On Average Zero-Correlation Zone of Golay Complementary Pairs

Dian Li, Chunlei Li
University of Bergen, Bergen, Norway
{dian.li, chunlei.li}@uib.no

Zilong Liu
University of Essex, Colchester, UK
zilong.liu@essex.ac.uk

Abstract

Understanding the average zero-correlation zone (ZCZ) width of sequence sets is of strong interest for enhanced spread-spectrum systems whereby multiple users are deployed in a randomly distributed manner. For the first time in the literature, we study the average ZCZ of Golay-Davis-Jedwab (GDJ) complementary pairs. For a certain set of GDJ pairs, we show that its average ZCZ is dependent on the associated permutation and identify the permutation yielding the largest ZCZ width.

1 Introduction

A pair of sequences whose out-of phase aperiodic autocorrelation sums are all zero is known as the Golay complementary pair [1]. GCPs and their generalization, complementary codes, have been employed in various fields including radar waveform design, channel estimation, peak-to-average power ratio reduction, multi-carrier code-division multiple access (MC-CDMA), etc. It is noted that the number of mutually orthogonal GCPs or complementary codes is upper bounded by that of the constituent sequences. For a larger set size, multiple sequence sets with low inter-set correlation property were introduced in [2]. Almost at the same time, Z-complementary code set (ZCCS) was proposed in [3]. In a ZCCS, every code (which can be regarded as a two-dimensional matrix through proper arranging) exhibits a zero-correlation zone (ZCZ) for the aperiodic autocorrelation sums. Likewise, every pair of two distinct codes exhibits a zero cross-correlation zone. In practice, a ZCCS can be deployed to mitigate the multiuser interference due to quasi-synchronous transmission of MC-CDMA signals. Since then, a number of constructions on various types of sequence sets with ZCZ or low-correlation zone (LCZ) properties have been proposed [4–10].

It is noted that the existing constructions are mostly focused on enlarging the minimum ZCZ width. Due to the statistical nature of multiuser transmission, we argue that it is equally important to maximize the average ZCZ width of sequence sets. As the first initiative on this problem, we aim to investigate the average ZCZ width of a large set of

GCPs. Based on the GCP construction in [11] by Davis and Jedwab, also known as Golay-Davis-Jedwab (GDJ) pairs, we characterize the pairwise ZCZ within a set of GDJ pairs. We show that the ZCZ width of two different GDJ pairs is related to the permutation and linear terms in the corresponding generalized Boolean functions. Further, we prove that under the permutation σ_m (as given in Proposition 15), the largest average ZCZ can be achieved.

The remainder of this paper is outlined as follows. In Section 2, we introduce the notations and definitions that will be used throughout this paper. In Section 3, we investigate the ZCZ width between two GDJ pairs. In Section 4, we demonstrate that the largest average ZCZ width can be achieved by certain permutation.

2 Preliminaries

Throughout this paper, $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$ is the set of integers modulo a positive integer q and $\xi = e^{2\pi\sqrt{-1}/q}$ denotes a q-th primitive root of unity.

Let $\mathbf{a} = (a_0, a_1, \ldots, a_{L-1})$, $\mathbf{b} = (b_0, b_1, \ldots, b_{L-1})$ be two length-L sequences over $\mathbb{Z}_q$. The aperiodic cross-correlation function between $\mathbf{a}$ and $\mathbf{b}$ at displacement u is given by

$$\rho(\mathbf{a}, \mathbf{b})(u) = \begin{cases} \sum_{i=0}^{L-1-u} \xi^{a_i - b_{i+u}}, & 0 \le u < L, \\ \sum_{i=0}^{L+u-1} \xi^{a_{i-u} - b_i}, & -L < u < 0. \end{cases}$$

If $\mathbf{a} = \mathbf{b}$, then $\rho(\mathbf{a}, \mathbf{b})(u)$ represents the aperiodic autocorrelation of $\mathbf{a}$ and is denoted as $\rho(\mathbf{a})(u)$. Next, we introduce the concept of ZCZ sequences below.

Let $\mathbf{S} = \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \ldots, \mathbf{s}_K\}$ be a set of K sequences where $\mathbf{s}_k = (s_{k,0}, s_{k,1}, \ldots, s_{k,L-1})$ for $1 \le k \le K$. $\mathbf{S}$ is called a Z-complementary set with ZCZ width Z if

$$\sum_{k=1}^{K} \rho(\mathbf{s}_k)(u) = \begin{cases} KL, & u = 0, \\ 0, & 1 \le |u| < Z. \end{cases} \tag{1}$$

If $Z = L$, a conventional complementary set is defined.

Definition 1. A set $\mathcal{C} = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_M\}$, where $\mathbf{C}_i$ is a set of K sequences of length L, is called an (M, K, L, Z)-ZCCS if

$$\rho(\mathbf{C}_i, \mathbf{C}_j)(u) = \sum_{k=1}^{K} \rho(\mathbf{s}_k^i, \mathbf{s}_k^j)(u) = \begin{cases} KL, & u = 0, i = j, \\ 0, & 0 < |u| < Z, i = j, \\ 0, & |u| < Z, i \ne j, \end{cases} \tag{2}$$

where Z denotes the ZCZ width and each $\mathbf{C}_i = \{\mathbf{c}_0^i, \mathbf{c}_1^i, \ldots, \mathbf{c}_{K-1}^i\}$ consists of K length-L sequences for $1 \le i \le M$.

In an (M, K, L, Z)-ZCCS, any two Z-complementary codes are called a Z-complementary mate. If $Z = L$, a Z-complementary mate becomes the conventional complementary mate. It is shown that the maximum number of distinct Z-complementary mates is upper bounded by $K\lfloor L/Z \rfloor$ which is greater than the number K of conventional complementary mates. When a Z-complementary code set achieves the bound, it is said to be optimal [12].

Definition 2. Consider $\mathcal{C} = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_M\}$, where each $\mathbf{C}_i$ is a set of K complementary sequences of length L. Denote by $Z(\mathbf{C}_i, \mathbf{C}_j)$ the mutual ZCZ width between $\mathbf{C}_i$ and $\mathbf{C}_j$ for $1 \le i, j \le M$. The average ZCZ of the set $\mathcal{C}$ is defined as follows:

$$\overline{Z} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{M} Z(\mathbf{C}_i, \mathbf{C}_j)}{M^2}. \tag{3}$$

In general, it is challenging to explicitly determine the average ZCZ width for a set $\mathcal{C}$ as in Definition 2. In this paper we will investigate this problem for a set of binary complementary pairs from generalized Boolean functions.

Recall that generalized Boolean function (GBF) f of the m variables $x_1, x_2, \ldots, x_m$ is a mapping from $\mathbb{Z}_2^m$ to $\mathbb{Z}_q$. The monomial of degree r is a product of r variables of the form $x_{j_1}x_{j_2}\ldots x_{j_r}$ where $1 \le j_1 < j_2 < \cdots < j_r \le m$. A GBF f can be uniquely expressed as a linear combination of these 2^m monomials $1, x_1, \ldots, x_m, \ldots, x_1x_2\cdots x_m$, where the coefficient of each monomial belongs to $\mathbb{Z}_q$. For a GBF f, we define a sequence $\mathbf{f} = (\xi^{f_0}, \xi^{f_1}, \ldots, \xi^{f_{2^m-1}})$ of length 2^m corresponding to f where $f_i = f(i_1, i_2, \ldots, i_m)$ and $(i_1, i_2, \ldots, i_m)$ is the binary representation of the integer $i = \sum_{j=1}^{m} i_j 2^{j-1}$.

Davis and Jedwab in [11] established the connection between binary GCPs with Boolean functions and studied q-ary GCPs with length 2^m using the tool of GBFs, where q is a power of 2. We recall their constructed GDJ pairs as follows:

Theorem 3. *[11] Let m be a positive integer and π a permutation of the symbols $\{1, 2, \cdots, m\}$. Let f be a GBF given by*

$$f(x_1, x_2, \cdots, x_m) = \frac{q}{2}\sum_{k=1}^{m-1} x_{\pi(k)}x_{\pi(k+1)} + \sum_{k=1}^{m} c_{\pi(k)}x_{\pi(k)}, \tag{4}$$

where q is a power of 2 and $c_{\pi(k)} \in \mathbb{Z}_q$. Then, for any choice $d, d' \in \mathbb{Z}_q$, the sequence pair

$$(\mathbf{a}_0, \mathbf{a}_1) = (\mathbf{f} + d, \mathbf{f} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d') \tag{5}$$

is a complementary pair over $\mathbb{Z}_q$ of length 2^m.

The work was later generalized in [13] where those GBFs have co-domain $\mathbb{Z}_q$ for any positive even integer q. In this paper, we consider the GBFs with co-domain $\mathbb{Z}_q$ where q is even.

3 ZCZ of two GDJ pairs

This section studies the ZCZ width for GDJ pairs constructed by GBFs.

Theorem 4. *Let m be a positive integer and π a permutation of the symbols $\{1, 2, \cdots, m\}$. Let f be a GBF as in (4) and g be a GBF given by*

$$g(x_1, x_2, \cdots, x_m) = \frac{q}{2}\sum_{k=1}^{m-1} x_{\pi(k)}x_{\pi(k+1)} + \sum_{k=1}^{m} c'_{\pi(k)}x_{\pi(k)}, \tag{6}$$

where the first position that $(c'_{\pi(1)}, \dots, c'_{\pi(m)})$ *and* $(c_{\pi(1)}, \dots, c_{\pi(m)})$ *differ is at the index* t, $1 \le t \le m$, *and* $c_{\pi(t)} - c_{\pi(t)'} = q/2$. *Then, the GDJ pairs*

$$(\mathbf{a}_0, \mathbf{a}_1) = (\mathbf{f} + d, \mathbf{f} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d'), \quad (\mathbf{b_0}, \mathbf{b_1}) = (\mathbf{g} + d, \mathbf{g} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$$

form a Z-complementary mate of ZCZ width

$$Z = \frac{1}{2}\Big(2^{\pi(t+1)} - \sum_{\substack{k=t+2 \\ \pi(k)<\pi(t+1)}}^{m} 2^{\pi(k)}\Big), \tag{7}$$

where the summation is deemed as zero when $t = m - 1$.

Proof. Note $\rho(\mathbf{a}, \mathbf{b})(u) = \rho^*(\mathbf{a}, \mathbf{b})(-u)$ for $(\mathbf{a}, \mathbf{b}) \in \{(\mathbf{a}_0, \mathbf{b}_0), (\mathbf{a}_1, \mathbf{b}_1)\}$. To demonstrate pairs $(\mathbf{a}_0, \mathbf{a}_1)$ and $(\mathbf{b}_0, \mathbf{b}_1)$ have the ZCZ width Z, below we will investigate the value of

$$\begin{aligned} \rho(\mathbf{a}_0, \mathbf{b}_0)(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u) &= \sum_{i=0}^{L-1-u} \xi^{a_{0,i} - b_{0,i+u}} + \sum_{i=0}^{L-1-u} \xi^{a_{1,i} - b_{1,i+u}} \\ &= \sum_{i=0}^{L-1-u} (\xi^{a_{0,i} - b_{0,i+u}} + \xi^{a_{1,i} - b_{1,i+u}}). \end{aligned} \tag{8}$$

For a given integer i, let $j = i + u$; also let $(i_1, i_2, \dots, i_m)$ and $(j_1, j_2, \dots, j_m)$ be the binary representations of i and j, respectively. Denoted by $v(i, j)$ the integer v such that

$$i_{\pi(v)} \neq j_{\pi(v)} \text{ and } i_{\pi(k)} = j_{\pi(k)}, \quad \forall\, 1 \le k < v. \tag{9}$$

We will simply denote $v(i, j)$ as v whenever there is no ambiguity. Then we consider four cases to show that for each (i, j) pair, either we have $\xi^{a_{0,i} - b_{0,j}} + \xi^{a_{1,i} - b_{1,j}} = 0$ or there exist integers $i' \le L - 1 - u$ and $j' = i' + u \le L - 1$ such that

$$\xi^{a_{0,i} - b_{0,j}} + \xi^{a_{1,i} - b_{1,j}} + \xi^{a_{0,i'} - b_{0,j'}} + \xi^{a_{1,i'} - b_{1,j'}} = 0.$$

Below we will divide our discussion into four cases.

Case 1 : When $v = 1$ which means $j_{\pi(1)} \neq i_{\pi(1)}$, we have

$$a_{0,i} - a_{1,i} - (b_{0,j} - b_{1,j}) = \frac{q}{2}(j_{\pi(1)} - i_{\pi(1)}). \tag{10}$$

Since $j_{\pi(1)} \neq i_{\pi(1)}$, from (10) we get $\frac{\xi^{a_{0,i} - a_{1,j}}}{\xi^{b_{0,i} - b_{1,j}}} = -1$, which implies $\xi^{a_{0,i} - b_{0,j}} + \xi^{a_{1,i} - b_{1,j}} = 0$.

Case 2 : When $1 < v \le t$, let $i' = (i_1, i_2, \dots, 1 - i_{\pi(v-1)}, \dots, i_m)$ and $j' = (j_1, j_2, \dots, 1 - j_{\pi(v-1)}, \dots, j_m)$ whose binary representations are different from i and j only at the position $\pi(v-1)$ respectively. It is clear that $j' = i' + u$. Then we have

$$a_{0,i'} - a_{0,i} = \frac{q}{2} i_{\pi(v-2)} + \frac{q}{2} i_{\pi(v)} + c_{\pi(v-1)} - 2 i_{\pi(v-1)} c_{\pi(v-1)}. \tag{11}$$

According to $i_{\pi(v-1)} = j_{\pi(v-1)}$ and $i_{\pi(v-2)} = j_{\pi(v-2)}$, we have

$$\begin{aligned}
a_{0,i} - a_{0,i'} - (b_{0,j} - b_{0,j'}) =& -\frac{q}{2} i_{\pi(v-2)} - \frac{q}{2} i_{\pi(v)} - c_{\pi(v-1)} + 2 i_{\pi(v-1)} c_{\pi(v-1)} \\
&+ \frac{q}{2} j_{\pi(v-2)} + \frac{q}{2} j_{\pi(v)} + c'_{\pi(v-1)} - 2 j_{\pi(v-1)} c'_{\pi(v-1)} \\
=& \frac{q}{2}(j_{\pi(v-2)} - i_{\pi(v-2)}) + \frac{q}{2}(j_{\pi(v)} - i_{\pi(v)}) + (c'_{\pi(v-1)} - c_{\pi(v-1)}) \\
&+ 2(c_{\pi(v-1)} i_{\pi(v-1)} - c'_{\pi(v-1)} j_{\pi(v-1)}) \\
\equiv& \frac{q}{2} + (2 i_{\pi(v-1)} - 1)(c_{\pi(v-1)} - c'_{\pi(v-1)}) \pmod q.
\end{aligned}$$

Since $c_{\pi(v-1)} = c'_{\pi(v-1)}$ we have

$$a_{0,i} - a_{0,i'} - (b_{0,j} - b_{0,j'}) \equiv \frac{q}{2} \pmod q. \tag{12}$$

Similarly,

$$a_{1,i} - a_{1,i'} - (b_{1,j} - b_{1,j'}) \equiv \frac{q}{2} \pmod q. \tag{13}$$

Hence, for a pair $(i, j = i + u)$, if $v(i, j) \le t$, from (12) (13) we can derive $\frac{\xi^{a_{0,i} - b_{0,j}}}{\xi^{a_{0,i'} - b_{0,j'}}} = -1$ and $\frac{\xi^{a_{1,i} - b_{1,j}}}{\xi^{a_{1,i'} - b_{1,j'}}} = -1$. Thus,

$$\xi^{a_{0,i} - b_{0,j}} + \xi^{a_{1,i} - b_{1,j}} + \xi^{a_{0,i'} - b_{0,j'}} + \xi^{a_{1,i'} - b_{1,j'}} = 0, \tag{14}$$

which implies $\rho(\mathbf{a}_0, \mathbf{b}_0)(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u) = 0$.

Case 3 : When $v = t + 1$, we have $c'_{\pi(v-1)} - c_{\pi(v-1)} = c'_{\pi(t)} - c_{\pi(t)} = q/2$ by assumption. Arguing as in *Case* 2, from (3) we can obtain

$$a_{0,i} - a_{0,i'} - (b_{0,j} - b_{0,j'}) \equiv 0 \pmod q$$

and

$$a_{1,i} - a_{1,i'} - (b_{1,j} - b_{1,j'}) \equiv 0 \pmod q.$$

Then we can derive $\xi^{a_{0,i} - b_{0,j}} = \xi^{a_{0,i'} - b_{0,j'}}$ and $\xi^{a_{1,i} - b_{1,j}} = \xi^{a_{1,i'} - b_{1,j'}}$. In this case, it is possible that

$$|\rho(\mathbf{a}_0, \mathbf{b_0})(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u)| \ge 0.$$

Case 4 : When $v > t + 1$, let i'', j'' be two integers different from i, j in the position $\pi(t)$, i.e. $i'' = (i_1, i_2, \ldots, 1 - i_{\pi(t)}, \ldots, i_m)$. Then we have

$$a_{0,i''} - a_{0,i} = \frac{q}{2} i_{\pi(t-1)} + \frac{q}{2} i_{\pi(t+1)} + c_{\pi(t)} - 2 i_{\pi(t)} c_{\pi(t)}.$$

Therefore,

$$\begin{aligned}
a_{0,i} - a_{0,i''} - (b_{0,j} - b_{0,j''}) =& -\frac{q}{2} i_{\pi(t-1)} - \frac{q}{2} i_{\pi(t+1)} - c_{\pi(t)} + 2 i_{\pi(t)} c_{\pi(t)} \\
&+ \frac{q}{2} j_{\pi(t-1)} + \frac{q}{2} j_{\pi(t+1)} + c'_{\pi(t)} - 2 j_{\pi(t)} c'_{\pi(t)} \\
=& \frac{q}{2}(j_{\pi(t-1)} - i_{\pi(t-1)}) + \frac{q}{2}(j_{\pi(t+1)} - i_{\pi(t+1)}) + (c'_{\pi(t)} - c_{\pi(t)}) \\
&+ 2(c_{\pi(t)} i_{\pi(t)} - c'_{\pi(t)} j_{\pi(t)}) \\
\equiv& (2 i_{\pi(t)} - 1)(c_{\pi(t)} - c'_{\pi(t)}) \pmod q.
\end{aligned}$$

By the assumption that $c_{\pi(t)} - c'_{\pi(t)} = q/2$, we have

$$a_{0,i} - a_{0,i''} - (b_{0,j} - b_{0,j''}) \equiv \frac{q}{2} \pmod q \tag{15}$$

and

$$a_{1,i} - a_{1,i''} - (b_{1,j} - b_{1,j''}) \equiv \frac{q}{2} \pmod q. \tag{16}$$

As discussed above, for a integer u, if $v(i,j) > t$, where $j = i + u$, then $\rho(\mathbf{a}_0, \mathbf{b}_0)(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u) = 0$. Based on the discussion for Cases 1-4, we see that $|\rho(\mathbf{a}_0, \mathbf{b}_0)(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u)| > 0$ can only occur in Case 3, namely, the integers i and $j = i + u$ satisfy that

$$i_{\pi(t+1)} = j_{\pi(t+1)} \text{ and } i_{\pi(k)} = j_{\pi(k)}, \quad \forall\, 1 \le k \le t, \tag{17}$$

which implies

$$u = j - i = \sum_{k=v+2}^{m} 2^{\pi(k)-1}(j_{\pi(k)} - i_{\pi(k)}). \tag{18}$$

Next we discuss the minimum value of $|u|$, which corresponds to the ZCZ width, for possible values of u of the above form. Denote $w_k = j_{\pi(k)} - i_{\pi(k)}$, which takes values from $\{0, \pm 1\}$. From (18) we have

$$\begin{aligned} |u| &= \left| 2^{\pi(t+1)-1} w_{t+1} + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k + \sum_{\substack{k=t+2 \\ \pi(k)<\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k \right| \\ &\ge \left| 2^{\pi(t+1)-1} w_{t+1} + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k \right| - \left| \sum_{\substack{k=t+2 \\ \pi(k)<\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k \right| \\ &\ge \left| 2^{\pi(t+1)-1} w_{t+1} + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k \right| - \sum_{\substack{k=t+2 \\ \pi(k)<\pi(t+1)}}^{m} 2^{\pi(k)-1}, \end{aligned} \tag{19}$$

where the last inequality holds due to the fact that $w_k \in \{0, \pm 1\}$. Furthermore, by the fact that $w_{t+1} = j_{\pi(t+1)} - i_{\pi(t+1)} \neq 0$ we have

$$2^{\pi(t+1)-1} w_{t+1} + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k = w_{t+1} 2^{\pi(t+1)-1} \left(1 + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-\pi(t+1)} \frac{w_k}{w_{t+1}} \right).$$

It is readily seen that

$$\left| 1 + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-\pi(t+1)} \frac{w_k}{w_{t+1}} \right| \ge 1,$$

which implies

$$\left| 2^{\pi(t+1)-1} w_{t+1} + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k \right| \ge 2^{\pi(t+1)-1}.$$

This together with (19) shows that for any u such that i, $j = i + u$ satisfying (17), one has

$$|u| \geq Z = 2^{\pi(t+1)-1} - \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-1}.$$

That is to say, for any $0 < |u| < Z$, we have $\rho(\mathbf{a}_0, \mathbf{b}_0)(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u) = 0$. □

Remark 5. As in many works [5] [14], the ZCZ width in Theorem 4 is essentially a lower bound of the actual ZCZ width of GDJ pairs. While it is not certain whether $|\rho(\mathbf{a}_0, \mathbf{b}_0)(Z) + \rho(\mathbf{a}_1, \mathbf{b}_1)(Z)| > 0$ in Case 3, experiment results show that Z in Theorem 4 is indeed the actual ZCZ width of GDJ pairs for most permutations.

Remark 6. Suppose in Theorem 4 we choose functions f and g differing at $c_{\pi(m)}, c'_{\pi(m)}$, namely, $c_{\pi(m)} - c'_{\pi(m)} = \frac{q}{2}$, and $c_{\pi(i)} = c'_{\pi(i)}$ for $1 \leq i \leq m-1$. It is easy to see that we don't need to discuss Cases 3 and 4 in the proof of Theorem 4. That is to say, for any $0 < |u| < L$, Cases 1 and 2 imply that $\rho(\mathbf{a}_0, \mathbf{b}_0)(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u) = 0$. This corresponds to the conventional Golay complementary mates.

From Theorem 4, we can easily obtain the following results.

Corollary 7. *Let* $(\mathbf{a}_0, \mathbf{a}_1) = (\mathbf{f} + d, \mathbf{f} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$ *and* $(\mathbf{b}_0, \mathbf{b}_1) = (\mathbf{g} + d, \mathbf{g} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$ *be GDJ pairs as in Theorem 4. Suppose that in f and g,* $c_{\pi(m-1)} - c'_{\pi(m-1)} = \frac{q}{2}$, *and* $c_{\pi(i)} = c'_{\pi(i)}$ *for* $1 \leq i \leq m-2$. *Then* $(\mathbf{a}_0, \mathbf{a}_1)$ *and* $(\mathbf{b}_0, \mathbf{b}_1)$ *have* ZCZ *of width* $2^{\pi(m)-1}$.

Corollary 8. *Let* $(\mathbf{a}_0, \mathbf{a}_1) = (\mathbf{f} + d, \mathbf{f} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$ *and* $(\mathbf{b}_0, \mathbf{b}_1) = (\mathbf{g} + d, \mathbf{g} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$ *be GDJ paris as defined in Theorem 4. Suppose that in the functions f and g,* $c_{\pi(m-2)} - c'_{\pi(m-2)} = \frac{q}{2}$, *and* $c_{\pi(i)} = c'_{\pi(i)}$ *for* $1 \leq i < m-2$. *Then the pairs* $(\mathbf{a}_0, \mathbf{a}_1)$ *and* $(\mathbf{b}_0, \mathbf{b}_1)$ *have* ZCZ *width* $\left|2^{\pi(m-1)-1} - 2^{\pi(m)-1}\right|$.

Proof. Substituting $t = m-2$ in Theorem 4, when $\pi(m) > \pi(m-1)$ we can derive $Z = 2^{\pi(m-1)-1}$ from (7). Similarly, if $\pi(m) < \pi(m-1)$ then $Z = 2^{\pi(m-1)-1} - 2^{\pi(m)-1}$. Therefore, the pairs $(\mathbf{a}_0, \mathbf{a}_1)$ and $(\mathbf{b}_0, \mathbf{b}_1)$ have ZCZ width $Z = \left|2^{\pi(m-1)-1} - 2^{\pi(m)-1}\right|$. □

The characterization on the ZCZ width of GDJ pairs in Theorem 4 motivates us to consider the average ZCZ width of a set of GDJ pairs. In Theorem 4 we have the condition $c_{\pi(t)} - c'_{\pi(t)} = q/2$. In next section we will consider the average ZCZ width of a set of binary GDJ pairs.

4 Average ZCZ widths for certain permutations

In this section we will investigate the average ZCZ property of a set of binary GDJ pairs. As shown in Theorem 3, we can denote by $f_{\mathbf{c},\pi}$ the m-variate Boolean function associated with the coefficient vector $\mathbf{c} \in \mathbb{Z}_2^m$ and the permutation π. Define a set

$$\mathcal{C}_\pi = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_M\}, \tag{20}$$

where $\mathbf{C}_i = (\mathbf{f}_{\mathbf{c}_i,\pi} + d, \mathbf{f}_{\mathbf{c}_i,\pi} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$ is a binary GDJ pair generated by the function $f_{\mathbf{c}_i,\pi}$ as described in Theorem 3 and $\mathbf{c}_i \in \mathbb{Z}_2^m$. It is clear that $M = 2^m$. We will investigate the average ZCZ width of $\mathcal{C}_\pi$, denoted as $\overline{Z_\pi}$, for different permutations π on $\{1, 2, \ldots, m\}$.

We first give an auxiliary result, which will be frequently used to explicitly calculate the average ZCZ witdh of $\mathcal{C}_\pi$ for some permutations π.

Lemma 9. *Let $\mathbf{C}_i$ be a binary GDJ pair in $\mathcal{C}_\pi = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_M\}$ as defined above, and $Z_{\pi,t}$ be given by as in (7) for integers t with $1 \le t \le m-1$. Then we have*

$$\#\{\mathbf{C}_j \in \mathcal{C}_\pi \mid Z(\mathbf{C}_i, \mathbf{C}_j) = Z_{\pi,t}\} = 2^{m-t},$$

where $Z(\mathbf{C}_i, \mathbf{C}_j)$ is the ZCZ width of $\mathbf{C}_i$ and $\mathbf{C}_j$.

Proof. Since $\mathbf{C}_i, \mathbf{C}_j$ are GDJ pairs which corresponding to $f_{\mathbf{c}_i,\pi}$ and $f_{\mathbf{c}_j,\pi}$ respectively. Given $f_{\mathbf{c}_i,\pi}$ where $\mathbf{c}_i = (c_{i,0}, \ldots, c_{i,k}, \ldots, c_{i,m})$, for $f_{\mathbf{c}_j,\pi}$ where $\mathbf{c}_j = (c_{j,0}, \ldots, c_{j,k}, \ldots, c_{j,m})$, if $c_{i,k}{=}c_{j,k}$ for $0 \le k < t$ then $Z(\mathbf{C}_i, \mathbf{C}_j) = Z_{\pi,t}$. As $(\mathbf{c}_{j,t+1}, \ldots, \mathbf{c}_{j,m}) \in \mathbb{Z}_2^{m-t}$ which means there are 2^{m-t} pairs $\mathbf{C}_j$ satisfying $Z(\mathbf{C}_i, \mathbf{C}_j) = Z_{\pi,t}$. $\square$

Lemma 9 facilitates the calculation of $\overline{Z_\pi}$ in this section. Based on Theorem 4 and this lemma, for any permutation π on $\{1, 2, \ldots, m\}$, we have

$$\begin{aligned}\overline{Z_\pi} &= \frac{\sum_{i=1}^{2^m}\sum_{j=1}^{2^m} Z(\mathbf{C}_i, \mathbf{C}_j)}{2^{2m}} = \frac{2^m(\sum_{t=1}^{m-1} 2^{m-t} Z_{\pi,t} + 2\cdot 2^m)}{2^{2m}} \\ &= 2^{-m}\sum_{t=1}^{m-1} 2^{m-t}\Big(2^{\pi(t+1)-1} - \sum_{\substack{t+2\le u\le m \\ \pi(u)<\pi(t+1)}} 2^{\pi(u)-1}\Big) + 2 \\ &= \sum_{j=2}^{m} \frac{1}{2^j}\Big(2^{\pi(j)} - \sum_{\substack{j+1\le u\le m \\ \pi(u)<\pi(j)}} 2^{\pi(u)}\Big) + 2 \\ &= \Psi_\pi + 1,\end{aligned} \tag{21}$$

where the second equality contains $2\cdot 2^m$ corresponding to $\mathbf{C}_i, \mathbf{C}_j$ being the same and complementary mate, the third equality follows from the form of $Z_{\pi,t}$ in (7), and

$$\Psi_\pi = \sum_{j=1}^{m} \Psi_\pi(j) = \sum_{j=1}^{m} \frac{1}{2^j}\Big(2^{\pi(j)} - \sum_{\substack{u=j+1 \\ \pi(u)<\pi(j)}}^{m} 2^{\pi(u)}\Big), \tag{22}$$

where $\Psi_\pi(1) = \frac{1}{2}\Big(2^{\pi(1)} - \sum_{\substack{u=2 \\ \pi(u)<\pi(1)}}^{m} 2^{\pi(u)}\Big) = \frac{1}{2}\Big(2^{\pi(1)} - (2^{\pi(1)-1} + 2^{\pi(1)-2} + \cdots + 2)\Big) = 1.$

Below we first determine the average ZCZ with $\overline{Z_\pi}$ for certain special permutations π.

Proposition 10. *Let $\pi_k = (k, \ldots, m, 1, \ldots, k-1)$ be the permutation on $\{1, 2, \ldots, m\}$, where $1 \le k \le m$. Then we have*

$$\overline{Z_{\pi_k}} = \frac{1}{2}\Big(2^k(m-k-1) + 2^{k-m}(2^k + k - 3) + 6\Big).$$

Proof. According to the definition of π_k, we have that $\pi_k(m-k+1) = m$ and

$$\sum_{\substack{j+1\le u\le m\\ \pi_k(u)<\pi_k(j)}} 2^{\pi_k(u)-1} = \begin{cases} \sum\limits_{u=m-k+2}^{m} 2^{\pi_k(u)-1}, & 1 \le j \le m-k+1; \\ 0, & m-k+2 \le j \le m. \end{cases}$$

Then it follows from (21) that

$$\begin{aligned} \overline{Z_{\pi_k}} &= \sum_{j=1}^{m-k+1} 2^{-j}\left(2^{\pi_k(j)} - \sum_{u=m-k+2}^{m} 2^{\pi_k(u)}\right) + \sum_{j=m-k+2}^{m} 2^{\pi_k(j)-j} + 1 \\ &= \sum_{j=1}^{m} 2^{-j}\cdot 2^{\pi_k(j)} - \sum_{j=1}^{m-k+1} 2^{-j}\left(\sum_{u=m-k+2}^{m} 2^{\pi_k(u)}\right) + 1 \\ &= (m-(k-1))2^{k-1} + (k-1)2^{k-m-1} + (2^k-2)(2^{-(m-k+1)}-1) + 1 \\ &= 2^{k-1}(m-k-1) + 2^{k-m}(2^{k-1} + \frac{k-3}{2}) + 3. \end{aligned}$$

This completes the proof. □

In the following, we will identify the permutation on $\{1, 2, \ldots, m\}$ such that the corresponding set $\mathcal{C} = \{\mathbf{C}_1, \ldots, \mathbf{C}_M\}$, where $M = 2^m$, has the maximum average ZCZ width. To this end, we first introduce some notations for presentation simplicity.

Denote by Π the set of all permutations on $\{1, 2, \ldots, m\}$. For a permutation $\pi \in \Pi$, we denote by $\pi^{-1}(t)$ the pre-image of t, where $1 \le t \le m$, under π, i.e., $\pi(\pi^{-1}(t)) = t$. Define sets

$$\begin{aligned} \Pi_1 &= \{\pi \in \Pi \,|\, \pi^{-1}(m) > \pi^{-1}(m-1)\}, \\ \Pi_2 &= \{\pi \in \Pi \,|\, \pi^{-1}(m) < \pi^{-1}(m-1)\}, \end{aligned} \tag{23}$$

and sets

$$\begin{aligned} \Pi_{1,1} &= \{\pi \in \Pi \,|\, \pi^{-1}(m) - \pi^{-1}(m-1) = 1\}, \\ \Pi_{1,2} &= \{\pi \in \Pi \,|\, \pi^{-1}(m) - \pi^{-1}(m-1) > 1\}. \end{aligned} \tag{24}$$

Clearly, $\Pi = \Pi_1 \sqcup \Pi_2$ and $\Pi_1 = \Pi_{1,1} \sqcup \Pi_{1,2}$.

To identify the permutation that gives the largest average ZCZ width, we need the following lemmas, which give auxiliary results for proving the main theorem.

Lemma 11. *Given a permutation $\rho \in \Pi_2$ with $s = \rho^{-1}(m)$ and $t = \rho^{-1}(m-1)$, choose $\pi \in \Pi_1$ such that $\pi(s) = m-1, \pi(t) = m$ and $\pi(j) = \rho(j)$ for $j \ne s, t$. Then $\overline{Z_\pi} \ge \overline{Z_\rho}$.*

Proof. Since $\pi(j) = \rho(j)$ for $j \ne s, t$, it's easy to see that $\Psi_\pi(j) = \Psi_\rho(j)$ for $j \in \{1, 2, \ldots, m\} \setminus \{s, t\}$. Hence, we have

$$\overline{Z_\pi} - \overline{Z_\rho} = \Psi_\pi(s) + \Psi_\pi(t) - \Psi_\rho(s) - \Psi_\rho(t) \tag{25}$$

and if $s=1$ clearly, $\Psi_\pi(s)-\Psi_\rho(s)=0$. By $\pi(s)=m$ and $\rho(t)=m-1$ we have

$$\begin{aligned}\Psi_\pi(s)-\Psi_\rho(s) &= 2^{-s}\left(2^{m-1}-\sum_{\substack{s+1\le u\le m\\ \pi(u)<m-1}}2^{\pi(u)}-(2^m-\sum_{s+1\le u\le m}2^{\rho(u)})\right)\\ &= 2^{-s}\left(-2^{m-1}+2^{\rho(t)}-\sum_{\substack{s+1\le u\le m\\ u\neq t}}2^{\pi(u)}+\sum_{\substack{s+1\le u\le m\\ u\neq t}}2^{\rho(u)}\right)\\ &= 0\end{aligned} \tag{26}$$

since $\pi(u)=\rho(u)$ for $s+1\le u\le m$ and $u\neq t$. Similarly, by $\pi(t)=m$ and $\rho(t)=m-1$ we have

$$\begin{aligned}\Psi_\pi(t)-\Psi_\rho(t) &= 2^{-t}\left(2^{m}-\sum_{t+1\le u\le m}2^{\pi(u)}-(2^{m-1}-\sum_{t+1\le u\le m}2^{\rho(u)})\right)\\ &= 2^{-t}\left(2^{m-1}-\sum_{\substack{s+1\le u\le m\\ u\neq t}}2^{\pi(u)}+\sum_{\substack{s+1\le u\le m\\ u\neq t}}2^{\rho(u)}\right)\\ &= 2^{m-t-1}.\end{aligned} \tag{27}$$

Thus, $\overline{Z_\pi}-\overline{Z_\rho}>0$. □

Lemma 12. *Given a permutation $\rho\in\Pi_{1,2}$ with $s=\rho^{-1}(m-1)$ and $t=\rho^{-1}(m)$, where $t\ge s+2$, choose a permutation $\pi\in\Pi_{1,1}$ such that $\pi(s+1)=m, \pi(t)=\rho(s+1)$, and $\pi(j)=\rho(j)$ for $j\neq s+1,t$. Then $\overline{Z_\pi}\ge\overline{Z_\rho}$.*

Proof. Since $\pi(j)=\rho(j)$ for $j\in\{1,\dots,m\}\setminus\{s+1,t\}$, it is easy to see that

$$\Psi_\pi(j)=\Psi_\rho(j) \text{ for } j=2,\dots,s, \text{ and } j=t+1,\dots,m,$$

where $\Psi_\pi(j)$, $\Psi_\rho(j)$ are given as in (22). Hence we have

$$\overline{Z_\pi}-\overline{Z_\rho}=\sum_{j=2}^{m}\left(\Psi_\pi(j)-\Psi_\rho(j)\right)=\sum_{j=s+1}^{t}\left(\Psi_\pi(j)-\Psi_\rho(j)\right).$$

By $\pi(s+1)=m$ and $\rho(t)=m$, we have

$$\begin{aligned}\Psi_\pi(s+1)-\Psi_\rho(s+1) &= 2^{-(s+1)}\left((2^m-\sum_{u=s+2}^{m}2^{\pi(u)})-(2^{\rho(s+1)}-\sum_{\substack{u=s+2\\ \rho(u)<\rho(s+1)}}^{m}2^{\rho(u)})\right)\\ &= 2^{-(s+1)}\left(2^m-2^{\rho(s+1)}-\sum_{\substack{u=s+2\\ \pi(u)\ge\rho(s+1)}}^{m}2^{\pi(u)}\right)\end{aligned} \tag{28}$$

and

$$\Psi_\pi(t)-\Psi_\rho(t)=2^{-t}\left((2^{\pi(t)}-\sum_{\substack{u=t+1\\\pi(u)<\pi(t)}}^{m}2^{\pi(u)})-(2^m-\sum_{u=t+1}^{m}2^{\rho(u)})\right)$$
$$=2^{-t}\left(2^{\pi(t)}-2^m+\sum_{\substack{u=t+1\\\pi(u)\geq\pi(t)}}^{m}2^{\pi(u)}\right),$$

since $\pi(u)=\rho(u)$ for $u=t+1,\ldots,m$.

For $s+2\leq j\leq t-1$, we have

$$\Psi_\pi(j)-\Psi_\rho(j)=2^{-j}\left((2^{\pi(j)}-\sum_{\substack{u=j+1\\\pi(u)<\pi(j)}}^{m}2^{\pi(u)})-(2^{\rho(j)}-\sum_{\substack{u=j+1\\\rho(u)<\rho(j)}}^{m}2^{\rho(u)})\right)$$
$$=\begin{cases}-2^{\pi(t)-j}, & \text{if } \pi(t)<\pi(j),\\ 0, & \text{otherwise,}\end{cases}$$

which implies

$$\sum_{j=s+2}^{t-1}(\Psi_\pi(j)-\Psi_\rho(j))=\begin{cases}0, & \text{if } \pi(t)=m-2,\\ \sum_{\substack{j=s+2\\\pi(j)>\pi(t)}}^{t-1}-2^{\pi(t)-j}, & \text{if otherwise.}\end{cases} \tag{29}$$

Thus, if $\pi(t)=\rho(s+1)=m-2$ then

$$\sum_{j=s+1}^{t}(\Psi_\pi(j)-\Psi_\rho(j))=2^{-(s+1)}(2^m-2^{\rho(s+1)})+2^{-t}\left(2^{\rho(s+1)}-2^m\right)$$
$$>0,$$

since $t\geq s+2$ and $\sum_{\substack{u=s+2\\\pi(u)\geq\rho(s+1)}}^{m}2^{\pi(u)}=\sum_{\substack{u=t+1\\\pi(u)\geq\pi(t)}}^{m}2^{\pi(u)}=0$. Otherwise, from (29) we have

$$\sum_{\substack{j=s+2\\\pi(j)>\pi(t)}}^{t-1}-2^{\pi(t)-j}\geq-2^{\pi(t)}(2^{-(s+2)}+\cdots+2^{-(t-1)})=-2^{\rho(s+1)}(2^{-(s+1)}-2^{-(t-1)}),$$

then

$$\sum_{j=s+1}^{t}(\Psi_\pi(j)-\Psi_\rho(j))\geq2^{-(s+1)}\left(2^m-2^{\rho(s+1)}-\sum_{\substack{u=s+2\\\pi(u)\geq\rho(s+1)}}^{m}2^{\pi(u)}\right)+2^{-t}\left(2^{\rho(s+1)}-2^m\right)-2^{\rho(s+1)}2^{-(s+1)}$$
$$\geq2^{-(s+1)}\left(2^m-3\cdot2^{\rho(s+1)}+2^{\rho(s+1)-(t-s-1)}-2^{m-(t-s-1)}\right)>0,$$

since $\rho(s+1)\leq m-3$. Thus, it shows $\overline{Z_\pi}\geq\overline{Z_\rho}$. $\square$

For any permutation $\pi \in \Pi_{1,1}$, define sets

$$\begin{aligned} P_1 &= \{\pi \in \Pi_{1,1} \,|\, \pi^{-1}(m-2) = 1, \pi^{-1}(m-1) = 2\}, \\ P_2 &= \{\pi \in \Pi_{1,1} \,|\, \pi^{-1}(m-2) < \pi^{-1}(m-1)\}, \\ P_3 &= \{\pi \in \Pi_{1,1} \,|\, \pi^{-1}(m-2) > \pi^{-1}(m)\}. \end{aligned} \tag{30}$$

Clearly, $\Pi_{1,1} = P_2 \sqcup P_3$, for these sets we have the following lemmas:

Lemma 13. *Given a permutation $\rho \in P_3$ with $s = \rho^{-1}(m-1)$ and $t = \rho^{-1}(m-2)$ where $s \geq 2$, choose a permutation $\pi \in P_2$ such that $\pi(s) = m-1, \pi(s-1) = m-2$ and $\pi(j) = \rho(j)$ for $j \neq s-1, t$. Then $\overline{Z_\pi} \geq \overline{Z_\rho}$.*

Proof. Since $\pi(j) = \rho(j)$ for $j \neq s-1, t$, we can derive that $\pi(t) = \rho(s-1)$ and $\pi(t) < m-2$. Then from 22, we have

$$\overline{Z_\pi} - \overline{Z_\rho} = \sum_{j=s-1}^{t} (\Psi_{\pi(j)} - \Psi_{\rho(j)}) \tag{31}$$

In (31), for $j = s-1$,

$$\begin{aligned} \Psi_{\pi(s-1)} - \Psi_{\rho(s-1)} &= 2^{-(s-1)} \left(2^{\pi(s-1)} - 2^{\rho(s-1)} - \sum_{\substack{u=s \\ \pi(u)<\pi(s-1)}}^{m} 2^{\pi(u)} + \sum_{\substack{u=s \\ \rho(u)<\rho(s-1)}}^{m} 2^{\rho(u)} \right) \\ &= 2^{-(s-1)} \left(2^{m-2} - 2 \cdot 2^{\pi(t)} - \sum_{\substack{u=s+2 \\ \pi(u)>\pi(t)}}^{m} 2^{\pi(u)} \right) \geq 0. \end{aligned}$$

For $s \leq j \leq t$, we have

$$\begin{aligned} \sum_{j=s}^{t} (\Psi_{\pi(j)} - \Psi_{\rho(j)}) &= (2^{-s} + 2^{-(s+1)})(2^{m-2} - 2^{\pi(t)}) - 2^{-j} \sum_{\substack{j=s+2 \\ \pi(j)>\pi(t)}}^{t-1} 2^{\pi(t)} - 2^{-t}(2^{m-2} - 2^{\pi(t)}) \\ &> (2^{-s} + 2^{-(s+1)})(2^{m-2} - 2^{\pi(t)}) - 2^{-(s+1)} 2^{\pi(t)} - 2^{-t}(2^{m-2} - 2^{\pi(t)}) > 0. \end{aligned}$$

Thus, we can derive that $\sum_{j=s-1}^{t} (\Psi_{\pi(j)} - \Psi_{\rho(j)}) > 0$ which implies $\overline{Z_\pi} > \overline{Z_\rho}$. □

Lemma 14. *For any permutation $\rho \in \Pi_{1,1} \setminus P_1$ and $\pi \in P_1$ with $\pi(1) = m-2$ and $\pi(2) = m-1$. Then $\overline{Z_\pi} \geq \overline{Z_\rho}$.*

Proof. Since $\pi \in P_1$ then we have

$$\overline{Z_\pi} = 2^{-2}(2^{m-2} + 2) + 2^{-3}(3 \cdot 2^{m-2} + 2) + \sum_{j=4}^{m} \Psi_\pi(j) + 2.$$

Suppose $\rho(s) = m-1$, there are three cases as below.

Case $1 : s = 1$, By assumption $\rho(1) = m-1$ and $\rho(2) = m$. Clearly $\rho^{-1}(m-2) \geq 2$. Suppose $\rho(t) = m-2$, when $t = 3$, chose $\pi \in P_1$ such that $\pi(j) = \rho(j)$ for $4 \leq j \leq m$ then

$$\overline{Z_\rho} = 2^{-2}(2^m - (2^{m-1} - 2)) + 2^{-2} + \sum_{j=4}^{m} \Psi_\rho(j) + 2.$$

Hence, we have

$$\overline{Z_\pi} - \overline{Z_\rho} = \sum_{j=2}^{m} (\Psi_\pi(j) - \Psi_\rho(j)) = 2^{-3} \cdot 2^{m-2} > 0 \quad , \tag{32}$$

since $\Psi_\pi(j) = \Psi_\rho(j)$ for $4 \leq j \leq m$. When $t > 3$, let $\pi(t) = \rho(3)$ and $\pi(j) = \rho(j)$ for $3 \leq j \leq m$ and $j \neq t$, then

$$\begin{aligned}
\overline{Z_\pi} - \overline{Z_\rho} &= 2^{-3}(2^{m-2} + 2) + \sum_{j=4}^{m} \Psi_\pi(j) - \sum_{j=3}^{m} \Psi_\rho(j) \\
&= 2^{-3}(2^{m-2} + 2) + \sum_{j=4}^{t} \Psi_\pi(j) - \sum_{j=3}^{t-1} \Psi_\rho(j) - \Psi_\rho(t) \\
&= 2^{-3}(2^{m-2} + 2) - 2^{-3}(2^{\rho(3)} - \sum_{\substack{u=4 \\ \rho(u)<\rho(3)}}^{m} 2^{\rho(u)}) - \sum_{\substack{j=4 \\ \pi(j)>\pi(t)}}^{t-1} 2^{-j}(2^{\pi(t)}) + (2^{\pi(t)} - 2^{m-2}) \\
&\geq \left(\frac{5}{3} \cdot 2^{m-6} - 2^{m-2-t} + 2^{m-2t+1} - 2^{-t} + \frac{2^{m-2t}}{3} \right) \\
&> 0.
\end{aligned}$$

Case $2 : s = 2$, It can be derived from Lemma 13 directly that $\overline{Z_\pi} - \overline{Z_\rho} > 0$.

Case $3 : s \geq 3$, According to Lemma 13, it's sufficient to consider the permutation ρ such that $\rho^{-1}(m-2) < s$. Thus there exists $\pi \in P_1$ such that $\pi(j) = \rho(j)$ for $s+2 \leq j \leq m$, then we have

$$\begin{aligned}
\overline{Z_\pi} - \overline{Z_\rho} = {} & 2^{-2}(2^{m-2} + 2)) + 2^{-3}(3 \cdot 2^{m-2} + 2) + \sum_{j=4}^{s+1} \Psi_\pi(j) \\
& - \sum_{j=2}^{s-1} \Psi_\rho(j) - 2^{-s} \left(2^{m-1} - \sum_{\substack{u=s+1 \\ \rho(u)<m-1}}^{m} 2^{\rho(u)} \right) + 2^{-(s+1)} \left(2^m - \sum_{\substack{u=s+2 \\ \rho(u)<m}}^{m} 2^{\rho(u)} \right),
\end{aligned}$$

When $s = 3$,

$$\overline{Z_\pi} - \overline{Z_\rho} > (2^{m-3} + 2^{-1} + 2^{m-5} + 2^{-2}) - 2^{-2} \left(2^{m-3} - 2\right) + 2^{-3}2^{m-1} + 2^{-4}2^m > 0,$$

and when $s > 3$,

$$\overline{Z_\pi} - \overline{Z_\rho} > (2^{m-3} + 2^{-1} + 2^{m-5} + 2^{-2}) - 2^{-2}(2^{m-1} + 2) + 2^{-3}(2^{m-3}) + 2^{-4}2^{m-2} > 0.$$

From the discussion above we show that $\overline{Z_\pi} > \overline{Z_\rho}$. □

Proposition 15. *Let $\sigma_1 = (1)$, $\sigma_2 = (1, 2)$ and $\sigma_3 = (1, 2, 3)$, and for $m \geq 3$, let*

$$\sigma_m = \begin{cases} (m-2, m-1, m)||\ldots||\sigma_1, & \text{if } m \equiv 1 \mod 3, \\ (m-2, m-1, m)||\ldots||\sigma_2, & \text{if } m \equiv 2 \mod 3, \\ (m-2, m-1, m)||\ldots||\sigma_3, & \text{if } m \equiv 3 \mod 3. \end{cases} \tag{33}$$

Then for any permutation $\pi \in \Pi_{1,1}$ with $(\pi(1), \pi(2), \pi(3)) = (m-2, m-1, m)$, we have $\overline{Z_{\sigma_m}} \geq \overline{Z_\pi}$.

Theorem 16. *Let Π be the set of permutations on $\{1, 2, \ldots, m\}$ and $\sigma_m \in \Pi$ be the permutation as given in (33). Then, among all permutations π in Π, the maximum average ZCZ width of $\mathcal{C}_\pi = \{\mathbf{C}_1, \ldots, \mathbf{C}_M\}$ is given by $\overline{Z_{\sigma_m}} = \Psi_{\sigma_m} + 1$, where*

$$\Psi_{\sigma_m} = \frac{1}{2^3}(5 \cdot 2^{m-2} + 14 + \Psi_{\sigma_{m-3}}),$$

and $\Psi_{\sigma_t} = t$ for $t \in \{1, 2, 3\}$; or equivalently,

$$\Psi_{\sigma_m} = 5 \cdot 2^{m-5} \cdot \frac{1 - 2^{-6m_1}}{1 - 2^{-6}} + \frac{14}{8} \cdot \frac{1 - 2^{-3m_1}}{1 - 2^{-3}} + \frac{t}{2^{3m_1}}, \tag{34}$$

where $m = 3m_1 + t$ with $t \in \{1, 2, 3\}$.

Proof. Recall that $\Pi = \Pi_1 \sqcup \Pi_2$, $\Pi_1 = \Pi_{1,1} \sqcup \Pi_{1,2}$ and $\Pi_1 = P_1 \sqcup P_2$, where $\sqcup$ denotes the union of disjoint sets. Suppose π is the permutation in Π such that the corresponding $\overline{Z_\pi}$. Lemmas 11 and 12 shows that π belongs to $\Pi_{1,1}$. Furthermore, by Proposition 15, we see that $\pi = \sigma_m$ is the permutation with the maximum average ZCZ width. According to (3) and (22), it suffices to consider Ψ_{σ_m} and we have

$$\begin{aligned}
\Psi_{\sigma_m} =& \sum_{j=1}^{m} \frac{1}{2^j} \Big(2^{\sigma_m(j)} - \sum_{\substack{u=j+1 \\ \sigma_m(u) < \sigma_m(j)}}^{m} 2^{\sigma_m(u)} \Big) \\
=& \frac{1}{2} \big(2^{m-2} - (2^{m-2} - 2) \big) + \frac{1}{2^2} \big(2^{m-1} - (2^{m-2} - 2) \big) \\
&+ \frac{1}{2^3} \big(2^m - (2^{m-2} - 2) \big) + \sum_{j=4}^{m} \frac{1}{2^j} \Big(2^{\sigma_m(j)} - \sum_{\substack{u=j+1 \\ \sigma_m(u) < \sigma_m(j)}}^{m} 2^{\sigma_m(u)} \Big) \\
=& \frac{1}{2^3}(5 \cdot 2^{m-2} + 14) + \frac{1}{2^3} \sum_{j=1}^{m-3} \frac{1}{2^j} \Big(2^{\sigma_{m-3}(j)} - \sum_{\substack{u=j+1 \\ \sigma_{m-3}(u) < \sigma_{m-3}(j)}}^{m-3} 2^{\sigma_{m-3}(u)} \Big) \\
=& \frac{1}{2^3}(5 \cdot 2^{m-2} + 14 + \Psi_{\sigma_{m-3}}).
\end{aligned}$$

Following the above recursive relation, the expression in (34) can be easily obtained. □

Below we list the maximum average ZCZ width for the Z-complementary set defined in (20) for small integers m with $3 \leq m \leq 10$.

m	3	4	5	6	7	8	9	10
$\overline{Z}_{\max}$	4	$\frac{43}{8}$	8	$\frac{105}{8}$	$\frac{1491}{64}$	$\frac{349}{8}$	$\frac{5393}{64}$	$\frac{84744}{512}$

We show the average ZCZ width of a set composed by all possible GDJ pairs generated by different GBFs. Now we show that according to the algorithm below we can construct a set with optimal average ZCZ width.

5 Conclusion

This paper focused on understanding the average ZCZ of complementary sequence sets motivated by their random deployment nature in practical spread-spectrum communication systems.

We have first derived a lower bound of their ZCZ width for two GDJ pairs, showing that the width is associated with the difference in linear coefficients and permutations within the corresponding GBF. Based on this finding, we have then studied the average ZCZ width of a set of GDJ pairs and provided the expression for a class of cyclic permutations. By comparing the average ZCZ width across different permutations, it is found that that the largest average ZCZ can be achieved by certain permutation family.

References

[1] M. Golay, "Complementary series," *IRE Transactions on Information Theory*, vol. 7, no. 2, pp. 82–87, 1961.

[2] G. Gong, "Constructions of multiple shift-distinct signal sets with low correlation," in *2007 IEEE International Symposium on Information Theory*. IEEE, 2007, pp. 2306–2310.

[3] P. Fan, W. Yuan, and Y. Tu, "Z-complementary binary sequences," *IEEE Signal Processing Letters*, vol. 14, no. 8, pp. 509–512, 2007.

[4] P. Sarkar, C. Li, S. Majhi, and Z. Liu, "New correlation bound and construction of quasi-complementary sequence sets," *IEEE Transactions on Information Theory*, 2024.

[5] P. Sarkar, S. Majhi, and Z. Liu, "Optimal Z-complementary code set from generalized Reed-Muller codes," *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 1783–1796, 2019.

[6] Z. Liu, U. Parampalli, Y. L. Guan, and S. Boztas, "Constructions of optimal and near-optimal quasi-complementary sequence sets from Singer difference sets," *IEEE Wireless Communications Letters*, vol. 2, no. 5, pp. 487–490, 2013.

[7] S. Das, U. Parampalli, S. Majhi, Z. Liu, and S. Budišin, "New optimal Z-complementary code sets based on generalized paraunitary matrices," *IEEE Transactions on Signal Processing*, vol. 68, pp. 5546–5558, 2020.

[8] H. Xiao and X. Cao, "New constructions of mutually orthogonal complementary sets and Z-complementary code sets based on extended Boolean functions," *Cryptography and Communications*, vol. 16, no. 1, pp. 167–184, 2024.

[9] T. Yu, A. R. Adhikary, Y. Wang, and Y. Yang, "New class of optimal Z-complementary code sets," *IEEE Signal Processing Letters*, vol. 29, pp. 1477–1481, 2022.

[10] X. Tang, P. Fan, and J. Lindner, "Multiple binary ZCZ sequence sets with good cross-correlation property based on complementary sequence sets," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 4038–4045, 2010.

[11] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Transactions on information theory*, vol. 45, no. 7, pp. 2397–2417, 1999.

[12] L. Feng, P. Fan, and X. Zhou, "Lower bounds on correlation of Z-complementary code sets," *Wireless personal communications*, vol. 72, no. 2, pp. 1475–1488, 2013.

[13] K. Paterson, "Generalized Reed-Muller codes and power control in OFDM modulation," *IEEE Transactions on Information Theory*, vol. 46, no. 1, pp. 104–120, 2000.

[14] P. Sarkar and S. Majhi, "A direct construction of optimal ZCCS with maximum column sequence PMEPR two for MC-CDMA system," *IEEE Communications Letters*, vol. 25, no. 2, pp. 337–341, 2020.