\ \kappa+1 \end{array} \right)}. \tag{24}$$

This reduces to

$$\frac{\Lambda}{\omega} \left(\frac{\Lambda-1}{\omega-1} \cdots \left(\frac{\Lambda-\kappa}{\omega-\kappa} \right) \right). \tag{25}$$

Note that every Steiner system is also a constant weight binary code and hence satisfies the Johnson Bound for 1-D codes with equality. However, Steiner systems do not exist for all possible values of κ, Λ, ω. Hence, using constant weight binary codes provides a more general construction.

A. Construction CP1: AM-OPPW, $\kappa < \omega \leq \Lambda,\ T$ is prime

For the case when T is prime and $\omega \leq T$, a code $\mathcal{C}_{oppw}$ of maximum-possible size T^κ can be constructed using construction P1. The overall size of the new 2-D OOC in this case is given by

$$\mid \mathcal{C}_{cw} \mid \ T^\kappa \ \leq \ T^\kappa \ \left\lfloor \frac{\Lambda}{\omega} \left\lfloor \frac{\Lambda-1}{\omega-1} \left\lfloor \frac{\Lambda-2}{\omega-2} \cdots \left\lfloor \frac{\Lambda-\kappa}{\omega-\kappa} \right\rfloor \right\rfloor \right\rfloor \right\rfloor .$$

Proposition 6: In the above construction, the resulting AM-OPPW 2-D OOC is asymptotically optimal, if the constant weight code is asymptotically optimal (in Johnson Bound).

For the proof, we refer the reader to Appendix G.

Example 2: In this example, we construct a $(7 \times 5, 3, 1)$ AM-OPPW 2-D OOC. We first need to choose a constant weight code of length 7, weight 3 and $\kappa = 1$. We know that the Singer construction [3], [63] for OOCs has the desired parameters and that its corresponding constant weight code is optimal and consists of the following codewords:

$$\{0,1,3\}, \{1,2,4\}, \{2,3,5\}, \{3,4,6\},$$
$$\{0,4,5\}, \{1,5,6\}, \{0,2,6\}$$

Using construction P1 for OPPW 2-D OOC, we construct a $(3 \times 5, 3, 1)$ OPPW 2-D OOC of size 5. Concatenating these two codes will result in a $(7 \times 5, 3, 1)$ AM-OPPW 2-D OOC of size 35, which is optimal by Proposition 3.

B. Construction CR1: AM-OPPW, $\omega \leq \Lambda,\ \kappa < \omega$ is even, $T = p^m + 1$

In a manner similar to the one described above, we compose the OPPW construction R1 with a constant weight binary code. The overall size of the new 2-D OOC is given by

$$\mid \mathcal{C} \mid \leq \left(\frac{c(\kappa')}{T} + 1 \right) \left\lfloor \frac{\Lambda}{\omega} \left\lfloor \frac{\Lambda-1}{\omega-1} \left\lfloor \frac{\Lambda-2}{\omega-2} \cdots \left\lfloor \frac{\Lambda-\kappa}{\omega-\kappa} \right\rfloor \right\rfloor \right\rfloor \right\rfloor .$$

Proposition 7: In the above construction, the resulting AM-OPPW 2-D OOC is asymptotically optimal, if the constant weight code is asymptotically optimal (in Johnson Bound).

Proof: Using equation (63) of Appendix E, we see that

$$\lim_{\Lambda, T \to \infty} |C| \geq T^\kappa, \tag{26}$$

which is the same as the number of codewords in construction P1. The rest of the proof follows from Appendix G.

■

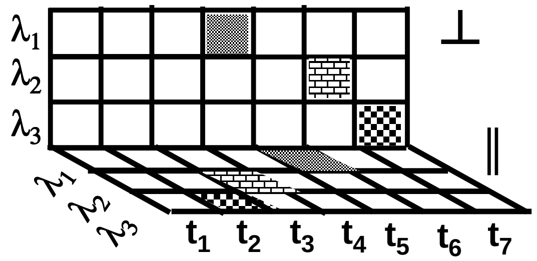

Fig. 3. Example of Polarization Rotation Invariant OOC

VII. Codes Exploiting Polarization

A third dimension that can be exploited to construct OOCs is the polarization dimension. Light propagates along two orthogonal polarization states. Under ideal conditions, these two polarization states will be perceived as being orthogonal at the receiver [64] despite polarization rotation.

If we can design codes with good correlation properties that are resilient to both timing and polarization ambiguity, we can use these codes, which we shall refer to as 3-D OOCs [62], [65], to spread the signal in time, wavelength and polarization.

A 3-D $(2\times\Lambda\times T,\omega,\kappa)$ OOC $\mathcal{C}$ is a family of $\{0,1\}$ $2\times\Lambda\times T$ arrays of constant weight ω. Every pair $\{A,B\}$ of arrays in $\mathcal{C}$ is required to satisfy:

$$\sum_{p=1}^{2}\sum_{\lambda=1}^{\Lambda}\sum_{t=0}^{T-1} A(p,\lambda,t)B((p\oplus_2\tau_1),\lambda,(t\oplus_T\tau_2)) \le \kappa \quad (27)$$

where either $A\neq B$, $\tau_1\neq 0$ or $\tau_2\neq 0$. All the bounds of Section III can be generalized to this class of OOCs.

Polarization Rotation Invariant Codes Construction: It is of course possible to construct a 3-D OOC by starting from a 1-D OOC and applying the Chinese Remainder Theorem (CRT) [66]. When the 3-D code is constructed from a 2-D code, however, then the transformation can be seen as a means of reducing the required chip rate.

Let $\mathcal{C}$ be a $(\Lambda\times(2T),\omega,\kappa)$ 2-D OOC where T is an odd integer. For every codeword in $\mathcal{C}$, apply the CRT mapping to each wavelength to spread that wavelength in time and polarization. The CRT mapping is a one-to-one mapping between a sequence and an array that preserves correlation values. It follows that by making use of the two orthogonal polarization states, we have in effect, reduced the needed chip rate by half.

Fig. 3 shows an example of a 3-D OOC with 3 wavelengths, 7 time slots, weight 6 and $\kappa=1$ constructed using the above construction.

VIII. Sequences for Phase-Encoded OCDMA

We now focus our attention to designing sequences for phase-encoded OCDMA.

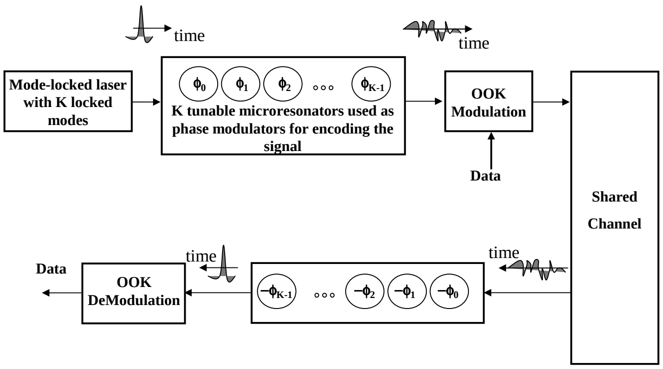
time
time
Mode-locked laser with K locked modes
ϕ_0 ϕ_1 ϕ_2 ∘∘∘ ϕ_{K-1}
K tunable microresonators used as phase modulators for encoding the signal
OOK Modulation
Data
Shared Channel
time
time
Data
OOK DeModulation
$-\phi_{K-1}$ ∘∘∘ $-\phi_2$ $-\phi_1$ $-\phi_0$

Fig. 4. Phase Encoding OCDMA system with Coherent Source.

The spectral encoding OCDMA system is harder to implement in comparison with direct-sequence OCDMA. That is perhaps the reason why most studies on spectral encoding systems have an implementation focus. There is not much literature on the subject of spreading sequence design with the exception of a few results on spectral amplitude encoding.

We first present a model of an asynchronous phase-encoded OCDMA system, and then identify a metric reflective of the amount of cross-correlation (other-user interference) in the system. Based on this model, we formulate the sequence design problem. As will be shown, this problem is closely related to the PAPR (peak to average power ratio) problem in OFDM [67]–[70]. Finally, in the next section, generalized bent functions [71] are used to construct efficient spreading sequences for an asynchronous system.

A. System Model

The system that we model in this section is a phase encoding OCDMA system with coherent laser source. A diagram of this system with a transmitter and receiver is shown in Fig. 4. The typical laser sources used for coherent transmission are mode locked lasers (MLL). The electrical field of a mode locked laser can be written as

$$E_{MLL}(t) = e^{i\omega_0 t}\sum_{k=0}^{K-1} e^{ik(\Delta\omega)t}\ . \quad (28)$$

In this equation, K is the number of modes in the mode locked laser, and $\Delta\omega$ is the channel spacing between two consecutive modes in the mode locked laser.

The output of the MLL is then passed through a phase encoder. In our model, the phase encoder applies different phase shifts to different modes of the MLL to spread it. Conventionally, the phase masks used in this approach consist of only $\{0,\pi\}$ phase shifts. Recently, Stapleton et al. [72], [73] showed that by using microdisk resonator technology, any phase can be applied to the different modes of the MLL. In light of this result, no restriction on the choice of phases is considered in this paper. The output of the phase encoder is of the form

$$E_{Enc}(t) = e^{i\omega_0 t}\sum_{k=0}^{K-1} e^{i(k(\Delta\omega)t+\phi_k)}\ , \quad (29)$$

where ϕ_k is the phase shift that the encoder applies to the k-th mode of the MLL. Upon OOK modulation with data bit d

$$E_{Tr}(t) = de^{i\omega_0 t} \sum_{k=0}^{K-1} e^{i(k(\Delta\omega)t+\phi_k)}, d \in \{0,1\} \ . \tag{30}$$

At the receiver, the phase decoder applies the inverse phase shift $-\phi_k$ to each mode k of the received signal

$$\begin{aligned} E_{Dec}(t) &= de^{i\omega_0 t} \sum_{k=0}^{K-1} e^{i(k(\Delta\omega)t+\phi_k-\phi_k)} \\ &= de^{i\omega_0 t} \sum_{k=0}^{K-1} e^{ik(\Delta\omega)t} \ , \end{aligned} \tag{31}$$

which is the original signal in (28) modulated by data bit d. After the phase decoder, a photo detector is used to detect the intensity of the received signal

$$|E_{Dec}(t)|^2 = \left| de^{i\omega_0 t} \sum_{k=0}^{K-1} e^{ik(\Delta\omega)t} \right|^2 = d \left| \sum_{k=0}^{K-1} e^{ik(\Delta\omega)t} \right|^2 \ . \tag{32}$$

If we sample this signal at time $t = 0$, then the received signal will be dK^2 and we can retrieve the transmitted data d using a threshold detector [74], [75].

Remark 7: In this model, no noise source is considered. This is because we wish to focus on the effect of multiple access interference (MAI).

When there is more than one user transmitting data, the receiver receives the superposition of the signals. Assume that users m and n are transmitting data simultaneously and asynchronously. Each user uses its own phase encoder $\Phi^{(\ell)} = \{\phi_0^\ell, \phi_1^\ell, \cdots, \phi_{K-1}^\ell\}$ where $\ell \in \{m, n\}$. Let the time difference between user m and n be denoted by τ ($\tau = 0$ in a synchronous system). The received signal is given by

$$\begin{aligned} E_{Tr}^{(m)}(t) + E_{Tr}^{(n)}(t+\tau) &= d^{(m)} e^{i\omega_0 t} \sum_{k=0}^{K-1} e^{i(k(\Delta\omega)t+\phi_k^{(m)})} + \\ & d^{(n)} e^{i\omega_0 (t+\tau)} \sum_{k=0}^{K-1} e^{i(k(\Delta\omega)(t+\tau)+\phi_k^{(n)})} \ . \end{aligned}$$

The signal at the output of the phase decoder tuned to user m takes on the form

$$\begin{aligned} & d^{(m)} e^{i\omega_0 t} \sum_{k=0}^{K-1} e^{i(k(\Delta\omega)t)} \ + \\ & \quad d^{(n)} e^{i\omega_0 (t+\tau)} \sum_{k=0}^{K-1} e^{i(k(\Delta\omega)(t+\tau)+(\phi_k^{(n)}-\phi_k^{(m)}))} \ . \end{aligned}$$

The output of the photo detector of this receiver will be the square of the magnitude of the above expression. As can be seen, there is multiple access interference (MAI) at the receiver output. Each transmitter-receiver pair is assumed to operate synchronously, and consequently, the receiver samples its output at time $t = 0$ to get

$$\begin{aligned} A &= \left| d^{(m)}K + d^{(n)} e^{i\omega_0 \tau} \sum_{k=0}^{K-1} e^{i(k(\Delta\omega)\tau+(\phi_k^{(n)}-\phi_k^{(m)}))} \right|^2 \\ &= d^{(m)}K^2 + d^{(n)} \left| \sum_{k=0}^{K-1} e^{i(k(\Delta\omega)\tau+(\phi_k^{(n)}-\phi_k^{(m)}))} \right|^2 + \\ & 2d^{(m)}d^{(n)}K\mathfrak{Re}\left(e^{-i\omega_0 \tau} \sum_{k=0}^{K-1} e^{-i(k(\Delta\omega)\tau+(\phi_k^{(n)}-\phi_k^{(m)}))} \right) \ . \end{aligned} \tag{33}$$

When $d^{(n)} = 0$, there is no interference and we are back to the single-user case. Hence, we assume $d^{(n)} = 1$ from now.

Remark 8: In the synchronous $\tau = 0$ case, if $\Phi^{(m)}$ and $\Phi^{(n)}$ are Walsh-Hadamard sequences, (i.e., each $\{\exp(i\phi_k^{(\ell)})\}$ is a sequence in a Walsh-Hadamard sequence family), the two summations in (33) become zero, and there is no interference. This is of course clearly not the case when $\tau \neq 0$ (see Example 3 and Fig. 5).

Setting

$$\Theta_{nm}(\tau) = \sum_{k=0}^{K-1} e^{-i[k(\Delta\omega)\tau+(\phi_k^{(n)}-\phi_k^{(m)})]} \ , \tag{34}$$

and noting that

$$| \ \mathfrak{Re}\left(e^{-i\omega_0\tau}\Theta_{nm}(\tau)\right) | \leq |\Theta_{nm}(\tau)| \ , \tag{35}$$

we obtain

$$\begin{aligned} & d^{(m)}K^2 + |\Theta_{nm}(\tau)|^2 - 2d^{(m)}K\,|\Theta_{nm}(\tau)| \leq A \\ & \leq d^{(m)}K^2 + |\Theta_{nm}(\tau)|^2 + 2d^{(m)}K\,|\Theta_{nm}(\tau)| \ . \end{aligned} \tag{36}$$

It follows that minimization of $|\Theta_{nm}(\tau)|$ for all τ is a reasonable criterion for signal design.

Remark 9: The above generalizes in a straightforward fashion to the case of more than 2 users.

B. Connection with PAPR problem

Our objective is thus the design of sequences of length K such that:

$$\max_{\tau\in[0,\frac{2\pi}{\Delta\omega})} \left| \sum_{k=0}^{K-1} e^{-i[k(\Delta\omega)\tau+(\phi_k^{(n)}-\phi_k^{(m)})]} \right| \tag{37}$$

is minimized for every sequence pair $\{\phi_k^{(n)}\}, \{\phi_k^{(m)}\}$. Equivalently, we seek to minimize

$$\max_{\tau\in[0,1)} \left| \sum_{k=0}^{K-1} e^{-ik2\pi\tau} e^{-i(\phi_k^{(n)}-\phi_k^{(m)})]} \right| \ . \tag{38}$$

The design of sequences with minimum PAPR (peak to average power ratio) crops up in conjunction with signal design for OFDM systems [67]–[70], [76]. Since designing for low PAPR is hard, the common design approach is to design for low PMEPR (peak-to-mean envelope power ratio), which is more tractable. The PMEPR problem (see [70]) is one of designing sequences $\{a_k\}$ that minimize :

$$\max_{\tau\in[0,1)} \left| \frac{1}{K} \sum_{k=0}^{K-1} a_k e^{-ik2\pi\tau} \right|^2 \ . \tag{39}$$

As can be seen, in our problem, we are interested in phase sequences $\Phi^{(m)}$ and $\Phi^{(n)}$ such that $\exp(-i(\Phi^{(n)} - \Phi^{(m)}))$ is a sequence with good PMEPR.

The results in [70] as applied to the present situation are stated below. Let

$$M_d^{(K)} = \max_{j=0,\cdots,K-1} \left| \sum_{k=0}^{K-1} e^{-ik2\pi\left(\frac{j}{K}\right)} e^{-i(\phi_k^{(n)} - \phi_k^{(m)})]} \right| \quad (40)$$

and

$$M_c^{(K)} = \max_{\tau\in[0,1)} \left| \sum_{k=0}^{K-1} e^{-ik2\pi\tau} e^{-i(\phi_k^{(n)} - \phi_k^{(m)})]} \right| . \quad (41)$$

From [70], we know

Theorem 8: $M_d^{(K)} \geq \sqrt{K}$.

Theorem 9: For $K > 3$:

$$\begin{aligned} \frac{2}{\pi}\ln K + 0.603 - \frac{1}{6K} &< \max_{F_K(t)} \left\{ \frac{M_c(F_K)}{M_d(F_K)} \right\} \\ &< \frac{2}{\pi}\ln K + 1.132 + \frac{3}{K} \end{aligned} \quad (42)$$

in which

$$F_K(t) = \sum_{k=0}^{K-1} a_k e^{2\pi ikt} \quad \text{such that} \quad \sum_{k=0}^{K-1} |a_k|^2 = K \quad (43)$$

and

$$\begin{aligned} M_d(F_K) &= \max_{j=0,\ldots,K-1} \left| F_K\left(\frac{j}{K}\right) \right| , \\ M_c(F_K) &= \max_{t\in[0,1)} |F_K(t)| . \end{aligned}$$

The implication of Theorem 9 is that, if we design sequences with good asynchronous properties for all the $\frac{j}{K}$ samples of τ, it is guaranteed that the same sequence has good asynchronous properties for all values of τ.

IX. Sequence Constructions based on Bent Functions

In this section we use generalized bent functions to design sequences with good asynchronous properties. Some preliminaries on generalized bent functions that we will use are introduced in the first subsection.

A. Generalized Bent Functions

Definition 1: [71] Let $\mathbb{Z}_q^m$ denote the set of m-tuples with elements drawn from the set of integers modulo q, $w = e^{i\left(\frac{2\pi}{q}\right)}$ and g a complex-valued function defined on $\mathbb{Z}_q^m$. The Fourier transform of g is then defined to be the function G given by:

$$G(\lambda) = \frac{1}{\sqrt{q^m}} \sum_{x\in\mathbb{Z}_q^m} g(x) w^{-\lambda^T x}, \quad \lambda \in \mathbb{Z}_q^m . \quad (44)$$

Definition 2: [71] A function f, $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ is said to be bent if all the Fourier transform coefficients of w^f have unit magnitude.

Theorem 10: [71] Every affine or linear translate of a bent function is also bent.

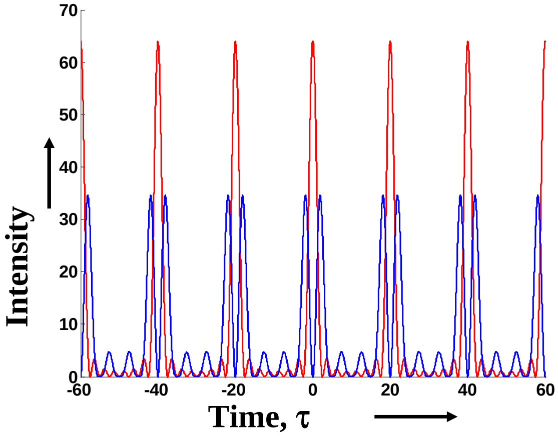

Fig. 5. An Example of Walsh-Hadamard Sequences with $K = 8$.

Theorem 11: [71] Let q be odd. Then the function f over $\mathbb{Z}_q$ defined by:

$$f(k) = k^2 + ck \quad \text{all} \quad k \in \mathbb{Z}_q . \quad (45)$$

is bent for all $c \in \mathbb{Z}_q$.

B. New Construction 1

Proposition 12: Let

$$\Phi = \left\{ \Phi^{(\ell)} \mid \Phi^{(\ell)} = \{\phi_0^\ell, \phi_1^\ell, \cdots, \phi_{K-1}^\ell\}, \ell \in \{1, 2, \cdots, L\} \right\}$$

be a family of phase sequences such that the difference sequence is associated to a bent function, i.e.,

$$\Phi^{(n)} - \Phi^{(m)} = \frac{2\pi}{K}(f(0), f(1), \cdots, f(K-1)), n \neq m$$

where $f(x)$ is a bent function over $\mathbb{Z}_K$. Then $\max|\Theta_{nm}(\tau)|$ is as small as it can possibly be over multiples τ of $\frac{2\pi}{K(\Delta\omega)}$, and thus these phase sequences are suitable for use in asynchronous phase-encoded OCDMA systems.

For the proof, we refer the reader to Appendix H

Proposition 13: The following phase sequences have the minimum possible value of $\max|\Theta_{nm}(\tau)|$ property to be used for asynchronous phase encoding OCDMA systems with K modes, where K is an odd prime:

$$\begin{gathered} \phi_k^{(m)} = (k^3 + a_m k^2 + b_m k + c_m)\frac{2\pi}{K}, \\ a_m, b_m, c_m \in \mathbb{Z}_K;\ m \neq n : a_m \neq a_n;\ K \text{ a prime} > 2. \end{gathered}$$

For the proof, we refer the reader to Appendix I

Example 3: Fig. 5 shows the application of Walsh-Hadamard sequences for asynchronous systems. In this graph, $K = 8$, $\omega_0 = \frac{\pi}{4}$, $\Delta\omega = \frac{\pi}{10}$, $\Phi^{(m)} = (0, 0, 0, 0, 0, 0, 0, 0)$ and $\Phi^{(n)} = (\pi, \pi, \pi, \pi, 0, 0, 0, 0)$. In this figure, the output of the MLL as it is seen after the photo detector is denoted by the graph that has a maxima above 60 (this curve is lighter in the print and is red colored in the soft copy). The other curve with a maxima just above 30 (which is darker in print and is blue colored in the soft copy) shows $|\Theta_{nm}(\tau)|^2$ at the output. As can be seen, the system has no interference for $\tau = 0$ (synchronous case). However, even for small deviations from

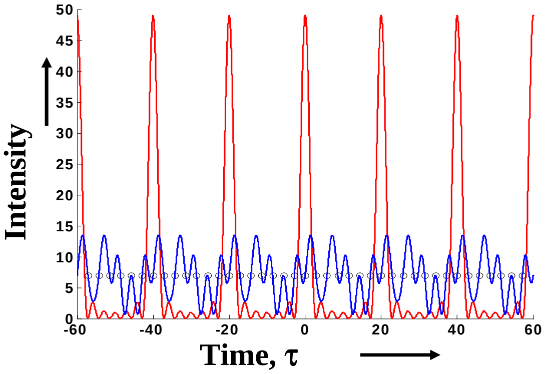

Fig. 6. An Example of application of Proposition 12 with $K = 7$.

$\tau = 0$, $|\Theta_{nm}(\tau)|^2$ increases significantly. Because of the high peak of $|\Theta_{nm}(\tau)|^2$, these phase sequence are not suitable for asynchronous transmission.

Example 4: Fig. 6 shows the application of the construction of Proposition 13, where $K = 7$, $\omega_0 = \frac{\pi}{4}$, $\Delta\omega = \frac{\pi}{10}$, $(a_m, b_m, c_m) = (2, 5, 3)$ and $(a_n, b_n, c_n) = (5, 4, 1)$. For this system $\Phi^{(m)} = (\frac{6\pi}{7}, \frac{8\pi}{7}, \frac{2\pi}{7}, 0, 0, 0, \frac{12\pi}{7})$ and $\Phi^{(n)} = (\frac{2\pi}{7}, \frac{8\pi}{7}, \frac{4\pi}{7}, \frac{2\pi}{7}, 0, \frac{10\pi}{7}, \frac{2\pi}{7})$. In this figure, the output of the MLL as seen after the photo detector is denoted by the curve that has its maxima around 50 (lighter curve in print, which is colored red in the soft copy). The other curve with maxima around 15 (darker curve in print, which is colored blue in the soft copy) shows $|\Theta_{nm}(\tau)|^2$ at the output. Here, the circles are samples of $|\Theta_{nm}(\tau)|^2$ for $\tau = \frac{2\pi j}{K(\Delta\omega)}$. As can be seen, all these values are equal to 7. It can be observed that $|\Theta_{nm}(\tau)|^2$ is low for all values of τ and the phase sequences are thus applicable for asynchronous transmission.

C. New Construction 2

The second construction is based on the following family of bent functions.

Theorem 14: [77] Let q be an integer which is neither the product of distinct primes nor equal to 2 modulo 4. Then the function $f(\cdot)$ over $\mathbb{Z}_q$, defined by

$$f(k+1) = f(k) + a_k, \quad \forall k,\ a_k \in \mathbb{Z}_q,\ f(0) \in \mathbb{Z}_q \tag{46}$$

is bent if the integers a_k satisfy the dual conditions:

$$\sum_{k=0}^{K-1} a_k = 0 \pmod{s}, \tag{47}$$

$$a_{k+ns} = a_k + c_1 ns \pmod{q}, \quad \forall k \in \mathbb{Z}_s, \forall n \in \mathbb{Z}_{q/s}, \tag{48}$$

where c_1 is any integer relatively prime to q and s is any integer greater than one that has the same parity as q and whose square divides q.

Let $g(k)$ be a second bent function over $\mathbb{Z}_q$ such that

$$g(k+1) = g(k) + b_k, \quad \forall k,\ b_k \in \mathbb{Z}_q, g(0) \in \mathbb{Z}_q \tag{49}$$

and

$$\sum_{k=0}^{K-1} b_k = 0 \pmod{s}, \tag{50}$$

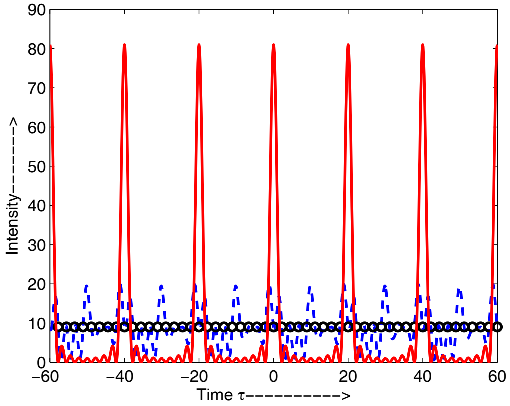

Fig. 7. An Example of Application of Proposition 15 with $q = 9$.

$$b_{k+ns} = b_k + c_2 ns \pmod{q}, \quad \forall k \in \mathbb{Z}_s, \forall n \in \mathbb{Z}_{q/s}, \tag{51}$$

where c_2 is any integer relatively prime to q.

Proposition 15: Let $h(k) = f(k) - g(k)$ be a function over $\mathbb{Z}_q$. Then $h(k)$ is a bent function in $\mathbb{Z}_q$ if $c_1 - c_2$ is relatively prime to q.

For the proof, we refer the reader to Appendix J.

Corollary 16: Let $q = \Pi_{j=1}^{n} {p_j}^{r_j}$ such that $p_{min} = \min\{p_j\}_{j=1}^{n}$, where p_j is a prime number. Then the maximum size is $p_{min} - 1$.

Proof: Suppose maximum size $\geq p_{min}$. Then c_i and c_j will exist such that

$$c_i = c_j \pmod{p_{min}}.$$

Hence, we can say that p_{min} divides $c_i - c_j$. Hence, $c_i - c_j$ is not relatively prime to q, which is a contradiction. ■

Corollary 17: Let $q = p^r$, where p is a prime and $r \geq 2$. Then the maximum size is $p - 1$.

Proof: Follows from above. ■

Example 5: Fig. 7 shows the application of the construction of Proposition 15, where $p = 3$, $r = 2$, $s = 2$, $q = p^r = 9$, $\omega_0 = \frac{\pi}{4}$, $\Delta\omega = \frac{\pi}{10}$, $(a_0, a_1, a_2) = (1, 3, 5)$ and $(b_0, b_1, b_2) = (3, 5, 7)$. For this system, $f(0) = 1$ and $g(0) = 1$. In this figure, the output of the MLL as it is seen after the photo detector is denoted by the graph that has its maxima around 80 (continuous curve, which is colored red in the soft copy). The dotted curve with its maxima around 20 (colored blue in the soft copy) shows $|\Theta_{nm}(\tau)|^2$ at the output. Here, the small circles around 10 are the samples of $|\Theta_{nm}(\tau)|^2$ for $\tau = \frac{2\pi j}{q(\Delta\omega)}$. As can be seen, all these values are equal to 9. It can be observed that $|\Theta_{nm}(\tau)|^2$ is low for all values of τ and hence these phase sequences are good for asynchronous transmission.

X. Conclusion

In this paper, we presented 9 families of 2-D OOCs. One of these families is optimal and the rest are asymptotically optimal with respected to the Johnson bound or with respect to the new bounds proposed in this paper. A novelty of our constructions is the large size. This was achieved by constructing optimal families for large values of the MCP since the optimal family size increases exponentially in the MCP.

Appendix A
Nonbinary Johnson Bound

(Proof of Proposition 2)

The proof is along the lines of the proof of the Johnson bound in the case of binary codes.

Assume a constant weight $(\Lambda, \omega, \kappa)$ code $\mathcal{C}$ of size $A_T(\Lambda, \omega, \kappa)$. If we arrange all the codewords along the rows of a matrix, the total weight of the matrix is $\omega A_T(\Lambda, \omega, \kappa)$, and thus each non-zero symbol is repeated on an average $\frac{\omega A_T(\Lambda,\omega,\kappa)}{T}$ times. Thus, there is a symbol α which occurs at least $\frac{\omega A_T(\Lambda,\omega,\kappa)}{T}$ times, and this symbol is repeated on an average $\frac{\omega A_T(\Lambda,\omega,\kappa)}{\Lambda T}$ times in each column. It follows that there exists a column c with at least $\frac{\omega A_T(\Lambda,\omega,\kappa)}{\Lambda T}$ occurrences of the symbol α. However, the number of occurrences of α in column c cannot exceed $A_T(\Lambda-1, \omega-1, \kappa-1)$. This is because if we select all the rows containing α in column c, and then delete this column c from all these rows, we will obtain a constant-weight code of length $\Lambda - 1$ and weight $\omega - 1$ with Hamming correlation $\leq \kappa - 1$.

It must therefore be that:

$$\frac{\omega A_T(\Lambda, \omega, \kappa)}{\Lambda T} \leq A_T(\Lambda-1, \omega-1, \kappa-1)$$

$$\Rightarrow A_T(\Lambda, \omega, \kappa) \leq \left\lfloor \frac{\Lambda T}{\omega} A_T(\Lambda-1, \omega-1, \kappa-1) \right\rfloor . \tag{52}$$

By repeating this procedure recursively κ times, we arrive at:

$$A_T(\Lambda, \omega, \kappa) \leq \tag{53}$$

$$\left\lfloor \frac{T\Lambda}{\omega} \left\lfloor \frac{T(\Lambda-1)}{\omega-1} \cdots \left\lfloor \frac{T(\Lambda-\kappa+1)}{\omega-\kappa+1} A_T(\Lambda-\kappa, \omega-\kappa, 0) \right\rfloor \right\rfloor \right\rfloor .$$

The proof is then completed by noting that

$$A_T(\Lambda-\kappa, \omega-\kappa, 0) \leq \left\lfloor \frac{(\Lambda-\kappa)T}{\omega-\kappa} \right\rfloor . \tag{54}$$

To see this, let us arrange all the codewords of a $(\Lambda - \kappa, \omega - \kappa, 0)$ constant weight code $\mathcal{C}$ along the rows of a matrix. To satisfy the constraint of zero Hamming correlation, each alphabet can occur only once in each column. Thus, there are at most T non-zero entries in each column. Since there are $\Lambda - \kappa$ different columns, the entire matrix can have at most $(\Lambda - \kappa)T$ non-zero entries. On the other hand, each row has exactly $\omega - \kappa$ non-zero entries, so that there are at most $\left\lfloor \frac{(\Lambda-\kappa)T}{\omega-\kappa} \right\rfloor$ rows in the matrix and the assertion is proved.

Appendix B
Bound on AM-OPPW Code Size

(Proof of Proposition 3)

Let $\mathcal{C}$ be an AM-OPPW 2-D OOC of size $\Phi(\Lambda \times T, \omega, \kappa)$. Create a code $\mathcal{C}'$ that consists of all T columnar cyclic shifts of each code in $\mathcal{C}$. This code is of size $\Phi'(\Lambda \times T, \omega, \kappa) = T\Phi(\Lambda \times T, \omega, \kappa)$.

By identifying each row of a code matrix in $\mathcal{C}'$ having a 1 in the t-th column with the symbol t belonging to $\{1, 2, \ldots, T\}$, and a blank row with the symbol 0, we obtain from the 2-D OOC, a 1-D constant weight code over the alphabet $\mathbb{Z}_{T+1}$. This 1-D constant weight code has parameters $(\Lambda, \omega, \kappa)$ and is of size $\Phi'(\Lambda \times T, \omega, \kappa)$ over an alphabet of size $T + 1$.

It follows from our bound above in Proposition 2 that

$$\Phi'(\Lambda \times T, \omega, \kappa) \leq \left\lfloor \frac{T\Lambda}{\omega} \left\lfloor \frac{T(\Lambda-1)}{\omega-1} \cdots \left\lfloor \frac{T(\Lambda-\kappa)}{\omega-\kappa} \right\rfloor \right\rfloor \right\rfloor$$

$$\Rightarrow \Phi(\Lambda \times T, \omega, \kappa) \leq \left\lfloor \frac{1}{T} \left\lfloor \frac{T\Lambda}{\omega} \left\lfloor \frac{T(\Lambda-1)}{\omega-1} \cdots \left\lfloor \frac{T(\Lambda-\kappa)}{\omega-\kappa} \right\rfloor \right\rfloor \right\rfloor \right\rfloor$$

$$\leq \left\lfloor \frac{\Lambda}{\omega} \left\lfloor \frac{T(\Lambda-1)}{\omega-1} \cdots \left\lfloor \frac{T(\Lambda-\kappa)}{\omega-\kappa} \right\rfloor \right\rfloor \right\rfloor .$$

Appendix C
Asymptotic Optimality of Construction P2

The number of codewords in this code are

$$\frac{1}{T} \sum_{d|(\Lambda-1)} \left(\Lambda^{\lceil \frac{\kappa+1}{d} \rceil} - 1 \right) \mu(d).$$

Consider the largest term in the summation - this corresponds to $d = 1$ and evaluates to

$$\frac{\Lambda^{\kappa+1} - 1}{T}.$$

Hence, the total number of codewords $|C|$ is given by

$$|C| = \frac{\Lambda^{\kappa+1} - 1}{T} + \frac{1}{T} \sum_{d|(\Lambda-1),\ d>1} \left(\Lambda^{\lceil \frac{\kappa+1}{d} \rceil} - 1 \right) \mu(d).$$

For Λ and T tending to infinity, we get

$$\lim_{\Lambda, T \to \infty} |C| \geq \frac{\Lambda^{\kappa+1}}{T}. \tag{55}$$

Since $\omega = T$ for this construction, the two-dimensional Johnson bound given by Theorem 1 specializes to

$$\begin{aligned} \Phi(\Lambda \times T, \omega, \kappa) \quad &\leq \quad \left\lfloor \frac{\Lambda}{T} \left\lfloor \frac{\Lambda T - 1}{T - 1} \cdots \left\lfloor \frac{\Lambda T - \kappa}{T - \kappa} \right\rfloor \right\rfloor \right\rfloor \\ &\leq \quad \frac{\Lambda}{T} \left(\frac{\Lambda T - 1}{T - 1} \cdots \left(\frac{\Lambda T - \kappa}{T - \kappa} \right) \right). \end{aligned}$$

For Λ and T tending to infinity, we get

$$\begin{aligned} \lim_{\Lambda, T \to \infty} \Phi(\Lambda \times T, \omega, \kappa) \quad &\leq \quad \frac{\Lambda}{T} \left(\frac{\Lambda T}{T} \cdots \left(\frac{\Lambda T}{T} \right) \right) \\ &= \quad \frac{\Lambda^{\kappa+1}}{T}. \end{aligned} \tag{56}$$

From (55) and (56), we can see that construction P2 is asymptotically optimal. The proof for asymptotic optimality of constructions P4 and P5 is along similar lines, since the expression for the total number of codewords is similar.

Appendix D
Asymptotic Optimality of construction P3

The number of codewords $|C|$ in this code are

$$\begin{aligned}|C| &= \frac{(T+1)^{\kappa+1}-1}{T}\\ &\geq \frac{T^{\kappa+1}-1}{T}.\end{aligned}$$

When Λ and T tend to infinity, we get

$$\begin{aligned}\lim_{\Lambda,T\to\infty}|C| &\geq \frac{T^{\kappa+1}}{T}\\ &= T^{\kappa}. \end{aligned}\tag{57}$$

Since this construction is AM-OPPW, we use the bound given by Proposition 3 to get

$$\begin{aligned}\Phi(\Lambda\times T,\omega,\kappa) &\leq \left\lfloor\frac{\Lambda}{\omega}\left\lfloor\frac{T(\Lambda-1)}{\omega-1}\cdots\left\lfloor\frac{T(\Lambda-\kappa)}{\omega-\kappa}\right\rfloor\right\rfloor\right\rfloor\\ &\leq \frac{\Lambda}{\omega}\left(\frac{T(\Lambda-1)}{\omega-1}\cdots\left(\frac{T(\Lambda-\kappa)}{\omega-\kappa}\right)\right)\\ &= \frac{\Lambda}{\Lambda-\kappa}\left(\frac{T(\Lambda-1)}{\Lambda-\kappa-1}\cdots\left(\frac{T(\Lambda-\kappa)}{\Lambda-\kappa-\kappa}\right)\right)\end{aligned}$$

since $\omega=\Lambda-\kappa$. When Λ and T tend to infinity, we get

$$\begin{aligned}\lim_{\Lambda,T\to\infty}\Phi(\Lambda\times T,\omega,\kappa) &\leq \frac{\Lambda}{\Lambda}\left(\frac{T\Lambda}{\Lambda}\cdots\left(\frac{T\Lambda}{\Lambda}\right)\right)\\ &= T^{\kappa}.\end{aligned}\tag{58}$$

Comparing (57) and (58), we can see that this construction is asymptotically optimal.

Appendix E
Asymptotic Optimality of construction R1

The number of codewords $|C|$ in this code is

$$|C| = \frac{c(\kappa')}{T}+1,$$

where

$$c(\kappa')=\begin{cases} q^{2\kappa'+1}-q, & \kappa'=1,2,3,4,5,6\\ \geq q^{2\kappa'+1}-\frac{q^{2\kappa'-6}}{7}, & \kappa'\geq 7.\end{cases}$$

We consider the two cases separately: $\kappa'\leq 6$ and $\kappa'\geq 7$. For $\kappa'\leq 6$, we have

$$\begin{aligned}|C| &= \frac{c(\kappa')}{T}+1\\ &\geq \frac{c(\kappa')}{T}\\ &= \frac{q^{2\kappa'+1}-q}{T}\\ &= \frac{(T-1)^{2\kappa'+1}-T+1}{T}.\end{aligned}\tag{59}$$

In the limit Λ, T tending to infinity, we get

$$\begin{aligned}\lim_{\Lambda,T\to\infty}|C| &\geq T^{2\kappa'}\\ &= T^{\kappa}.\end{aligned}\tag{60}$$

For $\kappa'\geq 7$, we have

$$\begin{aligned}|C| &= \frac{c(\kappa')}{T}+1\\ &\geq \frac{c(\kappa')}{T}\\ &\geq \frac{q^{2\kappa'+1}-\frac{q^{2\kappa'-6}}{7}}{T}\\ &= \frac{(T-1)^{2\kappa'+1}-\frac{(T-1)^{2\kappa'-6}}{7}}{T}.\end{aligned}\tag{61}$$

In the limit Λ, T tending to infinity, we get

$$\begin{aligned}\lim_{\Lambda,T\to\infty}|C| &\geq T^{2\kappa'}\\ &= T^{\kappa}.\end{aligned}\tag{62}$$

We can see that (60) and (62) are the same. Hence,

$$\lim_{\Lambda,T\to\infty}|C|\geq T^{\kappa}\tag{63}$$

for all values of κ', i.e., for all even values of κ.

The two-dimensional Johnson bound given by Theorem 1 is

$$\begin{aligned}\Phi(\Lambda\times T,\omega,\kappa) &\leq \left\lfloor\frac{\Lambda}{\omega}\left\lfloor\frac{\Lambda T-1}{\omega-1}\cdots\left\lfloor\frac{\Lambda T-\kappa}{\omega-\kappa}\right\rfloor\right\rfloor\right\rfloor\\ &\leq \frac{\Lambda}{\omega}\left(\frac{\Lambda T-1}{\omega-1}\cdots\left(\frac{\Lambda T-\kappa}{\omega-\kappa}\right)\right)\\ &= \frac{\Lambda}{\Lambda}\left(\frac{\Lambda T-1}{\Lambda-1}\cdots\left(\frac{\Lambda T-\kappa}{\Lambda-\kappa}\right)\right)\end{aligned}$$

since $\omega=\Lambda$ for this construction. In the limit Λ, T tending to infinity, we get

$$\lim_{\Lambda,T\to\infty}\Phi(\Lambda\times T,\omega,\kappa)\leq T^{\kappa}.\tag{64}$$

By comparing (63) and (64), we can see that this construction is asymptotically optimal.

Appendix F
Asymptotic Optimality of construction R2

The number of codewords $|C|$ in this code is

$$\begin{aligned}|C| &= \frac{M(d,T)}{T}\\ &= \frac{1}{T}\sum_{h(x)}\hat{\mu}(h(x))N(d-deg(h(x)),T).\end{aligned}$$

Note that $N(\cdot)$ is an increasing function in its first argument, which gets maximized when the degree of $h(x)$ is 0. Moreover, for $h(x)=1$, $\hat{\mu}(h(x))$ achieves its maximum value of 1. Since the summation above is greater than the largest term of the summation (which corresponds to $h(x)=1$), we conclude that

$$|C| \geq \frac{1}{T}N(d,T).$$

Since we are interested in proving the asymptotic optimality, it is sufficient to work with the highest order term. Substituting the value of $N(\cdot)$, the above sum simplifies to

$$|C| \geq \frac{u(1)}{T(q-1)}.$$

From the definition of $u(1)$ in (22), we notice that its maximum term corresponds to $l=1$. This is so because $y(\cdot)$ decreases exponentially with l. Moreover, $\mu(l)$ attains its maximum value of 1 for $l=1$. Substituting the value of (the largest term in the summation of) $u(1)$ from (22) into the above summation, we get

$$|C| \geq \frac{y(1)}{T(q-1)}. \qquad (65)$$

We now compute an approximation for $y(1)$ and then substitute it back in the above inequality. We do this by substituting $l=1$ in (22) to get the following approximation for $y(1)$

$$2\sum_{e_1=0}^{d}\left\{q^{d-e_1+1}-1\right\}\sum_{c=1}^{e_1}\left\{q^{d-e_1+c+1}-1\right\}+\sum_{e_1=0}^{d}\left\{q^{d-e_1+1}-1\right\}^2.$$

Each summation in this expression is a geometric progression. Summing the series and approximating (by neglecting the lower-order terms in the summation), we get

$$2q^{d+1}q^{d+1}+q^{2d+2}.$$

Substituting this value of $y(1)$ into (65), we get

$$\begin{aligned}|C| &\geq \frac{3q^{2d+2}}{T(q-1)}\\ &= \frac{3(\Lambda-1)^{\kappa+2}}{T\Lambda}\\ &\geq \frac{\Lambda^{\kappa+1}}{T}. \end{aligned} \qquad (66)$$

Comparing this with (56), we see that construction R2 is asymptotically optimal.

Appendix G
Asymptotic Optimality of Construction CP1

(Proof of Proposition 6)

$$\left\lfloor\frac{\Lambda}{\omega}\left\lfloor\frac{\Lambda-1}{\omega-1}\left\lfloor\frac{\Lambda-2}{\omega-2}\cdots\left\lfloor\frac{\Lambda-\kappa}{\omega-\kappa}\right\rfloor\right\rfloor\right\rfloor\right\rfloor \geq$$
$$\left(\frac{\Lambda}{\omega}\left(\frac{\Lambda-1}{\omega-1}\left(\frac{\Lambda-2}{\omega-2}\cdots\left(\frac{\Lambda-\kappa}{\omega-\kappa}-1\right)\cdots-1\right)-1\right)-1\right)$$
$$\Rightarrow \lim_{\Lambda\to\infty}\left\lfloor\frac{\Lambda}{\omega}\left\lfloor\frac{\Lambda-1}{\omega-1}\left\lfloor\frac{\Lambda-2}{\omega-2}\cdots\left\lfloor\frac{\Lambda-\kappa}{\omega-\kappa}\right\rfloor\right\rfloor\right\rfloor\right\rfloor \geq$$
$$\frac{\Lambda^{\kappa+1}}{\omega(\omega-1)\cdots(\omega-\kappa)}$$
$$\Rightarrow \lim_{\Lambda\to\infty} \mid \mathcal{C}_{cw} \mid T^{\kappa} \geq \frac{T^{\kappa}\Lambda^{\kappa+1}}{\omega(\omega-1)\cdots(\omega-\kappa)}.$$

On the other hand, from the bound in Proposition 3:

$$\Phi(\Lambda\times T,\omega,\kappa) \leq \left\lfloor\frac{\Lambda}{\omega}\left\lfloor\frac{T(\Lambda-1)}{\omega-1}\cdots\left\lfloor\frac{T(\Lambda-\kappa)}{\omega-\kappa}\right\rfloor\right\rfloor\right\rfloor \leq$$
$$\frac{\Lambda}{\omega}\frac{T(\Lambda-1)}{\omega-1}\cdots\frac{T(\Lambda-\kappa)}{\omega-\kappa} \leq \frac{T^{\kappa}\Lambda(\Lambda-1)\cdots(\Lambda-\kappa)}{\omega(\omega-1)\cdots(\omega-\kappa)}$$
$$\Rightarrow \lim_{\Lambda\to\infty}\Phi(\Lambda\times T,\omega,\kappa) \leq \frac{T^{\kappa}\Lambda^{\kappa+1}}{\omega(\omega-1)\cdots(\omega-\kappa)}\ ,$$

which establishes what we need to prove.

Appendix H
Proof of Proposition 12

$$\left|\Theta_{nm}\left(\frac{2\pi j}{K(\Delta\omega)}\right)\right| = \left|\sum_{k=0}^{K-1} e^{-i\left[k(\Delta\omega)\frac{2\pi j}{K(\Delta\omega)}+\frac{2\pi f(k)}{K}\right]}\right| =$$
$$\left|\sum_{k=0}^{K-1} e^{-i\frac{2\pi}{K}jk}e^{-i\frac{2\pi}{K}f(k)}\right| = \left|\sum_{k=0}^{K-1} w^{-jk}w^{-f(k)}\right| = F(j),$$

where $w=e^{i\frac{2\pi}{K}}$. Since the function $f(x)$ is a bent function:

$$\frac{1}{\sqrt{K}}F(j)=1 \Rightarrow F(j)=\sqrt{K}$$

so for all j, $\left|\Theta_{nm}(\frac{2\pi j}{K(\Delta\omega)})\right| = \sqrt{K}$, and by Theorem 8 this is the minimum value $\left|\Theta_{nm}(\frac{2\pi j}{K(\Delta\omega)})\right|$ can take.

By Theorem 9, this sequence is good for all values of τ.

Appendix I
Proof of Proposition 13

For any two different sets of phases $\Phi^{(n)}$,$\Phi^{(m)}$ from the given set of phase sequences, we have

$$\phi_k^{(m)} = (k^3+a_mk^2+b_mk+c_m)\frac{2\pi}{K}$$

and

$$\phi_k^{(n)} = (k^3+a_nk^2+b_nk+c_n)\frac{2\pi}{K}.$$

So

$$\phi_k^{(n)}-\phi_k^{(m)} =$$
$$\left((a_n-a_m)k^2+(b_n-b_m)k+(c_n-c_m)\right)\frac{2\pi}{K}.$$

Since we assume $a_n \neq a_m$, it implies that

$$(a_n - a_m)k^2 + (b_n - b_m)k + (c_n - c_m)$$

is a bent function by Theorems 10 and 11. So the given set of sequences satisfies the conditions of Proposition 12 and is good to be used with asynchronous phase encoding sequences.

For any two different set of phases $\Phi^{(i)}$,$\Phi^{(j)}$ from the above set of phases, we have: $\phi_k^{(i)} = (k^3 + a_i k^2 + b_i k + c_i)\frac{2\pi}{K}$ and $\phi_k^{(j)} = (k^3 + a_j k^2 + b_j k + c_j)\frac{2\pi}{K}$. Then

$$\phi_k^{(i)} - \phi_k^{(j)} = \left((a_i - a_j)k^2 + (b_i - b_j)k + (c_i - c_j)\right)\frac{2\pi}{K}. \quad (67)$$

Since we assume $a_i \neq a_j$, it implies that $(a_i - a_j)k^2 + (b_i - b_j)k + (c_i - c_j)$ is a bent function by Theorems 10 and 11. Hence,

$$\left| \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} w^{(a_i - a_j)k^2 + (b_i - b_j)k + (c_i - c_j)} w^{\lambda k} \right| = 1,$$

$$w = e^{i\left(\frac{2\pi}{K}\right)}, \lambda = 0, 1, \ldots, K-1$$

$$\Rightarrow \left| \sum_{k=0}^{K-1} e^{i\left[(a_i - a_j)k^2 + (b_i - b_j)k + (c_i - c_j)\right]\left(\frac{2\pi}{K}\right)} e^{i\left(\frac{\lambda 2\pi}{K}\right)k} \right| = \sqrt{K}$$

$$\Rightarrow \left| \sum_{k=0}^{K-1} e^{i\left(\frac{\lambda 2\pi}{K}\right)k} e^{i(\phi_k^{(i)} - \phi_k^{(j)})} \right| = \sqrt{K}. \quad (68)$$

So $|\Theta_{nm}(\tau)|$ for all $\tau = \frac{\lambda 2\pi}{K}$ is equal to $\sqrt{K}$. Using Theorem 8 we have met $M_d^{(K)}$. In addition, using Theorem 9, we can conclude that $|\Theta_{nm}(\tau)|$ is almost equal to $\sqrt{K}$ for all values of τ. So the sequences described above are good asynchronous phase encoding OCDMA sequences.

Appendix J
Proof of Proposition 15

We know that

$$\begin{aligned} h(k) &= f(k) - g(k) \\ \Rightarrow h(k+1) &= f(k+1) - g(k+1). \end{aligned}$$

Using equations (46) and (49), we get

$$\begin{aligned} h(k+1) &= (f(k) + a_k) - (g(k) + b_k) \\ &= (f(k) - g(k)) + (a_k - b_k). \end{aligned}$$

Hence, we can say that

$$h(k+1) = h(k) + p_k,$$

where $p_k = a_k - b_k$.

For $h(k)$ to be bent, p_k should satisfy the dual conditions. Consider

$$\sum_{k=0}^{K-1} p_k = \sum_{k=0}^{K-1} (a_k - b_k)$$

$$= \sum_{k=0}^{K-1} a_k - \sum_{k=0}^{K-1} b_k.$$

From equations (47) and (50), we know that both these sums are equal to 0, and so is the difference.

We next need to show that p_k satisfies the second condition:

$$p_{k+ns} = a_{k+ns} - b_{k+ns}. \quad (69)$$

Using equations (48) and (51), the above equation can be rewritten as

$$\begin{aligned} p_{k+ns} &= (a_k + c_1 ns(mod\ q)) - (b_k + c_2 ns(mod\ q)) \\ &= (a_k - b_k) + (c_1 - c_2)\, ns(mod\ q) \\ &= p_k + (c_1 - c_2)\, ns(mod\ q). \end{aligned}$$

Hence, p_k satisfies the dual conditions provided that c_1 c_2 is relatively prime to q. Hence, $h(k)$ is a bent function. Hence, the given set of sequences satisfies the condition of Proposition 12 and is good to be used with asynchronous phase-encoded OCDMA.

References

[1] J. A. Salehi, "Code division multiple-access techniques in optical fiber networks-part I: fundamental principles," *IEEE Trans. Communications*, vol. 37, pp. 824–833, Aug. 1989.

[2] L. Tančevski and I. Andonovic, "Hybrid wavelength hopping/time spreading schemes for use in massive optical networks with increased security," *IEEE Journal of Lightwave Tech.*, vol. 14, pp. 2636–2647, Dec. 1996.

[3] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: design, analysis, and applications," *IEEE Trans. Information Theory*, vol. 35, pp. 595–604, May 1989.

[4] H. Chung and P. V. Kumar, "Optical orthogonal codes - new bounds and an optimal construction," *IEEE Trans. Information Theory*, vol. 36, pp. 866–873, July 1990.

[5] Q. A. Nguyen, L. Györfi, and J. L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Information Theory*, vol. 38, pp. 940–949, May 1992.

[6] O. Moreno, Z. Zhang, P. V. Kumar, and V. A. Zinoviev, "New constructions of optimal cyclically permutable constant weight codes," *IEEE Trans. Information Theory*, vol. 41, pp. 448–455, Mar. 1995.

[7] S. Bitan and T. Etzion, "Constructions for optimal constant weight cyclically permutable codes and difference families," *IEEE Trans. Information Theory*, vol. 41, pp. 77–87, Jan. 1995.

[8] G. Yang and T. E. Fuja, "Optical orthogonal codes with unequal auto- and cross-correlation constraints," *IEEE Trans. Information Theory*, vol. 41, pp. 96–106, Jan. 1995.

[9] M. Buratti, "A powerful method for constructing difference families and optimal optical orthogonal codes," *Designs, Codes and Cryptography*, vol. 5, pp. 13–25, 1995.

[10] J. Yin, "Some combinatorial constructions for optical orthogonal codes," *Discrete Mathematics*, vol. 185, pp. 201–219, 1998.

[11] R. Fuji-Hara and Y. Miao, "Optical orthogonal codes: their bounds and new optimal constructions," *IEEE Trans. Information Theory*, vol. 46, pp. 2396–2406, Nov. 2000.

[12] G. Ge and J. Yin, "Constructions for optimal $(v, 4, 1)$ optical orthogonal codes," *IEEE Trans. Information Theory*, vol. 47, pp. 2998–3004, Nov. 2001.

[13] R. Fuji-Hara, Y. Miao, and J. Yin, "Optimal $(9v, 4, 1)$ optical orthogonal codes," *SIAM Journal on Discrete Mathematics*, vol. 14, pp. 256–266, 2001.

[14] Y. Tang and J. Yin, "The combinatorial construction for a class of optimal optical orthogonal codes," *Science in China (Series A)*, vol. 45, pp. 1268–1275, Oct. 2002.

[15] M. Buratti, "Cyclic designs with block size 4 and related optimal optical orthogonal codes," *Designs, Codes and Cryptography*, vol. 26, pp. 111–125, 2002.

[16] W. Chu and S. W. Golomb, "A new recursive construction for optical orthogonal codes," *IEEE Trans. Information Theory*, vol. 49, pp. 3072–3076, Nov. 2003.

[17] C. Ding and C. Xing, "Several classes of $(2^m - 1, w, 2)$ optical orthogonal codes," *Discrete Applied Mathematics*, vol. 128, pp. 103–120, 2003.

[18] Y. Chang, R. Fuji-Hara, and Y. Miao, "Combinatorial constructions of optimal optical orthogonal codes with weight 4," *IEEE Trans. Information Theory*, vol. 49, pp. 1283–1292, May 2003.

[19] Y. Chang and Y. Miao, "Constructions for optical orthogonal codes," *Discrete Mathematics*, vol. 261, pp. 127–139, 2003.

[20] Y. Chang and L. Ji, "Optimal $(4up, 5, 1)$ optical orthogonal codes," *Journal of Combinatorial Designs*, vol. 12, pp. 346–361, 2004.

[21] R. J. R. Abel and M. Buratti, "Some progress on $(v, 4, 1)$ difference families and optical orthogonal codes," *Journal of Combinatorial Theory, Series A*, vol. 106, pp. 59–75, 2004.

[22] Y. Chang and J. Yin, "Further results on optimal optical orthogonal codes with weight 4," *Discrete Mathematics*, vol. 279, pp. 135–151, 2004.

[23] W. Chu and C. J. Colbourn, "Optimal $(n, 4, 2)$-OOC of small orders," *Discrete Mathematics*, vol. 279, pp. 163–172, 2004.

[24] W. Chu and C. J. Colbourn, "Recursive constructions for optimal $(n, 4, 2)$-OOCs," *Journal of Combinatorial Designs*, vol. 12, pp. 333–345, 2004.

[25] N. Miyamoto, H. Mizuno, and S. Shinohara, "Optical orthogonal codes obtained from conics on finite projective planes," *Finite Fields and Their Applications*, vol. 10, pp. 405–411, 2004.

[26] O. Moreno, R. Omrani, P. V. Kumar, and H. Lu, "A generalized Bose-Chowla family of optical orthogonal codes and distinct difference sets," *IEEE Transactions on Information Theory*, vol. 53, no. 5, pp. 1907–1910, 2007.

[27] R. Omrani and P. V. Kumar, "Codes for optical CDMA," *Proc. of SETA 2006, Lecture Notes in Computer Science*, vol. 4086, pp. 34–46, 2006.

[28] A. Willner, J. Bannister, P. D. Dapkus, P. V. Kumar, and J. O'Brien, "Secure communication over LANs using optical CDMA technology: a unified novel architecture/coding/system/device approach," *DARPA OCDMA Program Grant No. N66001-02-1-8939*.

[29] A. M. Weiner, J. P. Heritage, and J. A. Salehi, "Encoding and decoding of femtosecond pulses," *Opt. Lett.*, vol. 13, pp. 300–302, Apr. 1988.

[30] J. A. Salehi, A. M. Weiner, and J. P. Heritage, "Coherent ultrashort light pulse code-division multiple access communication systems," *IEEE Journal of Lightwave Tech.*, vol. 8, pp. 478–491, Mar. 1990.

[31] S. Lee and S. Seo, "New construction of multiwavelength optical orthogonal codes," *IEEE Trans. Communications*, vol. 50, no. 12, pp. 2003–2008, 2002.

[32] S. Shurong, H. Yin, Z. Wang, and A. Xu, "A new family of 2-D optical orthogonal codes and analysis of its performance in optical CDMA access networks," *IEEE Journal of Lightwave Tech.*, vol. 24, no. 4, pp. 1646–1653, 2006.

[33] W. C. Kwong and G. C. Yang, "Extended carrier-hopping prime codes for wavelength-time optical code-division multiple access," *IEEE Trans. Communications*, vol. 52, pp. 1084–1091, 2004.

[34] G. C. Yang and W. C. Kwong, "Performance comparison of multiwavelength CDMA and WDMA+CDMA for fiber-optic networks," *IEEE Trans. Communications*, vol. 45, pp. 1426–1434, Nov. 1997.

[35] W. C. Kwong, G. C. Yang, V. Baby, C. S. Bres, and P. R. Prucnal, "Multiple-wavelength optical orthogonal codes under prime-sequence permutations for optical CDMA," in *IEEE Trans. Communications*, vol. 53, pp. 117–123, Jan. 2005.

[36] E. S. Shivaleela, K. N. Sivarajan, and A. Selvarajan, "Design of a new family of two-dimensional codes for fiber-optic CDMA networks," *IEEE Journal of Lightwave Tech.*, vol. 16, pp. 501–508, Apr. 1998.

[37] E. S. Shivaleela, A. Selvarajan, and T. Srinivas, "Two-dimensional optical orthogonal codes for fiber-optic CDMA networks," *IEEE Journal of Lightwave Tech.*, vol. 23, pp. 647–654, Feb. 2005.

[38] P. Saghari, R. Omrani, P. Ebrahimi, A. Willner, and P. V. Kumar, "Doubling the number of active users in a 2-D $t-\lambda$ O-CDMA network using a hard limiting receiver," *Quantum Electronics and Laser Science Conference, QELS '05*, vol. 3, pp. 1750–1752, May 2005.

[39] P. Saghari, R. Omrani, A. Willner, and P. V. Kumar, "Analytical interference model for two-dimensional (time-wavelength) asynchronous O-CDMA systems using various receiver structures," *IEEE Journal of Lightwave Tech.*, vol. 23, no. 10, pp. 3260–3269, 2005.

[40] E. Park, A. J. Mendez, and E. M. Garmire, "Temporal/spatial optical CDMA networks-design, demonstration, and comparison with temporal networks," *IEEE Photon. Technol. Lett.*, vol. 4, pp. 1160–1162, Oct. 1992.

[41] K. Kitayama, "Novel spatial spread spectrum based fiber optic CDMA networks for image transmission," *IEEE Journal on Selected Areas in Communications*, vol. 12, pp. 762–772, May 1994.

[42] L. Tančevski, I. Andonovic, M. Tur, and J. Budin, "Massive optical LANs using wavelength hopping/time spreading with increased security," *IEEE Photon. Technol. Lett.*, vol. 8, pp. 935–937, July 1996.

[43] G. C. Yang and W. C. Kwong, "Two-dimensional spatial signature patterns," *IEEE Trans. Communications*, vol. 44, pp. 184–191, Feb. 1996.

[44] H. Fathallah, L. A. Rusch, and S. LaRochelle, "Passive optical fast frequency-hop CDMA communications system," *IEEE Journal of Lightwave Tech.*, vol. 17, pp. 397–405, Mar. 1999.

[45] A. J. Mendez, R. M. Gagliardi, H. X. C. Feng, J. P. Heritage, and J. M. Morookian, "Strategies for realizing optical CDMA for dense, high-speed, long span, optical network applications," *IEEE Journal of Lightwave Tech.*, vol. 168, pp. 1685–1695, Dec. 2000.

[46] R. M. H. Yim, L. R. Chen, and J. Bajcsy, "Design and performance of 2-D codes for wavelength-time optical CDMA," *IEEE Photon. Technol. Lett.*, vol. 14, pp. 714–716, May 2002.

[47] A. J. Mendez, R. M. Gagliardi, V. J. Hernandez, C. V. Bennett, and W. J. Lennon, "Design and performance analysis of wavelength/time (W/T) matrix codes for optical CDMA," *IEEE Journal of Lightwave Tech.*, vol. 21, pp. 2524–2533, Nov. 2003.

[48] W. Liang, H. Yin, L. Qin, Z. Wang, and A. Xu, "A new family of 2D variable-weight optical orthogonal codes for OCDMA systems supporting multiple QoS and analysis of its performance," *Photonic Network Communications*, vol. 16, no. 1, pp. 53–60, 2008.

[49] K. Yu and N. Park, "Design of new family of two-dimensional wavelength-time spreading codes for optical code division multiple access networks," *Electronics Letters*, vol. 35, no. 10, pp. 830–831, 1999.

[50] W. Kwong, G. Yang, and Y. Liu, "A new family of wavelength-time optical CDMA codes utilizing programmable arrayed waveguide gratings," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 8, pp. 1564–1571, 2005.

[51] F. Gu and J. Wu, "Construction of two-dimensional wavelength/time optical orthogonal codes using difference family," *IEEE Journal of Lightwave Tech.*, vol. 23, no. 11, pp. 3642–3652, 2005.

[52] C. Chang, G. Yang, and W. Kwong, "Wavelength-time codes with maximum cross-correlation function of two for multicode-keying optical CDMA," *IEEE Journal of Lightwave Tech.*, vol. 24, no. 3, pp. 1093–1100, 2006.

[53] M. Morelle, C. Goursaud, A. Julien-Vergonjanne, C. Aupetit-Berthelemot, J. Cances, J. Dumas, and P. Guignard, "2-Dimensional optical CDMA system performance with parallel interference cancelation," *Microprocessors and Microsystems*, vol. 31, no. 4, pp. 215–221, 2007.

[54] J. Lin, J. Jhou, K. Lee, and J. Wen, "Construction and performance analysis of 2-D codes for M-ary OFFH-CDMA systems," *Communications, IET*, vol. 1, no. 1, pp. 113–121, 2007.

[55] G. C. Yang, W. C. Kwong, and C. Y. Chang, "Multiple-wavelength optical orthogonal codes under prime-sequence permutations," *IEEE International Symposium on Information Theory 2004*, p. 367, Sept. 2004.

[56] A. Lempel and H. Greenberger, "Families of sequences with optimal hamming correlation properties," *IEEE Trans. Information Theory*, vol. 20, pp. 90–94, Jan. 1974.

[57] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. McGraw-Hill, Inc., 2002.

[58] G. Einarsson, "Address assignment for a time-frequency-coded, spread-spectrum system," *Bell System Tech. Journal*, vol. 59, pp. 1241–1255, Sept. 1980.

[59] P. V. Kumar, "Frequency-hopping code sequence design having large linear span," *IEEE Trans. Information Theory*, vol. 34, pp. 146–151, Jan. 1988.

[60] D. V. Sarwate, "Reed-Solomon codes and the design of sequences for spread-spectrum multiple-access communications," in *Reed-Solomon Codes and Their Applications* (S. B. Wicker and V. K. Bhargava, eds.), Piscataway, NJ: IEEE Press, 1994.

[61] O. Moreno and S. V. Maric, "A new family of frequency-hop codes," *IEEE Trans. Communications*, vol. 48, pp. 1241–1244, Aug. 2000.

[62] S. Kim, K. Yu, and N. Park, "A new family of space/wavelength/time spread three-dimensional optical code for OCDMA networks," *IEEE Journal of Lightwave Tech.*, vol. 18, no. 43, pp. 502–511, 2000.

[63] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc.*, vol. 43, pp. 377–385, May 1938.

[64] J. E. McGeehan, S. Nezam, P. Saghari, A. Willner, R. Omrani, and P. V. Kumar, "Experimental demonstration of OCDMA transmission using a three-dimensional (time-wavelength-polarization) codeset," *IEEE Journal of Lightwave Tech.*, vol. 23, pp. 3282–3289, Oct. 2005.

[65] J. McGeehan, S. Nezam, P. Saghari, T. Izadpanah, A. Willner, R. Omrani, and P. V. Kumar, "3D time-wavelength-polarization OCDMA

coding for increasing the number of users in OCDMA LANs," *Optical Fiber Communication Conference 2004*, vol. 2, p. 3, Feb. 2004.

[66] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*. India: John Wiley & Sons, 2008.

[67] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Trans. Information Theory*, vol. 465, pp. 2397–2417, Nov. 1999.

[68] K. G. Paterson and V. Tarokh, "On the existence and construction of good codes with low peak-to-average power ratios," *IEEE Trans. Information Theory*, vol. 46, pp. 1974–1987, 2000.

[69] K. G. Paterson, "Sequences for OFDM and multi-code CDMA: two problems in algebraic coding theory," *Proc. of SETA 2001, Lecture Notes in Computer Science*, pp. 46–71, 2002.

[70] S. Litsyn and A. Yudin, "Discrete and continuous maxima in multicarrier communication," *IEEE Trans. Information Theory*, vol. 51, pp. 919–928, Mar. 2005.

[71] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," *Journal of Combinatorial Theory, Series A*, vol. 40, pp. 90–107, 1985.

[72] A. Stapleton, R. Shafiiha, H. Akhavan, S. Farrell, Z. Peng, S. J. Choi, W. Marshal, J. D. O'Brien, and P. D. Dapkus, "Experimental measurement of optical phase in microdisk resonators," in *IEEE/LEOS Summer Topical Meetings*, pp. 54–55, June 2004.

[73] A. Stapleton, S. Farrell, H. Akhavan, R. Shafiiha, Z. Peng, S. Choi, J. OBrien, P. Dapkus, and W. Marshall, "Optical phase characterization of active semiconductor microdisk resonators in transmission," *Applied Physics Letters*, vol. 88, 2006.

[74] P. Smith, "Mode-locking of lasers," *Proceedings of the IEEE*, vol. 58, no. 9, pp. 1342 – 1357, 1970.

[75] V. Hernandez, Y. Du, W. Cong, R. Scott, K. Li, J. Heritage, Z. Ding, B. Kolner, and S. Yoo, "Spectral phase-encoded time-spreading (spects) optical code-division multiple access for terabit optical access networks," *Lightwave Technology, Journal of*, vol. 22, no. 11, pp. 2671 – 2679, 2004.

[76] S. Litsyn, *Peak Power Control in Multicarrier Communications*. Cambridge University Press, 2007.

[77] H. Chung and P. V. Kumar, "A new general construction for generalized bent functions," *IEEE Trans. Information Theory*, vol. 35, pp. 206–209, Jan 1989.