Title	Optimal odd-length binary Z-complementary pairs
Author(s)	Liu, Zilong; Parampalli, Udaya; Guan, Yong Liang
Citation	Liu, Z., Parampalli, U., & Guan, Y. L. (2014). Optimal odd -length binary Z-complementary pairs. IEEE transactions on information theory, 60(9), 5768-5781.
Date	2014
URL	http://hdl.handle.net/10220/24581
Rights	© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [http://dx.doi.org/10.1109/TIT.2014.2335731].

Optimal Odd-Length Binary Z-Complementary Pairs

Zilong Liu, Udaya Parampalli, *Senior Member, IEEE*, Yong Liang Guan, *Member, IEEE*

***Abstract*—A pair of sequences is called a Golay complementary pair (GCP) if their aperiodic auto-correlation sums are zero for all out-of-phase time shifts. Existing known binary GCPs only have even-lengths in the form of $2^\alpha 10^\beta 26^\gamma$ (where α, β, γ are non-negative integers). To fill the gap left by the odd-lengths, we investigate the optimal odd-length binary pairs which display the closest correlation property to that of GCPs. Our criteria of "closeness" is that each pair has the maximum possible zero-correlation zone (ZCZ) width and minimum possible out-of-zone aperiodic auto-correlation sums. Such optimal pairs are called optimal odd-length binary Z-complementary pairs (OB-ZCP) in this paper. We show that each optimal OB-ZCP has maximum ZCZ width of $(N+1)/2$, and minimum out-of-zone aperiodic sum magnitude of 2, where N denotes the sequence length (odd). Systematic constructions of such optimal OP-ZCPs are proposed by insertion and deletion of certain binary GCPs, which settle the 2011 Li-Fan-Tang-Tu open problem positively. The proposed optimal OB-ZCPs may serve as a replacement for GCPs in many engineering applications where odd sequence lengths are preferred. In addition, they give rise to a new family of base-two almost difference families (ADF) which are useful in studying partially balanced incomplete block design (BIBD).**

***Index Terms*—Aperiodic correlation, almost difference set (ADS), almost difference families (ADF), Golay complementary pair (GCP), zero-correlation zone (ZCZ), Z-complementary pair (ZCP).**

I. Introduction

In 1951, Marcel J. E. Golay introduced the concept of "complementary pair" in the design of infrared multislit spectrometry that isolates the desired radiation with a fixed single wavelength from background radiation with many different wavelengths [1]. By definition, a complementary pair consists of a pair of sequences whose out-of-phase aperiodic autocorrelations sum to zero [2]. Such a sequence pair is called a Golay complementary pair (GCP), and either constituent sequence in a GCP is called a Golay sequence (GS). Starting with the work of Golay, several papers studied the constraints on the possible lengths (denoted by N) of binary GCPs:

1) N must be even and be the sum of two integer squares [2];
2) $N \neq 2 \cdot 9^t$ for any positive integer t [3];
3) $N \neq 2 \cdot 49^t$ for any positive integer t [4];
4) N cannot be divisible by a prime $\equiv 3 \pmod 4$ [5].

Note that existing known binary GCPs have even lengths of the form $2^\alpha 10^\beta 26^\gamma$ only, where α, β, γ are non-negative integers [6], [7]. In 2003, Borwein and Ferguson performed an exhaustive computer search which verified that all binary GCPs of lengths up to 100 satisfy $N = 2^\alpha 10^\beta 26^\gamma$ [8]. As a result, all possible lengths of binary GCPs for $N < 100$ are

$$2, 4, 8, 10, 16, 20, 26, 32, 40, 52, 64, 80.$$

Motivated by the limited admissible lengths of binary GCPs, Fan *et al* proposed "Z-complementary pair (ZCP)" which features zero aperiodic auto-correlation sums for certain out-of-phase time-shifts around the in-phase position [9]. Such a region is called a zero-correlation zone (ZCZ) and in this paper, such a ZCP is called a Type-I ZCP. Our study also extends to Type-II ZCPs, each having a ZCZ for time-shifts around the end-shift position (i.e., $\tau = N$).

GCPs have found a number of engineering applications owing to their attractive correlation properties. For instance, optimal intersymbol interference (ISI) channel estimation [10], [11], radar waveform design [12]−[15]. In particular, generalized GCPs, called "complementary codes"[1], have been employed for potential application in interference-free asynchronous multi-carrier code-division multiple-access (MC-CDMA) communications [21]−[23]. A drawback of complementary codes is that the set size is upper bounded by the number of constituent sequences in each complementary code [24]. To enlarge the set size beyond that of complementary codes, Liu *et al* proposed "quasi-complementary codes" which feature uniformly low auto- and cross- correlation sums over a time-shift zone or all (non-trivial) time-shifts [25], [26]. They also derived a tighter aperiodic correlation lower bound (over the Welch bound for quasi-complementary codes [24]) in [27] and [28]. GCPs have also been applied for peak-to-mean envelope power ratio (PMEPR) control in MC communications. Popović first pointed out that every GS has a PMEPR value of at most 2 if it is spread over the frequency domain [29]. Subsequently, Davis and Jedwab constructed polyphase GCPs of lengths 2^m from generalized Boolean functions and applied them for low-PMEPR code-keying MC communications [30]. In this paper, GCPs constructed by the approach in [30] are called Golay-Davis-Jedwab (GDJ) complementary pairs. To enable high-rate code-keying MC communications, it is desirable to construct more low PMEPR sequences with certain code distance. Toward this end, there have been intensive

Zilong Liu and Yong Liang Guan are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. E-mail: zilongliu@ntu.edu.sg; eylguan@ntu.edu.sg. Udaya Parampalli is with the Department of Computing and Information Systems, University of Melbourne, VIC 3010, Australia. E-mail: udaya@unimelb.edu.au.

The work of Zilong Liu and Yong Liang Guan was supported by the Advanced Communications Research Program DSOCL06271, a research grant from the Defense Research and Technology Office (DRTech), Ministry of Defence, Singapore. The work of U. Parampalli is supported in part by Australia-China Group Missions project, Department of Innovation, Industry, Science and Research (DIISR) Australia, under Grant ACSRF02361 and the Innovative Disciplines Intelligence Base 111 Project No. 111-2-14, of MoE, China.

The material in this paper was presented in part at the Proc. 2013 IEEE International Symposium on Information Theory (ISIT'2013), Istanbul, July 2013.

[1]Complementary codes is a set of two-dimensional matrices, each having two or more row sequences, with zero (non-trivial) aperiodic auto- and cross-correlation sums [16]−[20].

research activities for QAM GCP constructions [31]−[34]. In addition, "near-complementary pairs", which have slightly higher but acceptable PMEPRs (e.g., at most 4), are proposed [35], [36]. It is shown that more near-complementary sequences (over the total number of GSs) are available and thus a higher code rate is possible. We remark that existing near-complementary pairs (arising specifically for PMEPR control) don't necessarily possess the ZCZ property and thus they may not be applicable in asynchronous communications.

In recent years, quasi-synchronous CDMA (QS-CDMA) which is tolerant of small signal arrival delays (resulting from asynchronous transmission and multi-path propagation), has been proposed [37], [38]. Specifically, a single-carrier QS-CDMA using ZCZ sequences [39]−[41] can achieve interference-free performance provided that all interfering-signals (relative to the desired user signal) fall into the ZCZ. The same can be said for an MC-QS-CDMA using Z-complementary codes (generalized Type-I ZCPs) [9], [42]. Unlike Type-I ZCPs, Type-II ZCPs are useful in a wide-band wireless communication system where the minimum interfering-signal delay takes on a large value. In such a scenario, a Type-II ZCP is more efficient in rejecting asynchronous interference because its ZCZ is designed for large time-shifts. An example of such a channel with large delays may be in rural communication with few buildings nearby but large mountains at a distance away [43].

The main focus of this paper is optimal odd-length binary ZCPs (OB-ZCPs) which exhibit the closest correlation property to that of GCPs. Since existing known binary GCPs are available for certain even-lengths only, we aim to fill the gap left by the odd-lengths. In fact, this work is practically relevant as optimal OB-ZCPs contribute to more design flexibility in engineering applications. For instance, the authors in [10] differentiated the even- and odd- sequence lengths in their proposed ISI channel estimation scheme: for even-lengths, they suggested GCPs for optimal channel estimation[2], whereas for odd-lengths, they constructed "almost-complementary periodic sequence pairs", each of which is formed by a binary sequence with low auto-correlations, and the linear-phase transformed version of itself.

We first ask how close the (non-trivial) aperiodic auto-correlation sums of OB-ZCPs (Type-I or Type-II) approach zero. For asynchronous communications, we require "GCP-like" OB-ZCPs with large ZCZ widths and low out-of-zone aperiodic auto-correlation sums. The first condition is for a larger interference-free window to cater for more asynchronously arriving signals, whereas the second condition is for a higher detection probability (during code-acquisition stage) in noisy channels [44]. The second condition can also help suppress asynchronous interference caused by those interfering-signals falling outside of the ZCZ. For code-keying MC communications, intuitively, sequences from optimal "GCP-like" OB-ZCPs will possess low PMEPRs. It is known that every Type-I OB-ZCP has maximum ZCZ width of $(N+1)/2$, where N denotes the sequence length [9], [45]. Systematic construction of Type-I OB-ZCP with maximum ZCZ width was left open in [45]. This is referred to as "the Li-Fan-Tang-Tu open problem" in this paper. For each Type-I OB-ZCP with maximum ZCZ width, we investigate the magnitude lower bound of each out-of-zone aperiodic auto-correlation sum. Such an investigation is the key step in the search of the aforementioned optimal "GCP-like" OB-ZCPs. Similarly, we examine that of Type-II OB-ZCPs.

[2]with respect to the Crámer-Rao lower bound (CRLB).

This paper is organized as follows. In Section II, we define Type-I and Type-II ZCPs, introduce almost difference families (ADF) [46], then introduce the PMEPR control problem in code-keying MC communications. In Section III, we show that for a Type-I OB-ZCP with maximum ZCZ width, the magnitude of each out-of-zone aperiodic auto-correlation sum is lower bounded by 2. Interestingly, we show that each Type-II OB-ZCP of length N has the same maximum ZCZ width of $(N+1)/2$. It also has the property that the magnitude of every out-of-zone aperiodic auto-correlation sum is at least 2 when the maximum ZCZ-width is achieved. We say an OB-ZCP (Type-I or Type-II) is optimal if it has maximum ZCZ width of $(N+1)/2$ and minimum out-of-zone magnitude of 2. Furthermore, we show that each optimal OB-ZCP corresponds to a set of base-two almost difference families (ADF). In Section IV, by insertion and deletion of certain binary GDJ complementary pairs [30], we present systematic constructions of optimal OB-ZCPs (Type-I with lengths 2^m+1 and Type-II with lengths $2^m \pm 1$). The proposed constructions for optimal Type-I OB-ZCPs settle the Li-Fan-Tang-Tu open problem in [45] positively. We also generalize optimal Type-II OB-ZCPs to Type-II odd-length polyphase ZCPs (OP-ZCPs). We show that sequences from optimal OP-ZCPs all have PMEPR of at most 4 and therefore, by the framework in [36, *Theorem 2*], such optimal OP-ZCPs can be used as seed pairs to generate more near-complementary sequences for high-rate code-keying MC communications. Compared to the seed pairs in [36] which are specifically designed for PMEPR control and may not be applicable in asynchronous communications, our proposed seed pairs (i.e., Type-II OP-ZCPs) are superior. We summarize this paper in Section V.

II. Preliminaries

Throughout this paper, denote by $\mathbb{Z}_q = \{0, 1, \cdots, q-1\}$ the set of integers modulo q, where q is a positive integer. A length-N vector is called a binary sequence if it is over $\mathbb{Z}_2^N$. For convenience, whenever necessary, binary sequences may also be shown over $\{1, -1\}^N$. For $\mathbf{a} = (a_0, a_1, \cdots, a_{N-1})$ over $\mathbb{Z}_2^N$, let $\mathbf{a}(z)$ be the associated polynomial of z as follows,

$$\mathbf{a}(z) = \sum_{\tau=0}^{N-1} (-1)^{a_\tau} z^\tau. \tag{1}$$

For two binary sequences $\mathbf{a}$ and $\mathbf{b}$ over $\mathbb{Z}_2^N$, define

$$\rho_{\mathbf{a},\mathbf{b}}(\tau) = \begin{cases} \sum_{i=0}^{N-1-\tau} (-1)^{a_i + b_{i+\tau}}, & 0 \le \tau \le N-1; \\ \sum_{i=0}^{N-1-\tau} (-1)^{a_{i+\tau} + b_i}, & -(N-1) \le \tau \le -1; \\ 0, & |\tau| \ge N. \end{cases} \tag{2}$$

When $\mathbf{a} \neq \mathbf{b}$, $\rho_{\mathbf{a},\mathbf{b}}(\tau)$ is called the aperiodic cross-correlation function (ACCF) of $\mathbf{a}$ and $\mathbf{b}$; otherwise, it is called the aperiodic auto-correlation function (AACF). For simplicity, the AACF of $\mathbf{a}$ will be sometimes written as $\rho_{\mathbf{a}}(\tau)$.

Denote by $\oplus$ the modulo 2 addition. For $a, b \in \mathbb{Z}_2$, note that $(-1)^{a+b} = 1 - 2(a \oplus b)$. Therefore, for $0 \leq \tau \leq N-1$, $\rho_{\mathbf{a}}(\tau)$ can be rewritten as

$$\rho_{\mathbf{a}}(\tau) = (N-\tau) - 2 \cdot \left[\sum_{i=0}^{N-1-\tau} a_i \oplus a_{i+\tau} \right]. \tag{3}$$

In addition, denote by $\theta_{\mathbf{a},\mathbf{b}}(\tau)$ the periodic cross-correlation function, i.e.,

$$\theta_{\mathbf{a},\mathbf{b}}(\tau) = \rho_{\mathbf{a},\mathbf{b}}(\tau) + \rho_{\mathbf{b},\mathbf{a}}(N-\tau). \tag{4}$$

Similarly, we write the periodic auto-correlation function of $\mathbf{a}$ as $\theta_{\mathbf{a}}(\tau)$.

A. Binary Z-complementary pairs

Definition 1: [Type-I Binary Z-complementary pair] Let $\mathbf{a}$ and $\mathbf{b}$ be over $\mathbb{Z}_2^N$. $(\mathbf{a}, \mathbf{b})$ is said to be a Type-I binary Z-complementary pair (ZCP) with ZCZ width of Z if and only if

$$\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau) = 0, \quad \text{for any } 1 \leq \tau \leq Z-1. \tag{5}$$

In this case, $\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau)$ for $Z \leq \tau \leq N-1$, is called the out-of-zone aperiodic auto-correlation sum of $\mathbf{a}$ and $\mathbf{b}$ at time-shift τ. When $Z = N$, a Type-I ZCP is reduced to a Golay complementary pair (GCP) [2].

Definition 2: [Type-II Binary Z-complementary pair] Let $\mathbf{c}$ and $\mathbf{d}$ be over $\mathbb{Z}_2^N$. $(\mathbf{c}, \mathbf{d})$ is said to be a binary Type-II ZCP with ZCZ width of Z if and only if

$$\rho_{\mathbf{c}}(\tau) + \rho_{\mathbf{d}}(\tau) = 0, \quad \text{for any } N-Z+1 \leq \tau \leq N-1. \tag{6}$$

In this case, $\rho_{\mathbf{c}}(\tau) + \rho_{\mathbf{d}}(\tau)$ for $1 \leq \tau \leq N-Z$, is called the out-of-zone aperiodic auto-correlation sum of $\mathbf{c}$ and $\mathbf{d}$ at time-shift τ. When $Z = N$, a Type-II ZCP is also reduced to a GCP [2].

Example 1: Let

$$\begin{aligned} \mathbf{a} &= (1,1,1,-1,1,1,-1,1,1), \\ \mathbf{b} &= (1,1,1,-1,-1,-1,1,-1,1). \end{aligned}$$

$(\mathbf{a}, \mathbf{b})$ is a length-9 Type-I binary ZCP of $Z = 5$ because

$$\begin{aligned} \rho_{\mathbf{a}}(\tau) &= (9,0,-1,4,1,0,1,2,1), \\ \rho_{\mathbf{b}}(\tau) &= (9,0,1,-4,-1,-2,1,0,1), \\ \Big(\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau)\Big)_{\tau=0}^{8} &= (18,0,0,0,0,-2,2,2,2). \end{aligned}$$

Example 2: Let

$$\begin{aligned} \mathbf{c} &= (-1,1,1,1,-1,1,-1,1,1), \\ \mathbf{d} &= (-1,1,1,1,-1,-1,1,-1,-1). \end{aligned}$$

$(\mathbf{c}, \mathbf{d})$ is a length-9 Type-II binary ZCP of $Z = 5$ because

$$\begin{aligned} \rho_{\mathbf{c}}(\tau) &= (9,-2,1,-2,1,0,3,0,-1), \\ \rho_{\mathbf{d}}(\tau) &= (9,0,-3,0,1,0,-3,0,1), \\ \Big(\rho_{\mathbf{c}}(\tau) + \rho_{\mathbf{d}}(\tau)\Big)_{\tau=0}^{8} &= (18,-2,-2,-2,2,0,0,0,0). \end{aligned}$$

The following lemma is given in [45, *Theorem 1*].

Lemma 1: Each Type-I odd-length binary ZCP (OB-ZCP) $(\mathbf{a}, \mathbf{b})$ has the maximum ZCZ of width $(N+1)/2$, i.e.,

$$Z \leq (N+1)/2, \tag{7}$$

where N denotes the sequence length.

Similarly, we have the following lemma.

Lemma 2: Each Type-II OB-ZCP $(\mathbf{c}, \mathbf{d})$ also has the maximum ZCZ of width $(N+1)/2$, i.e.,

$$Z \leq (N+1)/2, \tag{8}$$

where N denotes the sequence length.

Definition 3: An OB-ZCP (Type-I or Type-II) is said to be *Z-optimal* if $Z = (N+1)/2$.

Remark 1: The Li-Fan-Tang-Tu open problem in [45]: How to construct *Z-optimal* Type-I OB-ZCPs systematically?

In addition, we need the following definition.

Definition 4: [Optimal OB-ZCP] An OB-ZCP (Type-I or Type-II) is said to be optimal if it is Z-optimal and every out-of-zone aperiodic auto-correlation sum takes on the magnitude value of 2.

A plot of the aperiodic auto-correlation sum magnitudes for OB-ZCPs in *Example 1* and *Example 2* is shown in Fig. 1. One can see that the OB-ZCPs in *Example 1* and *Example 2* are optimal. We will prove the above-mentioned magnitude lower bound of the out-of-zone aperiodic auto-correlation sums in Section III.

B. Almost Difference Families (ADF)

Almost difference families (ADF) are combinatorial objects and have applications in partially balanced incomplete block design (BIBD) [46]. In this subsection, we introduce definition and some properties of ADF which are required to establish their connection to optimal OB-ZCPs.

Define the support of $\mathbf{a}$, a binary sequence over $\mathbb{Z}_2^N$, as follows,

$$C_{\mathbf{a}} = \{0 \leq i \leq N-1 : a_i = 1\}.$$

Conversely, given a support, a binary sequence can be obtained. In this sense, the sequence $\mathbf{a}$ is called the characteristic sequence of the support set $C_{\mathbf{a}}$. Also, denote by $|C_{\mathbf{a}}|$ the number of elements in $C_{\mathbf{a}}$.

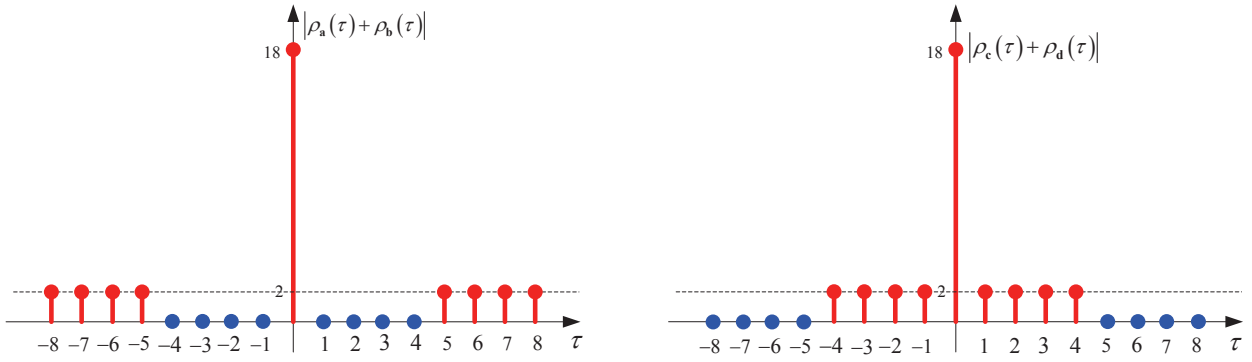
For any subset $A \subseteq \mathbb{Z}_N$, the difference function of A is defined as

$$d_A(\tau) = |(\tau + A) \cap A|, \quad \tau \in \mathbb{Z}_N.$$

Given the support of a binary sequence $\mathbf{a}$, the periodic auto-correlation function of $\mathbf{a}$ can be expressed as [47]

$$\theta_{\mathbf{a}}(\tau) = N - 4(k - d_{C_{\mathbf{a}}}(\tau)), \tag{9}$$

where $k = |C_{\mathbf{a}}|$.



(a) For OB-ZCP in *Example 1* (b) For OB-ZCP in *Example 2*

Fig. 1: AACF sum magnitudes of OB-ZCPs in *Example 1* and *Example 2*, respectively.

Let $\mathcal{D} = \{D_0, D_1\}$, where D_0 and D_1 are the supports of binary length-N sequences $\mathbf{a}$ and $\mathbf{b}$, respectively. For simplicity, let $g_0 = |D_0|$ and $g_1 = |D_1|$. $\mathcal{D}$ is said to be a set of $\{N; (g_0, g_1); \lambda; \nu\}$ almost difference families (ADF) if and only if

$$d_{\mathcal{D}}(\tau) = d_{D_0}(\tau) + d_{D_1}(\tau) \tag{10}$$

takes on the value λ for ν times, and the value $\lambda + 1$ for $N - 1 - \nu$ times, when τ ranges over $\{1, 2, \cdots, N-1\}$. In this case, either D_0 or D_1 is called a base, and therefore, $\mathcal{D}$ is said to be a set of base-two ADF [46]. Existing constructions of ADF in general are based on the tool of cyclotomy [46], [48], [49]. Although there are ADF of more than 2 bases, they are not our research focus in this paper. Note that ADF are a generalization of difference families (DF)[3] where $\nu = N - 1$ [51]. In [52], Doković presented a number of base-two DF obtained from computer search. ADF may also be regarded a generalization of "almost difference set (ADS)" which consists of one base only and is useful in optimal binary sequence design and cryptography [46]. For more information on ADS, the readers are referred to [47] and [53].

A necessary condition on the existence of a set of two-base ADF [46] is that

$$\sum_{i=0}^{1} g_i(g_i - 1) = \nu\lambda + (N - 1 - \nu)(\lambda + 1). \tag{11}$$

By (9) and (10), we have

$$\theta_{\mathbf{a}}(\tau) + \theta_{\mathbf{b}}(\tau) = \begin{cases} 2N, & \text{for } \tau = 0; \\ 2N - 4\left(g_0 + g_1 - d_{\mathcal{D}}(\tau)\right), & \text{for } \tau > 0. \end{cases} \tag{12}$$

By (12), we have the following lemma.

Lemma 3: Let D_0 and D_1 be the supports of binary length-N sequences $\mathbf{a}$ and $\mathbf{b}$, respectively, where $g_0 = |D_0|$ and $g_1 = |D_1|$. Then, $\mathcal{D} = \{D_0, D_1\}$ is a set of

$$\{N; (g_0, g_1); \lambda = g_0 + g_1 - (N+1)/2; \nu\}$$

ADF if and only if $\theta_{\mathbf{a}}(\tau) + \theta_{\mathbf{b}}(\tau) = \pm 2$, where ν is an integer in the range of $[1, N-1]$.

[3]which are also known as "supplementary difference sets (SDS)" in some literature [50].

C. PMEPR Control Problem in Code-Keying Multi-carrier Communication

Consider an MC system with N subcarriers, $\triangle f$ the subcarrier spacing and f_c the carrier frequency. For a length-N complex-valued codeword $\mathbf{a} = (a_0, a_1, \cdots, a_{N-1})$, its MC waveform signal in the symbol duration $0 \le t < 1/\triangle f$ is the real part of the following signal, i.e.,

$$T_{\mathbf{a}}(t) = \sum_{k=0}^{N-1} a_k \exp\left(\sqrt{-1}2\pi(f_c + \triangle f k)t\right). \tag{13}$$

In [30], it is shown that

$$|T_{\mathbf{a}}(t)|^2 = \rho_{\mathbf{a}}(0) + 2\sum_{\tau=1}^{N-1} \mathrm{Re}\left\{\rho_{\mathbf{a}}(\tau)\exp\left(\sqrt{-1}2\pi\triangle f\tau t\right)\right\}, \tag{14}$$

where $\mathrm{Re}\{x\}$ denotes the real part of the complex-valued data x.

For a polyphase sequence $\mathbf{a}$, the peak-to-mean power ratio (PMEPR) of its MC waveform signal is defined as

$$\mathrm{PMEPR}(\mathbf{a}) := \frac{1}{N}\sup_{0\le t<1/\triangle f} |T_{\mathbf{a}}(t)|^2. \tag{15}$$

Given a codebook S (which consists of a set of codewords), a specific codeword (say, $\mathbf{a}$) is selected in every symbol duration according to the input message (say, $\boldsymbol{x}$), i.e., code-keying. Therefore, the code rate of a code-keying MC system is defined as the ratio of the information word-length to the codeword length (which is equal to the number of subcarriers), i.e.,

$$\mathcal{R}(S) := \frac{\log_2|S|}{N}. \tag{16}$$

Remark 2: The PMEPR control problem in a code-keying MC system is to design a codebook S such that (1): all of its codewords feature low PMEPRs; (2): it features a large size to enable high-rate MC communications.

Let $(\mathbf{a}, \mathbf{b})$ be a pair of polyphase sequences of length N. By (14), the following equation is straightforward [35, *Theorem 2*].

$$|T_{\mathbf{a}}(t)|^2 + |T_{\mathbf{b}}(t)|^2 \leq 2N + 2\sum_{\tau=1}^{N-1} |\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau)|. \quad (17)$$

By (17), we have

$$\text{PMEPR}(\mathbf{a}) \leq 2 + \frac{2}{N}\sum_{\tau=1}^{N-1} |\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau)|. \quad (18)$$

III. Optimal odd-length binary Z-complementary pairs (OB-ZCPs)

In this section, we shall first prove that each out-of-zone aperiodic auto-correlation sum of an OB-ZCP (Type-I or Type-II) has a magnitude lower bound of 2 when its ZCZ is maximized. Then, we will give a necessary condition (via ADF) as well as several sequence properties of optimal OB-ZCPs.

For an odd-length binary sequence pair $(\mathbf{a}, \mathbf{b})$ over $\mathbb{Z}_2^N$, define

$$\mathcal{S}_{\mathbf{a},\mathbf{b}}(\tau) \triangleq \sum_{i=0}^{N-1-\tau} (a_i + b_i) + \sum_{i=\tau}^{N-1} (a_i + b_i). \quad (19)$$

We need the following lemma.

Lemma 4: For $1 \leq \tau \leq N-1$, $\mathcal{S}_{\mathbf{a},\mathbf{b}}(\tau) \equiv \mathcal{S}_{\mathbf{a},\mathbf{b}}(N-\tau) \pmod 2$.

Proof: The proof of this lemma is sufficient if we can show that this identity holds for any $1 \leq \tau \leq (N-1)/2$. By definition,

$$\mathcal{S}_{\mathbf{a},\mathbf{b}}(N-\tau) = \sum_{i=0}^{\tau-1}(a_i + b_i) + \sum_{i=N-\tau}^{N-1} (a_i + b_i).$$

Then by changing the limits of summations appropriately, we can see that

$$\begin{aligned}
\mathcal{S}_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{i=0}^{N-1-\tau} (a_i + b_i) + \sum_{i=\tau}^{N-1} (a_i + b_i) \\
&= \underbrace{\sum_{i=0}^{\tau-1}(a_i + b_i) + \sum_{i=\tau}^{N-1-\tau} (a_i + b_i)} \\
&\quad + \underbrace{\sum_{i=\tau}^{N-1-\tau} (a_i + b_i) + \sum_{i=N-\tau}^{N-1} (a_i + b_i)} \\
&\equiv \sum_{i=0}^{\tau-1}(a_i + b_i) + \sum_{i=N-\tau}^{N-1} (a_i + b_i) \pmod 2 \\
&= \mathcal{S}_{\mathbf{a},\mathbf{b}}(N-\tau) \pmod 2.
\end{aligned}$$

Thus, we complete the proof. ∎

Remark 3: Note that the identity in *Lemma 4* was used in arriving at the upper bound of the maximum ZCZ in [45, *Theorem 1*] for the specific case of $\tau = (N-1)/2$. The symmetric property of $\mathcal{S}_{\mathbf{a},\mathbf{b}}(\tau)$ is also useful in bounding the out-of-zone aperiodic auto-correlation sums as shown below.

In addition, by [45, (4)], we have

$$\mathcal{S}_{\mathbf{a},\mathbf{b}}(\tau) \equiv N - \tau \equiv \tau + 1, \text{ for } 1 \leq \tau \leq Z-1. \quad (20)$$

Suppose a Z-optimal Type-I OB-ZCP $(\mathbf{a}, \mathbf{b})$, i.e., $Z = (N+1)/2$. By *Lemma 4* and (20), we have

$$\begin{aligned}
&\frac{\rho_{\mathbf{a}}(N-\tau) + \rho_{\mathbf{b}}(N-\tau)}{2} \\
&\equiv \tau + \sum_{i=0}^{\tau-1}\Big[a_i \oplus a_{i+N-\tau} + b_i \oplus b_{i+N-\tau}\Big] \\
&\equiv \tau + \mathcal{S}_{\mathbf{a},\mathbf{b}}(N-\tau) \\
&\equiv \tau + \mathcal{S}_{\mathbf{a},\mathbf{b}}(\tau) \\
&\equiv 1 \pmod 2,
\end{aligned} \quad (21)$$

where $1 \leq \tau \leq (N-1)/2$. For a Z-optimal Type-II OB-ZCP $(\mathbf{c}, \mathbf{d})$, similarly we have

$$\frac{\rho_{\mathbf{c}}(N-\tau) + \rho_{\mathbf{d}}(N-\tau)}{2} \equiv 1 \pmod 2, \quad (22)$$

where $(N+1)/2 \leq \tau \leq N-1$.

With (21) and (22), we give the following two theorems.

Theorem 1: The magnitude of each out-of-zone aperiodic auto-correlation sum (OZ-AAS) for a Z-optimal Type-I OB-ZCP $(\mathbf{a}, \mathbf{b})$ is lower bounded by 2, i.e.,

$$\Big|\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau)\Big| \geq 2, \quad \text{for any } (N+1)/2 \leq \tau \leq N-1.$$

If $\Big|\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau)\Big| = 2$ holds for all $(N+1)/2 \leq \tau \leq N-1$, $(\mathbf{a}, \mathbf{b})$ is said to be an optimal Type-I OB-ZCP.

Some examples of optimal Type-I OB-ZCPs (obtained by computer search) of lengths up to 25 are shown in Table I.

Theorem 2: The magnitude of each out-of-zone aperiodic auto-correlation sum (OZ-AAS) for a Z-optimal Type-II OB-ZCP $(\mathbf{c}, \mathbf{d})$ is lower bounded by 2, i.e.,

$$\Big|\rho_{\mathbf{c}}(\tau) + \rho_{\mathbf{d}}(\tau)\Big| \geq 2, \quad \text{for any } 1 \leq \tau \leq (N-1)/2.$$

If $\Big|\rho_{\mathbf{c}}(\tau) + \rho_{\mathbf{d}}(\tau)\Big| = 2$ holds for all $1 \leq \tau \leq (N-1)/2$, $(\mathbf{c}, \mathbf{d})$ is said to be an optimal Type-II OB-ZCP.

Theorem 3: Suppose that $\mathcal{D} = \{D_0, D_1\}$ consists of the supports of an optimal OB-ZCP (Type-I or Type-II), where $g_0 = |D_0|$ and $g_1 = |D_1|$. Then, $\mathcal{D}$ should be a set of

$$\{N; (g_0, g_1); \lambda = g_0 + g_1 - (N+1)/2; \nu\},$$

ADF, where ν is an integer in the range of $[1, N-1]$. In particular, $\mathcal{D}$ reduces to a set of

$$\{N; (g_0, g_1); \lambda = g_0 + g_1 - (N+1)/2; N-1\}$$

DF if one of following conditions is satisfied:

1) For an optimal Type-I OB-ZCP $(\mathbf{a}, \mathbf{b})$,

$$\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau) = -2, \quad \text{for all } (N+1)/2 \leq \tau \leq N-1. \quad (23)$$

TABLE I: Optimal Type-I OB-ZCPs of lengths up to 25

N	$\begin{pmatrix}(-1)^{\mathbf{a}}\\(-1)^{\mathbf{b}}\end{pmatrix}$	$\Big(\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau)\Big)_{\tau=(N+1)/2}^{N-1}$
3	$\begin{pmatrix}+&+&+\\+&-&+\end{pmatrix}$	(2)
5	$\begin{pmatrix}+&+&+&+&-\\+&-&+&+&-\end{pmatrix}$	$(2,-2)$
7	$\begin{pmatrix}+&+&-&+&-&+&+\\+&-&-&+&+&+&+\end{pmatrix}$	$(-2,2,2)$
9	$\begin{pmatrix}-&+&-&+&+&+&+&-\\-&-&+&+&+&-&+&-\end{pmatrix}$	$(-2,-2,-2,2)$
11	$\begin{pmatrix}+&+&-&-&-&+&+&-&+&-\\+&-&+&-&+&+&+&+&+&-\end{pmatrix}$	$(-2,2,2,2,-2)$
13	$\begin{pmatrix}-&+&-&-&-&-&+&+&-&-&+&-\\-&-&+&-&-&+&+&+&+&-&+&-\end{pmatrix}$	$(-2,-2,2,2,-2,2)$
15	$\begin{pmatrix}+&-&+&+&-&+&+&+&+&+&+&-&-&+\\+&+&-&+&-&+&+&+&-&-&+&-&-&+\end{pmatrix}$	$(2,-2,-2,2,-2,-2,2)$
17	$\begin{pmatrix}+&+&-&+&+&-&-&+&-&+&-&-&+&+&+\\+&-&+&-&-&-&+&+&+&-&+&+&+&+&+\end{pmatrix}$	$(-2,-2,-2,-2,2,2,2,2)$
19	$\begin{pmatrix}+&+&-&+&+&-&+&+&+&+&-&+&-&+&-&-&+&+\\+&-&+&-&-&+&+&-&+&+&+&+&+&-&-&-&+&+\end{pmatrix}$	$(2,2,2,2,-2,-2,-2,2,2)$
21	$\begin{pmatrix}-&+&-&-&+&-&+&+&+&+&+&+&+&+&-&-&-&+&+&+&-\\-&-&+&-&+&+&+&-&+&+&-&+&+&-&+&+&+&-&+&+&-\end{pmatrix}$	$(-2,2,-2,2,-2,-2,2,-2,-2,2)$
23	$\begin{pmatrix}+&-&+&+&+&-&-&+&+&+&+&-&+&+&+&-&+&+&+&-&+&-&+\\+&+&-&-&+&+&-&+&+&+&+&+&-&-&-&+&-&-&+&-&+&-&+\end{pmatrix}$	$(2,2,2,-2,2,-2,2,-2,2,-2,2)$
25	$\begin{pmatrix}+&+&+&-&+&-&-&+&+&-&+&-&+&-&+&-&-&+&+&+&-&+&+&+&+\\+&-&-&+&-&-&-&-&+&-&-&+&+&-&+&+&+&-&-&-&+&+&+&+&+\end{pmatrix}$	$(-2,2,-2,-2,2,-2,-2,-2,-2,2,2,2,2)$

2) For an optimal Type-II OB-ZCP $(\mathbf{c},\mathbf{d})$,

$$\rho_{\mathbf{c}}(\tau)+\rho_{\mathbf{d}}(\tau)=-2,\ \text{ for all } 1\le\tau\le(N-1)/2. \quad (24)$$

Proof: We just show the proof for optimal Type-I OB-ZCP case. Starting from an optimal OB-ZCP $(\mathbf{a},\mathbf{b})$, we have

$$\Big|\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau)\Big|=\begin{cases}0, & \text{for } 0\le\tau\le(N-1)/2;\\ 2, & \text{for } (N+1)/2\le\tau\le N-1.\end{cases}$$

Thus, for any $1\le\tau\le N-1$,

$$\begin{aligned}&\Big|\theta_{\mathbf{a}}(\tau)+\theta_{\mathbf{b}}(\tau)\Big|\\ &=\Big|\underbrace{\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau)}+\underbrace{\rho_{\mathbf{a}}(N-\tau)+\rho_{\mathbf{b}}(N-\tau)}\Big| \quad (25)\\ &=2.\end{aligned}$$

Recalling *Lemma 3* completes the proof. ∎

Example 3: The optimal Type-I OB-ZCP in *Example 1* corresponds to a $\{9;(2,4);1;2\}$ base-two ADF $\mathcal{D}^1=\{D_{\mathbf{a}},D_{\mathbf{b}}\}$ where

$$D_{\mathbf{a}}=\{3,6\},\quad D_{\mathbf{b}}=\{3,4,5,7\}.$$

Also, the optimal Type-II OB-ZCP in *Example 2* corresponds to a $\{9;(3,5);3;6\}$ base-two ADF $\mathcal{D}^2=\{D_{\mathbf{c}},D_{\mathbf{d}}\}$ where

$$D_{\mathbf{c}}=\{0,4,6\},\quad D_{\mathbf{d}}=\{0,4,5,7,8\}.$$

In what follows, we give three additional properties of optimal OB-ZCPs, in order to show their close connections to binary GCPs. These properties, together with the necessary condition in *Theorem 3*, may be useful for the search of optimal OB-ZCPs of large lengths. As before, whenever a proof is needed, we show the proof of optimal Type-I OB-ZCPs only.

Property 1: Each sequence in an optimal OB-ZCP (Type-I or Type-II) has a PMEPR of at most 4.

Proof: Recalling (18) completes the proof. ∎

Remark 4: In contrast, each sequence in a GCP has a PMEPR of at most 2 [29], [30].

Property 2: For an optimal Type-I OB-ZCP $(\mathbf{a},\mathbf{b})$,

$$\begin{cases}a_0+a_{N-1}+b_0+b_{N-1} &\equiv 0 \pmod 2,\\ a_r+a_{N-1-r}+b_r+b_{N-1-r} &\equiv 1 \pmod 2,\end{cases} \quad (26)$$

where $1\le r\le(N-3)/2$. For an optimal Type-II OB-ZCP $(\mathbf{c},\mathbf{d})$,

$$c_r+c_{N-1-r}+d_r+d_{N-1-r}\equiv 1 \pmod 2, \quad (27)$$

where $0\le r\le(N-3)/2$.

Proof: To prove (26), we need an induction as follows. Since

$$\begin{aligned}&\rho_{\mathbf{a}}(N-1)+\rho_{\mathbf{b}}(N-1)\\ &=2-2\Big[a_0\oplus a_{N-1}+b_0\oplus b_{N-1}\Big]\\ &=\pm 2,\end{aligned}$$

Thus,

$$a_0+a_{N-1}+b_0+b_{N-1}\equiv 0 \pmod 2. \quad (28)$$

Also,

$$\begin{aligned}&\rho_{\mathbf{a}}(N-2)+\rho_{\mathbf{b}}(N-2)\\ &=4-2\Big[a_0\oplus a_{N-2}+a_1\oplus a_{N-1}+b_0\oplus b_{N-2}+b_1\oplus b_{N-1}\Big]\\ &=\pm 2,\end{aligned} \quad (29)$$

therefore,

$$\begin{aligned}&\underbrace{a_0+a_{N-1}+b_0+b_{N-1}}_{\equiv 0 \pmod 2 \text{ by } (28)}\\ &+\underbrace{a_1+a_{N-2}+b_1+b_{N-2}}\equiv 1 \pmod 2,\end{aligned} \quad (30)$$

leading to

$$a_1 + a_{N-2} + b_1 + b_{N-2} \equiv 1 \pmod 2. \tag{31}$$

Carrying on this induction until $\rho_{\mathbf{a}}\left(\frac{N+1}{2}\right) + \rho_{\mathbf{b}}\left(\frac{N+1}{2}\right)$, it is easy to see that

$$a_r + a_{N-1-r} + b_r + b_{N-1-r} \equiv 1 \pmod 2 \tag{32}$$

holds for any $1 \le r \le (N-3)/2$. Thus, we complete the proof of (26). ∎

Remark 5: In contrast to (26) and (27), a binary GCP $(\mathbf{a}, \mathbf{b})$ should satisfy the following condition

$$a_r + a_{N-1-r} + b_r + b_{N-1-r} \equiv 1 \pmod 2, \tag{33}$$

where $0 \le r \le N/2 - 1$ and N is even.

Property 3: For an optimal Type-I OB-ZCP $(\mathbf{a}, \mathbf{b})$, denote by g_0 and g_1 the numbers of ones in $\mathbf{a}$ and $\mathbf{b}$, respectively. Then we have

$$N + \underbrace{\sum_{\tau=(N+1)/2}^{N-1} \Big[\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau)\Big]} = (g_0 - g_1)^2 + (N - g_0 - g_1)^2. \tag{34}$$

For an optimal Type-II OB-ZCP $(\mathbf{c}, \mathbf{d})$ (similarly, define g_0 and g_1 for $\mathbf{c}$ and $\mathbf{d}$, respectively),

$$N + \underbrace{\sum_{\tau=1}^{(N-1)/2} \Big[\rho_{\mathbf{c}}(\tau) + \rho_{\mathbf{d}}(\tau)\Big]} = (g_0 - g_1)^2 + (N - g_0 - g_1)^2. \tag{35}$$

Proof: Recall the associated polynomial defined in Section II. Then, for $z \neq 0$, we obtain

$$\begin{aligned} &\mathbf{a}(z)\mathbf{a}(z^{-1}) + \mathbf{b}(z)\mathbf{b}(z^{-1}) \\ =&\sum_{\tau=0}^{N-1} \Big[(\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau)) \cdot \left(z^{\tau} + z^{-\tau}\right)\Big] \\ =&2N + \sum_{\tau=(N+1)/2}^{N-1} \Big[(\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau)) \cdot \left(z^{\tau} + z^{-\tau}\right)\Big]. \end{aligned} \tag{36}$$

Now setting $z = 1$ in (36), and recalling the ZCZ property of the optimal Type-I OB-ZCP, we have

$$\begin{aligned} &\Big|\mathbf{a}(1)\Big|^2 + \Big|\mathbf{b}(1)\Big|^2 \\ =&(N - 2g_0)^2 + (N - 2g_1)^2 \\ =&\rho_{\mathbf{a}}(0) + \rho_{\mathbf{b}}(0) + 2\sum_{\tau=(N+1)/2}^{N-1} \Big[\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau)\Big] \\ =&2N + 2\sum_{\tau=(N+1)/2}^{N-1} \Big[\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau)\Big]. \end{aligned} \tag{37}$$

By (37), the proof of (34) follows. ∎

Remark 6: The length of a binary GCP should satisfy the following condition [2].

$$N = (g_0 - g_1)^2 + (N - g_0 - g_1)^2. \tag{38}$$

Note that, disregarding the condition on N, (34) and (35) are also applicable to binary GCPs whose out-of-phase aperiodic autocorrelation sums are zero.

IV. Proposed Constructions for Optimal OB-ZCPs

In this section, we present constructions of optimal OB-ZCPs based on insertion and deletion of certain GDJ complementary pairs [30]. To this end, we first introduce the construction of GDJ complementary pairs below.

A. Golay-Davis-Jedwab (GDJ) Complementary pairs

For $\mathbf{x} = (x_1, x_2, \cdots, x_m) \in \mathbb{Z}_2^m$, a q-ary generalized Boolean function $f(\mathbf{x})$ [or $f(x_1, x_2, \cdots, x_m)$] is defined as a mapping $f : \mathbb{Z}_2^m \to \mathbb{Z}_q$. Let $(i_1, i_2, \cdots, i_m)$ be the binary representation of the integer $i = \sum_{k=1}^{m} i_k 2^{k-1}$, with i_m denoting the most significant bit (MSB). Given $f(\mathbf{x})$, let $f_i = f(i_1, i_2, \cdots, i_m)$, and define the associated sequence $\mathbf{f}$ as

$$\begin{aligned} \mathbf{f} :&= (f_0, f_1, \cdots, f_{2^m-1}) \\ &= \left(f(0,0,\cdots,0), f(1,0,\cdots,0), \cdots, f(1,1,\cdots,1)\right). \end{aligned}$$

Example 4: Let $m = 3$ and $q = 2$. The associated sequences for generalized Boolean functions of $1, x_1, x_3, x_1x_3$ are

$$\begin{aligned} \mathbf{1} &= (1,1,1,1,1,1,1,1), \\ \mathbf{x}_1 &= (0,1,0,1,0,1,0,1), \\ \mathbf{x}_3 &= (0,0,0,0,1,1,1,1), \\ \mathbf{x}_1\mathbf{x}_3 + \mathbf{1} &= (1,1,1,1,1,0,1,0), \end{aligned}$$

respectively.

We present the construction of GDJ complementary pairs in the following lemma.

Lemma 5: (Golay-Davis-Jedwab complementary pair [30]) Let

$$f(\mathbf{x}) = \frac{q}{2}\sum_{k=1}^{m-1} x_{\pi(k)}x_{\pi(k+1)} + \sum_{k=1}^{m} c_k x_k, \tag{39}$$

where q is even, π is a permutation of the set $\{1, 2, \cdots, m\}$, and $c_k \in \mathbb{Z}_q$. Then $(\mathbf{g}, \mathbf{h})$

$$\begin{aligned} \mathbf{g} &= \mathbf{f} + c \cdot \mathbf{1} \\ \mathbf{h} &= \mathbf{f} + \frac{q}{2}\mathbf{x}_{\pi(1)} + c' \cdot \mathbf{1} \end{aligned} \tag{40}$$

form a GCP of length 2^m, where $c, c' \in \mathbb{Z}_q$.

Next, we present an interesting property of GDJ complementary pairs. Such a property is useful in the proof of our proposed optimal OB-ZCPs.

Lemma 6: Let $q = 2$ and consider a length-2^m binary GDJ complementary pair $(\mathbf{g}, \mathbf{h})$ described in *Lemma 5*. Denote by $\mathbf{g}_0$ and $\mathbf{g}_1$ the first- and the second- halves of $\mathbf{g}$, respectively. Similarly, we define $\mathbf{h}_0$ and $\mathbf{h}_1$ for $\mathbf{h}$.

$$\begin{aligned} \mathbf{g}_0 &= (g_0, g_1, \cdots, g_{2^{m-1}-1}), \\ \mathbf{g}_1 &= (g_{2^{m-1}}, g_{2^{m-1}+1}, \cdots, g_{2^m-1}), \\ \mathbf{h}_0 &= (h_0, h_1, \cdots, h_{2^{m-1}-1}), \\ \mathbf{h}_1 &= (h_{2^{m-1}}, h_{2^{m-1}+1}, \cdots, h_{2^m-1}). \end{aligned}$$

Then, every sum of out-of-phase aperiodic auto-correlations of $\mathbf{g}_0, \mathbf{g}_1, \mathbf{h}_0, \mathbf{h}_1$ equals to zero, i.e.,

$$\rho_{\mathbf{g}_0}(\tau) + \rho_{\mathbf{g}_1}(\tau) + \rho_{\mathbf{h}_0}(\tau) + \rho_{\mathbf{h}_1}(\tau) = 0, \text{ for } \tau \neq 0. \quad (41)$$

In addition, every sum of aperiodic cross-correlations between $(\mathbf{g}_0, \mathbf{h}_0)$ and $(\mathbf{g}_1, \mathbf{h}_1)$ is zero, i.e.,

$$\rho_{\mathbf{g}_u, \mathbf{g}_{1-u}}(\tau) + \rho_{\mathbf{h}_u, \mathbf{h}_{1-u}}(\tau) = 0, \text{ for } u \in \{0, 1\}. \quad (42)$$

Proof: See Appendix A. ∎

B. Proposed Constructions

We need the following two definitions.

Definition 5: [*Insertion Function*] For a vector $\mathbf{w} = (w_0, w_1, \cdots, w_{N-1})$, an element d (to be inserted), and an integer $r \in \{0, 1, \cdots, N\}$ (the insertion position), define $\mathcal{I}(\mathbf{w}, d, r)$ as an insertion function as follows.

$$\mathcal{I}(\mathbf{w}, d, r) = \begin{cases} (d, w_0, w_1, \cdots, w_{N-1}), & \text{if } r = 0; \\ (w_0, w_1, \cdots, w_{N-1}, d), & \text{if } r = N; \\ (w_0, w_1, \cdots, w_{r-1}, d, w_r, \cdots, w_{N-1}), & \text{otherwise.} \end{cases} \quad (43)$$

Definition 6: [*Deletion Function*] For a vector $\mathbf{w} = (w_0, w_1, \cdots, w_{N-1})$ and an integer $r \in \{0, 1, \cdots, N-1\}$ (the deletion position), define $\mathcal{V}(\mathbf{w}, r)$ as a deletion function as follows.

$$\mathcal{V}(\mathbf{w}, r) = \begin{cases} (w_1, w_2, \cdots, w_{N-1}), & \text{if } r = 0; \\ (w_0, w_1, \cdots, w_{N-2}), & \text{if } r = N-1; \\ (w_0, w_1, \cdots, w_{r-1}, w_{r+1}, \cdots, w_{N-1}), & \text{otherwise.} \end{cases} \quad (44)$$

Based on the above definitions, we present below the following lemma on aperiodic auto-correlation functions of the insertion- and deletion- functions. We omit its proof as it is straightforward.

Lemma 7: For a binary vector $\mathbf{w}$ of length $N = 2^m$, denote by $\mathbf{w}_0$ and $\mathbf{w}_1$ the first- and the second- halves of $\mathbf{w}$, respectively, i.e.,

$$\begin{aligned} \mathbf{w}_0 &= (w_0, w_1, \cdots, w_{2^{m-1}-1}), \\ \mathbf{w}_1 &= (w_{2^{m-1}}, w_{2^{m-1}+1}, \cdots, w_{2^m-1}). \end{aligned}$$

The aperiodic auto-correlation function of $\mathcal{I}(\mathbf{w}, d, r)$ (where $d \in \mathbb{Z}_2$) is shown in (45). In addition, the aperiodic auto-correlation function of $\mathcal{V}(\mathbf{w}, r)$ is shown in (46).

Now, we are ready to present our proposed constructions for optimal Type-I OB-ZCPs.

Theorem 4: Let $(\mathbf{g}, \mathbf{h})$ be a length-2^m binary GDJ pair described in *Lemma 5*. Then, an optimal Type-I OB-ZCP $(\mathbf{a}, \mathbf{b})$ of length $2^m + 1$ is obtained by insertion of $(\mathbf{g}, \mathbf{h})$ in one of the cases in Table II.

Proof: See Appendix B. ∎

Next, we present below our proposed constructions for optimal Type-II OB-ZCPs.

Theorem 5: Let $(\mathbf{g}, \mathbf{h})$ be a length-2^m binary GDJ pair described in *Lemma 5*. Then, an optimal Type-II OB-ZCP $(\mathbf{c}, \mathbf{d})$ of length $2^m + 1$ or $2^m - 1$ is obtained by insertion or deletion of $(\mathbf{g}, \mathbf{h})$ in one of the cases in Table III.

Proof: See Appendix C. ∎

To illustrate the proposed constructions in *Theorem 4* and *Theorem 5*, we show an example below.

Example 5: Let $m = 4$, $\pi = (1, 3, 2, 4)$, and $(c_1, c_2, c_3, c_4, c, c') = (0, 0, 0, 1, 0, 0)$. By *Lemma 5*, we obtain a length-16 binary GCP $(\mathbf{g}, \mathbf{h})$ below

$$\begin{aligned} \mathbf{g} &= (+,+,+,+,+,-,-,+,-,-,+,+,-,+,-,+), \\ \mathbf{h} &= (+,-,+,-,+,+,-,-,-1,+,+,-,-,-,-,-). \end{aligned}$$

Let $d_1 = d_2 = 0$. Note that $\pi(m) = m$ and $d_1 + d_2 \equiv m + 1 + \sum_{k=1}^{m} c_k + c' - c \pmod 2$. Applying the Case 3 construction in *Theorem 4*, we obtain a length-17 optimal Type-I OB-ZCP $(\mathbf{a}, \mathbf{b})$

$$\mathbf{a} = \left((-1)^{d_1},\ \mathbf{g}\right), \quad \mathbf{b} = \left(\mathbf{h},\ (-1)^{d_2}\right),$$

with

$$\begin{aligned} &\left(\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau)\right)_{\tau=0}^{16} \\ =&(34, 0, 0, 0, 0, 0, 0, 0, 0, -2, 2, 2, 2, -2, 2, -2, -2). \end{aligned}$$

Also, applying the Case 3 construction in *Theorem 5*, we obtain a length-17 optimal Type-II OB-ZCP $(\mathbf{c}, \mathbf{d})$

$$\mathbf{c} = \left((-1)^{d_1},\ \mathbf{g}\right), \quad \mathbf{d} = \left(\mathbf{h},\ (-1)^{1+d_2}\right),$$

because

$$\begin{aligned} &\left(\rho_{\mathbf{c}}(\tau) + \rho_{\mathbf{d}}(\tau)\right)_{\tau=0}^{16} \\ =&(34, 2, 2, -2, 2, 2, 2, 2, -2, 0, 0, 0, 0, 0, 0, 0, 0). \end{aligned}$$

C. Further Remarks on PMEPR Control in Code-Keying Multi-carrier Communications

As pointed out in *Property 1*, each sequence in an optimal OB-ZCP possesses a PMEPR of at most 4. In this subsection, we make some further comments on PMEPR control in code-keying MC communications by the proposed optimal OB-ZCPs.

First, we note that the idea of insertion and deletion of GDJ complementary pair has also appeared in [36]. Specifically, in [36, *Theorem 2*], a framework has been proposed to generate polyphase near-complementary pairs based on two types of seed pairs, i.e., the "extended Golay complementary pairs" (by the end-position insertion) and "shortened Golay complementary pairs" (by the end-position deletion). It is shown that their near-complementary sequences also have PMEPR of at most 4. However, they don't necessarily possess large ZCZ widths and hence they may not be applicable in asynchronous communications.

$$\rho_{\mathcal{I}(\mathbf{w},d,r)}(\tau) = \begin{cases} \rho_{\mathbf{w}}(\tau) + (-1)^{d+w_{\tau-1}}, & \text{If } r = 0; \\ \rho_{\mathbf{w}}(\tau) + (-1)^{d+w_{2^m-\tau}}, & \text{If } r = 2^m; \\ \rho_{\mathbf{w}_0}(\tau) + \rho_{\mathbf{w}_1}(\tau) + \rho_{\mathbf{w}_1,\mathbf{w}_0}(2^{m-1}-\tau+1) & \\ \quad + (-1)^d \left[(-1)^{w_{2^{m-1}-\tau}} + (-1)^{w_{2^{m-1}+\tau-1}}\right], & \text{If } r = 2^{m-1} \text{ and } 1 \le \tau \le 2^{m-1}. \end{cases} \tag{45}$$

$$\rho_{\mathcal{V}(\mathbf{w},r)}(\tau) = \begin{cases} \rho_{\mathbf{w}}(\tau) + (-1)^{w_0+w_\tau+1}, & \text{If } r = 0; \\ \rho_{\mathbf{w}}(\tau) + (-1)^{w_{2^m-1}+w_{2^m-\tau-1}+1}, & \text{If } r = 2^m - 1; \\ \rho_{\mathbf{w}_0}(\tau) + \rho_{\mathbf{w}_1}(\tau) + \rho_{\mathbf{w}_1,\mathbf{w}_0}(2^{m-1}-\tau-1) & \\ \quad + (-1)^{w_{2^{m-1}-1}+1} \left[(-1)^{w_{2^{m-1}+\tau}} + (-1)^{w_{2^{m-1}-\tau-1}}\right], & \\ & \text{If } r = 2^{m-1}-1 \text{ and } 1 \le \tau \le 2^{m-1}-1; \\ \rho_{\mathbf{w}_0}(\tau) + \rho_{\mathbf{w}_1}(\tau) + \rho_{\mathbf{w}_1,\mathbf{w}_0}(2^{m-1}-\tau-1) & \\ \quad + (-1)^{w_{2^{m-1}}+1} \left[(-1)^{w_{2^{m-1}+\tau}} + (-1)^{w_{2^{m-1}-\tau-1}}\right], & \\ & \text{If } r = 2^{m-1} \text{ and } 1 \le \tau \le 2^{m-1}-1. \end{cases} \tag{46}$$

TABLE II: Four Cases of Optimal Type-I OB-ZCP of Length $2^m + 1$

Case No.	$\mathbf{a}$	$\mathbf{b}$	Constraints	Length
1	$\mathcal{I}(\mathbf{g}, d_1, 0)$	$\mathcal{I}(\mathbf{h}, d_2, 0)$	$\pi(1) = m, d_1, d_2 \in \mathbb{Z}_2$, $d_1 + d_2 \equiv c' - c + 1 \pmod 2$.	$2^m + 1$
2	$\mathcal{I}(\mathbf{g}, d_1, 2^m)$	$\mathcal{I}(\mathbf{h}, d_2, 2^m)$	$\pi(1) = m, d_1, d_2 \in \mathbb{Z}_2$, $d_1 + d_2 \equiv c' - c \pmod 2$.	
3	$\mathcal{I}(\mathbf{g}, d_1, 0)$	$\mathcal{I}(\mathbf{h}, d_2, 2^m)$	$\pi(m) = m, d_1, d_2 \in \mathbb{Z}_2$, $d_1 + d_2 \equiv m + 1 + \sum_{k=1}^{m} c_k + c' - c \pmod 2$.	
4	$\mathcal{I}(\mathbf{g}, d_1, 2^m)$	$\mathcal{I}(\mathbf{h}, d_2, 0)$	$\pi(m) = m, d_1, d_2 \in \mathbb{Z}_2$, $d_1 + d_2 \equiv m + \sum_{k=1}^{m} c_k + c' - c \pmod 2$.	

TABLE III: Eight Cases of Optimal Type-II OB-ZCP of Length $2^m + 1$ or $2^m - 1$

Case No.	$\mathbf{c}$	$\mathbf{d}$	Constraints	Length
1	$\mathcal{I}(\mathbf{g}, d_1, 0)$	$\mathcal{I}(\mathbf{h}, d_2, 0)$	$\pi(1) = m, d_1, d_2 \in \mathbb{Z}_2$, $d_1 + d_2 \equiv c' - c \pmod 2$.	$2^m + 1$
2	$\mathcal{I}(\mathbf{g}, d_1, 2^m)$	$\mathcal{I}(\mathbf{h}, d_2, 2^m)$	$\pi(1) = m, d_1, d_2 \in \mathbb{Z}_2$, $d_1 + d_2 \equiv c' - c + 1 \pmod 2$.	
3	$\mathcal{I}(\mathbf{g}, d_1, 0)$	$\mathcal{I}(\mathbf{h}, d_2, 2^m)$	$\pi(m) = m, d_1, d_2 \in \mathbb{Z}_2$, $d_1 + d_2 \equiv m + \sum_{k=1}^{m} c_k + c' - c \pmod 2$.	
4	$\mathcal{I}(\mathbf{g}, d_1, 2^m)$	$\mathcal{I}(\mathbf{h}, d_2, 0)$	$\pi(m) = m, d_1, d_2 \in \mathbb{Z}_2$, $d_1 + d_2 \equiv m + 1 + \sum_{k=1}^{m} c_k + c' - c \pmod 2$.	
5	$\mathcal{I}(\mathbf{g}, d_1, 2^{m-1})$	$\mathcal{I}(\mathbf{h}, d_2, 2^{m-1})$	$d_1, d_2 \in \mathbb{Z}_2$.	
6	$\mathcal{V}(\mathbf{g}, d(2^m - 1))$	$\mathcal{V}(\mathbf{h}, d(2^m - 1))$	$d \in \{0, 1\}, \pi(1) = m$.	$2^m - 1$
7	$\mathcal{V}(\mathbf{g}, d(2^m - 1))$	$\mathcal{V}(\mathbf{h}, (1-d)(2^m - 1))$	$d \in \{0, 1\}, \pi(m) = m$.	
8	$\mathcal{V}(\mathbf{g}, 2^{m-1} - d_1)$	$\mathcal{V}(\mathbf{h}, 2^{m-1} - d_2)$	$d_1, d_2 \in \{0, 1\}$.	

We also point out that the insertion and deletion in this paper apply not only to the start and the end positions, but also to the middle positions (see Case 5 and Case 8 in *Theorem 5*) of GDJ complementary pairs. Because of this, more seed sequences with PMEPRs of at most 4 have been constructed. To show this, we extend the Cases 5 and 8 constructions in *Theorem 5* to Type-II odd-length polyphase ZCPs in the following theorem.

Theorem 6: Let $(\mathbf{g}, \mathbf{h})$ be a length-2^m q-ary GDJ pair as described in *Lemma 5*. Construct odd-length q-ary $(\mathbf{c}, \mathbf{d})$ in one of the following cases.

1) For $N = 2^m + 1$,

$$\mathbf{c} = \mathcal{I}(\mathbf{g}, d_1, 2^{m-1}), \quad \mathbf{d} = \mathcal{I}(\mathbf{h}, d_2, 2^{m-1}),$$

where $d_1, d_2 \in \{a, a + q/2\}$ and $a \in \mathbb{Z}_q$.

2) For $N = 2^m - 1$,

$$\mathbf{c} = \mathcal{V}(\mathbf{g}, 2^{m-1} - d_1), \quad \mathbf{d} = \mathcal{V}(\mathbf{h}, 2^{m-1} - d_2),$$

where $d_1, d_2 \in \{0, 1\}$.

$(\mathbf{c}, \mathbf{d})$ is a Type-II polyphase ZCP which has ZCZ width of $(N+1)/2$ and magnitude of 2 for every out-of-zone aperiodic auto-correlation sum. By (18), each polyphase sequence in $(\mathbf{c}, \mathbf{d})$ also has a PMEPR of at most 4.

Proof: The proof is straightforward and thus is omitted. ■

V. Conclusions and Open Problems

This paper presents a study on optimal odd-length binary Z-complementary pairs (OB-ZCPs). Motivated by the fact that

all binary Golay complementary pairs (GCPs) are known to have even-lengths of the form $2^\alpha 10^\beta 26^\gamma$ only, our work targets at finding optimal odd-length binary pairs which display closest correlation property to that of GCPs. Such "GCP-like" sequence pairs should meet the following two conditions: (1), each pair has maximum possible zero-correlation zone (ZCZ) width; (2), each has minimum possible magnitude for every out-of-zone aperiodic auto-correlation sum. They may be used as an alternative of GCPs in many engineering applications (e.g., channel estimations) when odd sequence lengths are preferred. Depending on their ZCZs are defined around the in-phase position or the end-shift position, we have studied Type-I OB-ZCPs and Type-II OB-ZCPs, respectively.

We have made the following main contributions in this paper:

1) For a length-N OB-ZCP (Type-I or Type-II), we have shown that when the maximum ZCZ width, i.e., $(N+1)/2$, is achieved, each out-of-zone aperiodic auto-correlation sum has the magnitude lower bound of 2. An OB-ZCP with maximum ZCZ width and minimum out-of-zone magnitude is said to be optimal.
2) By insertion and deletion of certain binary Golay-Davis-Jedwab (GDJ) complementary pairs, we have by *Theorem 4* and *Theorem 5* constructed optimal Type-I OB-ZCPs of lengths 2^m+1 and optimal Type-II OB-ZCPs of lengths $2^m \pm 1$, respectively, where m is a positive integer. Our proposed constructions of optimal Type-I OB-ZCPs have settled the Li-Fan-Tang-Tu open problem in [45] on systematic construction of Type-I OB-ZCP (not necessarily be optimal) with maximum ZCZ width of $(N+1)/2$.
3) We have shown in *Theorem 3* that to construct an optimal OB-ZCP (Type-I or Type-II), it is necessary that its supports form a set of base-two almost difference families (ADF). Moreover, our proposed constructions in *Theorem 4* and *Theorem 5* provide infinite sets of base-two ADF which are useful in partially balanced incomplete block design (BIBD) [46].

We have also performed a search for optimal Type-I OB-ZCPs of lengths 2^m-1 using deletion of all possible binary GDJ complementary pairs. However, it seems that only length-3 optimal Type-I OB-ZCPs can be obtained. For instance, for a binary length-4 GDJ complementary pair $(\mathbf{g},\mathbf{h})$ below, a length-3 optimal Type-I OB-ZCP $(\mathbf{a},\mathbf{b})$ is formed by deleting the last elements[4] of $\mathbf{g}$ and $\mathbf{h}$, respectively.

$$\begin{aligned}&\mathbf{g}=(1,1,1,-1),\ \ \mathbf{a}=(1,1,1),\\ &\mathbf{h}=(1,-1,1,1),\ \ \mathbf{b}=(1,-1,1).\end{aligned}$$

We close this paper by proposing the following open question: are there any systematic constructions of optimal OB-ZCPs (Type-I and Type-II) in lengths other than the ones discussed in this paper? In particular, a generic construction of optimal Type-I OB-ZCPs of lengths 2^m-1 may be interesting.

[4]or the first elements.

APPENDIX A
PROOF OF *Lemma 6*

First, we prove (41). For $0 \le i < j = i+\tau \le 2^{m-1}-1$, let the binary representations of i and j be $\big(i_1, i_2, \cdots, i_{m-1}, 0\big)$ and $\big(j_1, j_2, \cdots, j_{m-1}, 0\big)$, respectively. As a result, the binary representations of $(i+2^{m-1})$ and $(j+2^{m-1})$ are $\big(i_1, i_2, \cdots, i_{m-1}, 1\big)$ and $\big(j_1, j_2, \cdots, j_{m-1}, 1\big)$, respectively. For $\tau > 0$, we have

$$\begin{aligned}&\rho_{\mathbf{g}_0}(\tau)+\rho_{\mathbf{g}_1}(\tau)+\rho_{\mathbf{h}_0}(\tau)+\rho_{\mathbf{h}_1}(\tau)\\ =&\sum_{i=0}^{2^{m-1}-\tau-1}\Big[(-1)^{g_i+g_j}+(-1)^{g_{i+2^{m-1}}+g_{j+2^{m-1}}}\\ &\qquad+(-1)^{h_i+h_j}+(-1)^{h_{i+2^{m-1}}+h_{j+2^{m-1}}}\Big].\end{aligned} \tag{47}$$

Let $\pi(p) = m$. We proceed with the discussions in the following cases.

Case 1: If $1 < p < m$, we have

$$\begin{cases} h_i = g_i + i_{\pi(1)} + c' - c,\\ h_j = g_j + j_{\pi(1)} + c' - c,\\ g_{i+2^{m-1}} = g_i + i_{\pi(p-1)} + i_{\pi(p+1)} + c_{\pi(p)},\\ g_{j+2^{m-1}} = g_j + j_{\pi(p-1)} + j_{\pi(p+1)} + c_{\pi(p)},\end{cases} \tag{48}$$

and

$$\begin{aligned}h_{i+2^{m-1}} &= g_i + i_{\pi(1)} + i_{\pi(p-1)} + i_{\pi(p+1)} + c_{\pi(p)} + c' - c,\\ h_{j+2^{m-1}} &= g_j + i_{\pi(1)} + j_{\pi(p-1)} + j_{\pi(p+1)} + c_{\pi(p)} + c' - c.\end{aligned} \tag{49}$$

Substituting (48) and (49) into (47), we have

$$\rho_{\mathbf{g}_0}(\tau)+\rho_{\mathbf{g}_1}(\tau)+\rho_{\mathbf{h}_0}(\tau)+\rho_{\mathbf{h}_1}(\tau) = 4\sum_{(i,j)\in\mathcal{S}_1}(-1)^{g_i+g_j}, \tag{50}$$

where $\mathcal{S}_1$ is given in (51).

Given permutation π, let the binary permutations of i and j be $\big(i_{\pi(1)}, i_{\pi(2)}, \cdots, i_{\pi(m)}\big)$ and $\big(j_{\pi(1)}, j_{\pi(2)}, \cdots, j_{\pi(m)}\big)$, respectively. Suppose that v is the smallest index for which $i_{\pi(v)} \ne j_{\pi(v)}$, i.e.,

$$\begin{aligned}&\big(j_{\pi(1)}, \cdots, j_{\pi(v-1)}, j_{\pi(v)}, j_{\pi(v+1)}, \cdots, j_{\pi(m)}\big)\\ =&\big(i_{\pi(1)}, \cdots, i_{\pi(v-1)}, 1-i_{\pi(v)}, j_{\pi(v+1)}, \cdots, j_{\pi(m)}\big).\end{aligned} \tag{52}$$

Obviously, $v \ge 2$ and $v \ne p$. It is noted that $v \ne p+1$. Otherwise, $i_{\pi(p-1)} + i_{\pi(p+1)} + j_{\pi(p-1)} + j_{\pi(p+1)} = 1 \pmod 2$ which contradicts with (51). Now, define another pair of integers i' and j' with the following binary permutations, respectively.

$$i'_{\pi(k)} = \begin{cases} 1-i_{\pi(k)}, & \text{for } k = v-1;\\ i_{\pi(k)}, & \text{otherwise,}\end{cases}$$

$$j'_{\pi(k)} = \begin{cases} 1-j_{\pi(k)}, & \text{for } k = v-1;\\ j_{\pi(k)}, & \text{otherwise.}\end{cases}$$

Since $v-1 \ne p$, we have

$$\begin{cases} i'_m = i'_{\pi(p)} = i_m = 0,\\ j'_m = j'_{\pi(p)} = j_m = 0.\end{cases}$$

It follows that $(i', j') \in \mathcal{S}_1$. Following a similar argument in [30, *Theorem 3*], we have

$$(-1)^{g_i+g_j} + (-1)^{g_{i'}+g_{j'}} = 0, \text{ for } (i,j) \in \mathcal{S}_1. \tag{53}$$

$$\mathcal{S}_1=\left\{(i,j)\;\middle|\;\begin{array}{c}0\le i<j=i+\tau\le 2^{m-1}-1, 1<p<m,\\ i_{\pi(1)}+j_{\pi(1)}=0\ (\mathrm{mod}\ 2),\\ i_{\pi(p-1)}+i_{\pi(p+1)}+j_{\pi(p-1)}+j_{\pi(p+1)}=0\ (\mathrm{mod}\ 2)\end{array}\right\}. \tag{51}$$

By (50) and (53), we have

$$\rho_{\mathbf{g}_0}(\tau)+\rho_{\mathbf{g}_1}(\tau)+\rho_{\mathbf{h}_0}(\tau)+\rho_{\mathbf{h}_1}(\tau)=0,\ \text{for}\ \tau\neq 0.$$

Case 2: If $p=m$, we have

$$\rho_{\mathbf{g}_0}(\tau)+\rho_{\mathbf{g}_1}(\tau)+\rho_{\mathbf{h}_0}(\tau)+\rho_{\mathbf{h}_1}(\tau)=4\sum_{(i,j)\in\mathcal{S}_2}(-1)^{g_i+g_j}, \tag{54}$$

where $\mathcal{S}_2$ is shown below.

$$\mathcal{S}_2=\left\{(i,j)\;\middle|\;\begin{array}{c}0\le i<j=i+\tau\le 2^{m-1}-1, p=m,\\ i_{\pi(1)}+j_{\pi(1)}=0\ (\mathrm{mod}\ 2),\\ i_{\pi(m-1)}+j_{\pi(m-1)}=0\ (\mathrm{mod}\ 2)\end{array}\right\}. \tag{55}$$

Similar to the proof for *Case 1*, we have

$$\rho_{\mathbf{g}_0}(\tau)+\rho_{\mathbf{g}_1}(\tau)+\rho_{\mathbf{h}_0}(\tau)+\rho_{\mathbf{h}_1}(\tau)=0,\ \text{for}\ \tau\neq 0.$$

Case 2: If $p=1$, we have

$$\rho_{\mathbf{g}_0}(\tau)+\rho_{\mathbf{g}_1}(\tau)+\rho_{\mathbf{h}_0}(\tau)+\rho_{\mathbf{h}_1}(\tau)=4\sum_{(i,j)\in\mathcal{S}_3}(-1)^{g_i+g_j}, \tag{56}$$

where

$$\mathcal{S}_3=\left\{(i,j)\;\middle|\;\begin{array}{c}0\le i<j=i+\tau\le 2^{m-1}-1, p=1,\\ i_{\pi(2)}+j_{\pi(2)}=0\ (\mathrm{mod}\ 2)\end{array}\right\}. \tag{57}$$

Similar to the proof for *Case 1*, we have

$$\rho_{\mathbf{g}_0}(\tau)+\rho_{\mathbf{g}_1}(\tau)+\rho_{\mathbf{h}_0}(\tau)+\rho_{\mathbf{h}_1}(\tau)=0,\ \text{for}\ \tau\neq 0.$$

Next, we prove (42). By (41) and (58), the proof for (42) follows.

Appendix B
Proof of *Theorem 4*

We prove Case 1 and Case 3 in what follows. The proof for Case 2 and Case 4 can be obtained easily by similar arguments for Case 1 and Case 3, respectively.

Proof for Case 1: By (45), for $\tau>0$, we have

$$\begin{aligned}&\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau)\\ =&\underbrace{\rho_{\mathbf{g}}(\tau)+\rho_{\mathbf{h}}(\tau)}_{=0}+(-1)^{d_1+g_{\tau-1}}+(-1)^{d_2+h_{\tau-1}}\\ =&(-1)^{g_{\tau-1}}\left[(-1)^{d_1}+(-1)^{d_2+(\tau-1)_{\pi(1)}+c'-c}\right]\\ =&(-1)^{d_1+g_{\tau-1}}\left[1+(-1)^{1+(\tau-1)_m}\right],\end{aligned} \tag{59}$$

where $(\tau-1)_m$ denotes the mth the bit of the binary representation of $\tau-1$. Note that the last step of (59) is obtained by substituting the constraints of Case 1. With

$$(\tau-1)_m=\begin{cases}0, & \text{for } 1\le\tau\le 2^{m-1}\\ 1, & \text{for } 2^{m-1}+1\le\tau\le 2^m-1.\end{cases} \tag{60}$$

we assert that the $(\mathbf{a},\mathbf{b})$ in Case 1 is an optimal Type-I OB-ZCP of length 2^m+1.

Proof for Case 3: By (45), for $\tau>0$, we have

$$\begin{aligned}&\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau)\\ =&\underbrace{\rho_{\mathbf{g}}(\tau)+\rho_{\mathbf{h}}(\tau)}_{=0}+(-1)^{d_1+g_{\tau-1}}+(-1)^{d_2+h_{2^m-\tau}}\\ =&(-1)^{d_1+g_{\tau-1}}+(-1)^{d_2+g_{2^m-\tau}+(2^m-\tau)_{\pi(1)}+c'-c},\end{aligned} \tag{61}$$

where $(2^m-\tau)_{\pi(1)}$ denotes the $\pi(1)$th bit of the binary representation of $2^m-\tau$. Note that $2^m-1=(\tau-1)+(2^m-\tau)$. Suppose that $(x_1,x_2,\cdots,x_m)$ is the binary representation of $\tau-1$, then the binary representation of $2^m-\tau$ will be $(1-x_1,1-x_2,\cdots,1-x_m)$. Therefore, we have

$$g_{2^m-\tau}\equiv g_{\tau-1}+m+1+(\tau-1)_{\pi(1)}+(\tau-1)_{\pi(m)}+\sum_{k=1}^{m}c_k\ (\mathrm{mod}\ 2). \tag{62}$$

By (62) and the constraints of Case 3, (61) can be simplified to

$$\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau)=(-1)^{d_1+g_{\tau-1}}\left[1+(-1)^{1+(\tau-1)_m}\right]. \tag{63}$$

With (60), we assert that the $(\mathbf{a},\mathbf{b})$ in Case 3 is an optimal Type-I OB-ZCP of length 2^m+1.

Appendix C
Proof of *Theorem 5*

The proof for Case 1-4 in *Theorem 5* can be obtained easily by the similar arguments for that of Case 1-4 in *Theorem 4*, respectively. We present the proof for Case 1 and Case 5-8 as follows.

Proof for Case 1: By (45), for $\tau>0$, we have

$$\rho_{\mathbf{c}}(\tau)+\rho_{\mathbf{d}}(\tau)=(-1)^{d_1+g_{\tau-1}}\left[1+(-1)^{(\tau-1)_m}\right]. \tag{64}$$

With (60), we assert that the $(\mathbf{c},\mathbf{d})$ in Case 1 is an optimal Type-II OB-ZCP of length 2^m+1.

Proof for Case 5: By (45), for $1\le\tau\le 2^{m-1}$, we have

$$\begin{aligned}&\rho_{\mathbf{c}}(\tau)+\rho_{\mathbf{d}}(\tau)\\ =&\underbrace{\rho_{\mathbf{g}_0}(\tau)+\rho_{\mathbf{h}_0}(\tau)+\rho_{\mathbf{g}_1}(\tau)+\rho_{\mathbf{h}_1}(\tau)}_{=0}\\ &+\underbrace{\rho_{\mathbf{g}_1,\mathbf{g}_0}(2^{m-1}-\tau+1)+\rho_{\mathbf{h}_1,\mathbf{h}_0}(2^{m-1}-\tau+1)}_{=0}\\ &+(-1)^{d_1}\left[(-1)^{g_{2^{m-1}-\tau}}+(-1)^{g_{2^{m-1}+\tau-1}}\right]\\ &+(-1)^{d_2}\left[(-1)^{h_{2^{m-1}-\tau}}+(-1)^{h_{2^{m-1}+\tau-1}}\right]\\ =&(-1)^{d_1}\left[(-1)^{g_{2^{m-1}-\tau}}+(-1)^{g_{2^{m-1}+\tau-1}}\right]\\ &+(-1)^{d_2}\left[(-1)^{h_{2^{m-1}-\tau}}+(-1)^{h_{2^{m-1}+\tau-1}}\right]\end{aligned} \tag{65}$$

$$\rho_{\mathbf{g}}(\tau)+\rho_{\mathbf{h}}(\tau)=\begin{cases}\rho_{\mathbf{g}_0}(\tau)+\rho_{\mathbf{g}_1}(\tau)+\rho_{\mathbf{h}_0}(\tau)+\rho_{\mathbf{h}_1}(\tau),\\ \quad+\rho_{\mathbf{g}_1,\mathbf{g}_0}(2^{m-1}-\tau)+\rho_{\mathbf{h}_1,\mathbf{h}_0}(2^{m-1}-\tau), & \text{for } 1\le\tau\le 2^{m-1}-1;\\ \rho_{\mathbf{g}_0,\mathbf{g}_1}(\tau-2^{m-1})+\rho_{\mathbf{h}_0,\mathbf{h}_1}(\tau-2^{m-1}), & \text{for } 2^{m-1}\le\tau\le 2^m-1.\end{cases} \tag{58}$$

where the last step of (65) is obtained by the property in *Lemma 6*. For any permutation π, since

$$\begin{aligned}&g_{2^{m-1}-\tau}+h_{2^{m-1}-\tau}+g_{2^{m-1}+\tau-1}+h_{2^{m-1}+\tau-1}\\ &\equiv(2^{m-1}-\tau)_{\pi(1)}+(2^{m-1}+\tau-1)_{\pi(1)}\\ &\equiv 1 \pmod 2,\end{aligned} \tag{66}$$

thus

$$\begin{aligned}(-1)^{g_{2^{m-1}-\tau}}+(-1)^{g_{2^{m-1}+\tau-1}}&=0,\\ (-1)^{h_{2^{m-1}-\tau}}+(-1)^{h_{2^{m-1}+\tau-1}}&=\pm 2,\end{aligned} \tag{67}$$

or

$$\begin{aligned}(-1)^{g_{2^{m-1}-\tau}}+(-1)^{g_{2^{m-1}+\tau-1}}&=\pm 2,\\ (-1)^{h_{2^{m-1}-\tau}}+(-1)^{h_{2^{m-1}+\tau-1}}&=0.\end{aligned} \tag{68}$$

Therefore, for $1\le\tau\le 2^{m-1}$, we have $\rho_{\mathbf{c}}(\tau)+\rho_{\mathbf{d}}(\tau)=\pm 2$. On the other hand, for $2^{m-1}+1\le\tau\le 2^m$,

$$\rho_{\mathbf{c}}(\tau)+\rho_{\mathbf{d}}(\tau)=\rho_{\mathbf{g}_0,\mathbf{g}_1}(\tau-2^{m-1}-1)+\rho_{\mathbf{h}_0,\mathbf{h}_1}(\tau-2^{m-1}-1)=0.$$

Hence, we assert that $(\mathbf{c},\mathbf{d})$ in Case 5 is an optimal Type-II OB-ZCP of length 2^m+1.

Proof for Case 6: By (46), for $d=0$ and $\tau>0$, we have

$$\begin{aligned}&\rho_{\mathbf{c}}(\tau)+\rho_{\mathbf{d}}(\tau)\\ =&(-1)^{g_0+g_\tau+1}+(-1)^{h_0+h_\tau+1}\\ =&(-1)^{g_0+g_\tau+1}\left[1+(-1)^{\tau_{\pi(1)}}\right]\end{aligned} \tag{69}$$

With $\pi(1)=m$ and

$$\tau_m=\begin{cases}0, & \text{for } 1\le\tau\le 2^{m-1}-1,\\ 1, & \text{for } 2^{m-1}\le\tau\le 2^m-1\end{cases} \tag{70}$$

we assert that the $(\mathbf{c},\mathbf{d})$ in Case 6 for $d=0$ is an optimal Type-II OB-ZCP of length 2^m-1. In a similar argument, we can prove Case 6 for $d=1$.

Proof for Case 7: By (46), for $d=0$ and $\tau>0$, we have

$$\rho_{\mathbf{c}}(\tau)+\rho_{\mathbf{d}}(\tau)=(-1)^{g_0+g_\tau+1}+(-1)^{h_{2^m-1}+h_{2^m-\tau-1}+1}. \tag{71}$$

Suppose that $(x_1,x_2,\cdots,x_m)$ is the binary representation of τ, then the binary representation of $2^m-\tau-1$ will be $(1-x_1,1-x_2,\cdots,1-x_m)$. Similar to (62), we have

$$g_{2^m-\tau-1}\equiv g_\tau+m+1+\tau_{\pi(1)}+\tau_{\pi(m)}+\sum_{k=1}^{m}c_k \pmod 2. \tag{72}$$

With $\pi(m)=m$ and (72), we have

$$\rho_{\mathbf{c}}(\tau)+\rho_{\mathbf{d}}(\tau)=(-1)^{g_0+g_\tau+1}\left[1+(-1)^{\tau_m}\right]. \tag{73}$$

Recalling (70) completes the proof of Case 7 for $d=0$. In a similar argument, we can prove Case 7 for $d=1$.

Proof for Case 8: By (46), for $1\le\tau\le 2^{m-1}-1$, we have

$$\begin{aligned}&\rho_{\mathbf{c}}(\tau)+\rho_{\mathbf{d}}(\tau)\\ =&\underbrace{\rho_{\mathbf{g}_0}(\tau)+\rho_{\mathbf{h}_0}(\tau)\rho_{\mathbf{g}_1}(\tau)+\rho_{\mathbf{h}_1}(\tau)}_{=0}\\ &+\underbrace{\rho_{\mathbf{g}_1,\mathbf{g}_0}(2^{m-1}-\tau-1)+\rho_{\mathbf{h}_1,\mathbf{h}_0}(2^{m-1}-\tau-1)}_{=0}\\ &+(-1)^{g_{2^{m-1}-d_1}+1}\left[(-1)^{g_{2^{m-1}+\tau}}+(-1)^{g_{2^{m-1}-\tau-1}}\right]\\ &+(-1)^{h_{2^{m-1}-d_2}+1}\left[(-1)^{h_{2^{m-1}+\tau}}+(-1)^{h_{2^{m-1}-\tau-1}}\right]\\ =&(-1)^{g_{2^{m-1}-d_1}+1}\left[(-1)^{g_{2^{m-1}+\tau}}+(-1)^{g_{2^{m-1}-\tau-1}}\right]\\ &+(-1)^{h_{2^{m-1}-d_2}+1}\left[(-1)^{h_{2^{m-1}+\tau}}+(-1)^{h_{2^{m-1}-\tau-1}}\right],\end{aligned} \tag{74}$$

where the last step of (74) is obtained by the property in *Lemma 6*. Similar to (66), for any permutation π, we have

$$\begin{aligned}&g_{2^{m-1}+\tau}+h_{2^{m-1}+\tau}+g_{2^{m-1}-\tau-1}+h_{2^{m-1}-\tau-1}\\ &\equiv(2^{m-1}+\tau)_{\pi(1)}+(2^{m-1}-\tau-1)_{\pi(1)}\\ &\equiv 1 \pmod 2.\end{aligned} \tag{75}$$

Thus,

$$\begin{aligned}(-1)^{g_{2^{m-1}+\tau}}+(-1)^{g_{2^{m-1}-\tau-1}}&=0,\\ (-1)^{h_{2^{m-1}+\tau}}+(-1)^{h_{2^{m-1}-\tau-1}}&=\pm 2,\end{aligned} \tag{76}$$

or

$$\begin{aligned}(-1)^{g_{2^{m-1}+\tau}}+(-1)^{g_{2^{m-1}-\tau-1}}&=\pm 2,\\ (-1)^{h_{2^{m-1}+\tau}}+(-1)^{h_{2^{m-1}-\tau-1}}&=0.\end{aligned} \tag{77}$$

Therefore, for $1\le\tau\le 2^{m-1}-1$, we have $\rho_{\mathbf{c}}(\tau)+\rho_{\mathbf{d}}(\tau)=\pm 2$. On the other hand, for $2^{m-1}\le\tau\le 2^m-2$,

$$\rho_{\mathbf{c}}(\tau)+\rho_{\mathbf{d}}(\tau)=\rho_{\mathbf{g}_0,\mathbf{g}_1}(\tau-2^{m-1})+\rho_{\mathbf{h}_0,\mathbf{h}_1}(\tau-2^{m-1})=0.$$

Hence, we assert that the $(\mathbf{c},\mathbf{d})$ in Case 8 is an optimal Type-II OB-ZCP of length 2^m-1.

REFERENCES

[1] M. J. E. Golay, "Statatic multislit spectroscopy and its application to the panoramic display of infrared spectra," *J. Opt. Soc. Amer.*, vol. 41, pp. 468-472, 1951.

[2] M. J. E. Golay, "Complementary series," *IRE Trans. Inf. Theory*, vol. IT-7, pp. 82-87, Apr. 1961.

[3] M. Griffin, "There are no Golay complementary sequences of length 2×9^t," *Aequationes Math.*, vol. 15, pp. 73-77, 1977.

[4] S. Kounias, C. Koukouvinos, and K. Sotirakoglou "On Golay sequences," *Discrete Mathematics*, vol. 92, pp. 177-185, 1991.

[5] S. Eliahou, M. Kervaire, and B. Saffari, "A new restriction on the lengths of Golay complementary sequences," *Journ. Comb. Theory*, Ser. A 55, pp. 49-59, Sept. 1990.

[6] P. Fan and M. Darnell, "Sequence Design for Communications Applications". New York: Wiley, 1996.

[7] M. G. Parker, K. G. Paterson, and C. Tellambura, "Golay complementary sequences," *Wiley Encyclopedia of Telecommunications*, J. G. Proakis, Ed. New York: Wiley Interscience, 2002.

[8] P. B. Borwein and R. A. Ferguson, "A complete description of Golay pairs for lengths up to 100," *Mathematics of Computation*, vol. 73, pp. 967-985, July 2003.

[9] P. Fan, W. Yuan, and Y. Tu, "Z-complementary binary sequences," *IEEE Signal Process. Lett.*, vol. 14, pp. 401-404, Aug. 2007.

[10] P. Spasojevic and C. N. Georghiades, "Complementary sequences for ISI channel estimation," *IEEE Trans. Inf. Theory*, vol. 47, pp. 1145-1152, Mar. 2001.

[11] S. Wang, A. Abdi, "MIMO ISI channel estimation using uncorrelated Golay complementary sets of polyphase sequences," *IEEE Trans. Veh. Tech.*, vol. 56, pp. 3024-3040, Sept. 2007.

[12] G. Welti, "Quaternary codes for pulsed radar," *IRE Trans. Inf. Theory*, vol. II-6, pp. 400-408, June 1960.

[13] R. Turyn, "Ambiguity functions of complementary sequences," *IEEE Trans. Inf. Theory*, vol. IT-9, pp. 46-47, Jan. 1963.

[14] S. Z. Budisin, "Efficient pulse compressor for Golay complementary sequences," *IEE Electron. Lett.*, vol. 27, pp. 219-220, Jan. 1991.

[15] A. Pezeshki, A. R. Calderbank, W. Moran, and S. D. Howard, "Doppler resilient Golay complementary waveforms," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4254-4266, Sept. 2008.

[16] C. Tseng and C. Liu, "Complementary sets of sequences," *IEEE Trans. Inf. Theory,* vol. IT-18, pp. 644-665, Sept. 1972.

[17] N. Suehiro and M. Hatori, "N-Shift cross-orthogonal sequences," *IEEE Trans. Inf. Theory,* vol. IT-34, pp. 143-146, Jan. 1988.

[18] K. G. Paterson, "Generalized Reed-Muller codes and power control in OFDM modulation," *IEEE Trans. Inf. Theory*, vol. 46, pp. 104-120, Jan. 2000.

[19] A. Rathinakumar and A. K. Chaturvedi, "Complete mutually orthogonal Golay complementary sets from Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 54, pp. 1339-1346, Mar. 2008.

[20] Z. Liu, Y. L. Guan and U. Parampalli, "New Complete Complementary Codes for the Peak-to-Mean Power Control in MC-CDMA," *IEEE Trans. Commun.*, vol. 62, pp. 1105-1113, Mar. 2014.

[21] H. H. Chen, J. F. Yeh, and N. Seuhiro, "A multicarrier CDMA architecture based on orthogonal complementary codes for new generations of wideband wireless communications," *IEEE Commun. Magazine*, vol. 39, pp. 126-135, Oct. 2001.

[22] H. H. Chen, *The Next Generation CDMA Techonolgies*, John Wiley & Sons, July 2007.

[23] Z. Liu, Y. L. Guan and H. H. Chen, "Fractional-Delay-Resilient Receiver for Interference-Free MC-CDMA Communications Based on Complete Complementary Codes," *IEEE Trans. Wireless Commun.*, Jan. 2014. Submitted for publication.

[24] L. R. Welch, "Lower bounds on the maximum cross-correlation of signals," *IEEE Trans. Inf. Theory,* vol. IT-20, pp. 397-399, May 1974.

[25] Z. Liu, Y. L. Guan, B. C. Ng, and H. H. Chen, "Correlation and set size bounds of complementary sequences with low correlation zones," *IEEE Trans. Commun.*, vol. 59, pp. 3285-3289, Dec. 2011.

[26] Z. Liu, U. Parampalli, Y. L. Guan and S. Boztaş, "Constructions of optimal and near-optimal quasi-complementary sequence sets from Singer difference sets," *IEEE Wireless Commun. Letters*, vol. 2, pp. 487-490, Oct. 2013.

[27] Z. Liu, Y. L. Guan, and W. H. Mow, "Improved lower bound for quasi-complementary sequence sets," in *Proc. 2011 IEEE Int. Symposium on Information Theory (ISIT'2011)*, St. Petersburg, Russia, Aug. 2011, pp. 489-493.

[28] Z. Liu, Y. L. Guan and W. H. Mow, "A tighter correlation lower bound for quasi-complementary sequence sets," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 388-396, Jan. 2014.

[29] B. M. Popović, "Synthesis of power efficient multitone signals with flat amplitude spectrum," *IEEE Trans. Commun.,* vol. 39, pp. 1031-1033, July 1991.

[30] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2397-2417, Nov. 1999.

[31] C. Rößing and V. Tarokh, "A construction of 16-QAM Golay complementary sequences," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 2091-2093, Jul. 2001.

[32] C. V. Chong, R.Venkataramani, and V. Tarokh, "A new construction of 16-QAM Golay complementary sequences," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 2953-2959, Nov. 2003.

[33] Y. Li, "A Construction of General QAM Golay Complementary Sequences," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5765-5771, Nov. 2010.

[34] Z. Liu, Y. Li, and Y. L. Guan, "New constructions of general QAM Golay complementary sequences," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7684-7692, Nov. 2013.

[35] K.-U. Schmidt, "On cosets of the generalized first-order Reed-Muller code with low PMEPR," *IEEE Trans. Inf. Theory*, vol. 52, pp. 3220-3232, July 2006.

[36] N. Y. Yu and G. Gong, "Near-complementary sequences with low PMEPR for peak power control in multicarrier communications," *IEEE Trans. Inf. Theory*, vol. 57, pp. 505-513, Jan. 2011.

[37] N. Suehiro, "A signal design without co-channel interference for approximately synchronized CDMA system," *IEEE J. Sel. Areas Commun.*, vol. 12, pp. 837-841, June 1994.

[38] B. Long, P. Zhang, and J. Hu, "A generalised QS-CDMA system and the design of new spreading codes," *IEEE Trans. Veh. Technol.*, vol. 47, pp. 1268-1275, Nov. 1998.

[39] P. Fan, N. Suehiro, N. Kuroyanagi, and X. Deng, "A class of binary sequences with zero correlation zone," *Electron. Lett.*, vol. 35, pp. 77-79, May 1999.

[40] X. Tang, P. Fan, and J. Lindner, "Multiple binary ZCZ sequence sets with good cross-correlation property based on complementary sequence sets," *IEEE Trans. Inf. Theory*, vol. 56, pp. 4038-4045, Aug. 2010.

[41] X. Tang and W. H. Mow, "Design of spreading codes for quasi-synchronous CDMA with intercell interference," *IEEE J. Sel. Areas Commun.*, vol. 24, pp. 84-93, Jan. 2006.

[42] J. Li, A. Huang, M. Guizani, and H. H. Chen, "Inter-group complementary codes for interference-resistant CDMA wireless communications," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 166-174, Jan. 2008.

[43] William C. Y. Lee, *Mobile Communications Design Fundamentals*, 2nd ed., New York, John Wiley & Sons, Inc., 1993.

[44] J. S. Lee and L. E. Miller, *CDMA Systems Engineering Handbook*, Mobile Communications series, Artech House Publishers, 1998.

[45] X. Li, P. Fan, X. Tang, Y. Tu, "Existence of binary Z-complementary pairs," *IEEE Signal Process. Lett.*, vol. 18, pp. 63-66, Jan. 2011.

[46] C. Ding and J. Yin, "Constructions of almost difference families," *Discrete Mathematics*, vol. 308, pp. 4941-4954, 2008.

[47] C. Ding, T. Helleseth, and K. Y. Lam, "Several classes of binary sequences with three-level autocorrelation," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2606-2612, Nov. 1999.

[48] X. Wang and D. Wu, "The existence of almost difference families," *Journal of Statistical Planning and Inference*, vol. 139, pp. 4200-4205, 2009.

[49] X. Wang and J. Wang, "A note on cyclic almost difference families," *Discrete Mathematics*, vol. 311, pp. 628-633, 2011.

[50] J. S. Wallis, "Some remarks on supplementary difference sets," *Infinite and Finite Sets*, vol. III, pp. 1503-1526, North-Holland, Amsterdam, 1975.

[51] C. Ding, "Two constructions of $(v, (v-1)/2, (v-3)/2)$ difference families," *J. Combinatorial Designs*, vol. 16, pp. 164-171, 2008.

[52] D. Ž. Doković, "Cyclic $(v; r, s; \lambda)$ difference families with two base blocks and $v \leq 50$," *Ann. Comb.*, vol. 15, pp. 233-254, 2011.

[53] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar, and H. Martinsen, "Almost difference sets and their sequences with optimal autocorrelation," *IEEE Trans. Inf. Theory*, vol. 47, pp. 2934-2943, Nov. 2001.

[54] L. Bömer and M. Antweiler, "Periodic Complimentary Binary Sequences," *IEEE Trans. Inf. Theory,* vol. 36, pp. 1487-1494, Nov. 1990.