ON THE EQUIVALENCE OF SEVERAL CLASSES OF QUATERNARY SEQUENCES WITH OPTIMAL AUTOCORRELATION AND LENGTH $2^p$

PINHUI KE* AND PANPAN QIAO

Fujian Provincial Key Laboratory of Network Security and Cryptology
College of Mathematics and Informatics
Fujian Normal University, Fuzhou, Fujian 350117, China

YANG YANG
School of Mathematics
Southwest Jiaotong University
Chengdu 611756, China

(Communicated by Wai Ho Mow)

Abstract. Quaternary sequences with optimal autocorrelation property are preferred in applications. Cyclotomic classes of order 4 are widely used in the constructions of quaternary sequences due to the convenience of defining a quaternary sequence with the cyclotomic classes of order 4 as its support set. Recently, several classes of optimal quaternary sequences of period $2^p$, which are all closely related to the cyclotomic classes of order 4 with respect to $\mathbb{Z}_p$ were introduced in the literature. However, less attention has been paid to the equivalence between these known results. In this paper, we introduce the unified form of this kind of quaternary sequences to classify these known results and then conclude the unified forms of these optimal quaternary sequences. By doing this, we disclose the relationship between the optimal quaternary sequences derived from different methods in the literature on one hand. And on the other hand, when the new obtained optimal quaternary sequence period is $2^p$ and the cyclotomic classes of order 4 are involved, the methods and the results given in this paper can be used to identify if the sequence is new or not.

1. INTRODUCTION

Let $a = (a(0), a(1), \cdots, a(N-1))$ be a sequence of period $N$ over the integer ring $\mathbb{Z}_m = \{0, 1, \cdots, m-1\}$. Specifically, $a$ is called a binary or quaternary sequence when $m = 2$ or $m = 4$, respectively. For each $k \in \mathbb{Z}_m$, we define $N_k(a) = |\{t | a(t) = k, 0 \leq t \leq N-1\}|$. A sequence $a$ is then called balanced if $\max_{k \in \mathbb{Z}_m} N_k(a) - \min_{k \in \mathbb{Z}_m} N_k(a) \leq 1$. Given two sequences $a = (a(0), a(1), \cdots, a(N-1))$ and $b = (b(0), b(1), \cdots, b(N-1))$ of period $N$ over the integer ring $\mathbb{Z}_m$, the cross-correlation

2020 Mathematics Subject Classification: Primary: 94A55, 11T71; Secondary: 05B10.
Key words and phrases: Quaternary sequences, autocorrelation, equivalence.

The authors are supported by National Natural Science Foundation of China (No. 61772292, 61772476, 61771016), Natural Science Foundation of Fujian Province (No. 2019J01273) and Fujian Normal University Innovative Research Team (IRTL1207).

* Corresponding author: Pinhui Ke.
function of $a$ and $b$ at shift phase $\tau$ is defined by

$$R_{ab}(\tau) = \sum_{t=0}^{N-1} \xi_m^b(t+\tau-a(t)), \quad 0 \leq \tau < N,$$

where $\xi_m = \exp\left(\frac{2\pi i}{m}\right)$ is a complex primitive $m$-th root of unity and the addition $t + \tau$ is performed modulo $N$. If $a = b$, (1) becomes the autocorrelation function of $a$ and is denoted as $R_a(\tau)$. It is easy to see that $R_a(0)$ equals to $N$ trivially. Hence, for the autocorrelation function, only the shift phases $\tau \neq 0$ (also referred to as out-of-phase autocorrelations) are considered. The maximum nontrivial autocorrelation is denoted as $R_{\text{max}}(a) = \{ |R_a(\tau)|, 1 \leq \tau < N \}$.

Pseudorandom sequences with low autocorrelation property have important applications in many areas such as communications, radar and cryptography, etc. [5]. Due to their simplicity of implementation, binary and quaternary sequences with optimal autocorrelation magnitude are preferred in applications. For the binary sequences with optimal autocorrelation magnitude, the readers may refer to [1] for instance. For the quaternary sequences, the situations are closely related to the period of the sequences. If the period is odd, its maximum out-of-phase autocorrelation magnitude is greater than or equal to 1. However, up to now, only one class of quaternary sequences $a$ with $R_{\text{max}}(a) = 1$ is known [13]. The next known smallest values for the maximum out-of-phase autocorrelation magnitude of a quaternary sequence $a$ of odd period are $R_{\text{max}}(a) = \sqrt{5}$ or 3, see [6, 10, 15, 18, 20, 21, 14, 12]. If the period is even, an elegant result was given by Tang et al. in [19]. They proved that the smallest values for the maximum out-of-phase autocorrelation magnitude of the quaternary sequence with even period is 2. Hence, a quaternary sequence is called optimal if $R_{\text{max}}(a) = 2$. In recent years, several classes of optimal quaternary sequences with even period have been proposed [8, 9, 7, 14, 17, 11, 2].

For our purpose, let us review the known constructions of optimal quaternary sequences with even period in detail. In [8], Kim et al. constructed optimal quaternary sequences by using the inverse Gray mapping and the Sidelnikov sequences. In [9], Kim et al. used the inverse Gray mapping and the Legendre sequences of period $p$ to construct optimal quaternary sequences of period $2p$ with ideal autocorrelation property. Also, Jang et al. used the inverse Gray mapping and binary sequences of period $2^n - 1$ with ideal autocorrelation property to construct quaternary sequences of period $2(2^n - 1)$ with optimal autocorrelation property and balance property [7]. In [4], Edemskiy constructed quaternary sequences with $R_{\text{max}}(a) \in \{ \sqrt{8}, 4 \}$ by using the Chinese Remainder Theorem (CRT, for short) and cyclotomic classes of order four. Furthermore, Shen et al. [14] improved the constructions and proposed several classes of optimal quaternary sequences of length $2p$. Very recently, using the interleaving method, Su et al. [17] introduced a generic construction of quaternary sequences of even length. When twin-prime sequences pairs, GMW sequences pairs or sequences defined by cyclotomic classes of order four were used as component sequences, new classes of optimal quaternary sequences were obtained. Also in [11], Luo et al. constructed a class of optimal quaternary sequences of period $2p$ via interleaving two inequivalent Tang-Lindner sequences [18], which can also be described by the CRT and the cyclotomic classes of order four modulo $p$ equivalently.

In the literature, the results were always claimed to be new. However, it is easy to see that when a sequence is added a constant or shifted cyclicly, the resulting sequence shares the same autocorrelation distribution with the original one. Additionally, for some known optimal quaternary sequences with the same period, they
On the equivalence of several classes of quaternary sequences

seem to be equivalent (the definition of equivalence will be given in Sec. 2), although they were obtained by different methods. Hence, here is the question. Are the known optimal quaternary sequences different from each other? Is there any kind of “standard”, by which one could determine if the sequence is new or not?

It seems difficult to consider the general case. In this paper, we will focus on the optimal quaternary sequences with fixed length $2p$. Specifically, we will pay attention to those construction closely related to cyclotomic classes of order 4. To the best of our knowledge, the only known result is [12], in which the authors mentioned that some constructions given by Shen et al. in [14] can also be derived from the Chung’s construction with Ding-Helleseth-Martinsen sequences as component sequences. We will explain their relationships more clearly in Remark 3.2. In general, we will define the equivalence of quaternary sequences with respect to the autocorrelation. Then we will give the definition of unified form according to which we can classify the known results.

The rest of this paper is organized as follows. In Section 2, some basic notations and definitions will be introduced. And the known constructions of optimal quaternary sequences of length $2p$ will be reviewed. In Section 3, we will study the equivalence of the quaternary sequences with respect to their autocorrelations. We then introduce the definition of unified form for a quaternary sequence with its support set defined by the cyclotomic classes of order 4. By presenting the unified forms of the known optimal quaternary sequences with which we are concerned, we analyse the relations between these results. In Section 4, we conclude this paper.

2. Preliminaries

Let $p$ be a prime with $p \equiv 1 \pmod{4}$, and $\alpha$ be a primitive element modulo $p$. Define

$$D_0 = \{ \alpha^{4i} | i = 0, 1, \cdots, \frac{p-1}{4} - 1 \},$$

and

$$D_i = \alpha^i D_0, \quad 0 \leq i < 4.$$ 

Then $D_i, \quad 0 \leq i < 4$ are called the cyclotomic classes of order four with respect to $\mathbb{Z}_p$. By the CRT, we know that

$$\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p.$$

In detail, let us define

$$\psi: \mathbb{Z}_2 \times \mathbb{Z}_p \rightarrow \mathbb{Z}_{2p},$$

$$(x, y) \mapsto px + (p+1)y \pmod{2p}.$$

Then $\psi$ is an isomorphism between $\mathbb{Z}_2 \times \mathbb{Z}_p$ and $\mathbb{Z}_{2p}$. It is obvious that

$$\mathbb{Z}_2 \times \mathbb{Z}_p = \{(0,0), (1,0)\} \cup \mathbb{Z}_2 \times \mathbb{Z}_p^* = \{(0,0), (1,0)\} \cup \bigcup_{i,j=0}^{3} \{0\} \times D_i \cup \{1\} \times D_j,$$

and

$$\mathbb{Z}_{2p} = \{\psi(0,0), \psi(1,0)\} \cup \bigcup_{i,j=0}^{3} \{\psi(0) \times D_i \cup \psi(1) \times D_j\}.$$ 

Let $a = (a(0), a(1), \cdots, a(p-1))$ be a sequence of period $p$, and $\tau$ be an integer with $0 \leq \tau < p$. Then $(a(\tau), a(\tau+1), \ldots, a(\tau + (p-1) \pmod{p}))$ is called a (left)
cyclic shift of \(a\), denoted by \(L^\tau(a)\). Let \(b = (b(0), b(1), \ldots, b(p-1))\) be another sequence of period \(p\). Define a sequence \(c = (c(0), c(1), \ldots, c(p-1))\) as follows

\[
c(i) = \begin{cases} 
  a\left(\frac{i}{2}\right), & \text{if } i \text{ is even;} \\
  b\left(\frac{i-1}{2}\right), & \text{if } i \text{ is odd.}
\end{cases}
\]

If we arrange the elements of \(c\) row by row into an array of size \(p \times 2\),

\[
c = \begin{bmatrix}
  a(0) & b(0) \\
  a(1) & b(1) \\
  \vdots & \vdots \\
  a(p-1) & b(p-1)
\end{bmatrix} \triangleq I[a, b],
\]

then the sequence \(c\) is also called the interleaving of \(a\) and \(b\).

Let \(p \equiv 5 \pmod{8}\) be a prime. Ding et al. [3] presented an elegant construction of optimal binary sequences of period \(N = 2p\), which have optimal autocorrelation magnitude 2. They are always called the Ding-Helleseth-Martinsen (DHM, for abbreviation) sequences.

**Theorem 2.1.** [3] Let \(p \equiv 5 \pmod{8} = x^2 + 4y^2\) be a prime, where \(x \equiv 1 \pmod{4}\). Define \(D = \{0\} \times (D_i \cup D_j) \cup \{1\} \times (D_j \cup D_i) \cup \{(0,0)\}\).

1. If \(x = 1\), \((i, j, l) \in \{(0,1,2), (0,3,2), (1,0,3), (1,2,3)\}\), or

2. If \(y = 1\), \((i, j, l) \in \{(0,1,3), (0,2,3), (1,2,0), (1,3,0)\}\),

then the binary sequence with support set \(\psi(D)\), denoted by \(s_{\psi(D)}\) is balanced and optimal, i.e., \(R_{s_{\psi(D)}}(\tau) \in \{\pm 2\}\), for all \(\tau \neq 0 \pmod{p}\).

As it was pointed out in [3][16], \(y\) in the above theorem is two-valued, depending on the choice of the primitive root employed to define the cyclotomic classes. In detail, let the primitive root be \(\alpha\) in the case \(y = 1\). When we use \(\alpha^{-1}\) as primitive root, \(y\) will change to be \(-1\). Recall that the cyclotomic number \((i, j)\) is defined by

\[
(i, j) = |(D_i + 1) \cap D_j|.
\]

Let \(p = 4f + 1 = x^2 + 4y^2\). There are at most five distinct cyclotomic numbers of order 4 when \(f\) is odd [16]. Since

\[
(3, 1) = \frac{p + 1 + 2x + 8y}{16}, \quad (1, 3) = \frac{p + 1 + 2x - 8y}{16},
\]

we have \(y = (3, 1) - (1, 3)\). By this way, we can check the sign of \(y\). Furthermore, since \(p \equiv 5 \pmod{8}\), the cyclotomic cosets \(D_1\) and \(D_3\) will be interchanged. Then we get the following corollary immediately.

**Corollary 2.1.** Let \(p \equiv 5 \pmod{8} = x^2 + 4y^2\) be a prime, where \(x \equiv 1 \pmod{4}\). Define \(D = \{0\} \times (D_i \cup D_j) \cup \{1\} \times (D_j \cup D_i) \cup \{(0,0)\}\).

If \(y = -1\) and \((i, j, l) \in \{(0,3,1), (0,2,1), (1,0,2), (1,3,2)\}\), then the binary sequence with support set \(\psi(D)\), denoted by \(s_{\psi(D)}\) is balanced and optimal.

At the end of this section, we summarize the four known classes of optimal quaternary sequences of length \(2p\). In Table 1 we give the sketches of the constructions of these sequences. For the convenience of the reader, we also give the details of their constructions in Appendix A.
Table 1. Known Optimal Quaternary Sequences of Length $2p$

| Sequence | Construction (Sketch) | Constrains |
|----------|------------------------|------------|
| Chung et al. [12] [2] | $s = \phi^{-1}(a, L^{p}(b))$ | $p \equiv 5 \pmod{8}$ |
| Su et al. [17] | $s = \phi^{-1}(c, d)$ | $p \equiv 1 \pmod{4}$ |
| Shen et al. [14] | $s = I(a_{0}, c(0) + L^{n}(a_{1}))$ | $p \equiv 1 \pmod{4}$ |
| Luo et al. [11] | $s = I(u_{0}, L^{n}(v_{0}) + 2)$ | $p \equiv 1 \pmod{4}$ |

Note.
- $\phi^{-1}$ denotes the inverse Gray mapping with
  \[ \phi^{-1}(0, 0) = 0, \phi^{-1}(0, 1) = 1, \phi^{-1}(1, 1) = 2, \phi^{-1}(1, 0) = 3; \]
- $D_{i}, 0 \leq i \leq 3$ are the cyclotomic classes of order 4 with respect to $\mathbb{Z}_{p}$;
- $s_{1}, s_{2}, \cdots, s_{6}$ are six binary sequences of length $p$ with support sets $D_{0} \cup D_{1}, D_{0} \cup D_{2}, D_{0} \cup D_{3}, D_{1} \cup D_{2}, D_{1} \cup D_{3}, D_{2} \cup D_{3}$, respectively;
- $\text{Supp}_{2}(t) = \{i | s(i) = t, 0 \leq i < 2p\}, \quad 0 \leq t \leq 3$.

**Remark 2.1.** In the original version of the main theorem in [14] (Theorem 4.3 in Appendix A), the condition of case (2) was $y = 1$. It is incorrect. For instance, let $p = 13$. Take 7 as the primitive root modulo $p$. The cyclotomic classes of order 4 are

\[ D_{0} = \{1, 3, 9\}, D_{1} = \{7, 8, 11\}, D_{2} = \{4, 10, 12\}, D_{3} = \{2, 5, 6\}. \]

By equality (3), $y = (3, 1) - (1, 3) = 1$. The quaternary sequence is

\[ s = [0, 2, 3, 2, 1, 3, 3, 0, 2, 2, 1, 0, 1, 2, 0, 0, 3, 0, 1, 3, 3, 2, 0, 0, 1, 2, 1], \]

and

\[ [R_{b}(\tau)]_{\tau=1}^{25} = \{-2, -6, -2, 2, -6, 2, -6, -2, 2, 2, -2, 2, 2, -2, -6, 2, -6, 2, 2, -2, -6, 2\}. \]

So the sequence $s$ is not optimal. If we use $2(\equiv 7^{-1} \pmod{13})$ as the primitive root modulo $p$, then $y = (3, 1) - (1, 3) = -1$. The quaternary sequence is

\[ s = [0, 2, 2, 2, 1, 0, 2, 3, 3, 2, 1, 3, 1, 2, 0, 0, 0, 1, 2, 0, 3, 3, 0, 1, 3, 1], \]

and

\[ [R_{b}(\tau)]_{\tau=1}^{25} = \{-2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2\}. \]

Hence $s$ is optimal.
3. Equivalence between the optimal quaternary sequences with period 2\(p\)

In this section, we will introduce the equivalence of quaternary sequences with respect to their autocorrelations. Then we give the definition of unified form of a quaternary sequence with even period. To compare the optimal quaternary sequences introduced in the previous section, we will present their unified forms. Lastly, the known unified forms of the optimal quaternary sequences will be summarized.

Let us begin with the definitions of equivalence between sequences. Let \(s, s'\) be two quaternary sequences of period \(N\). If one of following cases holds

(i) \(s' = L^\tau(s)\), for \(\tau, 0 \leq \tau < N\);
(ii) \(s' = s + a = \{s(t) + a\}_{t=0}^{N-1}\), for \(a \in \mathbb{Z}_4\);
(iii) \(s' = a \cdot s = \{a \cdot s(t)\}_{t=0}^{N-1}\), for \(a \in \mathbb{Z}_4^*\),

then the sequences \(s\) and \(s'\) are called equivalent. It is obvious that two equivalent sequences have the same autocorrelation magnitude.

For quaternary sequences of even length, more operations can be performed on the sequences while preserving their autocorrelation magnitudes when the structure of a sequence is considered. Assume that the sequence \(s\) is the interleaving of \(s_1\) and \(s_2\), i.e., \(s = I[s_1, s_2]\). It is well known that

\[
\begin{align*}
R_s(\tau) &= \begin{cases} 
R_{s_1}(\tau_1) + R_{s_2}(\tau_1), & \text{if } \tau = 2\tau_1; \\
R_{s_1,s_2}(\tau_1) + R_{s_2,s_1}(\tau_1 + 1), & \text{if } \tau = 2\tau_1 + 1.
\end{cases}
\end{align*}
\]

By (4), it can be easily verified that if the sequences \(s_1\) and \(s_2\) are added constants \(a\) and \(b\), where \(a, b \in \mathbb{Z}_4\) and \(a \equiv b \mod 2\), respectively, the resulting sequence has the same autocorrelation magnitude with \(s\). So we formulate above operations as follows.

(iv) \(s' = I[s_1 + a, s_2 + b] \triangleq I[s_1, s_2] + (a, b)\), where \(a, b \in \mathbb{Z}_4\) and \(a \equiv b \mod 2\).

**Definition 3.1.** Let \(s, s'\) be two quaternary sequences of even period \(N\). Then \(s\) and \(s'\) are said to be equivalent with respect to autocorrelation, if one of cases (i) – (iv) holds.

To compare the quaternary sequences obtained from different methods, we shall convert them into unified forms without changing their autocorrelation magnitude.

**Definition 3.2.** Let \(N = 2p\), where \(p\) is a prime. Let \(s\) be a quaternary sequence with period \(N\), which are closely related to the cyclotomic classes of order 4 with respect to \(\mathbb{Z}_p\). If

\[
\text{Supp}_s(t) \supseteq \psi(\{0\} \times D_{i_l} \cup \{1\} \times D_{i_m}), \quad \text{for } t = 0, 1,
\]

\[
\text{Supp}_s(t) = \psi(\{0\} \times D_{j_l} \cup \{1\} \times D_{j_m}), \quad \text{for } t = 2, 3,
\]

where \(i_l \neq i_m\) and \(j_l \neq j_m\), if \(l \neq m\), and \((s(0), s(p)) \in \{(0, 0), (0, 1), (1, 0)\}\), then we call such a quaternary sequence is unified. And we denote it as

\[
s = [(i_0, i_1, i_2, i_3), (j_0, j_1, j_2, j_3)](s(0), s(p)).
\]

In the above definition we adopt the notations in [14]. However, different from the notations in [14], we require that \((s(0), s(p)) \in \{(0, 0), (0, 1), (1, 0)\}\). Note that for any \((s(0), s(p)) \in \mathbb{Z}_4 \times \mathbb{Z}_4\), we always can choose appropriate \(c, c' \in \mathbb{Z}_4\) with \(|c - c'| = 0\) or 2, so that \((s(0) + c, s(p) + c') \in \{(0, 0), (0, 1), (1, 0)\}\), which implies that for any quaternary sequences with the cyclotomic classes of order 4 as defining sets, we always can transform them into unified forms without changing their autocorrelation magnitude.
Proposition 3.1. Let \( p \) be a prime such that \( p = 4f + 1 = x^2 + 4y^2 \).

1) If \( x = 1 \) and \( y \) is even, then the unified form of the quaternary sequence in (7) belongs to one of the following cases:

\[
[(0,1,2,3),(2,1,0,3)]_{(0,0)}, [(1,0,3,2),(3,0,1,2)]_{(0,0)},
\]

\[
[(2,1,0,3),(0,1,2,3)]_{(0,0)}, [(3,0,1,2),(1,0,3,2)]_{(0,0)}.
\]

2) If \( y = -1 \), then the unified form of the quaternary sequence in (7) belongs to one of the following cases:

\[
[(0,2,1,3),(0,3,1,2)]_{(0,0)}, [(1,0,2,3),(1,3,2,0)]_{(0,0)},
\]

\[
[(2,0,3,1),(2,1,3,0)]_{(0,0)}, [(3,1,0,2),(3,2,0,1)]_{(0,0)}.
\]

Proof. Since \( s(p) = 2 \), we add 2 to the second column sequence of interleaving the quaternary sequence, which preserves the autocorrelation magnitude by Definition 3.1. Then the unified form of the sequence can be derived directly by taking \((i_0,i_1,i_2,i_3)\) and \((j_2,j_3,j_0,j_1)\) as the first tuple and the second tuple of the unified form, respectively.\( \square \)

Second, for the optimal quaternary sequences given by Chung’s construction (for consistency, case 2) in Theorem 2.1 is replaced by the cases in Corollary 2.1), we have following results.

Proposition 3.2. Let \( p \equiv 5 \) (mod 8) = \( x^2 + 4y^2 \) be a prime, \( x \equiv 1 \) (mod 4),

\[
D = \{0\} \times (D_i \cup D_j) \cup \{1\} \times (D_j \cup D_i) \cup \{(0,0)\}.
\]

Let

\[
u = \phi^{-1}(s_{\psi(D)}, L^p(s_{\psi(D)})),
\]

where \( s_{\psi(D)} \) denotes the DHM sequences with support set \( D \) and \( \tilde{s} \) denotes the complementary of \( s \). Then \( \nu \) is optimal and the unified form of \( \nu \) is listed as follows.

1) \[
[(0,1,2,3),(0,3,2,1)]_{(0,0)}, [(0,3,2,1),(0,1,2,3)]_{(0,0)},
\]

\[
[(1,0,3,2),(1,2,3,0)]_{(0,0)}, [(1,2,3,0),(1,0,3,2)]_{(0,0)}, \quad \text{if } x = 1.
\]

2) \[
[(0,3,1,2),(0,2,1,3)]_{(0,0)}, [(0,2,1,3),(0,3,1,2)]_{(0,0)},
\]

\[
[(1,0,2,3),(1,3,2,0)]_{(0,0)}, [(1,3,2,0),(1,0,2,3)]_{(0,0)}, \quad \text{if } y = -1.
\]

Proof. Since DHM sequences are optimal with \( R_{s_{\psi(D)}}(\tau) \in \{\pm 2\}, 1 \leq \tau \leq N \), \( \nu \) is optimal by Theorem 4.1 in Appendix A.

By definition, \( Z_p \setminus \{0\} = D_i \cup D_j \cup D_i \cup D_k, \) where \( \{i,j,k\} = \{0,1,2,3\} \). Then the support of the binary sequence \( \tilde{s}_{\psi(D)} \) is

\[\psi\{(0) \times (D_i \cup D_k) \cup \{1\} \times (D_k \cup D_i) \cup \{(1,0)\}\}].\]
Furthermore, the support of $LP(\tilde{s}_\psi(D))$ is
\[ \psi(\{(0) \times (D_1 \cup D_k) \cup \{(1) \times (D_l \cup D_1) \cup \{(0,0)\}). \]

By $u = \phi^{-1}(s_\psi(D), LP(\tilde{s}_\psi(D)))$, we have
\[
\begin{align*}
\text{Supp}_u(0) &= \psi(\{(0) \times D_l \cup \{(1) \times D_1\)), \\
\text{Supp}_u(1) &= \psi(\{(0) \times D_k \cup \{(1) \times D_k\)), \\
\text{Supp}_u(2) &= \psi(\{(0) \times D_l \cup \{(1) \times D_1\)), \\
\text{Supp}_u(3) &= \psi(\{(0) \times D_j \cup \{(1) \times D_j\)).
\end{align*}
\]

Assume $u = I(u_1, u_2)$, then the unified form of $u$ can be obtained by adding 2 to $u_1$. By Definition 3.1, this operation is permitted without changing the autocorrelation magnitude of the original sequence. We obtain the unified form of $u$ as follows
\[ [(i, j, l, k), (i, k, l, j)]_{(0,0)}. \]

The proof is then finished by taking the triples $(i, j, l)$ in Theorem 2.1 and Corollary 2.1 into above unified form directly. \hfill \square

Remark 3.1. If $u$ is defined by $u = \phi^{-1}(s_\psi(D), LP(\tilde{s}_\psi(D)))$, where $s_\psi(D)$ is a DHM sequence, by Theorem 4.1 in Appendix A, then they are also optimal. However, they share the same unified forms listed above according to our computation.

Lemma 3.3. [3] Let $(s_\psi(D)(t))$ be a DHM sequence associated with a triple $(i, j, l)$ in Theorem 2.1. Then $(s_\psi(D)(N - t))$ is also an optimal binary sequence with the support set determined by the triple $(i + 2, j + 2, l + 2)$.

The following corollary will be used to explain that in the case $p \equiv 5 \pmod{8} = 4f + 1$, $f$ being odd, the construction given by Shen et al. (Case 2 in Proposition 3.1) is a special case of Chung’s construction (Case 2 in Proposition 3.2) by taking DHM sequences as component sequences.

Corollary 3.1. Let $p \equiv 5 \pmod{8} = x^2 + 4$ be a prime. The quaternary sequences with unified forms
\[ [(2, 0, 3, 1), (2, 1, 3, 0)]_{(0,0)}, [(3, 1, 0, 2), (3, 2, 0, 1)]_{(0,0)} \]
are equivalent with respect to autocorrelation to the quaternary sequences derived from the Chung’s construction. Thus, if $p = 4f + 1$ with $f$ being odd, then the quaternary sequences constructed by Shen et al. in [14] are equivalent to the sequences constructed by Chung et al. with DHM sequences as component sequences.

Proof. If we take the triples $(0, 2, 1)$ and $(1, 3, 2)$ in DHM, then the results can be obtained from Proposition 3.2, Definition 3.1 and the fact that
\[ (0, 2, 1) + 2 = (2, 0, 3), (1, 3, 2) + 2 = (3, 1, 0). \]
\hfill \square

Remark 3.2. In [12], it is remarked that some of the sequences constructed by Shen et al. [14] are covered by those constructed by Chung et al. [2] with DHM sequences as component sequences, which can also be checked by Proposition 3.1, Proposition 3.2 and Corollary 3.1. In detail, for $p = 4f + 1 = x^2 + 4y^2$, both the cases of even $f$ and odd $f$ were considered in Shen’s construction [14], while only odd $f$ was considered in the latter one. However, for odd $f$, only the case $y = -1$ was considered in the former one, while both the cases of $x = 1$ and $y = -1$ are considered in the latter one.
Now let us turn to the optimal quaternary sequences of length $2p$ by Su et al. in [17] (Theorem 4.2 in Appendix A). We have the following observations.

- For case 1) in Theorem 4.2, since $(a_0, a_1, a_2, a_3)$ satisfies $a_0 = a_2$ and $a_1 = a_3$, the obtained sequence $u$ takes value 0 or 2. Similarly, for case 4), if
\[
(a_0, a_1, a_2, a_3) \in \left\{ (s_4, s_6, s_3, s_1), (s_3, s_6, s_4, s_1), (s_6, s_4, s_1, s_3), (s_1, s_4, s_6, s_3) \right\},
\]
we know that $u(t) \in \{1, 3\}$ for all $t \neq 0, p$ by our computation. Thus these sequences are two-valued or almost two valued, so that they are all not balanced as quaternary sequences. Although they also have optimal autocorrelation, we will not discuss these cases in this paper.

- For cases 2) and 4) in Theorem 4.2, $e = (e(0), e(1), e(2))$ satisfies $e(0) + e(1) + e(2) \equiv 0$ (mod 2) in Theorem 4.2. It seems that we have a lot of cases to be analyzed for our purpose, since $(e(0), e(1), e(2))$ may take value $(0, 0, 0), (0, 1, 1), (1, 0, 1),$ or $(1, 1, 0)$. However, no new unified form of the optimal quaternary sequence could be found by our computation. For instance, if $(a_0, a_1, a_2, a_3) = (s_1, s_2, s_2, s_1)$, then
\[
\text{Supp}_u(0) = \psi(\{0\} \times D_0 \cup \{1\} \times D_0 \cup \{(0,0), (1,0)\}),
\]
\[
\text{Supp}_u(1) = \psi(\{0\} \times D_3 \cup \{1\} \times D_2),
\]
\[
\text{Supp}_u(2) = \psi(\{0\} \times D_1 \cup \{1\} \times D_1),
\]
\[
\text{Supp}_u(3) = \psi(\{0\} \times D_2 \cup \{1\} \times D_3),
\]
as we will show in Proposition 3.3. If $(e(0), e(1), e(2)) = (1, 0, 1)$, then the resulted sequence have
\[
\text{Supp}_u(0) = \psi(\{0\} \times D_0 \cup \{1\} \times D_1 \cup \{(0,0)\}),
\]
\[
\text{Supp}_u(1) = \psi(\{0\} \times D_3 \cup \{1\} \times D_3),
\]
\[
\text{Supp}_u(2) = \psi(\{0\} \times D_1 \cup \{1\} \times D_0 \cup \{(1,0)\}),
\]
\[
\text{Supp}_u(3) = \psi(\{0\} \times D_2 \cup \{1\} \times D_2).
\]
Adding 2 to the second column sequence of the interleaving of the quaternary sequence, we arrived at the unified form of the quaternary sequence
\[
[(0, 3, 1, 2), (0, 2, 1, 3)]_{(0,0)},
\]
which is exactly the same with the original one. In conclusion, to get the unified form of the optimal sequences of cases 2) and 4) in Theorem 4.2, we only need to consider the case $e(0) = e(1) = e(2) = 0$.

**Proposition 3.3.** Let $p = 4f + 1 = x^2 + 4y^2$ be a prime.

- Assume $y = -1$. Let
\[
(a_0, a_1, a_2, a_3) \in \left\{ (s_1, s_2, s_2, s_1), (s_2, s_1, s_1, s_2), (s_2, s_6, s_6, s_2), (s_6, s_2, s_2, s_6),
\right\}
\]
\[
\left\{ (s_4, s_5, s_5, s_4), (s_5, s_4, s_4, s_5), (s_5, s_3, s_3, s_5), (s_3, s_5, s_5, s_3) \right\}.
\]

Then the unified form of the optimal quaternary sequence $u$ constructed in Theorem 4.2 belongs to one of the following cases
\[
[(0, 3, 1, 2), (0, 2, 1, 3)]_{(0,0)}, [(0, 2, 1, 3), (0, 3, 1, 2)]_{(0,0)},
\]
\[
[(1, 0, 2, 3), (1, 3, 2, 0)]_{(0,0)}, [(1, 3, 2, 0), (1, 0, 2, 3)]_{(0,0)}.
\]
Assume $f$ is even and $x = \pm 1$. Let
\[(a_0, a_1, a_2, a_3) \in \{ (s_6, s_3, s_4, s_1), (s_6, s_4, s_3, s_1), (s_4, s_1, s_6, s_3), (s_4, s_6, s_1, s_3) \} \cup \{ (s_3, s_1, s_6, s_4), (s_1, s_3, s_1, s_6), (s_1, s_4, s_3, s_6) \} .
\]

Then the unified form of the optimal quaternary sequence $u$ constructed in Theorem 4.2 belongs to one of the following cases
\[
\begin{align*}
&\{ (0, 1, 2, 3), (2, 1, 0, 3) \}\times (0, 0), [(2, 1, 0, 3), (0, 1, 2, 3)] \times (0, 0), \\
&\{ (1, 0, 3, 2), (3, 0, 1, 2) \}\times (0, 0), [(3, 0, 1, 2), (1, 0, 3, 2)] \times (0, 0), \\
&\{ (2, 3, 0, 1), (0, 3, 2, 1) \}\times (0, 0), [(0, 3, 2, 1), (2, 3, 0, 1)] \times (0, 0), \\
&\{ (3, 2, 1, 0), (1, 2, 3, 0) \}\times (0, 0), [(1, 2, 3, 0), (3, 2, 1, 0)] \times (0, 0) .
\end{align*}
\]

Proof. As we have mentioned in the above observation, to get the unified form of the sequence with concern, only the case $e(0) = e(1) = e(2) = 0$ needs to be considered. By the definition in (6) in Appendix A, $c = I(a_0, L^\lambda(a_1))$, $d = I(a_2, L^\lambda(a_3))$. For $c = I(a_2, L^\lambda(a_3))$, let us assume that
\[
\text{Supp}(a_0) = D_1 \cup D_3, \quad \text{Supp}(a_1) = D_k \cup D_l .
\]

Then the support of the binary sequence $c$ is
\[
\{2i | i \in D_1 \cup D_3 \} \cup \{1 + 2i | i \in D_k \cup D_l \} = \{2(D_1 \cup D_3) \cup (1 + 2(D_k \cup D_l - \lambda)\}
\]
\[
= \{2(D_1 \cup D_3) \cup (p + 2(D_k \cup D_l)\}
\]

Assume that $2 \in D_l$, then by the CRT, the support of the binary sequence $c$ in $\mathbb{Z}_2 \times \mathbb{Z}_p$ is
\[
\{0\} \times (D_i + D_j) \cup \{1\} \times (D_k + D_l) .
\]

The support of $d$ can be obtained similarly.

(i) If $y = -1$, then $f$ is odd. We have $p \equiv 5 \pmod{8}$, and then $2 \not\in \text{NQR}_p$. So that $2 \in D_1$ or $2 \in D_3$. Since the proof is similar, we only prove the case $(a_0, a_1, a_2, a_3) = (s_1, s_2, s_3, s_1)$. By definition, $\text{Supp}(s_1) = D_0 \cup D_1$ and $\text{Supp}(s_2) = D_0 \cup D_2$.

If $2 \in D_1$, the support of the binary sequence $c$ is
\[
\{0\} \times (D_1 \cup D_2) \cup \{1\} \times (D_1 \cup D_3) .
\]

The support of the binary sequence $d$ is
\[
\{0\} \times (D_1 \cup D_3) \cup \{1\} \times (D_1 \cup D_2) .
\]

By $u = \phi^{-1}(c, d)$, we have
\[
\begin{align*}
&\text{Supp}_u(0) = \psi(\{0\} \times D_0 \cup \{1\} \times D_0 \cup \{(0, 0), (1, 0)\}) , \\
&\text{Supp}_u(1) = \psi(\{0\} \times D_3 \cup \{1\} \times D_2) , \\
&\text{Supp}_u(2) = \psi(\{0\} \times D_1 \cup \{1\} \times D_1) , \\
&\text{Supp}_u(3) = \psi(\{0\} \times D_2 \cup \{1\} \times D_3) .
\end{align*}
\]

Hence, the unified form of the sequence $u$ is
\[
\{ (0, 3, 1, 2), (0, 2, 1, 3) \}\times (0, 0) .
\]

If $2 \in D_3$, then the support of the binary sequence $c$ is
\[
\{0\} \times (D_0 \cup D_3) \cup \{1\} \times (D_1 \cup D_3) .
\]

The support of the binary sequence $d$ is
\[
\{0\} \times (D_1 \cup D_3) \cup \{1\} \times (D_0 \cup D_3) .
\]
By \( u = \phi^{-1}(c, d) \), we have

\[
\begin{align*}
\text{Supp}_{u}(0) &= \psi(\{0\} \times D_2 \cup \{1\} \times D_2 \cup \{(0, 0), (1, 0)\}), \\
\text{Supp}_{u}(1) &= \psi(\{0\} \times D_1 \cup \{1\} \times D_0), \\
\text{Supp}_{u}(2) &= \psi(\{0\} \times D_3 \cup \{1\} \times D_3), \\
\text{Supp}_{u}(3) &= \psi(\{0\} \times D_0 \cup \{1\} \times D_1).
\end{align*}
\]

Hence, the unified form of the sequence \( u \) is

\[
[(2, 1, 3, 0), (2, 0, 3, 1)](0, 0).
\]

Similar to the proof in Corollary 3.1, the binary sequence determined by the triple \((2, 1, 3)\) is equivalent to the binary sequence defined by \((2, 1, 3)+2 = (0, 3, 1)\). Hence, the above unified form is in agreement with the case of \( 2 \in D_1 \).

(ii) If \( f \) is even, then we have \( p \equiv 1 \pmod{8} \), and \( 2 \in \text{QR}_p \). So that \( 2 \in D_0 \) or \( 2 \in D_2 \). The proof is similar, let us take \((a_0, a_1, a_2, a_3) = (s_6, s_3, s_4, s_5)\) for instance. By definition, \( \text{Supp}(s_6) = D_2 \cup D_3 \), \( \text{Supp}(s_3) = D_0 \cup D_3 \), \( \text{Supp}(s_4) = D_1 \cup D_2 \), \( \text{Supp}(s_5) = D_0 \cup D_1 \).

If \( 2 \in D_2 \), the support of the binary sequence \( c \) is

\[
\{0\} \times (D_0 \cup D_1) \cup \{1\} \times (D_1 \cup D_2).
\]

The support of the binary sequence \( d \) is

\[
\{0\} \times (D_0 \cup D_3) \cup \{1\} \times (D_2 \cup D_3).
\]

By \( u = \phi^{-1}(c, d) \), we have

\[
\begin{align*}
\text{Supp}_{u}(0) &= \psi(\{0\} \times D_2 \cup \{1\} \times D_0 \cup \{(0, 0), (1, 0)\}), \\
\text{Supp}_{u}(1) &= \psi(\{0\} \times D_3 \cup \{1\} \times D_3), \\
\text{Supp}_{u}(2) &= \psi(\{0\} \times D_0 \cup \{1\} \times D_2), \\
\text{Supp}_{u}(3) &= \psi(\{0\} \times D_1 \cup \{1\} \times D_1).
\end{align*}
\]

Hence, the unified form of the sequence \( u \) is

\[
[(2, 3, 0, 1), (0, 3, 2, 1)](0, 0).
\]

If \( 2 \in D_0 \), we can obtain the unified form of the sequence \( u \)

\[
[(0, 1, 2, 3), (2, 1, 0, 3)](0, 0).
\]

For the other cases, since the proofs are similar we omit them. \( \square \)

**Remark 3.3.**

- By Propositions 3.2 and 3.3, we find that the unified forms appear in pair, that is, if we exchange the columns of a unified form, we will arrive at a new one.
- By Propositions 3.1 and 3.3, four more unified forms can be obtained by the construction given by Su et al. in [17].

**Proposition 3.4.** Let \( p = 4f + 1 = x^2 + 4y^2 \) be a prime and \( y = -1 \). Let \( e = (e(0), e(1), e(2)) \) satisfy \( e(0) + e(1) + e(2) \equiv 1 \pmod{2} \) and

\[
(a_0, a_1, a_2, a_3) \in \left\{ (s_2, s_1, s_6, s_2), (s_2, s_6, s_1, s_2), (s_5, s_3, s_4, s_5), (s_5, s_4, s_3, s_5), (s_6, s_2, s_1, s_1), (s_1, s_2, s_2, s_6), (s_3, s_5, s_5, s_4), (s_4, s_5, s_5, s_1) \right\}.
\]
Then the unified form of the optimal quaternary sequence $u$ constructed in Theorem 4.2 belongs to one of the following cases

\[
\begin{align*}
&[(0, 2, 1, 3), (0, 2, 1, 3)](1, 0), [(1, 3, 2, 0), (1, 0, 2, 3)](1, 0), \\
&[(2, 0, 3, 1), (2, 0, 3, 1)](1, 0), [(2, 0, 3, 1), (3, 2, 0, 1)](1, 0), \\
&[(1, 2, 0, 3), (0, 2, 1, 3)](1, 0), [(2, 3, 1, 0), (1, 3, 2, 0)](1, 0), \\
&[(3, 0, 2, 1), (2, 2, 0, 1)](1, 0), [(0, 1, 3, 2), (3, 1, 0, 2)](1, 0), \\
&[(0, 3, 1, 2), (0, 2, 1, 3)](0, 1), [(1, 1, 2, 3), (1, 3, 2, 0)](0, 1), \\
&[(2, 1, 3, 0), (2, 0, 3, 1)](0, 1), [(3, 2, 0, 1), (3, 1, 0, 2)](0, 1), \\
&[(0, 2, 1, 3), (1, 2, 0, 3)](0, 1), [(1, 3, 2, 0), (2, 3, 1, 0)](0, 1), \\
&[(2, 0, 3, 1), (3, 0, 2, 1)](0, 1), [(3, 1, 0, 2), (0, 1, 3, 2)](0, 1).
\end{align*}
\]

Since the proof is similar to that of Proposition 3.3, the proof of Proposition 3.4 is given in Appendix B.

**Remark 3.4.** For the quaternary sequences with the unified forms given in Proposition 3.4, we readily find that they also appear in pairs, that is, they share the same autocorrelation distributions if we exchange the columns of the unified forms.

Last, let us analyse the constructions given by Luo et al. in [11]. We have the following result.

**Proposition 3.5.** Let conditions defined as in Appendix A (iv). Then the unified forms of the optimal quaternary sequence $s$ are

\[
\begin{align*}
&[(0, 1, 2, 3), (0, 3, 2, 1)](0, 0), [(1, 2, 3, 0), (1, 0, 3, 2)](0, 0), \\
&[(0, 1, 2, 3), (2, 1, 0, 3)](0, 0), [(1, 2, 3, 0), (3, 2, 1, 0)](0, 0), \\
&[(2, 3, 0, 1), (0, 3, 2, 1)](0, 0), [(3, 0, 1, 2), (1, 0, 3, 2)](0, 0),
\end{align*}
\]

when $f$ is odd and

\[
\begin{align*}
&[(0, 1, 2, 3), (2, 1, 0, 3)](0, 0), [(1, 2, 3, 0), (3, 2, 1, 0)](0, 0), \\
&[(2, 3, 0, 1), (0, 3, 2, 1)](0, 0), [(3, 0, 1, 2), (1, 0, 3, 2)](0, 0),
\end{align*}
\]

when $f$ is even.

**Proof.** The constant $c$ used in the construction can be assumed to be 0, otherwise by Definition 3.1 we add $-c$ to the $u_c$ and $v_c$ simultaneously. By the definition of the sequence $s$, we have

\[
\begin{align*}
\text{Supp}_s(0) &= (2D_m \pmod{2p}) \cup (2(D_{n+2} - \lambda) + 1 \pmod{2p}) \cup \{0\} \\
&= (2D_m \pmod{2p}) \cup (2D_{n+2} + p) \pmod{2p}) \\
&= \psi\{0\} \times (2D_m \pmod{p}) \cup \{1\} \times (2D_{n+2} \pmod{p}) \cup \{(0, 0)\}.
\end{align*}
\]

Similarly, we can prove that

\[
\begin{align*}
\text{Supp}_s(1) &= \psi\{0\} \times (2D_{m+1} \pmod{p}) \cup \{1\} \times (2D_{n+1} \pmod{p})}, \\
\text{Supp}_s(2) &= \psi\{0\} \times (2D_{m+2} \pmod{p}) \cup \{1\} \times (2D_{n} \pmod{p}) \cup \{(1, 0)\}, \\
\text{Supp}_s(3) &= \psi\{0\} \times (2D_{m+3} \pmod{p}) \cup \{1\} \times (2D_{n+3} \pmod{p})
\end{align*}
\]

By definition, $s(p) = 2$. To get the unified form of the sequence, we add to 2 to the second column sequence of $s$, which is equivalent to exchanging the support of 0 and 2, the support of 1 and 3 of the second column sequence, respectively.
Let $p$ be a prime. Then the known optimal and balanced quaternary sequences with period $2p$, where $p = 4f + 1$ is a prime, if their supports are related to the cyclotomic classes of order 4 with respect to $\mathbb{Z}_p$, then they are equivalent to the sequences by Chung’s construction or equivalent to the sequences by Su’s construction. We summarize their unified forms in the following theorem.

**Theorem 3.3.** Let $p = 4f + 1 = x^2 + 4y^2$ be a prime. Then the known optimal and balanced quaternary sequences using the cyclotomic classes of order 4 with respect to $\mathbb{Z}_p$ are equivalent with respect to autocorrelation to one of the quaternary sequences with the following unified forms (or the ones by exchanging their columns if needed).

1. If $f$ is odd and $x = 1$,
   
   $[((0, 1, 2, 3), (0, 3, 2, 1))_{(0, 0)}, [(1, 0, 3, 2), (1, 2, 3, 0)]_{(0, 0)}$.

2. If $f$ is even and $x = \pm 1$
   
   $[((0, 1, 2, 3), (2, 1, 0, 3))_{(0, 0)}, [(1, 0, 3, 2), (3, 0, 1, 2)]_{(0, 0)}$,
   $[((0, 3, 2, 1), (2, 3, 0, 1))_{(0, 0)}, [(1, 2, 3, 0), (3, 2, 1, 0)]_{(0, 0)}$.

3. If $f$ is odd and $y = -1$,
   
   $[((0, 3, 1, 2), (0, 2, 1, 3))_{(0, 0)}, [(1, 0, 2, 3), (1, 3, 2, 0)]_{(0, 0)}$.

**Remark 3.5.** By Propositions 3.2, 3.3 and 3.5, the unified forms of the sequences in [11] correspond to two unified forms of the case 1) in Proposition 3.2 when $f$ is odd and correspond to two unified forms of the case 2) in Proposition 3.3 when $f$ is even, respectively. In another word, the optimal quaternary sequences in [11] are not new.

In conclusion, for the optimal and balanced quaternary sequences with period $2p$, where $p = 4f + 1$ is a prime, if their supports are related to the cyclotomic classes of order 4 with respect to $\mathbb{Z}_p$, then they are equivalent to the sequences by Chung’s construction or equivalent to the sequences by Su’s construction. We summarize their unified forms in the following theorem.
(4) If \( f \) is odd and \( y = -1 \),
\[
\begin{align*}
[(0, 3, 1, 2), (0, 2, 1, 3)]_{(0,1)}, & [(1, 0, 2, 3), (1, 3, 2, 0)]_{(0,1)}, \\
[(2, 1, 3, 0), (2, 0, 3, 1)]_{(0,1)}, & [(3, 2, 0, 1), (3, 1, 0, 2)]_{(0,1)}, \\
[(0, 2, 1, 3), (1, 2, 0, 3)]_{(0,1)}, & [(1, 3, 2, 0), (2, 3, 1, 0)]_{(0,1)}, \\
[(2, 0, 3, 1), (3, 0, 2, 1)]_{(0,1)}, & [(3, 1, 0, 2), (0, 1, 3, 2)]_{(0,1)}. \\
\end{align*}
\]

Remark 3.6. For cases (1)-(3), the out-of-phase autocorrelation values belong to \( \{\pm 2\} \), while for case (4) the out-of-phase autocorrelation values belong to \( \{0, -2, \pm 2\xi_4\} \), where \( \xi_4 = \exp(\frac{2\pi i}{4}) \). We conjecture that the above listed unified forms of the quaternary sequences are complete for all the constructions related to cyclotomic classes of order 4 with respect to \( \mathbb{Z}_p \).

4. Conclusion

In this paper, we review several classes of optimal quaternary sequences of period \( 2p \), which are all closely related to the cyclotomic classes of order 4 with respect to \( \mathbb{Z}_p \). We introduce the unified form to classify these sequences and then conclude the unified forms of these optimal quaternary sequences. By doing this, we wish to establish some kinds of “standard”, by which the researches are able to identify if their construction is new or not.

Acknowledgments

The authors would like to thank the reviewers and the editor Sihem Mesnager for their detailed and constructive comments, which substantially improved the presentation of the paper.

References

[1] Y. Cai and C. Ding, Binary sequences with optimal autocorrelation, Theoret. Comput. Sci., 410 (2009), 2316–2322.
[2] J. Chung, Y. K. Han and K. Yang, New quaternary sequences with even period and three-valued autocorrelation, IEICE Trans. Fundam. Electron. Commun. Comput. Sci., E93-A(1) (2010), 309–315.
[3] C. Ding, T. Helleseth and H. M. Martinsen, New families of binary sequences with optimal three-level autocorrelation, IEEE Trans. Inf. Theory, 47(2001), 428–433.
[4] V. Edemskiy and A. Ivanov, Autocorrelation and linear complexity of quaternary sequences of period \( 2p \) based on cyclotomic classes of order four, 2013 IEEE International Symposium on Information Theory, (2013), 3120–3124.
[5] G. Golomb and G. Gong, Signal Designs with Good Correlations: For Wireless Communications, Cryptography and Radar Applications, Cambridge University Press, Cambridge, 2005.
[6] D. H. Green and P. R. Green, Polyphase-related prime sequences, IEEE Proc. Comput. Digit. Tech., 148 (2001), 53–62.
[7] J. W. Jang, Y. S. Kim, S. H. Kim and J. S. No, New quaternary sequences with ideal autocorrelation constructed from binary sequences with ideal autocorrelation, Proc. ISIT 2009, Seoul, Korea, (2009), 278–281.
[8] Y. S. Kim, J. W. Jang, S. H. Kim and J. S. No, New construction of quaternary sequences with ideal autocorrelation from Legendre sequences, Proc. ISIT 2009, Seoul, Korea, (2009), 282–285.
[9] Y. S. Kim, J. W. Jang, S. H. Kim and J. S. No, New quaternary sequences with optimal autocorrelation, Proc. ISIT 2009, Seoul, Korea, (2009), 286–289.
[10] N. Li, X. H. Tang and T. Helleseth, New M-ary sequences with low autocorrelation from interleaved technique, Des. Codes Cryptogr., 73 (2014), 237–249.
Known quaternary sequences with optimal autocorrelation and length $2p$

(i) In [2], the authors had an interesting observation that if one performed the Gray inverse mapping to a sequence pair, which are composed of a binary sequence of even length and a sequence of its appropriate cyclic shift, then one could get quaternary sequences which preserve the period and autocorrelation of the given binary sequence. Furthermore, Michel et al. mentioned in [12] that the result also holds if one replaces the cyclic shift sequence with the complementary sequence of the cyclic shift sequence.

**Theorem 4.1.** [12] [2] Let $a$ be a binary sequence with even period $N$ and optimal autocorrelation. Define

$$s = \phi^{-1}(a, L_N^\tau(a)) \text{ or } s = \phi^{-1}(a, L_N^\tau(a) + 1),$$

where $\phi^{-1}$ is the inverse Gray mapping, then $R_s(\tau) = R_a(\tau)$ for any $\tau, 0 \leq \tau < N$.

Obviously, if the DHM sequence is plugged in the construction in Theorem 4.1, then quaternary sequences with optimal autocorrelation magnitude could be obtained.

(ii) Let $N = 2p$, $\lambda = \frac{p+1}{2}$ and $e = (e(0), e(1), e(2))$ with $e(i) \in \mathbb{Z}_2$. Define binary sequences $c$ and $d$ with period $N$ as follows

$$c = I(a_0, e(0) + L^\lambda(a_1)), \quad d = I(e(1) + a_2, e(2) + L^\lambda(a_3)).$$

Then a quaternary sequence $u = \{u(i)\}_{i=0}^{N-1}$ is obtained by defining

$$u(i) = \phi^{-1}(c(i), d(i)),

where $\phi^{-1}$ is the inverse Gray mapping.
When twin-prime sequences pairs, GMW sequences pairs or sequences defined by cyclotomic classes of order 4 are used as the component sequences in above construction, then quaternary sequences with optimal autocorrelation could be obtained. For our purpose, let us pay attention to the case of sequences defined by cyclotomic classes of order 4. Let \( p \) be a prime, \( D_i, 0 \leq i \leq 3 \) be the cyclotomic classes of order 4 with respect to \( \mathbb{Z}_p \).

Let \( s_1, s_2, \ldots, s_6 \) be six binary sequences of length \( p \) with support sets \( D_0 \cup D_1, D_0 \cup D_2, D_0 \cup D_3, D_1 \cup D_2, D_1 \cup D_3, D_2 \cup D_3 \), respectively.

**Theorem 4.2.** [17] (Theorem 7-10) Let \( p = 4f + 1 = 4y^2 + x^2 \) be a prime.

1) Let \( f \) be odd, \( y = -1 \). Let \( e = (e(0), e(1), e(2)) \) satisfy \( e(0)+e(1)+e(2) \equiv 0 \) (mod 2) and

\[
(a_0, a_1, a_2, a_3) \in \left\{ \left( s_2, s_1, s_2, s_1 \right), \left( s_1, s_2, s_1, s_2 \right), \left( s_6, s_2, s_6, s_2 \right), \left( s_2, s_6, s_2, s_6 \right) \right\}.
\]

2) Let \( f \) be odd, \( y = -1 \). Let \( e = (e(0), e(1), e(2)) \) satisfy \( e(0)+e(1)+e(2) \equiv 0 \) (mod 2) and

\[
(a_0, a_1, a_2, a_3) \in \left\{ \left( s_1, s_2, s_1, s_2 \right), \left( s_2, s_1, s_2, s_1 \right), \left( s_2, s_6, s_2, s_6 \right), \left( s_6, s_2, s_6, s_2 \right) \right\}.
\]

3) Let \( f \) be odd, \( y = -1 \). Let \( e = (e(0), e(1), e(2)) \) satisfy \( e(0)+e(1)+e(2) \equiv 1 \) (mod 2) and

\[
(a_0, a_1, a_2, a_3) \in \left\{ \left( s_2, s_1, s_6, s_2 \right), \left( s_2, s_6, s_1, s_2 \right), \left( s_5, s_3, s_1, s_5 \right), \left( s_5, s_1, s_3, s_5 \right) \right\}.
\]

4) Let \( f \) be even, \( x = \pm 1 \). Let \( e = (e(0), e(1), e(2)) \) satisfy \( e(0)+e(1)+e(2) \equiv 0 \) (mod 2) and

\[
(a_0, a_1, a_2, a_3) \in \left\{ \left( s_6, s_3, s_4, s_1 \right), \left( s_6, s_4, s_3, s_1 \right), \left( s_4, s_6, s_3, s_1 \right), \left( s_3, s_6, s_4, s_1 \right) \right\}.
\]

Then the sequence given by (6) is optimal.

(iii) Let \( p = 4f + 1 = 4y^2 + x^2 \) be a prime. For \( 0 \leq i \leq 3 \), denote \( F_0,i = \psi(\{0\} \times D_i), F_1,i = \psi(\{1\} \times D_i) \), where \( \psi \) is the mapping defined in (2) and \( D_i \) is the cyclotomic classes of order 4 with respect to \( \mathbb{Z}_p \). Define \( C_k = F_{0,i_k} \cup F_{1,j_k}, k = 0, 1, 2, 3 \), where \( i_k \neq i_m \) and \( j_k \neq j_m \), if \( k \neq m \). It is easy to see that

\[
\mathbb{Z}_{2p} = \{0, p\} \cup \bigcup_{k=0}^{3} C_k.
\]

Then a quaternary sequence \( s \) is obtained by defining

\[
s(t) = \begin{cases} 
0, & \text{if } t \equiv 0 \pmod{2p} \in C_0 \cup \{0\}; \\
1, & \text{if } t \equiv 2 \pmod{2p} \in C_1; \\
2, & \text{if } t \equiv 0 \pmod{2p} \in C_2 \cup \{p\}; \\
3, & \text{if } t \equiv 4 \pmod{2p} \in C_3.
\end{cases}
\]

**Theorem 4.3.** [14] Let \( p \) be a prime such that \( p = 4f + 1 = x^2 + 4y^2 \).

1) If \( x = 1 \), \( y \) is even, and

\[
([i_0, i_1, i_2, i_3], [j_0, j_1, j_2, j_3]) \in \left\{ \left( [0, 1, 2, 3], [0, 3, 2, 1] \right), \left( [1, 0, 3, 2], [1, 2, 3, 0] \right) \right\}.
\]
2) If \( y = -1 \), and

\[
[(i_0, i_1, i_2; i_3), (j_0, j_1, j_2; j_3)] \in \left\{ \begin{array}{ll}
[(0, 2, 1, 3), (1, 2, 0, 3)], & [(1, 0, 2, 3), (2, 0, 1, 3)] \\
[(2, 0, 3, 1), (3, 0, 2, 1)], & [(3, 1, 0, 2), (0, 1, 3, 2)]
\end{array} \right.,
\]

then the sequence defined in (7) is balanced and optimal.

(iv) Let \( p = 4f + 1 \) be a prime, \( D_i, 0 \leq i \leq 3 \) be the cyclotomic classes of order 4 with respect to \( \mathbb{Z}_p \). Let \( m, n, c, j \in \mathbb{Z}_4 \), Tang-Lindner sequences \( u_c \) and \( v_c \) are quaternary sequences of length \( p \) defined by

\[
u_c(i) = \begin{cases}
  c, & \text{if } i = 0; \\
  j, & \text{if } i \in D_{(m+j)} \pmod 4,
\end{cases}
\]

and

\[
u_c(i) = \begin{cases}
  c, & \text{if } i = 0; \\
  j, & \text{if } i \in D_{(n+3j)} \pmod 4.
\end{cases}
\]

**Theorem 4.4.** [11] Let \( p = 4f + 1 = x^2 + 4y^2 \) be a prime with \( x = 1, \lambda = \frac{p+1}{2} \).

Quaternary sequence \( s \) of period \( 2p \) is constructed by

\[ s = I(u_c, L^\lambda(v_c) + 2). \]

If \((m, n, c, f)\) satisfies (i) \( f \) is odd and \( m - n \equiv 2c \pmod 4 \) or (ii) \( f \) is even and \( m - n \equiv 2c + 2 \pmod 4 \), then the quaternary sequence \( s \) is balanced and optimal.

**Appendix B**

**Proof of proposition 3.4**

Since \( e = (e(0), e(1), e(2)) \) satisfies \( e(0) + e(1) + e(2) \equiv 1 \pmod 2 \), for each \((a_0, a_1, a_2, a_3)\) four cases \((e(0), e(1), e(2))\) need to be considered, i.e.,

\[ (e(0), e(1), e(2)) \in \{(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 1)\}. \]

Additionally, since \( f \) is odd, we have \( p \equiv 5 \pmod 8 \) and \( 2 \in \text{NQR}_p \). So that \( 2 \in D_1 \) or \( 2 \in D_3 \). Therefore, for each \((a_0, a_1, a_2, a_3)\) eight cases should be considered according to different \((e(0), e(1), e(2))\) and \( 2 \in D_1 \) or \( 2 \in D_3 \).

Since the proofs are similar, we only prove the case \((a_0, a_1, a_2, a_3) = (s_2, s_1, s_6, s_2)\) when \( 2 \in D_1 \). By definition, \( \text{Supp}(s_1) = D_0 \cup D_1 \), \( \text{Supp}(s_2) = D_0 \cup D_2 \) and \( \text{Supp}(s_6) = D_2 \cup D_3 \).

(i) Suppose that \( 2 \in D_1 \) and \((e(0), e(1), e(2)) = (0, 0, 1)\), then by definition, we have \( c = I(a_0, L^\lambda(a_1)) \), \( d = I(a_2, L^\lambda(a_3) + 1) \), so that the support of the binary sequence \( c \) is

\[ \{0\} \times (D_1 \cup D_3) \cup \{1\} \times (D_1 \cup D_2). \]

The support of the binary sequence \( d \) is

\[ \{0\} \times (D_0 \cup D_3) \cup \{1\} \times (D_0 \cup D_2) \cup \{(1, 0)\}. \]

By \( u = \phi^{-1}(c, d) \), we have

\[
\text{Supp}_u(0) = \psi(\{0\} \times D_2 \cup \{1\} \times D_3 \cup \{0, 0\})), \\
\text{Supp}_u(1) = \psi(\{0\} \times D_0 \cup \{1\} \times D_0 \cup \{1, 0\})), \\
\text{Supp}_u(2) = \psi(\{0\} \times D_3 \cup \{1\} \times D_2), \\
\text{Supp}_u(3) = \psi(\{0\} \times D_1 \cup \{1\} \times D_1).
\]
Hence, the unified form of the sequence \( \mathbf{u} \) is
\[
[(2, 0, 3, 1), (3, 0, 2, 1)]_{(0, 1)}.
\]

(ii) Suppose that \( 2 \in D_1 \) and \((e(0), e(1), e(2)) = (1, 1, 1)\), then the support of the binary sequence \( \mathbf{c} \) is
\[
\{0\} \times (D_1 \cup D_3) \cup \{1\} \times (D_0 \cup D_3) \cup \{(0, 0)\}.
\]
The support of the binary sequence \( \mathbf{d} \) is
\[
\{0\} \times (D_1 \cup D_2) \cup \{1\} \times (D_0 \cup D_2) \cup \{(1, 0)\}.
\]

By \( \mathbf{u} = \phi^{-1}(\mathbf{c}, \mathbf{d}) \), we have
\[
\text{Supp}_u(0) = \psi(\{0\} \times D_0 \cup \{1\} \times D_1),
\]
\[
\text{Supp}_u(1) = \psi(\{0\} \times D_2 \cup \{1\} \times D_2 \cup \{(0, 0)\}),
\]
\[
\text{Supp}_u(2) = \psi(\{0\} \times D_1 \cup \{1\} \times D_0 \cup \{(1, 0)\}),
\]
\[
\text{Supp}_u(3) = \psi(\{0\} \times D_3 \cup \{1\} \times D_3).
\]

Hence, by our notation, the sequence \( \mathbf{u} \) can be written as
\[
[(0, 2, 1, 3), (1, 2, 0, 3)]_{(1, 2)}.
\]

Adding 3 to the both column sequences of \( \mathbf{u} \), we get the unified form of the sequence \( \mathbf{u} \)
\[
[(2, 1, 3, 0), (2, 0, 3, 1)]_{(0, 1)}.
\]

(iii) Suppose that \( 2 \in D_1 \) and \((e(0), e(1), e(2)) = (1, 0, 0)\), similar to the above discussion, we get the unified form of the sequence \( \mathbf{u} \) as follows
\[
[(1, 2, 0, 3), (0, 2, 1, 3)]_{(1, 0)}.
\]

(iv) Suppose that \( 2 \in D_1 \) and \((e(0), e(1), e(2)) = (1, 0, 0)\), similar to the above discussion, we get the unified form of the sequence \( \mathbf{u} \) as follows
\[
[(0, 2, 1, 3), (0, 3, 1, 2)]_{(1, 0)}.
\]
Combining above cases, the proof is thus completed.

Received April 2020; 1st revision April 2020; final revision July 2020.

E-mail address: keph@fjnu.edu.cn
E-mail address: 1750930248@qq.com
E-mail address: yang.data@swjtu.edu.cn