TWO NEW CLASSES OF BINARY SEQUENCE PAIRS WITH THREE-LEVEL CROSS-CORRELATION

XIAOHUI LIU AND JINHUA WANG*

School of Sciences
Nantong University
Nantong, Jiangsu 226007, China

DIANHUA WU

Department of Mathematics
Guangxi Normal University
Guilin, Guangxi 541004, China

(Communicated by Cunsheng Ding)

Abstract. A pair of binary sequences is generalized from the concept of a two-level autocorrelation function of single binary sequence. In this paper, we describe two classes of binary sequence pairs of period \( N = 2^q \), where \( q = 4f + 1 \) is an odd prime and \( f \) is an even integer. Those classes of binary sequence pairs are based on cyclic almost difference set pairs. They have optimal three-level cross-correlation, and either balanced or almost balanced.

1. Introduction

Let \( s = (s(0), s(1), \cdots, s(N-1)) \) and \( t = (t(0), t(1), \cdots, t(N-1)) \) be two binary (0,1)-sequences of the same period \( N \). The periodic cross-correlation function of the sequence pair \( (s, t) \) at shift \( 0 \leq \tau < N \) is defined as

\[
R_{(s, t)}(\tau) = \sum_{j=0}^{N-1} (-1)^{s(j)-t(j+\tau)}
\]

where subscript \( j+\tau \) takes modulo \( N \).

When sequences \( s \) and \( t \) are identical, their correlation is called an auto-correlation and denoted by \( R_s(\tau) \). Generally, a periodic binary sequence is said to have two-level auto-correlation if all its out-of-phase correlation coefficients are some fixed constant which is different from the in-phase correlation value, that is

\[
R_s(\tau) = \begin{cases} 
N, & \text{if } \tau = 0; \\
E(\neq N), & \text{otherwise}, 
\end{cases}
\]

and when \( E = 0 \) we say that \( s \) is a perfect binary sequence. Sequences with good auto-correlation properties have wide applications. When the absolute value of \( E \) is as small as possible, it is quite useful for many applications in measurement, digital communication, and radar. An important problem in sequence design is to find sequences with optimal auto-correlation. However, it is believed that no binary

2010 Mathematics Subject Classification: Primary: 05B10; Secondary: 94A55.

Key words and phrases: Binary sequence pair, almost difference set pair, three-level cross-correlation, optimal correlation value, cyclotomy.

* Corresponding author.
perfect sequences of length other than 4 exist [9]. As a further possible remedy, Zhao in [18] introduced a new class of discrete signal sequence pair \((s, t)\). The desired information is extracted from the received signal using the periodic cross-correlation of the transmitter signal \(s\) and the receiver signal \(t\). In such way, many more useful signals can be used in many areas of engineering and sciences.

Let \((s, t)\) be a sequence pairs and \(H\) be a subset of \(\mathbb{Z}_N^* = \mathbb{Z}_N \setminus \{0\}\). Let the periodic cross-correlation function of the sequence pair \((s, t)\)

\[
R_{(s, t)}(\tau) = \sum_{j=0}^{N-1} (-1)^{s(j) - t(j+\tau)} = \begin{cases} 
F, & \tau = 0 \text{ and } F \neq E_1, E_2; \\
E_1, & \tau \in H; \\
E_2, & \tau \in \mathbb{Z}_N^* - H.
\end{cases}
\]

where the set \(\mathbb{Z}_N^* - H\) is formed by the elements that are present in \(\mathbb{Z}_N^*\), but not in \(H\). When \(E_1 = E_2 = 0\), the sequence pair \((s, t)\) is called a \textit{perfect binary sequence pair}, otherwise we call it the sequence pair with \textit{two-level or three-level correlation} [11, 12]. The concept of perfect binary sequence pair was first introduced in [18]. Jin and Song in [8] constructed a class of perfect binary sequence pair whose in-phase correlation is 4 and period is every multiple of 4. When \(E_1 = E_2 = -1\), the binary sequence pair is called \textit{the ideal two-level correlation binary sequence pair} which was first introduced in [12] and constructed in [7] based on cyclotomic classes of order 2, 4, and 6. From Lemma 2.2 in Section 2, we can prove that the even period binary sequence pair has even out-of-phase correlation values and the odd period binary sequence pair has odd out-of-phase correlation values. When \(N\) is even, it is concluded that the smallest difference number of the two out-of-phase correlations \(|E_1 - E_2|\) is 4 and the smallest out-of-phase correlation values are \(\{0, -4\}\), \(\{0, 4\}\) or \(\{2, -2\}\). In this case, we say the sequence pair with \textit{optimal correlation value}.

Peng et. al in [13] gave two new constructions of binary sequence pairs with out-of-phase correlations \(\{0, -4\}\) and period \(N \equiv 0 \pmod{4}\) based on cyclotomy and interleaving technique.

In this paper, we will present two new classes of binary sequence pairs with out-of-phase correlations \(\{2, -2\}\) and period \(N = 2q\), where \(q \equiv 1 \pmod{16}\) is prime and has a quadratic partition of form \(q = 1 + 4y^2\). The sequence will be either balanced or almost balanced, that is, two more zeros than ones in each period. See Table 1 for all the lengths \(N \leq 15000\) our construction applies for.

**Table 1.** Sequence pairs with out-of-phase correlations \(\{2, -2\}\) and period \(N = 2q\) covered by theorems in this paper

| Period \(N = 2q\) | Prime \(q\) | Optimal correlation value by theorem |
|-------------------|-------------|------------------------------------|
| 34                | 17          | Theorems 4.2, 5.1, 5.2             |
| 514               | 257         | Theorems 4.2, 5.1, 5.2             |
| 802               | 401         | Theorems 4.2, 5.1, 5.2             |
| 1154              | 577         | Theorems 4.2, 5.1, 5.2             |
| 2594              | 1297        | Theorems 4.2, 5.1, 5.2             |
| 3202              | 1601        | Theorems 4.2, 5.1, 5.2             |
| 14114             | 7057        | Theorems 4.2, 5.1, 5.2             |

This paper is organized as follows. Section 2 introduces the notation and the related results required for our constructions, including the important notion of difference set pair, almost difference set pair, and cyclotomy. In Section 3, we present the idea of our constructions for the binary sequence pairs with three-level
correlation. In Sections 4 and 5, we give two new constructions of binary sequence pairs with out-of-phase correlations \(\{2, -2\}\) based on cyclotomy.

2. Preliminaries

It is well known that a binary sequence with two-level auto-correlation is equivalent to a difference set \([1]\), and a binary sequence with three-level auto-correlation is equivalent to an almost difference set \([4, 5]\). As an analogy, Xu in \([17]\) proposed the concept of difference set pair (DSP) and established the relationship between binary sequence pair with two-level cross-correlation and difference set pair. Li and Ke in \([10]\) introduced the concept of almost difference set pair (ADSP) and the relationship between binary sequence pair with three-level cross-correlation and almost difference set pair was also built. Many more examples can be seen in \([7, 11, 16]\).

Let \(U = \{u_i \mid 1 \leq i \leq k\}\) and \(V = \{v_i \mid 1 \leq i \leq k'\}\) be two subsets of \(Z_N\) with \(k\) and \(k'\) elements, respectively. Let \(e = |U \cap V|\), where \(|A|\) denotes the number of elements in the set \(A\). Then \((U, V)\) is called an \((N, k, k', e, \lambda)-difference\) set pair (DSP) if every nonzero element \(g \in Z_N^*\) can be expressed in exactly \(\lambda\) ways in the form \(u_i - v_j \equiv g \pmod{N}\), where \(u_i \in U\) and \(v_j \in V\). Furthermore, let \(H\) be the nonzero subset of \(Z_N\), then \((U, V)\) is called an \((N, k, k', e, \lambda_1, \lambda_2)-almost\) difference set pair (ADSP) if the list of differences \(u_i - v_j : u_i \in U,\) and \(v_j \in V\) contains each nonzero element of \(H\) exactly \(\lambda_1\) times and each element of \(Z_N - H\) exactly \(\lambda_2\) times. If \(\lambda_1 = \lambda_2\), \((U, V)\) is called a difference set pair. And if \(U = V\), an almost difference set pair is called an almost difference set. We define the difference function

\[
d_{(U,V)}(\tau) = |\{(U \cap (V + \tau)\}|
\]

where \(V + \tau := \{v + \tau \mid v \in V\}\). Then \((U, V)\) is an \((N, k, k', e, \lambda_1, \lambda_2)-ADSP\) in \(Z_N\) if and only if \(d_{(U,V)}(\tau)\) takes on the value \(\lambda_1\) altogether \(h\) times and the value \(\lambda_2\) altogether \(N - 1 - h\) times when \(\tau\) ranges over all the nonzero elements of \(Z_N\). Thus, we have

**Lemma 2.1.** For \((N, k, k', e, \lambda_1, \lambda_2)-ADSP\) in \(Z_N\), we have the following necessary condition:

\[
kk' = e + \lambda_1 h + (N - 1 - h) \lambda_2
\]

where \(h = |H|\).

Let \(s = (s(0), s(1), \cdots, s(N - 1))\) be an \(N\)-periodic binary sequence, and \(U\) be a subset of \(Z_N\). If \(U = \{j : s(j) = 1, 1 \leq j < N\}\), the set \(U\) is called the characteristic set of \(s\), and \(s\) is called the characteristic sequence of \(U\).

The following lemma establishes the connection between the correlation of binary sequence pair with three-level cross-correlation and almost difference set pair.

**Lemma 2.2** \([10]\). Let \(U\) and \(V\) be two subsets of \(Z_N\), and \(H\) be the nonzero subset of \(Z_N\), \(s = (s(0), s(1), \cdots, s(N - 1))\) and \(t = (t(0), t(1), \cdots, t(N - 1))\) be two characteristic sequences of \(U\) and \(V\) respectively, then the relationship between the parameters \((N, k, k', e, \lambda_1, \lambda_2)\) of ADSP \((U, V)\) and periodic cross-correlation of binary sequence pair \((s, t)\) is

\[
R_{(s,t)}(\tau) = \begin{cases} 
N - 2(k + k') + 4e, & \text{for } \tau = 0; \\
N - 2(k + k') + 4\lambda_1, & \text{for } \tau \in H; \\
N - 2(k + k') + 4\lambda_2, & \text{for } \tau \in Z_N^* - H.
\end{cases}
\]
Cyclotomy is a powerful method for constructing almost difference set pairs. We introduce a number of results related to cyclotomy, which will be needed in the sequel.

Let \( q \) be a power of an odd prime, and let \( \alpha \) be a generator of \( GF(q)^* \). Assume that \( q - 1 = ef \), where \( e > 1 \) and \( f > 1 \) are integers. Define \( D_0^{(e)} \) to be the subgroup of \( GF(q)^* \) generated by \( \alpha^e \), and let \( D_i^{(e)} = \alpha^i D_0^{(e)} \) for each \( i \) with \( 0 \leq i \leq e - 1 \). These \( D_i^{(e)} \) are called cyclotomic classes of order \( e \) with respect to \( GF(q) \).

The cyclotomic numbers of order \( e \), denoted \((i, j)_e\), is the number of solutions of the equation

\[
x + 1 = y, \quad x \in D_i^{(e)}, \quad y \in D_j^{(e)},
\]

that is, the number \((i, j)_e = |(D_i^{(e)} + 1) \cap D_j^{(e)}|\), where \( 0 \leq i, j \leq e - 1 \).

The following lemma concludes several well-known properties of cyclotomic numbers.

**Lemma 2.3** ([2, 3, 14, 15]). Let symbols and notations be the same as before. Then

1. \((i, j)_e = (i', j')_e\), where \( i \equiv i' \mod e \) and \( j \equiv j' \mod e \);
2. \((i, j)_e = (e - i, j - i)_e = \begin{cases} (j, i)_e, & \text{if } f \text{ even;} \\ (j + e/2, i + e/2)_e, & \text{if } f \text{ odd;} \end{cases}\)
3. \(\sum_{i=0}^{e-1}(i, i+j)_e = \begin{cases} f - 1, & \text{if } j = 0; \\ f, & \text{if } j \neq 0; \end{cases}\)
4. \(\sum_{j=0}^{e-1}(i, j)_e = f - \theta_i\), where
   \[
   \theta_i = \begin{cases} 1, & \text{if } i = 0 \text{ and } f \text{ even;} \\ 1, & \text{if } i = \frac{e}{2} \text{ and } f \text{ odd;} \\ 0, & \text{otherwise;} \end{cases}\)
5. \(\sum_{i=0}^{e-1}(i, j)_e = f - \eta_j\), where
   \[
   \eta_j = \begin{cases} 1, & \text{if } j = 0; \\ 0, & \text{otherwise}. \end{cases}\)

**Lemma 2.4** ([2, 3]). Let symbols and notations be the same as before and \( g \in D_k^{(e)} \). Then the number of solutions \((x, y)\) of the equation

\[
x + g = y, x \in D_i^{(e)}, y \in D_j^{(e)}
\]

is \((i - k, j - k)_e\).

**Lemma 2.5** ([14, p. 51]). Let \( q - 1 = 4f \), where \( f \) is even. The cyclotomic numbers of order 4 are determined by Table 2 together with the relations

\[
16A = q - 11 - 6x, \\
16B = q - 3 + 2x + 8y, \\
16C = q - 3 + 2x, \\
16D = q - 3 + 2x - 8y, \\
16E = q + 1 - 2x,
\]

where \( q = x^2 + 4y^2, x \equiv 1 \text{ (mod 4)} \) is the proper representation of \( q = p^n \) if \( p \equiv 1 \text{ (mod 4)} \); the sign of \( y \) is ambiguously determined.
3. The idea of our construction

In this paper, we will give several new families of binary sequence pairs of period \( N = 2q \) with optimal correlation \( \{2, -2\} \), where \( q \) is an odd prime. Finding sequence pairs with three-level correlation will be equivalent to constructing almost difference set pairs, as made clear before.

By the Chinese Remainder Theorem, \( Z_N \cong Z_2 \times Z_q \) under the isomorphism \( \phi: \omega \to (\omega \pmod{2}, \omega \pmod{q}) \) (see, [6]). Therefore, construction of almost difference set pairs over \( Z_N \) is equivalent to that of almost difference set pairs over \( Z_2 \times Z_q \).

Let \( U' = \{0\} \times C_0 \cup \{1\} \times C_1, V' = \{0\} \times C_2 \cup \{1\} \times C_3 \), where \( C_i \subseteq Z_q, 0 \leq i \leq 3 \). Define \( \tau = (\omega_1, \omega_2) \in Z_2 \times Z_q \). Then we may evaluate the difference function as follows:

\[
d_{(U', V')}((\omega_1, \omega_2)) = |U' \cap (V' + (\omega_1, \omega_2))| \]
\[
= |(\{0\} \times C_0 \cup \{1\} \times C_1) \cap (\{0\} \times C_2 \cup \{1\} \times C_3 + (\omega_1, \omega_2))| \]
\[
= |\{0\} \times C_0 \cap (\{0\} \times C_2 + (\omega_1, \omega_2))| + |\{0\} \times C_0 \cap (\{1\} \times C_3 + (\omega_1, \omega_2))| \]
\[
+ |\{1\} \times C_1 \cap (\{0\} \times C_2 + (\omega_1, \omega_2))| + |\{1\} \times C_1 \cap (\{1\} \times C_3 + (\omega_1, \omega_2))| \]
\[
= |\{0\} \times C_0 \cap \{\omega_1\} \times (C_2 + \omega_2)| \]
\[
+ |\{0\} \times C_0 \cap \{1 + \omega_1\} \times (C_3 + \omega_2)| \]
\[
+ |\{1\} \times C_1 \cap \{\omega_1\} \times (C_2 + \omega_2)| \]
\[
+ |\{1\} \times C_1 \cap \{1 + \omega_1\} \times (C_3 + \omega_2)| \]
\[
= \begin{cases} 
| C_0 \cap C_2 | + | C_1 \cap C_3 |, & \text{if } \omega_1 = 0, \omega_2 = 0; \\
| C_0 \cap (C_2 + \omega_2) | + | C_1 \cap (C_3 + \omega_2) |, & \text{if } \omega_1 = 0, \omega_2 \neq 0; \\
| C_0 \cap (C_3 + \omega_2) | + | C_1 \cap (C_2 + \omega_2) |, & \text{if } \omega_1 = 1, \omega_2 \neq 0; \\
| C_0 \cap C_3 | + | C_1 \cap C_2 |, & \text{if } \omega_1 = 1, \omega_2 = 0. 
\end{cases} 
\tag{3.7}
\]

Let \( U = \phi^{-1}(U') \), \( V = \phi^{-1}(V') \), and \( s, t \) be two characteristic sequences of \( U \) and \( V \), respectively. If \( (U, V) \) is an almost difference set pair and \( (s, t) \) is a binary sequence pair with optimal correlation \( \{2, -2\} \) of length \( N = 2q \), then by Lemma 2.2,

\[
N - 2(k + k') + 4d_{(U', V')}(\tau) = \pm 2, 
\tag{3.8}
\]

which means

\[
d_{(U', V')}(\tau) = \frac{2(k + k' \pm 1) - N}{4}. 
\tag{3.9}
\]
So we have
\begin{equation}
(3.10) \quad |C_0 \cap C_3| + |C_1 \cap C_2| = \frac{2(k + k' \pm 1) - N}{4} = \frac{k + k' \pm 1 - q}{2}
\end{equation}
where \(k = |U| = |C_0| + |C_1|, \quad k' = |V| = |C_2| + |C_3|\). This gives us some hint about how we should choose our \(C_i\). In the following two sections, we shall use cyclotomic classes to form our \(C_i\) and then look for conditions to ensure that our \((U, V)\) is an almost difference set pair. Such an almost difference set pair will give us a binary sequence pair with optimal correlation \(\{2, -2\}\).

4. Construction of almost balance sequence pairs with optimal three-level cross-correlation

In the remainder of this paper, we consider cyclotomic classes \(D_i^{(4)}\) with respect to \(GF(q)\) and cyclotomic numbers of order 4. For simplicity, let \(D_i\) denote \(D_i^{(4)}\). And all symbols and notations are the same as in Sections 2 and 3. Let \(|U'| = k, |V'| = k', s, t\) be two characteristic sequences of \(U\) and \(V\). If \(k = k' = N/2\), we say that \(s, t\) are balanced. If \(k = k' = N/2 - 1\), we say that \(s, t\) are almost balanced. For almost balance sequence pairs, by (3.9) we have
\begin{equation}
d_{(U, V')}(\tau) = \frac{2(k + k' \pm 1) - N}{4} = \frac{2(N - 2 \pm 1) - N}{4} = \frac{N - 2}{4} \quad \text{or} \quad \frac{N - 6}{4}.
\end{equation}
So we have \(|C_0 \cap C_3| + |C_1 \cap C_2| = \frac{N - 2}{4}\) or \(\frac{N - 6}{4}\), since \(N = 2q\), which is equivalent to \(\frac{q - 1}{2}\) or \(\frac{q - 3}{2}\).

Now we shall use cyclotomic classes to form our \(C_i\) and then look for conditions to ensure that our \((U, V)\) is an almost difference set pair.

Let \(q = 4f + 1\) be a prime and \(f\) be even, and let \(U' = \{0\} \times C_0 \cup \{1\} \times C_1, V' = \{0\} \times C_2 \cup \{1\} \times C_3\), where
\begin{equation}
C_0 = D_i \cup D_j, C_1 = D_i \cup D_k, C_2 = D_l \cup D_k, C_3 = D_l \cup D_j
\end{equation}
and \(i, j, l, k\) are four pairwise distinct integers between 0 and 3. It is clear that
\begin{equation}
|C_0| = |C_1| = |C_2| = |C_3| = \frac{q - 1}{2}.
\end{equation}
We now consider the number of times each element appears in differences of two elements of \(U'\) and \(V'\). Recall Eq. 3.7, we have:

For \(\omega_1 = 0, \omega_2 = 0\), it is clear that
\begin{equation}
d_{(U', V')}(\omega_1, \omega_2) = |C_0 \cap C_2| + |C_1 \cap C_3| = 0.
\end{equation}

For \(\omega_1 = 1, \omega_2 = 0\), it is clear that
\begin{equation}
d_{(U', V')}(\omega_1, \omega_2) = |C_0 \cap C_3| + |C_1 \cap C_2| = \frac{q - 1}{2}.
\end{equation}

For \(\omega_1 = 0, \omega_2 \neq 0\), or \(\omega_2 \in D_k\), then we have
\begin{equation}
d_{(U', V')}(\omega_1, \omega_2) = |C_0 \cap (C_2 + \omega_2)| + |C_1 \cap (C_3 + \omega_2)| = |(D_i \cup D_j) \cap (D_l \cup D_k + \omega_2)| + |(D_i \cup D_k) \cap (D_l \cup D_j + \omega_2)| = |D_i \cap (D_l + \omega_2)| + |D_i \cap (D_k + \omega_2)| + |D_j \cap (D_l + \omega_2)| + |D_j \cap (D_k + \omega_2)| + |D_k \cap (D_l + \omega_2)| + |D_k \cap (D_j + \omega_2)| + |D_l \cap (D_j + \omega_2)| + |D_l \cap (D_k + \omega_2)|.
Note that Eq 4.15 and Eq 4.16 are also from Lemmas 2.4 and 2.3, respectively.

For \( n_0 \) (4.15)

\[
\sum_{t=0}^{\frac{3}{2}} (t, i - h) - (i - h, i - h)
\]

\[
+ \sum_{t=0}^{\frac{3}{2}} (l - h, t) - (l - h, l - h) + 2(k - h, j - h)
\]

\[
= \begin{cases} 
  f - (l - i, l - i) + f - 1 - (0, 0) + 2(k - i, j - i), & \text{if } h = i; \\
  f - (l - j, l - j) + f - (i - j, i - j) + 2(k - j, 0), & \text{if } h = j; \\
  f - (l - k, l - k) + f - (i - k, i - k) + 2(0, j - k), & \text{if } h = k; \\
  f - 1 - (0, 0) + f - (i - l, i - l) + 2(k - l, j - l), & \text{if } h = l.
\end{cases}
\]

Note that Eq 4.13 and Eq 4.14 are from Lemmas 2.4 and 2.3, respectively.

For \( \omega_1 = 1, \omega_2 \neq 0 \), let \( \omega_2 \in D_h \), then we have

\[
d_{(U, V)}((\omega_1, \omega_2)) = |C_0 \cap (C_3 + \omega_2)| + |C_1 \cap (C_2 + \omega_2)|
\]

\[
= |(D_1 \cup D_2) \cap (D_1 \cup D_2 + \omega_2)| + |(D_3 \cup D_4) \cap (D_3 \cup D_4 + \omega_2)|
\]

\[
= |D_1 \cap (D_1 + \omega_2)| + |D_1 \cap (D_1 + \omega_2)|
\]

\[
+ |D_2 \cap (D_2 + \omega_2)| + |D_2 \cap (D_2 + \omega_2)|
\]

\[
+ |D_3 \cap (D_3 + \omega_2)| + |D_3 \cap (D_3 + \omega_2)|
\]

\[
+ |D_4 \cap (D_4 + \omega_2)| + |D_4 \cap (D_4 + \omega_2)|
\]

\[
(4.15)
\]

\[
= \sum_{t=0}^{\frac{3}{2}} (t, i - h) - (i - h, i - h)
\]

\[
+ \sum_{t=0}^{\frac{3}{2}} (l - h, t) - (l - h, l - h) + 2(k - h, j - h)
\]

\[
= \begin{cases} 
  f - 1 - (0, 0) + f - (l - i, l - i) + (j - i, j - i) + (k - i, k - i), & \text{if } h = i; \\
  f - (i - j, i - j) + f - (l - j, l - j) + (0, 0) + (k - j, k - j), & \text{if } h = j; \\
  f - (i - k, i - k) + f - (l - k, l - k) + (j - k, j - k) + (0, 0), & \text{if } h = k; \\
  f - (i - l, i - l) + f - 1 - (0, 0) + (j - l, j - l) + (k - l, k - l), & \text{if } h = l.
\end{cases}
\]

Note that Eq 4.15 and Eq 4.16 are also from Lemmas 2.4 and 2.3, respectively.

We have defined that \( U \) and \( V \) are the characteristic sets for \( s \) and \( t \). The quaternion \((i, j, l, k)\) will be called the defining set for the sequences \( s \) and \( t \). Recall Lemma 2.2 that the cross-correlation values are dependent on the difference function. The next result gives us the evaluation of this function for a certain defining set \((i, j, l, k)\).

**Lemma 4.1.** For \((i, j, l, k) = (1, 2, 3, 0)\), we have

\[
d_{(U, V)}((\omega_1, \omega_2)) = \begin{cases} 
  0, & \text{if } \omega_1 = 0, \omega_2 = 0; \\
  \frac{q - 1}{2}, & \text{if } \omega_1 = 0, \omega_2 \neq 0; \\
  \frac{q^2 - 2}{2}, & \text{if } \omega_1 = 1, \omega_2 \in D_0 \text{ or } \omega_2 \in D_2; \\
  \frac{q^2 + q - 2}{2}, & \text{if } \omega_1 = 1, \omega_2 \in D_1 \text{ or } \omega_2 \in D_3; \\
  \frac{q^2 - 1}{2}, & \text{if } \omega_1 = 1, \omega_2 = 0.
\end{cases}
\]
Proof. For \( \omega_1 = 0, \omega_2 = 0 \), the conclusion is from Eq 4.11. For \( \omega_1 = 1, \omega_2 = 0 \), the conclusion is from Eq 4.12. For \( \omega_1 = 0, \omega_2 \neq 0 \), applying Eq 4.14 and Lemma 2.5 gives the conclusion. Similarly, for \( \omega_1 = 1, \omega_2 \neq 0 \), applying Eq 4.16 and Lemma 2.5 gives the desired. This completes the proof. \( \square \)

In the same manner, we may calculate \( d_{(U',V')}(\omega_1,\omega_2) \) for possible defining sets \((i,j,l,k)\). In fact, if \((i,j,l,k) = (3,2,1,0), (1,0,3,2)\) or \((3,0,1,2)\), we may calculate the results which are similar to that of Lemma 4.1.

**Theorem 4.2.** Let \( q = 4f + 1 = x^2 + 4y^2 \), where \( x = 1 \) and \( f \) is even, and let \( U' = \{0\} \times (D_1 \cup D_2) \cup \{1\} \times (D_1 \cup D_3) \), \( V' = \{0\} \times (D_1 \cup D_2) \cup \{1\} \times (D_1 \cup D_3) \), then \((U',V')\) is an \((N,N/2-1,N/2-1,0,(N-2)/4,(N-6)/4)\)-ADSP, and the length \( N = 2q \) characteristic sequence pair \((s,t)\) of \((U,V)\) has optimal cross-correlation if the defining set \((i,j,l,k) = (1,2,3,0),(3,2,1,0),(1,0,3,2)\) or \((3,0,1,2)\) when \( x = 1 \) the value set of

\[
d_{(U',V')}(\omega_1,\omega_2) = \frac{q-1}{2} \quad \text{or} \quad \frac{q-3}{2},
\]

whenever \((\omega_1,\omega_2) \neq (0,0)\). Then \((U',V')\) is an \((N,N/2-1,N/2-1,0,(N-2)/4,(N-6)/4)\)-ADSP.

From Lemma 2.2, the sequence pairs induced by the almost difference set pairs have three cross-correlation values:

\[
R_{(s,t)}((\omega_1,\omega_2)) = \begin{cases} 
-N + 4, & \text{if } (\omega_1,\omega_2) = (0,0); \\
-2, & \text{if } \omega_1 = 1,\omega_2 \in D_0 \text{ or } \omega_2 \in D_2; \\
2, & \text{otherwise}.
\end{cases}
\]

This completes the proof. \( \square \)

To illustrate the sequences described in Theorem 4.2, we consider the following example.

**Example 4.3.** Take \( q = 17 = 1 + 4 \times 2^2 \), and define \( N = 2q = 34 \). We use the primitive root 3 modulo 17 to define the cyclotomic classes. Then \( D_0 = \{1,13,16,4\}, D_1 = \{3,5,14,12\}, D_2 = \{9,15,8,2\}, D_3 = \{10,7,11,6\} \). We take \((i,j,l,k) = (1,2,3,0)\). Then \( U' = \{0\} \times D_1 \cup \{0\} \times D_2 \cup \{1\} \times D_1 \cup \{1\} \times D_0 \), \( V' = \{0\} \times D_3 \cup \{0\} \times D_0 \cup \{1\} \times D_3 \cup \{1\} \times D_2 \). Hence

\[
U = \phi^{-1}(U') = \{20,22,14,12,26,32,8,2,3,5,31,29,1,13,33,21\},
\]

\[
V = \phi^{-1}(V') = \{10,24,28,6,18,30,16,4,27,7,11,23,9,15,25,19\}.
\]

The corresponding binary sequence pair is

\[(s,t) = (01110100100011110000011100010010111, 000010110110001101100011101101000)\]

which has optimal cross-correlation.
5. Construction of balance sequence pairs with optimal three-level cross-correlation

The sequence pairs with optimal three-level cross-correlation constructed in Section 4 are almost balanced. In this section, we modify the construction and give a class of balanced binary sequence pairs with optimal three-level cross-correlation.

We define the sets \( U \) and \( V \) in a slightly different way. We complement the bit in position 0 or \( q \) of the sequences given in Section 4. As in Section 4, let
\[
U' = \{0\} \times C_0 \cup \{1\} \times C_1, \quad V' = \{0\} \times C_2 \cup \{1\} \times C_3,
\]
and
\[
C_0 = D_i \cup D_j, \quad C_1 = D_i \cup D_k, \quad C_2 = D_l \cup D_k, \quad C_3 = D_l \cup D_j,
\]
where \( i, j, l \) and \( k \) are pairwise distinct integers between 0 and 3. To complement the bit in position 0, define
\[
U_0' = \{0\} \times C_0 \cup \{1\} \times C_1, \quad V_0' = \{0\} \times C_2 \cup \{1\} \times C_3,
\]
and
\[
C_0 = D_i \cup D_j \cup \{0\}, \quad C_1 = D_i \cup D_k, \quad C_2 = D_l \cup D_k \cup \{0\}, \quad C_3 = D_l \cup D_j,
\]
and to complement the bit in position \( q \), define
\[
U_q' = \{0\} \times C_0 \cup \{1\} \times C_1, \quad V_q' = \{0\} \times C_2 \cup \{1\} \times C_3,
\]
and
\[
C_0 = D_i \cup D_j, \quad C_1 = D_i \cup D_k \cup \{0\}, \quad C_2 = D_l \cup D_k, \quad C_3 = D_l \cup D_j \cup \{0\}.
\]

Let
\[
U_0 = \phi^{-1}(U_0'), \quad V_0 = \phi^{-1}(V_0'), \quad U_q = \phi^{-1}(U_q'), \quad V_q = \phi^{-1}(V_q')
\]
and \((s, t)\) be a corresponding characteristic sequence pair for \((U_0, V_0)\) or \((U_q, V_q)\). As we did before, we must calculate the difference function for \((U_0', V_0')\) and \((U_q', V_q')\).

For \((U_0', V_0')\),
\[
d(U_0', V_0')((\omega_1, \omega_2))
\]
\[
= |U_0' \cap (V_0' + (\omega_1, \omega_2))| = |((\{0\} \times C_0 \cup \{1\} \times C_1) \cap (\{0\} \times C_2 \cup \{1\} \times C_3) + (\omega_1, \omega_2))|
\]
\[
= \begin{cases} 
|C_0 \cap C_2| + |C_1 \cap C_3|, & \text{if } \omega_1 = 0, \omega_2 = 0, \\
|C_0 \cap (C_2 + \omega_2)| + |C_1 \cap (C_3 + \omega_2)|, & \text{if } \omega_1 = 0, \omega_2 \neq 0, \\
|C_0 \cap (C_3 + \omega_2)| + |C_1 \cap (C_2 + \omega_2)|, & \text{if } \omega_1 = 1, \omega_2 \neq 0, \\
|C_0 \cap C_3| + |C_1 \cap C_2|, & \text{if } \omega_1 = 1, \omega_2 = 0,
\end{cases}
\]
\[
= \begin{cases} 
1, & \text{if } \omega_1 = 0, \omega_2 = 0, \\
d(U, V)((\omega_1, \omega_2)) + |D_i \cap \{\omega_2\}| + |D_j \cap \{\omega_2\}| + |\{0\} \cap \{\omega_2\}| + |\{0\} \cap (D_i + \omega_2)|, & \text{if } \omega_1 = 0, \omega_2 \neq 0, \\
d(U, V)((\omega_1, \omega_2)) + |\{0\} \cap (D_i + \omega_2)| + |D_i \cap \{\omega_2\}|, & \text{if } \omega_1 = 1, \omega_2 \neq 0, \\
q^{-1}, & \text{if } \omega_1 = 1, \omega_2 = 0.
\end{cases}
\]
Theorem 5.1. Let \( q = 4f + 1 = x^2 + 4y^2 \), where \( x = 1 \) and \( f \) is even, and let \( U'_0 = \{0\} \times \{D_1 \cup D_2 \cup \{0\}\} \cup \{1\} \times \{D_1 \cup D_2 \cup \{0\}\}, V'_0 = \{0\} \times \{D_1 \cup D_2 \cup \{0\}\} \cup \{1\} \times \{D_1 \cup D_2 \cup \{0\}\} \), then \((U'_0, V'_0)\) is an \((N, N/2, N/2, 1, (N - 2)/4, (N + 2)/4)\)-ADSP, and the length \( N = 2q \) characteristic sequence pair \((s, t)\) of \((U_0, V_0)\) has optimal cross-correlation if the defining set \((i, j, l, k)\) is \((1, 2, 3, 0), (3, 2, 1, 0), (1, 0, 3, 2)\) or \((3, 0, 1, 2)\).

Proof. We have given the value of \( d_{(U'_0, V'_0)}(\omega_1, \omega_2) \) by Lemma 4.1 for \((i, j, l, k) = (1, 2, 3, 0)\). By the discussion before Theorem 5.1, we have

\[
d_{(U'_0, V'_0)}(\omega_1, \omega_2) = \begin{cases} 
1, & \text{if } \omega_1 = 0, \omega_2 = 0, \\
\frac{q + 1}{2}, & \text{if } \omega_1 = 0, \omega_2 \neq 0, \\
\frac{q - x}{2}, & \text{if } \omega_1 = 1, \omega_2 \neq D_0 \text{ or } \omega_2 \in D_2, \\
\frac{q + y}{2}, & \text{if } \omega_1 = 1, \omega_2 \in D_1 \text{ or } \omega_2 \in D_3, \\
\frac{q + 1}{2}, & \text{if } \omega_1 = 1, \omega_2 = 0.
\end{cases}
\]

When \( x = 1 \), the value set of

\[
d_{(U'_0, V'_0)}(\omega_1, \omega_2) = \frac{q - 1}{2} \text{ or } \frac{q + 1}{2}
\]

whenever \((\omega_1, \omega_2) \neq (0, 0)\). Thus \((U'_0, V'_0)\) is an \((N, N/2, N/2, 1, (N - 2)/4, (N + 2)/4)\)-ADSP.

From Lemma 2.2, the sequence pairs induced by the almost difference set pairs have three cross-correlation values:

\[
R_{(s, t)}((\omega_1, \omega_2)) = \begin{cases} 
-N + 4, & \text{if } (\omega_1, \omega_2) = (0, 0), \\
-2, & \text{if } \omega_1 = 1, \omega_2 \in D_0 \text{ or } \omega_2 \in D_2, \\
2, & \text{otherwise}.
\end{cases}
\]

This completes the proof. \(\square\)

For \((U'_q, V'_q)\), the conclusion is similar as Theorem 5.1.

Theorem 5.2. Let \( q = 4f + 1 = x^2 + 4y^2 \), where \( x = 1 \) and \( f \) is even, and let \( U'_q = \{0\} \times \{D_1 \cup D_2 \cup \{0\}\} \cup \{1\} \times \{D_1 \cup D_2 \cup \{0\}\}, V'_q = \{0\} \times \{D_1 \cup D_2 \cup \{0\}\} \cup \{1\} \times \{D_1 \cup D_2 \cup \{0\}\} \), then \((U'_q, V'_q)\) is an \((N, N/2, N/2, 1, (N - 2)/4, (N + 2)/4)\)-ADSP, and the length \( N = 2q \) characteristic sequence pair \((s, t)\) of \((U_q, V_q)\) has optimal cross-correlation if the defining set \((i, j, l, k)\) is \((1, 2, 3, 0), (3, 2, 1, 0), (1, 0, 3, 2)\) or \((3, 0, 1, 2)\).

To illustrate the sequences described in Theorem 5.1, we consider the following example.

Example 5.3. Take \( q = 17 = 1 + 4 \times 2^2 \), and define \( N = 2q = 34 \). We use the primitive root 3 modulo 17 to define the cyclotomic classes. Then \( D_0 = \{1, 13, 16, 4\}, D_1 = \{3, 5, 14, 12\}, D_2 = \{9, 15, 8, 2\}, D_3 = \{10, 7, 11, 6\} \). We take \((i, j, l, k) = (1, 2, 3, 0)\). Then \( U'_0 = \{0\} \times D_1 \cup \{0\} \times D_2 \cup \{1\} \times D_1 \cup \{1\} \times D_0 \cup \{0\} \times D_3 \cup \{0\} \times D_2 \cup \{1\} \times D_3 \cup \{1\} \times D_2 \cup \{0\} \). Hence

\[
U'_0 = \phi^{-1}(U'_0) = \{0, 20, 22, 14, 12, 26, 32, 8, 2, 3, 5, 31, 29, 1, 13, 33, 21\},
\]

\[
V'_0 = \phi^{-1}(V'_0) = \{0, 10, 24, 28, 6, 18, 30, 16, 4, 27, 7, 11, 23, 9, 15, 25, 19\}.
\]

The corresponding binary sequence pair is

\[(s, t) = (11110100000000001100000100101111, 10000101110010110111011010100000).
\]

which has optimal cross-correlation.
6. Conclusion

In this paper, we presented several classes of almost difference set pairs based on cyclotomic class of order 4. And we got several classes of binary sequence pairs with three-level cross-correlation. As mentioned earlier, finding binary sequence pairs with three-level cross-correlation values is equivalent to finding almost difference set pairs with corresponding parameters. We also constructed almost difference set pairs by using cyclotomic classes of order 2. It is necessary to point out that the existed almost difference set pair would correspond to a binary sequence pair with bad cross-correlation. For example, let $N = 2q$, where $q$ is an odd prime, we can construct almost difference set pair $(U, V) = (\{0\} \times D^{(2)}_0 \cup \{1\} \times D^{(2)}_0, \{0\} \times D^{(2)}_1 \cup \{1\} \times D^{(2)}_0)$ based on cyclotomic classes of order 2 with parameters $(N, \frac{N}{2} - 1, \frac{N}{2} - 1, \frac{N}{4} - \frac{1}{2}, \frac{N}{4} - \frac{1}{2}, \frac{N}{4} - \frac{1}{2})$. The corresponding binary sequence pair has in-phase cross-correlation value 2, and out-phase cross-correlation value $\{2, -2\}$. It is clear that this kind of almost difference set pairs are unsuitable to get binary sequence pairs.

Acknowledgments

The authors are grateful to the referees for their careful reading of the original version of this paper, their detailed comments and the suggestions that much improved the quality of this paper. The work of Xiaohui Liu and Jinhua Wang is supported by the Natural Science Foundation of Nantong University under Grant No. 12Z029 and the National Natural Science Foundation of China under Grant No. 11371207, respectively. The work of Dianhua Wu is supported in part by the National Natural Science Foundation of China under Grant No. 11271089, Guangxi Nature Science Foundation under Grant No. 2014GXNSFDA118001, Program on the High Level Innovation Team and Outstanding Scholars in Universities of Guangxi Province, and Guangxi “Ba Gui” Team for Research and Innovation.

References

[1] L. D. Baumert, Cyclic Difference Sets, Springer-Verlag, 1971.
[2] T. W. Cusick, C. Ding and A. Renvall, Stream Ciphers and Number Theory, North-Holland/Elsevier, Amsterdam, 1998.
[3] L. E. Dickson, Cyclotomy, higher congruences, and Waring’s problem, Amer. J. Math., 57 (1935), 391–424.
[4] C. Ding, T. Helleseth and K. Y. Lam, Several classes of binary sequences with three-level autocorrelation, IEEE Trans. Inf. Theory, 45 (1999), 2606–2612.
[5] C. Ding, T. Helleseth and H. Martinsen, New families of binary sequences with optimal three-level autocorrelation, IEEE Trans. Inf. Theory, 47 (2001), 428–433.
[6] C. Ding, D. Pei and A. Salomaa, Chinese Remainder Theorem: Applications in Computing, Cryptography, World Scientific, Singapore, 1996.
[7] H. L. Jin and C. Q. Xu, The study of methods for constructing a family of pseudorandom binary sequence pairs based on the cyclotomic class (in Chinese), Acta Electr. Sin., 38 (2010), 1608–1611.
[8] S. Y. Jin and H. Y. Song, Note on a pair of binary sequences with ideal two-level crosscorrelation, in Proc. ISIT2009, Seoul, 2009, 2603–2607.
[9] D. Jungnickel and A. Pott, Difference sets: an introduction, in Difference Sets, Sequences and Their Correlation Properties (eds. A. Pott, P.V. Kumar, T. Helleseth and D. Jungnickel), Kluwer Academic Publishers, 1999, 259–295.
[10] J. Z. Li and P. H. Ke, Study on the almost difference set pairs and almost perfect autocorrelation binary sequence pairs (in Chinese), J. Wuyi University, 27 (2008), 10–14.
[11] K. Liu and C. Q. Xu, On binary sequence pairs with two-level periodic cross-correlation function, *IEICE Trans. Funda.*, **E93-A** (2010), 2278–2285.

[12] F. Mao, T. Jiang, C. L. Zhao and Z. Zhou, Study of pseudorandom binary sequence pairs (in Chinese), *J. Commun.*, **26** (2005), 94–98.

[13] X. P. Peng, C. Q. Xu and K. T. Arasu, New families of binary sequence pairs with two-level and three-level correlation, *IEEE Trans. Inf. Theory*, **58** (2012), 2968–2978.

[14] T. Storer, *Cyclotomy and Difference Sets*, Markham, Chicago, 1967.

[15] T. W. Sze, S. Chanson, C. Ding, T. Helleseth and M. G. Parker, Logarithm authentication codes, *Infor. Comput.*, **148** (2003), 93–108.

[16] Y. Z. Wang and C. Q. Xu, Divisible difference set pairs and approach for the study of almost binary sequence pair (in Chinese), *Acta Electr. Sin.*, **37** (2009), 692–695.

[17] C. Q. Xu, Difference set pairs and approach for the study of perfect binary array pairs (in Chinese), *Acta Electr. Sin.*, **29** (2001), 87–89.

[18] X. Q. Zhao, W. C. He, Z. W. Wang and S. L. Jia, The theory of the perfect binary array pairs (in Chinese), *Acta Electr. Sin.*, **27** (1999), 34–37.

Received June 2014; revised August 2014.

E-mail address: lhx600@ntu.edu.cn
E-mail address: jhwang@ntu.edu.cn
E-mail address: wangjh@sjtu.org
E-mail address: dhwu@gxnu.edu.cn