A New Construction of Three-Phase Z-Complementary Triads Based on Extended Boolean Functions

Xiuping PENG†,††, Yinna LIU†, Nonmembers, and Hongbin LIN†††, Member

SUMMARY In this letter, we propose a novel direct construction of three-phase Z-complementary triads with flexible lengths and various widths of the zero-correlation zone based on extended Boolean functions. The maximum width ratio of the zero-correlation zone of the construction can reach 3/4. And the proposed sequences can exist for all lengths other than powers of three. We also investigate the peak-to-average power ratio properties of the proposed ZCTs.

key words: Z-complementary triad, aperiodic correlation, extended Boolean functions, zero-correlation zone

1. Introduction

A pair of sequences is known as a Golay complementary pair (GCP), if their aperiodic autocorrelation sums are zero at each non-zero time shift. The GCP was first proposed by Golay in 1951 [1]. Complementary sequences have been found several applications in radar [2], peak-to-average power ratio (PAPR) control in orthogonal frequency division multiplexing (OFDM) [3]–[5] and channel estimation [6], [7]. However, binary GCP only exists in length $2^n10^{p26^n}$, where $\alpha, \beta, \gamma \in \mathbb{Z}^+$. So the binary GCP was extended to complex GCP [8], Golay complementary set (GCS) [9] and Z-complementary sequences [10], [11]. Unlike GCPs, Z-complementary pairs (ZCPs) can have various lengths. Binary ZCPs were introduced in [12]. In [13], a construction of optimal binary ZCPs of length $2m \pm 1$ was proposed.

In [14], binary GCP was extended to Golay complementary triad (GCT) over three-phase alphabet $\{1, \omega, \omega^2\}$, where $\omega = e^{2\pi \sqrt{-1}}$. A three-phase GCT consists of three sequences, whose aperiodic autocorrelations sum-up to zero except at zero shift. The three-phase alphabet has been attracted to multiple applications because of its existence with flexible length and smaller number of phase, which guarantees its identifiability at the receiver. For example, binary GCPs up to 10 have lengths of 2 and 10, while three-phase GCTs with lengths of 2, 3, 5, 6, 7, 8 and 9 exist. In [15], Avis gave the first complete counts of three-phase GCTs of length up to 22 and conjectured that there is no three-phase GCT with the length of $N \equiv 4 \pmod{6}$. In [16], Avis et al. proved this conjecture. In order to find three-phase triads of length $N \equiv 4 \pmod{6}$, three-phase Z-complementary triads (ZCTs) were proposed. In [17], three-phase ZCT and almost-complementary triad (ACT) were constructed mainly by indirect construction methods.

The construction method based on Boolean functions is a direct construction and it is helpful for the rapid generation used in several fields. In [18], a construction of GCP over $\mathbb{Z}_{2k} = \{0, 1, \ldots, 2^k-1\}$ for $k \geq 1$ was provided based on generalized Boolean functions. The $q$-ary Z-complementary pairs (ZCPs) for $q$ is even based on generalized Boolean functions were constructed in [19], [20]. The construction of Golay ZCZ sequence sets based on extended generalized Boolean functions were proposed, in which the sequence length and $q$ were flexible for $q \geq 2$ [21]. In this letter, we propose a direct construction of three-phase ZCTs with flexible lengths based on extended Boolean functions. Our construction can obtain the sequences of all lengths other than powers of three.

The rest of this letter is organized as follows. Some necessary definitions are introduced in Sect. 2. In Sect. 3, a construction of ZCTs is proposed. Finally, concluding remarks are drawn in Sect. 4.

2. Preliminaries

Definition 1 ([20]): Let $a = (a_0, a_1, \ldots, a_{N-1})$ be a sequence of $\mathbb{Z}_q$ values of length $N$, where $a_i$ is in the alphabet $\mathbb{Z}_q$. The aperiodic autocorrelation function $R(a)$ at shift $\tau$ is defined as

$$R(a; \tau) = \frac{\sum_{k=0}^{N-1-\tau} \omega^{a_k-a_{k+\tau}}}{\sum_{k=0}^{N-1+\tau} \omega^{a_k-a_{k-\tau}}}, \quad 0 \leq \tau \leq N-1$$

$$R(a; \tau) = \frac{\sum_{k=0}^{N-1-\tau} \omega^{a_k+a_{k+\tau}}}{\sum_{k=0}^{N-1+\tau} \omega^{a_k-a_{k-\tau}}}, \quad -N+1 \leq \tau < 0$$

(1)

where $\omega = e^{2\pi \sqrt{-1}/q}$.

Definition 2 ([17]): Let $a$, $b$ and $c$ be three sequences of length $N$. The triplet $(a, b, c)$ is said to be a Z-complementary triad denoted by ($N, Z$)-ZCT, if

Copyright © 2024 The Institute of Electronics, Information and Communication Engineers
In this section, we will introduce two lemmas firstly, which

\[ R(a; \tau) + R(b; \tau) + R(c; \tau) = \begin{cases} 0, & 0 < \tau < Z \\ 0, & \tau = 0 \end{cases} \tag{2} \]

where \( Z \) is zero correlation zone (ZCZ) width. When \( Z = N \), the triad \((a, b, c)\) is known as a GCT.

**Definition 3** ([23]): For a sequence \( a = (a_0, a_1, \ldots, a_{N-1}) \) over \( \mathbb{Z}_3 \), the OFDM signal of \( N \) subcarriers is the real part of

\[ S_a(t) = \sum_{k=0}^{N-1} \omega^{a_k} e^{2\pi \sqrt{-1} k t}, 0 \leq t < 1. \]

The instantaneous-to-average power ratio (IAPR) of \( a \) is

\[ \text{IAPR}_a(t) = |S_a(t)|^2 / N. \]

And the PAPR of sequence \( a \) is defined to be

\[ \text{PAPR}(a) = \max_{0 < t < 1} \text{IAPR}_a(t). \]

Let \( G = (a, b, c) \) be a three-phase complementary triad with length \( N \). The PAPR of \( G \) is given by

\[ \text{PAPR}(G) = \max \{ \text{PAPR}(a), \text{PAPR}(b), \text{PAPR}(c) \}. \]

Then we can obtain

\[ \text{PAPR}(G) \leq 3 + \frac{2}{N} \sum_{t=1}^{N-1} |R(a; \tau) + R(b; \tau) + R(c; \tau)|. \]

**Definition 4** ([22]): An extended Boolean function (EBF) is a function \( f : \mathbb{Z}_q^d \to \mathbb{Z}_q \) defined on \( n \) variables \((x_1, x_2, \ldots, x_n)\) where \( x_i \in \mathbb{Z}_q \) for \( i = 1, 2, \ldots, n \). The product of \( s \) distinct variables is defined as a monomial of degree \( s \). Let \( f = (f_0, f_1, \ldots, f_{q^n-1}) \) be a sequence of length \( q^n \) related to an extended Boolean function \( f \) by letting \( f_i = f(i_1, i_2, \ldots, i_n) \) where \((i_1, i_2, \ldots, i_n)\) is the representation of integer \( i = \sum_{0 \leq i \leq n-1} i_d q^k \) and \( i_1 \) is the least significant bit. Additionally, we denote the first \( N \) elements of the truncated sequence \( f \) by \( f^{(N)} \). For simplicity, we do not write the superscript of \( f^{(N)} \) in the following when the length \( N \) of the sequence has been specified.

In this letter, we set \( q = 3 \).

### 3. Proposed ZCTs Based on EBF

In this section, we will introduce two lemmas firstly, which are important in proving Theorem 1.

**Lemma 1:** With an integer \( k, 3^{n-1} + \sum_{\mu=h+1}^{n-1} p_\mu 3^{\mu-1} \leq k \leq 3^{n-1} + \sum_{\mu=h+1}^{n-1} p_\mu 3^{\mu-1} + 3^s \) where \( 1 \leq s \leq n-2, p_\mu \in \{0, 1, 2\}, n \geq 2 \) and \( h > s \), let \((k_1, k_2, \ldots, k_n)\) be the ternary representation of \( k \) then \( k' \) is an integer with ternary representation as \((k_1, k_2, \ldots, k_{n-1}, \beta + k_n, k_{n+1}, \ldots, k_n)\), where \( \beta \in \{1, 2\} \) and \( u \leq s \), then we obtain \( 3^{n-1} + \sum_{\mu=h+1}^{n-1} p_\mu 3^{\mu-1} \leq k' \leq 3^{n-1} + \sum_{\mu=h+1}^{n-1} p_\mu 3^{\mu-1} + 3^s \).

**Proof:** Let \((l_1, l_2, \ldots, l_n)\) be the ternary representation of \( l \) and \( l = k - 3^{n-1} - \sum_{\mu=h+1}^{n-1} p_\mu 3^{\mu-1} \). Therefore, \( 0 \leq l \leq 3^{s-1} \) which implies \( l = 0 \) for \( r \geq s + 1 \). Let \((l_1', l_2', \ldots, l_n')\) be the ternary representation of \( l' \) and \( l' = k' - 3^{n-1} - \sum_{\mu=h+1}^{n-1} p_\mu 3^{\mu-1} \). Due to the fact that \( k \) and \( k' \) vary in only one position \( u \leq s, l \) and \( l' \) are also differ in only one position \( u \). Then we can obtain \( l' = l = 0 \) for \( r \geq s + 1 \), which implies \( 0 \leq l' \leq 3^{s-1} \). Hence, we have \( 3^{s-1} + \sum_{\mu=h+1}^{n-1} p_\mu 3^{\mu-1} \leq k' \leq 3^{n-1} + \sum_{\mu=h+1}^{n-1} p_\mu 3^{\mu-1} + 3^s \).

**Lemma 2:** For the nonnegative integers \( s < h < n \), let \((k_1, k_2, \ldots, k_n)\) and \((l_1, l_2, \ldots, l_n)\) be the ternary representations of \( k \) and \( l \), respectively. Suppose \( k_r = 0, l_r = \beta \) \((\beta \in \{1, 2\})\) for some \( r > h \) and \( k_i = l_i \) for \( i = 1, 2, \ldots, s, h \), and \( r+1, r+2, \ldots, n \). Therefore, we obtain \( l - k \geq 2 \cdot 3^{h-1} + 3^s \).

**Proof:** The result that we obtain is
\[ l - k = \beta \cdot 3^{r-1} + \sum_{i=r+1,i \neq h} \sum_{s=1}^{n-1} p_i 3^{i-1} \geq \sum_{i=r+1,i \neq h} \sum_{s=1}^{n-1} 3^{i-1} - 3^{h-1} + 3^{s} + 2 \cdot 3^h \geq 2 \cdot 3^{h-1} + 3^s. \]

**Theorem 1:** For the integers \( s < h < n \), let \( \pi \) be a permutation of \( \{1, 2, \ldots, h\} \) with \( \pi(s + 1) = h \). Then we have the extended Boolean function

\[ f = \sum_{k=1}^{h-1} d_k x_{\pi(k)} x_{\pi(k+1)} + \sum_{k=s+1}^{n-1} c_k x_k. \]

**Proof:** For a ZCT \((a, b, c)\) with ZCZ width \( 2 \cdot 3^{h-1} + 3^s \), we have to show that \( R(a; \tau) + R(b; \tau) + R(c; \tau) \leq 2 \cdot 3^{h-1} + 3^s \).

**Case 1:** Suppose \( k_{\pi(1)} \neq l_{\pi(1)} \), we obtain \( \text{PAPR}(a, b, c) \leq 3 + \sum_{k=h+1}^{n-1} p_\mu 3^{\mu-1} \).

**Case 2:** Assume \( k_{\pi(1)} = l_{\pi(1)} \), \( k_h = l_h = 1 \) and \( k_{h+\mu} = l_{h+\mu} = 2 \) for all \( \mu = 1, 2, \ldots, n - h - 1 \). Then we have \( k_r = 0 \) for \( r = s + 1, s + 2, \ldots, h \). Let \( u \) be the smallest integer that makes \( k_{\pi(u)} \neq l_{\pi(u)} \) and we get \( \pi(u) - 1 \leq s \). Let \( k' \) and \( k'' \) be two integers different from \( k \) in only one position, i.e., \( k'_{\pi(u-1)} = \pi(u-1) + 1 \), \( k''_{\pi(u-1)} = 2 + k_{\pi(u-1)} \).
Similarly, we let \( l' \) and \( l'' \) differ from \( l \) in only one position, i.e., \( l'_{(u-1)} = 1 + l_{(u-1)} \) \( l''_{(u-1)} = 2 + l_{(u-1)} \). Then we have, 
\[ l' = k' + \tau \text{ and } l'' = k'' + \tau. \]
According to Lemma 1, we obtain \( k', k'', l', l'' \leq 3n^1 + \sum_{\mu=1}^{n-1} 2 \cdot 3^{\mu+1} + 3s - 1 \leq N - 1 \).
Then we have 
\[
\begin{align*}
    a_k - a_k &= d_{u-2}(k_{(u-2)}k_{(u-1)} - k_{(u-2)}k_{(u-1)}) \\
    &+ d_{u-1}(k'_{(u-1)}k_{(u-1)}) - k_{(u-1)}k_{(u-1)}) \\
    &+ \epsilon(u_{(1)}, l, k_{(u-1)}) = (k_{(u-1)})^2 = (k_{(u-1)})^2) \\
    &+ \epsilon(u_{(1)}, 1, (k'_{(u-1)} - k_{(u-1)})) \\
    &= d_{u-2}k_{(u-2)} + d_{u-1}k_{(u-1)} + c_{(u-1), 1} \\
    &+ c_{(u-1), 2}(1 + 2k_{(u-1)}).
\end{align*}
\]
Therefore, 
\[
\begin{align*}
    a_k - a_k &= a_{u-2}(l_{(u-2)}k_{(u-2)} - k_{(u-2)}k_{(u-2)}) \\
    &= d_{u-2}l_{(u-2)}k_{(u-2)}(l_{(u-2)}k_{(u-2)}) \\
    &= 2d_{u-1}(l_{(u-2)}k_{(u-2)}) - l_{(u-2)}k_{(u-2)}.
\end{align*}
\]

Similarly, we let 
\[ \pi_{(1)} \text{ and } k_{(1)} \text{ be the integers in Case 2. Hence, we obtain} \]
\[
\begin{align*}
    &a_k - a_k = \omega^{a_1-a_1} + \omega^{a_{u-2}-a_2} + \omega^{a_{u-1}-a_1} + \omega^{b_1-b_1} + \omega^{b_{u-2}-b_2} + \omega^{b_{u-1}-b_1} \\
    &+ \omega^{c_1-c_1} + \omega^{c_{u-2}-c_2} + \omega^{c_{u-1}-c_1} = 0.
\end{align*}
\]

**Remark 1:** The ZCT constructed in Theorem 1 can exist for all lengths other than powers of three. Additionally, in order to obtain a larger ZCT width, we set \( h = n - 1, s = n - 2 \) and \( p_\mu = 0 \), for \( \mu = 0, 1, \ldots, n - 1 \) in Theorem 1. Thus, we can obtain ZCTs of length \( N = 3n^1 + 3n^2 \) with ZCT width \( Z = 3n^1 \). And the width ratio of ZCT can reach a maximum of 3/4.

**Corollary 1:** When \( h = n - 1 \) and \( p_\mu = 0 \), for all \( \mu \), the PAPR upper bound for the ZCTs obtained through Theorem 1 is 5.

**Proof:** According to the proof of Theorem 1, Case 4 is the only case that needs to be considered here. In Case 4, we need to make \( \pi(u - 1) \leq s \). Since \( \{\pi(1), \pi(2), \ldots, \pi(s)\} = \{1, 2, \ldots, s\} \), we have \( u - 1 \leq s \) and \( u + s \leq 1 \). It can be obtained \( R(a; \tau) + R(b; \tau) + R(c; \tau) \neq 0 \) while \( k_{\pi(i)} = l_{\pi(i)} \) for \( i = 1, 2, \ldots, s + 1 \). So the number of \( \tau \) is \( 3n^s - 2 \) such that \( R(a; \tau) + R(b; \tau) + R(c; \tau) \neq 0 \). Additionally, when \( R(a; \tau) + R(b; \tau) + R(c; \tau) \neq 0 \), the maximum value for \( |R(a; \tau) + R(b; \tau) + R(c; \tau)| \) is \( 3n^s + 1 \). Therefore,
\[
\begin{align*}
    \text{PAPR}(G) &\leq 3 + 2 \sum_{\tau=1}^{N-1} |R(a; \tau) + R(b; \tau) + R(c; \tau)| \\
    &\leq 3 + 2 \cdot 3^s + 3^n - 2 = 3 + 2 \cdot 3n^1 - N \leq 5.
\end{align*}
\]

**Example 1:** Taking \( n = 4, h = 3, s = 2, \pi = (2, 1, 3), d_1 = 2, d_2 = 1, c_{h, 1} = 0, c_{h, 2} = 0, c_{h, 3} = 0 \) and \( p_\mu = 0 \) for all \( k \) and \( \mu \), by the construction in Theorem 1 the extended Boolean function is \( f = 2x_1x_2 + x_3x_4 \). Since we have a three phase (36, 27)-ZCT. And the PAPRs of \( a, b \) and \( c \) are 4,000, 4,019 and 4,020, respectively. We illustrate their IAPRs in Fig. 1.

Table 1 illustrates the comparisons of our construction with existing constructions about 3-phase ZCTs and binary ZCPs. Our proposed EGBF direct construction methods achieve the advantages of more flexible lengths and larger ZCT ratios simultaneously.
4. Conclusion

In this letter, a construction based on extended Boolean functions has been presented for the three-phase ZCTs with all lengths other than powers of three. The width ratio of ZCZ can also reach the value $3/4$, which is a relatively large value obtained through existing direct methods in the literature. In addition, the upper bound of the PAPR for the constructed ZCTs has been obtained in Corollary 1.

References


Table 1 A comparison of the main parameters.

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Form</th>
<th>Length</th>
<th>max ZCZ Method ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>[24]</td>
<td>3-phase GCT</td>
<td>$3^n$</td>
<td>EGBF</td>
</tr>
<tr>
<td>[17]</td>
<td>3-phase ZCT</td>
<td>$3M + 1$</td>
<td>$\approx 2/3$</td>
</tr>
<tr>
<td>[19]</td>
<td>Binary ZCP</td>
<td>$2^{n-1} + 2^s$</td>
<td>2/3</td>
</tr>
<tr>
<td>[20]</td>
<td>Binary ZCP</td>
<td>$2^{n-1} + \sum_{l=k+1}^{n} a_l 2^{l-1} + 2^u$</td>
<td>2/3</td>
</tr>
<tr>
<td>[25]</td>
<td>Binary ZCP</td>
<td>$2^{m-1} + 2$</td>
<td>3/4</td>
</tr>
</tbody>
</table>

Here, $n \geq 2$, $s \leq n - 2$, $p_M \in (0, 1, 2)$, $M \neq 4 \pmod{6}$, $0 < k < n, \pi (v + 1) = k$ and $m \geq 4$. 