On optimal binary Z-complementary pair of odd period

Zilong Liu, Yong Liang Guan
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore
Email: {zilongliu,eylguan}@ntu.edu.sg

Udaya Parampalli
Department of Computer Science and Software Engineering
University of Melbourne
VIC 3010, Australia
Email: udaya@cs.mu.oz.au

***Abstract*—In this paper we introduce the optimal odd-period binary Z-complementary pairs (OB-ZCPs), which display properties similar to Golay complementary pairs. These pairs have the maximum possible zero-correlation-zone (ZCZ) of width $(N+1)/2$, where N denotes the sequence length, and the minimum possible magnitude of 2 for each *out-of-zone aperiodic auto-correlation sum*. Furthermore, we show that the optimal OB-ZCPs correspond to sets of almost difference families and present some of their interesting properties.**

I. INTRODUCTION

Let $\mathbf{a}=\{a_i\}$ and $\mathbf{b}=\{b_i\}$ be two N-length binary sequences, then the aperiodic cross-correlation function (ACCF) is defined as

$$\rho_{\mathbf{a},\mathbf{b}}(\tau)=\sum_{i=0}^{N-1-\tau}(-1)^{a_i+b_{i+\tau}},\quad 0\leq\tau\leq N-1. \tag{1}$$

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).

A pair of sequences is called a Golay complementary pair (GCP) if their aperiodic autocorrelation sums are equal to zero for all non-zero time shifts [1]. Golay complementary pairs, first introduced by Marcel Golay in 1961 in the context of an optical problem in multislit spectrometry, have been used extensively in communication engineering.

It is conjectured that binary GCPs can only be found for sequence lengths of the form $2^{\alpha}10^{\beta}26^{\gamma}$, where α,β,γ are non-negative integers. This has been verified for binary GCPs of length up to 100 [2]. In this paper we are concerned with binary sequence pairs of odd length, which are not in the form $2^{\alpha}10^{\beta}26^{\gamma}$.

For sequence lengths which are not in the form of $2^{\alpha}10^{\beta}26^{\gamma}$, Fan *et al* proposed the binary Z-complementary pair (ZCP), whose non-trivial aperiodic autocorrelation sums are zero within a window which is less than the whole sequence length [3]. A pair $(\mathbf{a},\mathbf{b})$ is said to be a Z-complementary pair (ZCP) of zero-correlation-zone (ZCZ) Z if and only if

$$\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau)=0,\quad \text{for } 1\leq\tau\leq Z-1. \tag{2}$$

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 autocorrelation sum* of $\mathbf{a}$ and $\mathbf{b}$ at time-shift τ. When $Z=N$, each ZCP is reduced to a GCP [1].

The following result from [4] gives us the maximum possible ZCZ length for an OB-ZCP pair.

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

$$Z\leq(N+1)/2, \tag{3}$$

where N denotes the sequence length.

In this paper we are concerned with binary sequence pairs of odd-period which display properties closer to those of GCPs. We prove the following theorem.

***Theorem** 1:* The magnitude of each *out-of-zone aperiodic auto-correlation sum (OZ-AAS)* for any Z*-optimal* odd-period binary ZCP (OB-ZCP) $(\mathbf{a},\mathbf{b})$ takes on the value of $2p$, where p is a positive odd integer. In other words,

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

It should be noted that in practice, the magnitudes of the *out-of-zone aperiodic autocorrelation sums* of the ZCP should also be minimized. This is because in CDMA communication, lower *out-of-zone aperiodic autocorrelation sums* will improve the code-acquisition detection probability in the noise channel [5]. These observations motivate us to introduce the following optimality criteria for OB-ZCPs.

***Definition** 1 (Z-Optimal odd-period binary ZCP):* An odd-period binary ZCP is said to be Z*-optimal* if $Z=(N+1)/2$.

***Definition** 2 (Optimal odd-period binary ZCP):* An OB-ZCP is said to be *optimal* if it is Z*-optimal* and each *out-of-zone aperiodic autocorrelation sum* takes on the magnitude of 2.

In this paper, we further establish a connection between the *optimal* OB-ZCPs to sets of almost difference families (ADF) introduced by C. Ding [6]. We show that each *optimal* OB-ZCP corresponds to a set of almost difference families (ADF) [6]. In addition, we present several interesting properties of the *optimal* OB-ZCPs.

This paper is organized as follows. In Section II, we give prelimaries needed for the paper and review the ADF. In Section III, we prove Theorem 1, the main result of the paper. Section IV demonstrates a connection between OB-ZCPs and the ADF. In Section V, we present several interesting properties for the optimal OB-ZCPs. We summarize this paper in Section VI.

II. Preliminaries

The following notations will be used throughout this paper.

– $\mathbf{Z}_q = \{0, 1, \cdots, q-1\}$ is the set of integers modulo q;
– $\underline{\mathbf{a}}$ denotes the reversal of sequence $\mathbf{a}$;
– For length-N binary sequence $\mathbf{a} = (a_0, a_1, \cdots, a_{N-1})$ over $\mathbf{Z}_2$, denote by $\mathbf{a}(z)$ the associated polynomial of z as follows,

$$\mathbf{a}(z) = \sum_{\tau=0}^{N-1} (-1)^{a_\tau} z^\tau. \tag{4}$$

A. Almost difference families (ADF)

Define the *support* of $\mathbf{a}$, a binary length-N sequence over $\mathbf{Z}_2$, as follows,

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

$\mathbf{a}$ is called the *characteristic sequence* of $C_{\mathbf{a}}$. Also, denote by $|C_{\mathbf{a}}|$ the number of elements in $C_{\mathbf{a}}$.

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

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

Given the *support* of any binary sequence $\mathbf{a}$, the periodic auto-correlation function of $\mathbf{a}$ can be expressed as [9]

$$\theta_{\mathbf{a}}(\tau) = N - 4(k - d_{C_{\mathbf{a}}}(\tau)), \tag{5}$$

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

Let $\mathcal{D} = \{D_0, D_1\}$, where D_0 and D_1 are the *supports* of the 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

$$d_{\mathcal{D}}(\tau) = d_{D_0}(\tau) + d_{D_1}(\tau) \tag{6}$$

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 will also be called a base, and therefore, $\mathcal{D}$ will also be called a set of ADF of two bases. Although there are ADF of more than 2 bases [6], they are not our research focus in this paper. Note that ADF are a generalization of the *difference families (DF)* (where $\nu = N-1$) [7],[8]. ADF may also be regarded a generalization of the almost difference set (ADS) which is useful in optimal binary sequence design and cryptography [6]. For more information on ADS, the readers are referred to [9],[10].

Obviously, the necessary condition for the existence of the ADF of two bases is that

$$\sum_{i=0}^{1} g_i(g_i - 1) = \nu\lambda + (N-1-\nu)(\lambda+1). \tag{7}$$

By (5) and (6), we have [11]

$$\begin{aligned} &\theta_{\mathbf{a}}(\tau) + \theta_{\mathbf{b}}(\tau) \\ &= \begin{cases} 2N, & \text{for } \tau = 0; \\ 2N - 4\left(g_0 + g_1 - d_{\mathcal{D}}(\tau)\right), & \text{for } \tau > 0. \end{cases} \end{aligned} \tag{8}$$

By (8) have,

***Lemma** 2:* $\mathcal{D}$ is a set of

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

ADF if and only if

$$\theta_{\mathbf{a}}(\tau) + \theta_{\mathbf{b}}(\tau) = \pm 2. \tag{9}$$

Moreover, an odd-period binary sequence $\mathbf{a}$ is said to be *balanced* if $g_0 = (N-1)/2$ or $(N+1)/2$. The same can be said for binary sequence $\mathbf{b}$ by replacing g_0 with g_1.

III. Proof of Theorem 1

We first prove that each *out-of-zone aperiodic autocorrelation sum* of the odd-period binary Z-complementary pair (OB-ZCP) has a magnitude lower bound of 2.

For a *Z-optimal* OB-ZCP $(\mathbf{a}, \mathbf{b})$, we have $Z = (N+1)/2$, i.e.,

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

where $\oplus$ denotes the modulo 2 addition, and $1 \leq \tau \leq (N-1)/2$. Therefore,

$$\sum_{i=0}^{N-1-\tau} \Big[a_i \oplus a_{i+\tau} + b_i \oplus b_{i+\tau}\Big] = N - \tau, \tag{10}$$

for $1 \leq \tau \leq (N-1)/2$. Let

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

By (10), we have

$$\begin{aligned} \mathcal{S}_{\mathbf{a},\mathbf{b}}(\tau) &\equiv N - \tau \pmod 2 \\ &\equiv \tau + 1 \pmod 2, \quad \text{for } 1 \leq \tau \leq n-1. \end{aligned} \tag{11}$$

We note that

Remark 1: For $1 \le \tau \le (N-1)/2$,

$$\mathcal{S}_{\mathbf{a},\mathbf{b}}(\tau) \equiv \mathcal{S}_{\mathbf{a},\mathbf{b}}(N-\tau) \pmod 2.$$

Proof: By noting

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

and

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

completes the proof. ■

For $1 \le \tau \le (N-1)/2$, we have

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

This completes the proof of Theorem 1.

We have shown certain *optimal* OB-ZCPs of lengths up to 25 in TABLE I. For convenience, these *optimal* OB-ZCPs are shown over $\{1,-1\}$.

IV. Connection between the optimal OB-ZCPs and the Almost Difference Families

We have the following theorem.

***Theorem** 2:* The necessary condition to build an *optimal* OB-ZCP is that the *supports* of $(\mathbf{a},\mathbf{b})$ form a set of

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

ADF. Moreover, it is reduced to a set of

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

Difference Families (DF) if the following equation is satisfied:

$$\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau) = -2, \quad \text{for any } (N+1)/2 \le \tau \le N-1. \tag{12}$$

Proof: Starting from an optimal OB-ZCP, 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 $1 \le \tau \le N-1$,

$$\begin{aligned}&\Big|\theta_{\mathbf{a}}(\tau)+\theta_{\mathbf{b}}(\tau)\Big|\\ &= \Big|\underbrace{\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau)}+\underbrace{\rho_{\mathbf{a}}(N-\tau)+\rho_{\mathbf{b}}(N-\tau)}\Big|\\ &= 2.\end{aligned} \tag{13}$$

Recalling ***Lemma** 2* completes the proof. ■

V. Properties of the optimal odd-period binary ZCP

In this section, we give several properties of the *optimal* OB-ZCPs. Again, Let g_0 and g_1 denote the numbers of ones in $\mathbf{a}$ and $\mathbf{b}$, respectively.

A. Property 1

$$\begin{cases} a_0+a_{N-1}+b_0+b_{N-1} & \equiv\ 0 \pmod 2,\\ a_r+a_{N-1-r}+b_r+b_{N-1-r} & \equiv\ 1 \pmod 2\end{cases} \tag{14}$$

where $1 \le r \le (N-3)/2$.

Proof: 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,

$$a_0+a_{N-1}+b_0+b_{N-1} \equiv 0 \pmod 2. \tag{15}$$

Also,

$$\begin{aligned}&\rho_{\mathbf{a}}(N-2)+\rho_{\mathbf{b}}(N-2)\\ &=4-2\Big[a_0\oplus a_{N-2}+a_1\oplus a_{N-1}+b_0\oplus b_{N-2}+b_1\oplus b_{N-1}\Big]\\ &=\pm 2,\end{aligned} \tag{16}$$

therefore,

$$\begin{aligned}&\underbrace{a_0+a_{N-1}+b_0+b_{N-1}}\\ &\quad+\underbrace{a_1+a_{N-2}+b_1+b_{N-2}} \equiv 1 \pmod 2,\end{aligned} \tag{17}$$

leading to

$$a_1+a_{N-2}+b_1+b_{N-2} \equiv 1 \pmod 2. \tag{18}$$

TABLE I
OPTIMAL BINARY ZCPS OF ODD-PERIOD UP TO 25

N	$\begin{pmatrix} (-1)^{\mathbf{a}} \\ (-1)^{\mathbf{b}} \end{pmatrix}$	$\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau), \tau \geq (N+1)/2$
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	$\begin{pmatrix} +++-+--++-+-+-+--+++-++++ \\ +--+----+--++-++++---++++ \end{pmatrix}$	$(-2,2,-2,-2,2,-2,-2,-2,2,2,2,2)$

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

$$a_r + a_{N-1-r} + b_r + b_{N-1-r} \equiv 1 \pmod 2 \tag{19}$$

holds for any $1 \leq r \leq (N-3)/2$. ■

***Remark** 2:* In contrast to (14), it is noted that the binary Golay complementary pair (GCP) should have an even length and satisfy the following condition:

$$a_r + a_{N-1-r} + b_r + b_{N-1-r} \equiv \ 1 \pmod 2 \tag{20}$$

for any $0 \leq r \leq N-1$.

B. Property 2

$$\begin{aligned} &\overbrace{N + \sum_{\tau=(N+1)/2}^{N-1} \Big[\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau)\Big]} \\ &\quad = (g_0-g_1)^2 + (N-g_0-g_1)^2 \\ &1 \leq (g_0-g_1)^2 + (N-g_0-g_1)^2 \leq 2N-1. \end{aligned} \tag{21}$$

Proof: Recall the associated polynomial defined in Section II, for $z \neq 0$, it is easy to show that

$$\begin{aligned} &\mathbf{a}(z)\mathbf{a}(z^{-1})+\mathbf{b}(z)\mathbf{b}(z^{-1}) \\ =&\sum_{\tau=0}^{N-1}\Big[\big(\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau)\big)\cdot\big(z^{\tau}+z^{-\tau}\big)\Big] \\ =&2N+\sum_{\tau=(N+1)/2}^{N-1}\Big[\big(\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau)\big)\cdot\big(z^{\tau}+z^{-\tau}\big)\Big]. \end{aligned} \tag{22}$$

Now setting $z=1$, and recalling the ZCZ property of the *optimal* OB-ZCP, we have

$$\begin{aligned} &\Big|\mathbf{a}(1)\Big|^2+\Big|\mathbf{b}(1)\Big|^2 \\ =&(N-2g_0)^2+(N-2g_1)^2 \\ =&\rho_{\mathbf{a}}(0)+\rho_{\mathbf{b}}(0)+2\sum_{\tau=(N+1)/2}^{N-1}\Big[\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau)\Big] \\ =&2N+2\sum_{\tau=(N+1)/2}^{N-1}\Big[\rho_{\mathbf{a}}(\tau)+\rho_{\mathbf{b}}(\tau)\Big]. \end{aligned} \tag{23}$$

Dividing both sides of (23) by 2 completes the proof for the first equation of (21). By recalling the *out-of-zone aperiodic auto-correlation sum properties* of the *optimal* OB-ZCP, we complete the proof for the second equation of (21). ■

***Remark** 3:* If (12) is satisfied, then

$$\theta_{\mathbf{a}}(\tau)+\theta_{\mathbf{b}}(\tau) = -2, \quad \text{for any } 1 \leq \tau \leq N-1. \tag{24}$$

Also, in this case, by the first equation of (21), we have

$$g_0, g_1 \in \Big\{(N-1)/2, (N+1)/2\Big\},$$

therefore, each binary sequence in the OB-ZCP $(\mathbf{a},\mathbf{b})$ should be *balanced*.

***Remark** 4:* In contrast to (21), it is noted that the length of the binary Golay complementary pair (GCP) should satisfy the following condition:

$$N = (g_0-g_1)^2 + (N-g_0-g_1)^2. \tag{25}$$

C. Property 3

Let $(\mathbf{a}, \mathbf{b})$ be an *optimal* OB-ZCP of length N, and $(\mathbf{c}, \mathbf{d})$ be a Golay complementary pair of length M. Then $(\mathbf{e}, \mathbf{f})$

$$\begin{aligned}(-1)^{\mathbf{e}} &= (-1)^{\mathbf{a}} \otimes \left(\frac{(-1)^{\mathbf{c}}+(-1)^{\mathbf{d}}}{2}\right)\\ &\quad + (-1)^{\underline{\mathbf{b}}} \otimes \left(\frac{(-1)^{\mathbf{c}}-(-1)^{\mathbf{d}}}{2}\right),\\ (-1)^{\mathbf{f}} &= (-1)^{\mathbf{b}} \otimes \left(\frac{(-1)^{\mathbf{c}}+(-1)^{\mathbf{d}}}{2}\right)\\ &\quad - (-1)^{\underline{\mathbf{a}}} \otimes \left(\frac{(-1)^{\mathbf{c}}-(-1)^{\mathbf{d}}}{2}\right)\end{aligned} \tag{26}$$

will be a binary ZCP of length-MN and with ZCZ width of $M(N+1)/2$, where $\otimes$ denotes the Kronecker product and $\underline{\mathbf{a}}$ denotes the reversal of $\mathbf{a}$ [12]. More specifically,

$$|\rho_{\mathbf{e}}(\tau)+\rho_{\mathbf{f}}(\tau)| = \begin{cases} 2MN, & \text{if } \tau = 0;\\ 2M, & \text{if } \tau = mM;\\ 0, & \text{otherwise}\end{cases} \tag{27}$$

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

Proof: Note that

$$\begin{aligned}\mathbf{e}(z) &= \mathbf{a}\left(z^{M}\right)\left[\frac{\mathbf{c}(z)+\mathbf{d}(z)}{2}\right]\\ &\quad + z^{M(N-1)}\mathbf{b}\left(z^{-M}\right)\left[\frac{\mathbf{c}(z)+\mathbf{d}(z)}{2}\right],\\ \mathbf{f}(z) &= \mathbf{b}\left(z^{M}\right)\left[\frac{\mathbf{c}(z)+\mathbf{d}(z)}{2}\right]\\ &\quad - z^{M(N-1)}\mathbf{a}\left(z^{-M}\right)\left[\frac{\mathbf{c}(z)+\mathbf{d}(z)}{2}\right].\end{aligned} \tag{28}$$

Also,

$$\mathbf{c}(z)\mathbf{c}\left(z^{-1}\right)+\mathbf{d}(z)\mathbf{d}\left(z^{-1}\right) = 2M. \tag{29}$$

Therefore, we have

$$\begin{aligned}&\mathbf{e}(z)\mathbf{e}\left(z^{-1}\right)+\mathbf{f}(z)\mathbf{f}\left(z^{-1}\right)\\ &= \left[\mathbf{a}\left(z^{M}\right)\mathbf{a}\left(z^{-M}\right)+\mathbf{b}\left(z^{M}\right)\mathbf{b}\left(z^{-M}\right)\right]\\ &\quad \cdot \left[\mathbf{c}(z)\mathbf{c}\left(z^{-1}\right)+\mathbf{d}(z)\mathbf{d}\left(z^{-1}\right)\right]/2\\ &= 2MN\\ &+ M\sum_{m=(N+1)/2}^{N-1}\left[\rho_{\mathbf{a}}(m)+\rho_{\mathbf{b}}(m)\right]\cdot\left[z^{mM}+z^{-mM}\right].\end{aligned} \tag{30}$$

By noting that $(\mathbf{a}, \mathbf{b})$ is an *optimal* OB-ZCP completes the proof. ■

VI. Conclusions

In this paper, we have proposed the *optimal* odd-period binary Z-complementary pair (OB-ZCP). Our main contribution is the proof that the OB-ZCP with maximum zero-correlation-zone (ZCZ) has its *out-of-zone aperiodic autocorrelation sum* lower bounded by the value of 2. Furthermore we have shown that to construct the *optimal* OB-ZCP, it is necessary that their *support* forms a set of almost difference families (ADF). We have also presented several interesting properties of the *optimal* OB-ZCPs. These results may be useful in searching longer *optimal* OB-ZCPs.

We point out that the optimality of *optimal* OB-ZCPs are twofold: first, they achieve their upper bound on ZCZ, i.e., $(N+1)/2$; second, the magnitude of each *out-of-zone aperiodic autocorrelation sum* achieves its lower bound, i.e. 2.

In the end, we note that the proposed *optimal* OB-ZCP provides a source for ADF of base two. For instance, by the *optimal* OB-ZCP of length 23 in TABLE I, let

$$\begin{aligned}D_0 &= \{1, 5, 6, 7, 12, 15, 19, 21\}\\ D_1 &= \{2, 3, 6, 13, 14, 15, 16, 18, 19, 21\}.\end{aligned}$$

Then $\mathcal{D} = \{D_0, D_1\}$ is a set of $\{23; (8, 10); 6; 8\}$ ADF.

VII. Acknowledgements

The work of Zilong Liu and Yong Liang Guan was supported in full 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 Udaya Parampalli was supported in part by the Australia-China Group Missions project supported by Department of Innovation, Industry, Science and Research (DIISR) Australia, under Grant ACSRF02361.

References

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

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

[3] P. Fan, W. Yuan, and Y. Tu, "Z-complementary binary sequences", *IEEE Signal Process. Lett.*, vol. 14, no. 6, pp. 401-404, 2007.

[4] X. Li, P. Fan, X. Tang, Y. Tu, "Existence of Binary Z-Complementary Pairs", *IEEE Signal Process. Lett.*, vol. 18, no. 1, pp. 63-66, 2011.

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

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

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

[8] C. Ding, "Two constructions of $(v, (v-1)/2, (v-3)/2)$ difference families", *J. Combinatorial Designs*, Vol. 16, No. 2, pp. 164-171, 2008.

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

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

[11] L. Bömer and M. Antweiler, "Periodic Complimentary Binary Sequences," *IEEE Trans. Info. Theory,* vol. 36, no. 6, pp. 1487-1494, 1990.

[12] R. Turyn, "Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression and surface wave encodings," *J. Combin. Theory (A)*, vol. 16, pp. 313-333, 1974.