ON THE LINEAR COMPLEXITY AND AUTOCORRELATION OF GENERALIZED CYCLOTOMIC BINARY SEQUENCES WITH PERIOD $4p^n$

LIN YI, XIANGYONG ZENG*, ZHIMIN SUN AND SHASHA ZHANG

Hubei Key Laboratory of Applied Mathematics
Faculty of Mathematics and Statistics
Hubei University, Wuhan 430062, China

(Communicated by Zhengchun Zhou)

Abstract. In this paper, a new class of generalized cyclotomic binary sequences with period $4p^n$ is proposed. These sequences are almost balanced, and the explicit formulas of their linear complexity and autocorrelation are presented.

1. Introduction

Pseudo-random sequences are widely applied in digital communication and cryptography. In practical applications, the pseudo-random sequences are usually required to possess good autocorrelation and a high linear complexity in a suitable sense. The linear complexity of a sequence is defined as the length of the shortest linear feedback shift registers that can generate this sequence. To resist the well-known Berlekamp-Massey algorithm [17], sequences should have large enough linear complexity from the perspective of cryptography. On the other hand, the autocorrelation of a sequence is another measure for application to communication systems [14]. In order to eliminate the multipath effect, the absolute value of the out-of-phase autocorrelation of a pseudo-random sequence is expected to be as small as possible.

Cyclotomy is a classic topic of the elementary number theory and closely related to difference sets, sequences, coding theory and cryptography. During the last decades, a considerable amount of research had been conducted on constructing generalized cyclotomy [6, 7, 13, 19, 25]. To search for residue difference sets, Whiteman introduced a generalized cyclotomy with respect to $pq$ [19]. Whiteman’s generalized cyclotomy of order 2 was extended to the case with respect to $p_1^{e_1} \cdots p_t^{e_t}$ [7]. However, Whiteman’s generalized cyclotomy does not include the classical cyclotomy. A new generalized cyclotomy with respect to $p_1^{e_1} \cdots p_t^{e_t}$ that includes the classical cyclotomy as a special case was later presented by Ding and Helleseth [6], and it is

2020 Mathematics Subject Classification: Primary: 94A55; Secondary: 94A60.

Key words and phrases: Binary sequence, generalized cyclotomy, linear complexity, autocorrelation, almost balanced.

The work was supported by Application foundation frontier project of Wuhan Science and Technology Bureau under Grant 2020010601012189, and by the National Nature Science Foundation of China (NSFC) under Grant 62072161. The work of Sun was supported by the Natural Science Foundation of Hubei under Grant 2019CFB544. The work of Zhang was supported by the Research Foundation of Education Bureau of Hubei Province, China under Grant D2020104.

* Corresponding author: Xiangyong Zeng.
referred to as Ding-Helleseth’s generalized cyclotomy. Based on the isomorphism of residue class rings, a unified approach that determines both of the Whiteman’s and Ding-Helleseth’s generalized cyclotomy was proposed by Fan and Ge [13]. Recently, to construct optimal frequency hopping sequences, another generalized cyclotomy with respect to \( p_{e_1}^{e_1} \cdots p_{e_t}^{e_t} \) was introduced in [25], where the order of the generalized cyclotomy depends on the choice of parameters.

Generalized cyclotomic sequences constructed by the generalized cyclotomy are a class of significant cryptographic sequences. Many researchers have focused on the linear complexity and autocorrelation of generalized cyclotomic sequences. Based on Whiteman’s generalized cyclotomy of order 2, Ding presented a class of generalized cyclotomic sequences with period \( pq \), and calculated their linear complexity in [4] and autocorrelation in [5] respectively. However, these sequences are not balanced. In [7], Ding and Helleseth constructed a class of almost balanced binary sequences via their generalized cyclotomic classes of order 2, and the linear complexity and autocorrelation of the proposed sequences were determined by Bai [1] and Yan et al. [24] respectively. Subsequently, the linear complexity and autocorrelation of Whiteman’s and Ding-Helleseth’s generalized cyclotomic sequences with different periods had been extensively studied [9, 16, 21, 22]. With the generalized cyclotomy in [25], a new family of generalized cyclotomic binary sequences of period \( p^n \) was presented and their linear complexity was determined for \( n = 2 \) and \( f = 2^r \) with a positive integer \( r \) [20]. Moreover, based on experimental results, they proposed a conjecture that the linear complexity of these sequences is very close to \( p^n \) when the positive integer \( n \) is large enough. Later, this conjecture was proved by Edemskiy et al. in [11].

All the above mentioned generalized cyclotomic sequences have odd periods. For the case of even period, their linear complexity and autocorrelation had also been widely studied [8, 10, 12, 15, 26]. Two classes of generalized cyclotomic sequences with period \( 2p^n \) were constructed, and their linear complexity was determined [26]. Subsequently, new classes of generalized cyclotomic sequences with period \( 2p^n \) that includes the sequence presented in [26] as a special case were proposed by Ke et al. [15], and they determined the linear complexity and autocorrelation of the proposed sequences. With Whiteman’s generalized cyclotomy, Dong constructed four generalized cyclotomic sequences with period \( 4p^n \) and proved that these sequences have maximum linear complexity [8]. Edemskiy and his coauthors investigated generalized cyclotomic binary sequences of length \( 2^mp^n \) and evaluated their linear complexity and autocorrelation [10]. Recently, new generalized cyclotomic sequences with period \( 2^mp^n \) were proposed with a different method, and the sufficient conditions for these sequences with high linear complexity were given [12].

The purpose of this paper is to find more cyclotomic binary sequences with good properties. Our contributions are to construct a new class of generalized cyclotomic binary sequences with period \( 4p^n \), and evaluate their linear complexity and autocorrelation. In Section 2, we present the construction of these sequences. In Section 3, the linear complexity of these sequences is determined by the method described in [9]. The main idea is to establish the relationship between generating polynomials of new sequences and classical cyclotomic sequences with period \( p \), and then use the properties of the generating polynomial of classical cyclotomic sequences to their determine linear complexity. Our results show that the proposed sequences have large linear complexity. In Section 4, we present an explicit formula
of their autocorrelation by using the cyclotomic numbers of order 2 modulo \( p \). Finally, a conclusion is given in Section 5.

2. Generalized cyclotomic binary sequences of period \( 4p^n \)

In this section, we will recall basic definitions and introduce the construction of new generalized cyclotomic sequences with period \( 4p^n \).

For a positive integer \( N \), let \( \mathbb{Z}_N \) denote the residue class ring modulo \( N \) and \( \mathbb{Z}_N^* \) be the set of all invertible elements of \( \mathbb{Z}_N \). For a subset \( H \) of \( \mathbb{Z}_N \) and an element \( a \) in \( \mathbb{Z}_N \), define \( a + H = \{ a + h \ (\text{mod} \ N) \mid h \in H \} \) and \( aH = \{ ah \ (\text{mod} \ N) \mid h \in H \} \). An integer \( a \) is called a primitive root modulo \( N \) if the multiplicative order of \( a \) modulo \( N \) is equal to \( \phi(N) \), where \( \phi(\cdot) \) denotes the Euler’s function and \( \gcd(a, N) = 1 \). It is well known that only integers 1, 2, 4, \( p \) are common primitive roots modulo both 4 and \( p \).

For a positive integer \( n \), let \( \mathbb{Z}_n \) be an odd prime. The Chinese Remainder Theorem guarantees that there is at most one integer \( g \) satisfying \( \{ \phi(p^n) - 1 \mid j = 0, 1 \} \). Defining

\[
D_{0}^{(4p^n)} = \left\{ g^{2s}y^{j} \ (\text{mod} \ 4p^n) \mid 0 \leq s \leq \frac{\phi(p^n)}{2} - 1, j = 0, 1 \right\} \quad \text{and} \quad D_{1}^{(4p^n)} = gD_{0}^{(4p^n)}.
\]

Then \( D_{0}^{(4p^n)} \) and \( D_{1}^{(4p^n)} \) are called generalized cyclotomic classes of order 2 with respect to \( 4p^n \). It can be verified that

\[
\mathbb{Z}_{4p^n}^* = D_{0}^{(4p^n)} \cup D_{1}^{(4p^n)} \quad \text{and} \quad D_{0}^{(4p^n)} \cap D_{1}^{(4p^n)} = \emptyset,
\]

where \( \emptyset \) denotes the empty set. Likewise, for \( 1 \leq k \leq n - 1 \), we get

\[
\mathbb{Z}_{4p^k}^* = D_{0}^{(4p^k)} \cup D_{1}^{(4p^k)} \quad \text{and} \quad D_{0}^{(4p^k)} \cap D_{1}^{(4p^k)} = \emptyset,
\]

where \( D_{0}^{(4p^k)} = D_{0}^{(4p^n)} \ (\text{mod} \ 4p^k) \) and \( D_{1}^{(4p^k)} = gD_{0}^{(4p^k)} \).

For \( r = p^k \) or \( 2p^k \), \( 1 \leq k \leq n \), let

\[
D_{0}^{(r)} = \left\{ g^{2s} \ (\text{mod} \ r) \mid 0 \leq s \leq \frac{\phi(p^k)}{2} - 1 \right\} \quad \text{and} \quad D_{1}^{(r)} = gD_{0}^{(r)}.
\]

It follows that \[15\]

\[
\mathbb{Z}_c^* = D_{0}^{(r)} \cup D_{1}^{(r)} \quad \text{and} \quad D_{0}^{(r)} \cap D_{1}^{(r)} = \emptyset.
\]
Based on the fact that $\mathbb{Z}_N \setminus \{0\} = \bigcup_{1 < c, e | N} \frac{N}{\gcd(c, e)} \mathbb{Z}_c^*$, we have

$$
\mathbb{Z}_{4p^n} = \bigcup_{k=1}^{n} p^{n-k} \left( \mathbb{Z}_{4p^k}^* \cup 2\mathbb{Z}_{2p^k}^* \cup 4\mathbb{Z}_{p^k}^* \right) \cup p^n \mathbb{Z}_2^* \cup 2p^n \mathbb{Z}_2^* \cup \{0\}
$$

$$
= \bigcup_{k=1}^{n} p^{n-k} \left( D_0^{(4p^k)} \cup D_1^{(4p^k)} \cup 2D_0^{(2p^k)} \cup 2D_1^{(2p^k)} \cup 4D_0^{(p^k)} \cup 4D_1^{(p^k)} \right)
$$

$$
\cup \{0, p^n, 2p^n, 3p^n\}.
$$

For abbreviation, let

$$
H_i^{(4p^k)} = p^{n-k} D_i^{(4p^k)}, \quad H_i^{(2p^k)} = p^{n-k} D_i^{(2p^k)}, \quad H_i^{(p^k)} = p^{n-k} D_i^{(p^k)}
$$

for $1 \leq k \leq n$ and $i = 0, 1$.

In the following, motivated by the generalized cyclotomic sequences of period $2p^n$ in [15], we construct a class of generalized cyclotomic sequences of period $4p^n$.

The defining vector $\mathcal{I} = (i_1, i_2, \cdots, i_n)$ denotes any fixed binary vector in $\mathbb{Z}_2^n$.

Define

$$
C_{1}^{(d,e)} = \bigcup_{k=1}^{n} \left( H_i^{(4p^k)} \cup 2H_i^{(2p^k)} \cup 4H_i^{(p^k)} \right) \cup \{0\} \quad \text{and} \quad C_{0}^{(d,e)} = \mathbb{Z}_{4p^n} \setminus C_{1}^{(d,e)}
$$

where $i_k + d$ and $i_k + e$ are performed modulo 2 and $d, e \in \{0, 1\}$. For simplicity, the modulo operation is omitted in this paper. By the definitions of $C_{0}^{(d,e)}$ and $C_{1}^{(d,e)}$, it follows that $\{C_{0}^{(d,e)}, C_{1}^{(d,e)}\}$ forms a partition of $\mathbb{Z}_{4p^n}$ and $|C_{0}^{(d,e)}| - |C_{1}^{(d,e)}| = 2$. Now we construct a class of almost balanced binary sequences of period $4p^n$ that admits $C_{1}^{(d,e)}$ as the support set, i.e., the sequences $S^{(d,e)} = \left( s_0^{(d,e)}, s_1^{(d,e)}, \cdots, s_{4p^n-1}^{(d,e)} \right)$ are defined by

$$(1) \quad s_t^{(d,e)} = \begin{cases} 1, & \text{if } t \pmod{4p^n} \in C_{1}^{(d,e)}; \\ 0, & \text{if } t \pmod{4p^n} \in C_{0}^{(d,e)}. \end{cases}$$

3. The linear complexity of generalized cyclotomic binary sequences of period $4p^n$

Let $S = (s_0, s_1, \cdots, s_{N-1})$ be a binary sequence of period $N$ over the finite field $\mathbb{F}_2$. The generating polynomial of $S$ is defined as $S(x) = s_0 + s_1 x + \cdots + s_{N-1} x^{N-1}$. It is well known that the minimal polynomial of $S$ is $\frac{x^N - 1}{\gcd(x^N - 1, S(x))}$ and the linear complexity of $S$ [3]

$$(2) \quad LC(S) = N - \deg(\gcd(x^N - 1, S(x))).$$

In this section, we apply (2) to determine the linear complexity of new generalized cyclotomic binary sequences $S^{(d,e)}$ with period $4p^n$. Let

$$
S^{(d,e)}(x) = 1 + \sum_{k=1}^{n} \left( \sum_{j \in H_0^{(4p^k)}} x^j + \sum_{j \in 2H_1^{(2p^k)}} x^j + \sum_{j \in 4H_1^{(p^k)}} x^j \right)
$$

$$
= 1 + \sum_{k=1}^{n} \left( \sum_{j \in H_0^{(4p^k)}} x^j + \sum_{j \in 2H_1^{(2p^k)}} x^j + \sum_{j \in 4H_1^{(p^k)}} x^j \right)
$$
be the generating polynomial of $S^{(d,c)}$ for two given integers $d$ and $e$ with $0 \leq d, e \leq 1$. Note that $N = 4p^n$. Hence, we have $x^{4p^n} - 1 = (x^{p^n} - 1)^4$ over $F_2$. Thus

\begin{equation}
LC(S^{(d,c)}) = 4p^n - \deg \left( \gcd \left( (x^{p^n} - 1)^4, S^{(d,c)}(x) \right) \right).
\end{equation}

Let $m$ be the order of 2 modulo $p^n$ and $\theta$ be a primitive $p^n$-th root of unity over the finite field $F_{2^m}$, that is, $F_{2^m}$ is the splitting field of $x^{p^n} - 1$. Assume that $\theta_k = \theta^{p^{n-k}}$ with $1 \leq k \leq n$, then $\theta_k$ is a primitive $p^k$-th root of unity over $F_{2^m}$. Thus, to determine the linear complexity of sequences $S^{(d,c)}$, it is sufficient to count the number and the multiplicity of roots of $S^{(d,c)}(x)$ in the set $\{\theta^n | 0 \leq a \leq p^n - 1\}$.

To calculate the linear complexity of sequences defined in (1), the following lemmas are needed.

**Lemma 3.1.** [2, 3] Let notations be defined as above. Then $2 \pmod{p} \in D_0^{(p)}$ if $p \equiv \pm 1 \pmod{8}$, and $2 \pmod{p} \in D_1^{(p)}$ if $p \equiv \pm 3 \pmod{8}$.

**Lemma 3.2.** [15, 22] Let notations be defined as above. Then

\begin{enumerate}[(i)]
\item $2 \in D_i^{(p)}$ if and only if $2 \in D_i^{(p^k)}$ for $k \geq 1$ and $i = 0, 1$;
\item $\sum_{t \in D_0^{(p)}} \theta_i^t = 1 + \sum_{t \in D_1^{(p)}} \theta_i^t$ and $\sum_{t \in D_0^{(p^k)}} \theta_i^t = \sum_{t \in D_1^{(p^k)}} \theta_i^t = 0$ for $k \geq 2$, that is,
\end{enumerate}

\[\sum_{t \in \mathbb{Z}_{p^k}^*} \theta_i^t = \begin{cases} 1, & \text{if } k = 1, \\ 0, & \text{if } k \geq 2. \end{cases} \]

For brevity, we introduce the auxiliary polynomials used in following lemma. Let

\begin{align*}
U_i^{(k)}(x) &= \sum_{t \in H_i^{(p^k)}} x^t, & V_i^{(k)}(x) &= \sum_{t \in 2H_i^{(p^k)}} x^t, \\
W_i^{(k)}(x) &= \sum_{t \in 4H_i^{(p^k)}} x^t, & L_i(x) &= \sum_{t \in D_i^{(p)}} x^t
\end{align*}

for $1 \leq k \leq n$ and $l \in \{0, 1\}$. It follows from Lemma 3.2 (ii) that $L_i(\theta_1) + L_{i+1}(\theta_1) = 1$.

**Lemma 3.3.** Let notations be defined as above. Let $1 \leq p^f b \leq p^n - 1$ with $\gcd(b, p) = 1$ and $0 \leq f \leq n - 1$. Then for $k = 1, 2, \ldots, n$ and $l = 0, 1$, we have

\begin{enumerate}[(i)]
\item $U_i^{(k)}(\theta^{p^f} b) = \begin{cases} 0, & \text{if } k \neq f + 1, \\ 1, & \text{if } k = f + 1; \end{cases}$
\item $V_i^{(k)}(\theta^{p^f} b) = \begin{cases} \frac{p-1}{2}, & \text{if } k \leq f, \\ L_{i+1}(\theta_i^1), & \text{if } k = f + 1, \\ 0, & \text{if } k > f + 1, \end{cases}$
\end{enumerate}

if $2 \in D_j^{(p)}$ with $j \in \{0, 1\}$.
Proof. (i) Note that $\theta$ is a primitive $p^n$-th root of unity and $D_l(4p^k) \pmod{p^k}$ for $l = 0, 1$. Let $a = p^f b$, from the definition of $U_l^{(k)}(x)$ in (5), we get
\[ U_l^{(k)}(\theta^a) = \sum_{t \in H^{(4p^k)}} \theta^{t \theta^a} = \sum_{t \in p^n f - k D_i(4p^k)} \theta^t = \sum_{t \in p^n f - k \mathbb{Z}_{p^k}^*} \theta^t. \]

Hence each term in $U_l^{(k)}(\theta^a)$ equals to 1 when $k \leq f$. Therefore $U_l^{(k)}(\theta^a) = |\mathbb{Z}_{p^k}^*| = \varphi(p^k) = p^{k-1}(p-1) \equiv 0 \pmod{2}$. When $k \geq f + 1$, we have
\[ U_l^{(k)}(\theta^a) = \sum_{t \in \mathbb{Z}_{p^k}^*} \theta^{p^{n-f} t} = \sum_{t \in \mathbb{Z}_{p^k}^*} \theta^{t_{k-f}^l} \]
since $\theta_{k-f}^l = \theta^{p^{n-k-f}}$ is a primitive $p^{k-f}$-th root of unity. It is obvious that $\theta_{k-f}^l = \theta_{k-f}^{t_{k-f}^l}$ if and only if $t \equiv t' \pmod{p^{k-f}}$. Therefore, by Lemma 3.2 (ii), we have
\[ U_l^{(k)}(\theta^a) = \frac{\varphi(p^k)}{\varphi(p^{k-f})} \sum_{t \in \mathbb{Z}_{p^k}^*} \theta_{k-f}^t = \frac{p^f}{\varphi(p^{k-f})} \sum_{t \in \mathbb{Z}_{p^k}^*} \theta_{k-f}^t \pmod{2} = \begin{cases} 1, & \text{if } k = f + 1; \\ 0, & \text{if } k > f. \end{cases} \]

(ii) By the definitions of $V_l^{(k)}(x)$ and $W_l^{(k)}(x)$ in (5), we have
\[ V_l^{(k)}(\theta^a) = \sum_{t \in 2H^{(2p^k)}} \theta^{t \theta^a} = \sum_{t \in 2p^n f - k D_i(2p^k)} \theta^t = \sum_{t \in 2p^n f - k 2D_i(p^k)} \theta^t, \]
\[ W_l^{(k)}(\theta^a) = \sum_{t \in 4H^{(p^k)}} \theta^{t \theta^a} = \sum_{t \in p^n f - k 4D_i(p^k)} \theta^t. \]

With the same method as in (i), we have $V_l^{(k)}(\theta^a) = W_l^{(k)}(\theta^a) = |D_i(p^k)| = \frac{\varphi(p^k)}{2} \equiv \frac{p^f-1}{2} \pmod{2}$ when $k \leq f$, and
\[ V_l^{(k)}(\theta^a) = \sum_{t \in 2D_i(p^k f)} \theta_{k-f}^t, \quad W_l^{(k)}(\theta^a) = \sum_{t \in 4D_i(p^k f)} \theta_{k-f}^t \]
when $k \geq f + 1$. If $2 \in D_j(p)$ with $j \in \{0, 1\}$, then $4 \in D_0(p)$. Hence, by (i) and (ii) in Lemma 3.2, we get
\[ V_l^{(k)}(\theta^a) = \begin{cases} \frac{p^f-1}{2}, & \text{if } k \leq f; \\ L_{l+j}(\theta^1), & \text{if } k = f + 1; \\ 0, & \text{if } k > f + 1, \end{cases} \]
\[ W_l^{(k)}(\theta^a) = \begin{cases} \frac{p^f-1}{2}, & \text{if } k \leq f; \\ L_i(\theta^1), & \text{if } k = f + 1; \\ 0, & \text{if } k > f + 1. \end{cases} \]

Lemma 3.4. Let $S^{(d,e)}$ be the binary sequence defined in (1) and its generating polynomial be $S^{(d,e)}(x)$ given in (3), where $0 \leq d, e \leq 1$. Then $S^{(d,e)}(x)$ has no multiple roots, whose form is one of $\theta^a$, $1 \leq a \leq p^n - 1$. \qed
Proof. Suppose that \( S(x) = S^{(d,e)}(x) \) and its formal derivative is \( S'(x) \in \mathbb{F}_2[x] \), we have

\[
S'(x) = \sum_{k=1}^n \left( \sum_{j \in H_{ik+d}^{4p^k}} jx^{j-1} + \sum_{j \in 2H_{ik}^{2p^k}} jx^{j-1} + \sum_{j \in 4H_{ik}^{p^k}} jx^{j-1} \right)
\]

\[
= x^{-1} \sum_{k=1}^n \sum_{j \in H_{ik+d}^{4p^k}} x^j = x^{-1} \sum_{k=1}^n U_{ik+d}^{(k)}(x)
\]

by the definition of \( U_{ik+d}^{(k)}(x) \).

Assume that \( S(\theta^a) = 0 \) for each \( 1 \leq a \leq p^n - 1 \). To prove that \( S^{(d,e)}(x) \) has no multiple roots, it suffices to prove \( S'(\theta^a) \neq 0 \). Note that \( a = pm b \) with \( \gcd(b,p) = 1 \) and \( 0 \leq f \leq n - 1 \). It follows from Lemma 3.3 (i) that

\[
\sum_{k=1}^n U_{ik+d}^{(k)}(\theta^a) = U_{f+1}^{(f+1)}(\theta^a) = 1.
\]

Hence, we get \( S'(\theta^a) = \theta^{-1} \sum_{k=1}^n U_{ik+d}^{(k)}(\theta^a) \neq 0 \). Thus the assertion holds.

Now we calculate the linear complexity of sequences defined by (1).

**Theorem 3.5.** Let \( S^{(d,e)} \) be the binary sequence of period \( 4p^n \) defined by (1), where \( d,e \in \{0,1\} \). Its linear complexity satisfies

\[
\text{LC}(S^{(d,e)}) = \begin{cases} 
3p^n + 1, & \text{if } p \equiv \pm 1 \pmod{8}, \quad e = 0 \text{ or } p \equiv \pm 3 \pmod{8}, \quad e = 1; \\
4p^n, & \text{if } p \equiv 3 \pmod{8}, \quad e = 0 \text{ or } p \equiv 1 \pmod{8}, \quad e = 1.
\end{cases}
\]

**Proof.** Using above notations, the generating polynomial \( S^{(d,e)}(x) \) of \( S^{(d,e)} \) can be written as

\[
S^{(d,e)}(x) = 1 + \sum_{k=1}^n \left( U_{ik+d}^{(k)}(x) + V_{ik}^{(k)}(x) + W_{ik+d}^{(k)}(x) \right).
\]

For \( a = 0 \), we have \( S^{(d,e)}(\theta^a) = 1 \). For \( 2 \in D_{(p)}^{(p)} \) and \( 1 \leq a \leq p^n - 1 \), \( a = pm b \) with \( \gcd(b,p) = 1 \) and \( 0 \leq f \leq n - 1 \), it follows from Lemma 3.3 that

\[
S^{(d,e)}(\theta^a) = L_{i_f+1}(\theta_1^a) + L_{i_f+1+e}(\theta_1^a) = L_{i_f+1+e}(\theta_1^a),
\]

where \( L_l(x) \) is defined in (5). By Lemma 3.1, we know that \( j = 0 \) if \( p \equiv \pm 1 \pmod{8} \) and \( j = 1 \) if \( p \equiv \pm 3 \pmod{8} \). It follows that

\[
S^{(d,e)}(\theta^a) = \begin{cases} 
L_{i_f+1}(\theta_1) + L_{i_f+1+e}(\theta_1), & \text{if } p \equiv \pm 1 \pmod{8}; \\
L_{i_f+1+1}(\theta_1) + L_{i_f+1+e}(\theta_1), & \text{if } p \equiv \pm 3 \pmod{8}.
\end{cases}
\]

Therefore,

\[
S^{(d,e)}(\theta^a) = \begin{cases} 
L_{i_f+1}(\theta_1) + L_{i_f+1}(\theta_1) = 0, & \text{if } p \equiv \pm 1 \pmod{8}; \\
L_{i_f+1+1}(\theta_1) + L_{i_f+1}(\theta_1) = 1, & \text{if } p \equiv \pm 3 \pmod{8}.
\end{cases}
\]

for \( e = 0 \), and

\[
S^{(d,e)}(\theta^a) = \begin{cases} 
L_{i_f+1}(\theta_1) + L_{i_f+1+1}(\theta_1) = 1, & \text{if } p \equiv \pm 1 \pmod{8}; \\
L_{i_f+1+1}(\theta_1) + L_{i_f+1+1}(\theta_1) = 0, & \text{if } p \equiv \pm 3 \pmod{8}.
\end{cases}
\]
for \( e = 1 \). Applying Lemma 3.4 and the formula (4), we obtain the desired result. \( \square \)

4. The autocorrelation of generalized cyclotomic binary sequences of period \( 4p^n \)

Let \( S = \{s_0, s_1, \cdots, s_{N-1} \} \) be a binary sequence with period \( N \) and its autocorrelation function be defined as [14]

\[
R_S(\tau) = \sum_{t=0}^{N-1} (-1)^{s_t+s_{t+\tau}}, \quad 0 \leq \tau \leq N - 1,
\]

and these \( R_S(\tau), 0 < \tau < N, \) are called the out-of-phase autocorrelation values. In this section, we will calculate the autocorrelation of generalized cyclotomic binary sequences defined by (1). To this end, we measure the autocorrelation function by applying the method of [15] and the cyclotomic numbers of order 2 with respect to \( p \) [3].

Let \( D_0^{(p)} \) and \( D_1^{(p)} \) be the cyclotomic classes of order 2 with respect to \( p \). The cyclotomic numbers of order 2 with respect to \( p \) are defined as

\[
(i,j) = \left| \left(D_i^{(p)} + 1 \right) \cap D_j^{(p)} \right|, \quad i,j \in \{0,1\}.
\]

For simplicity, when \( i \) and \( j \) are nonnegative integers, we denote \( (i,j)_2 = (i',j') \), where \( i' \equiv i \) (mod 2), \( j' \equiv j \) (mod 2) with \( i',j' \in \{0,1\} \).

**Lemma 4.1.** [3] (i) If \( p \equiv 1 \) (mod 4), then

\[
(0,1) = (1,0) = (1,1) = \frac{p-1}{4}, \quad (0,0) = \frac{p-5}{4}.
\]

(ii) If \( p \equiv 3 \) (mod 4), then

\[
(1,0) = (0,0) = (1,1) = \frac{p-3}{4}, \quad (0,1) = \frac{p+1}{4}.
\]

**Lemma 4.2.** [15] For any \( \tau \in \mathbb{Z}_{p^k}^* \), \( k = 1,2,\cdots,n \) and \( i,j,h \in \{0,1\} \), we have

(i)

\[
\left| \left(D_i^{(p^k)} + \tau \right) \pmod{p^k} \cap D_j^{(p^k)} \right| = p^{k-1}(i+h,j+h) \quad \text{for} \quad \tau \in D_k^{(p^k)};
\]

(ii)

\[
\bigcup_{l=1}^{k-1} p^{k-l} \mathbb{Z}_{p^l}^* \cup \{0\} \subseteq \left(D_i^{(p^k)} + \tau \right) \pmod{(-\tau) \pmod{p}} \quad \text{for} \quad (\tau) \pmod{p} \in D_i^{(p)}.
\]

The following lemmas present some properties of the generalized cyclotomy with respect to \( 4p^k \) for \( 1 \leq k \leq n \). For brevity, let

\[
D_{i,j}^{(4p^k)} = \left\{ g^{i+2sy^l} \pmod{4p^k} \mid 0 \leq s \leq \frac{\varphi(p^k)}{2} - 1 \right\} \quad \text{and} \quad H_{i,j}^{(4p^k)} = p^{n-k} D_{i,j}^{(4p^k)}
\]

for \( 1 \leq k \leq n \) and \( i,j \in \{0,1\} \), then we have

\[
D_0^{(4p^k)} = D_{0,0}^{(4p^k)} \cup D_{0,1}^{(4p^k)}, \quad D_1^{(4p^k)} = D_{1,0}^{(4p^k)} \cup D_{1,1}^{(4p^k)},
\]

\[
H_0^{(4p^k)} = H_{0,0}^{(4p^k)} \cup H_{0,1}^{(4p^k)}, \quad H_1^{(4p^k)} = H_{1,0}^{(4p^k)} \cup H_{1,1}^{(4p^k)}.
\]
Lemma 4.3. Let notations be defined as above. Assume that $b$ is an odd integer; then for $1 \leq k \leq n$ and $0 \leq i,j \leq 1$, we have

(i) $D^{(p^k)}_i + pb \pmod{p^k} = D^{(p^k)}_{i,j}$;
(ii) \[ 2D^{(p^k)}_i + pb \pmod{2p^k} = D^{(2p^k)}_{i+1,j} \quad \text{for} \quad 2 \in D^{(p)}_j, \]
(iii) \[ D^{(2p^k)}_i + pb \pmod{2p^k} = 2D^{(p^k)}_{i+1,j} \quad \text{for} \quad 2 \in D^{(p)}_j, \]
(iv) $D^{(2p^k)}_i + 2pb \pmod{2p^k} = D^{(2p^k)}_i$;
(v) \[ D^{(4p^k)}_{0,i} + pb \pmod{4p^k} = \begin{cases} 2D^{(2p^k)}_{i+1,j}, & \text{if } pb \equiv 1 \pmod{4} \text{ and } 2 \in D^{(p)}_j, \\ 4D^{(p^k)}_i, & \text{if } pb \equiv 3 \pmod{4}, \end{cases} \]
(vi) \[ D^{(4p^k)}_{1,i} + pb \pmod{4p^k} = \begin{cases} 4D^{(p^k)}_{i+1,j}, & \text{if } pb \equiv 1 \pmod{4}, \\ 2D^{(2p^k)}_{i+1,j}, & \text{if } pb \equiv 3 \pmod{4} \text{ and } 2 \in D^{(p)}_j, \end{cases} \]
(vii) \[ 2D^{(2p^k)}_i + pb \pmod{4p^k} = \begin{cases} D^{(4p^k)}_{i+1,j+1}, & \text{if } pb \equiv 1 \pmod{4} \text{ and } 2 \in D^{(p)}_j, \\ D^{(4p^k)}_{0,i+1,j}, & \text{if } pb \equiv 3 \pmod{4}, \end{cases} \]
(viii) \[ 4D^{(p^k)}_i + pb \pmod{4p^k} = \begin{cases} D^{(4p^k)}_{0,i+1,j}, & \text{if } pb \equiv 1 \pmod{4}, \\ D^{(4p^k)}_{i+1,j}, & \text{if } pb \equiv 3 \pmod{4}, \end{cases} \]
(ix) \[ D^{(4p^k)}_{i,j} \quad \text{and} \quad 4pb \pmod{4p^k} = D^{(4p^k)}_{i,j}. \]

Proof. The cases (i) and (ii) follow from Lemma 2 of [23] and Lemma 5 of [15], respectively. For the case (iii), we only prove the formula (8) since others can be proved in the same way.

For any $x \in D^{(4p^k)}_{0,i}$, there exists a positive integer $s$ with $0 \leq s \leq \frac{\varphi(p^k)}{2} - 1$ such that $x = g^{s+b}$. Since $g \equiv 3 \pmod{4}$ and $y \equiv 1 \pmod{4}$, it follows that
\[ x + pb \pmod{4} = \begin{cases} 2, & \text{if } pb \equiv 1 \pmod{4}; \\ 4, & \text{if } pb \equiv 3 \pmod{4}. \end{cases} \]

On the other hand, $D^{(4p^k)}_{0,i} \pmod{p} = D^{(2p^k)}_i \pmod{p} = D^{(p^k)}_i \pmod{p} = D^{(p)}_i$ and $2D^{(p)}_i = D^{(p)}_i$ if $2 \in D^{(p)}_j$. Hence, by Lemma 3.2 (ii), one has
\[ x + pb \pmod{4p^k} \in \begin{cases} 2D^{(2p^k)}_{i+1,j}, & \text{if } pb \equiv 1 \pmod{4} \text{ and } 2 \in D^{(p)}_j; \\ 4D^{(p^k)}_i, & \text{if } pb \equiv 3 \pmod{4}. \end{cases} \]

Combining it with $|D^{(4p^k)}_{0,i}| = |D^{(2p^k)}_i| = |D^{(p^k)}_i|$, we obtain the desired result. \qed

Lemma 4.4. For $k = 1, 2, \cdots, n$, we have

(i) $\left\lfloor -1 \pmod{r} \right\rfloor \in \begin{cases} D^{(p^k)}_0, & \text{if } r = p^k; \\ D^{(p^k)}_0, & \text{if } r = 2p^k; \\ D^{(4p^k)}_{1,1}, & \text{if } r = 4p^k \end{cases}$.
if and only if \( p \equiv 1 \pmod{4} \).

(ii) 

\[-1 \pmod{r} \in \begin{cases} 
D^{(p^k)}_1, & \text{if } r = p^k; \\
D^{(2p^k)}_1, & \text{if } r = 2p^k; \\
D^{(4p^k)}_{1,0}, & \text{if } r = 4p^k
\end{cases}

if and only if \( p \equiv 3 \pmod{4} \).

\[\text{Proof.}\] We only prove that \(-1 \pmod{4p^k} \in D^{(4p^k)}_{1,1}\) if and only if \( p \equiv 1 \pmod{4} \), others can be proved similarly and so their proofs are omitted here.

Note that \( D^{(4p^k)}_{0,0}(mod \, p) = D^{(4p^k)}_1(mod \, p) = D^{(p)}_0\) and \(-1 \pmod{p} \in D^{(p)}_0\) if and only if \( p \equiv 1 \pmod{4} \). It follows that \(-1 \pmod{4p^k}\) belongs to either \( D^{(4p^k)}_{0,0}\) or \( D^{(4p^k)}_{1,1} \) if and only if \( p \equiv 1 \pmod{4} \). On the other hand, for any integer \( a \in \mathbb{Z}_{4p^k}^*\), one obtains that \( a \equiv 1 \pmod{4} \) if \( a \in D^{(4p^k)}_{0,0}\) and \( a \equiv 3 \pmod{4} \) if \( a \in D^{(4p^k)}_{1,1}\). Note that \(-1 \equiv 3 \pmod{4}\). Hence, \(-1 \pmod{4p^k} \in D^{(4p^k)}_{1,1}\) if and only if \( p \equiv 1 \pmod{4} \). \(\Box\)

Let \( R_{S^{(d,c)}}(\tau)\) be the autocorrelation function of the sequence \( S^{(d,c)}\) defined by (I) for \( 0 \leq \tau \leq 4p^k - 1 \). Then 

\[ R_{S^{(d,c)}}(\tau) = \sum_{t \in \{0, p^n, 2p^n, 3p^n\}} (-1)^{s_t+s_t} + \sum_{k=1}^{n} \sum_{t \in H^{(4p^k)}_0 \cup H^{(4p^k)}_1} (-1)^{s_t+s_t} + \sum_{k=1}^{n} \sum_{t \in 2H^{(2p^k)}_0 \cup 2H^{(2p^k)}_1} (-1)^{s_t+s_t}.
\]

Hence, to calculate the autocorrelation of generalized cyclotomic sequences \( S^{(d,c)}\), it is necessary to determine the elements of \( \{0, p^n, 2p^n, 3p^n\} + \tau, H^{(4p^k)}_1 + \tau, 2H^{(2p^k)}_1 + \tau \) and \( 4H^{(p^k)}_1 + \tau \), where \( 1 \leq k \leq n \) and \( i = 0, 1 \). With the help of Lemmas 4.1-4.4, we investigate the elements of these four sets in the following.

**Lemma 4.5.** Assume that \( \tau = p^f \tau_1 \in p^f \mathbb{Z}_{4p^n-f}^*\), \( f = 0, 1, \ldots, n-1 \) and \( i, j, r, h, h' \in \{0, 1\} \), then

(I) when \( k > n - f \), we get

\[ H^{(4p^k)}_{i,j} + \tau = \begin{cases} 
2H^{(2p^k)}_{i+j+r}, & \text{if } \tau_1 \in D^{(4p^n-f)}_{i+r+1,h} \text{ and } 2 \in D^{(p)}_{r}, \\
4H^{(p^k)}_{i+j}, & \text{if } \tau_1 \in D^{(4p^n-f)}_{i+r+1,h},
\end{cases}
\]

\[ H^{(4p^k)}_{i,i+j} = \begin{cases} 
4H^{(4p^k)}_{j}, & \text{if } \tau_1 \in D^{(4p^n-f)}_{i+r+1,h}, \\
2H^{(2p^k)}_{j+r} + \tau, & \text{if } \tau_1 \in D^{(4p^n-f)}_{i+r+1,h} \text{ and } 2 \in D^{(p)}_{r},
\end{cases}
\]

where

\[ \nu = \begin{cases} 
0, & \text{if } p \equiv 3 \pmod{4} \text{ and } f - n + k \text{ is even or } p \equiv 1 \pmod{4}, \\
1, & \text{if } p \equiv 3 \pmod{4} \text{ and } f - n + k \text{ is odd};
\end{cases}
\]

(II) when \( k = n - f \), we get
\( \Omega = \{ \tau \in D_{i,h}^{(4p^k)} \} \) when 

\[ (H_{i,h'}^{(4p^k)} + \tau) \cap 2H_j^{(2p^k)} = \begin{cases} p^{k-1}(h+h', i+h+j+r+1, h+h'+1), & \text{if } \tau \in D_{i,h}^{(4p^k)} \\
0, & \text{if } \tau \in D_{i+1,h}^{(4p^k)} \end{cases} \]

\[ \bigcup_{l \in \Omega} 2p^{n-l}Z_{2p^l} \cup \{ 2p^n \} \subseteq H_{i+1,h+1}^{(4p^k)} + \tau \text{ for } -\tau \in D_{i,h}^{(4p^k)}, \]

\[ (H_{i,h'}^{(4p^k)} + \tau) \cap 4H_j^{(p^k)} = \begin{cases} 0, & \text{if } \tau \in D_{i,h}^{(4p^k)} \\
p^{k-1}(i+h+j+r+1, h+h'+1), & \text{if } \tau \in D_{i+1,h}^{(4p^k)} \end{cases} \]

\[ \bigcup_{l \in \Omega} \left( H_i^{(4p^k)} + \tau \right) \subseteq H_{i+1,h+1}^{(4p^k)} + \tau \text{ for } -\tau \in D_{i,h}^{(4p^k)}, \]

where \( \Omega = \{ 1, 2, \ldots, k-1 \} \), \( \bar{H}_i = \bigcup_{l \in \Omega, (n-l) \text{ is odd}} H_i^{(4p^k)} \bigcup_{l \in \Omega, (n-l) \text{ is even}} H_{i+1}^{(4p^k)} \), 

\[ \eta_i = \begin{cases} p^n, & \text{if } i = 0, \\
3p^n, & \text{if } i = 1, \\
0, & \text{if } n-k \text{ is odd}, \\
1, & \text{if } n-k \text{ is even} \end{cases} \]

\[ \zeta = \begin{cases} 0, & \text{if } n \text{ is odd or } i = 1, n \text{ is even}, \\
1, & \text{if } n \text{ is odd or } i = 1, n \text{ is even} \end{cases} \]

\[ \delta_{i,n} = \begin{cases} p^n, & \text{if } i = 0, n \text{ is odd or } i = 1, n \text{ is even}, \\
3p^n, & \text{if } i = 0, n \text{ is even or } i = 1, n \text{ is odd} \end{cases} \]

(III) when \( k < n - f \), we get

\[ 2H_j^{(2p^k)} + \tau \subseteq H_{i+1,h+1}^{(4p^{n-f})} \text{ for } \tau \in D_{i,h}^{(4p^{n-f})}, \]

\[ 4H_j^{(p^k)} + \tau \subseteq H_{i,h}^{(4p^{n-f})} \text{ for } \tau \in D_{i,h}^{(4p^{n-f})}, \]

\[ H_i^{(4p^k)} + \tau \subseteq \begin{cases} 2H_{i+h+r+\mu}^{(2p^{n-f})}, & \text{if } \tau \in D_{i+h+\mu}^{(4p^{n-f})} \text{ and } 2 \in D_i^{(p^k)}, \\
4H_{i+h+r+\mu+1}^{(p^{n-f})}, & \text{if } \tau \in D_{i+h+\mu+1}^{(4p^{n-f})}, \end{cases} \]
where
\[
\mu = \begin{cases} 
0, & \text{if } p \equiv 3 \pmod{4} \text{ and } n - f - k \text{ is even or } p \equiv 1 \pmod{4}, \\ 
1, & \text{if } p \equiv 3 \pmod{4} \text{ and } n - f - k \text{ is odd.} 
\end{cases}
\]

The proof of Lemma 4.5 is presented in Appendix A. Similar to Lemma 4.5, we can obtain the following lemmas.

**Lemma 4.6.** Assume that \( \tau = 2p^f \tau_1 \in 2p^f \mathbb{Z}_{2p^{n-f}}, f = 0, 1, \cdots, n - 1 \) and \( i, j, h, r \in \{0, 1\} \), then
(I) when \( k > n - f \), we get
\[
H_i^{(4p^k)} + \tau = H_i^{(4p^k)} \\text{ for } k > n - f, \quad 2H_i^{(2p^k)} + \tau = 4H_i^{(p^k)} \text{ for } 2 \in D_i^{(p)},
\]
\[
4H_i^{(p^k)} + \tau = 2H_i^{(2p^k)} \text{ for } 2 \in D_i^{(p)};
\]
(II) when \( k = n - f \), we get
\[
\left|\left(2H_i^{(2p^k)} + \tau\right) \cap 4H_i^{(p^k)}\right| = p^{k-1}(i + h, j + h + r)2 \text{ for } \tau_1 \in D_h^{(2p^k)} \text{ and } 2 \in D_i^{(p)},
\]
\[
\left|\left(4H_i^{(p^k)} + \tau\right) \cap 2H_i^{(2p^k)}\right| = p^{k-1}(i + h + r, j + h)2 \text{ for } \tau_1 \in D_h^{(2p^k)} \text{ and } 2 \in D_i^{(p)},
\]
\[
\left|H_i^{(4p^k)} + \tau\right| \cap H_i^{(4p^k)} = \begin{cases} 
0, & \text{if } \tau_1 \in D_h^{(2p^k)} \text{ and } j = i, \\
p^{k-1}(p - 2), & \text{if } \tau_1 \in D_h^{(2p^k)} \text{ and } j = i + 1,
\end{cases}
\]
\[
\bigcup_{i \in \Omega} 4p^{n-i} \mathbb{Z}_{p^i} \cup \{0\} \subseteq 2H_h^{(2p^k)} + \tau \text{ for } -\tau_1 \in D_h^{(2p^k)},
\]
\[
\bigcup_{i \in \Omega} 2p^{n-i} \mathbb{Z}_{p^i} \cup \{2p^n\} \subseteq 4H_h^{(p^k)} + \tau \text{ for } -\tau_1 \in D_h^{(2p^k)} \text{ and } 2 \in D_i^{(p)},
\]
\[
\bigcup_{i \in \Omega} H_i^{(4p^k)} \cup \{\eta_i\} \subseteq H_i^{(4p^k)} + \tau_1 \in D_h^{(2p^k)}, 2 \in D_i^{(p)} \text{ and } p \equiv 1 \pmod{4},
\]
\[
\bar{H}_i \cup \{\delta_{i,n}\} \subseteq H_i^{(4p^k)} + \tau_1 \in D_h^{(2p^k)}, 2 \in D_i^{(p)} \text{ and } p \equiv 3 \pmod{4},
\]
where \( \Omega, \eta_i, \bar{H}_i, \delta_{i,n} \) and \( \zeta \) are defined in Lemma 4.5 and \( \zeta' = \zeta + 1 \pmod{2} \);
(III) when \( k < n - f \), we get
\[
2H_n^{(2p^k)} + \tau \subseteq 4H_n^{(p^n-f)} \text{ for } \tau_1 \in D_h^{(2p^n-f)} \text{ and } 2 \in D_i^{(p)},
\]
\[
4H_n^{(p^k)} + \tau \subseteq 2H_n^{(2p^n-f)} \text{ for } \tau_1 \in D_h^{(2p^n-f)},
\]
\[
H_i^{(4p^k)} + \tau \subseteq H_i^{(4p^n-f)} \text{ for } \tau_1 \in D_h^{(2p^n-f)} \text{ and } 2 \in D_i^{(p)},
\]
where \( \mu \) is defined in Lemma 4.5 and \( \mu' = \mu + 1 \pmod{2} \).

**Lemma 4.7.** Assume that \( \tau = 4p^f \tau_1 \in 4p^f \mathbb{Z}_{p^{n-f}}, f = 0, 1, \cdots, n - 1 \) and \( i, j, h, r \in \{0, 1\} \), then
(I) when \( k > n - f \), we have
\[
H_i^{(4p^k)} + \tau = H_i^{(4p^k)}, \quad 2H_i^{(2p^k)} + \tau = 2H_i^{(2p^k)}, \quad 4H_i^{(p^k)} + \tau = 4H_i^{(p^k)};
\]
(II) when \(k = n - f\), we have
\[
\begin{align*}
\left| 2H_i^{(2^k)} + \tau \right| \cap 2H_j^{(2^k)} & = p^{k-1}(i + h + r, j + h + r)_2 \quad \text{for } \tau_1 \in D_h^{(p^k)}, 2 \in D_r^{(p)}, \\
\left| 4H_i^{(p^k)} + \tau \right| \cap 4H_j^{(p^k)} & = p^{k-1}(i + h, j + h)_2 \quad \text{for } \tau_1 \in D_h^{(p^k)}, \\
\left( H_i^{(4^k)} + \tau \right) \cap H_j^{(4^k)} & = \begin{cases} p^{k-1}(p - 2), & \text{if } \tau_1 \in D_h^{(p^k)} \text{ and } j = i, \\ 0, & \text{if } \tau_1 \in D_h^{(p^k)} \text{ and } j = i + 1, \end{cases}
\end{align*}
\]

\[
\bigcup_{i \in \Omega} 2p^{n-f-1}Z^{(2^k)}_p \cup \{2^n\} \subseteq 2H_{h+r}^{(2^k)} + \tau \quad \text{for } \tau_1 \in D_h^{(p^k)} \text{ and } 2 \in D_r^{(p)},
\]

\[
\bigcup_{i \in \Omega} 4p^{n-f-1}Z^{(p^k)}_p \cup \{0\} \subseteq 4H_{h}^{(p^k)} + \tau \quad \text{for } \tau_1 \in D_h^{(p^k)},
\]

\[
\bigcup_{i \in \Omega} H_i^{(4^k)} \cup \{\eta_i\} \subseteq H_i^{(4^k)} + \tau \quad \text{for } \tau_1 \in D_h^{(p^k)} \text{ and } p \equiv 1 \pmod{4},
\]

\[
\bar{H}_i \cup \{\delta_i, n\} \subseteq H_i^{(4^k)} + \tau \quad \text{for } \tau_1 \in D_h^{(p^k)} \text{ and } p \equiv 3 \pmod{4},
\]

where \(\Omega, \eta_i, \bar{H}_i, \delta_i, n\) and \(\zeta\) are defined in Lemma 4.5;

(III) when \(k < n - f\), we have
\[
\begin{align*}
2H_h^{(2^k)} + \tau & \subseteq 2H_h^{(2^{n-f})} \text{ for } \tau_1 \in D_h^{(p^{n-f})} \text{ and } 2 \in D_r^{(p)}, \\
4H_h^{(p^k)} + \tau & \subseteq 4H_h^{(p^{n-f})} \text{ for } \tau_1 \in D_h^{(p^{n-f})}, \\
H_i^{(4^k)} + \tau & \subseteq H_i^{(4^{n-f})} \text{ for } \tau_1 \in D_h^{(p^{n-f})},
\end{align*}
\]

where \(\mu\) is defined in Lemma 4.5.

Now we calculate the autocorrelation of generalized cyclotomic binary sequences \(S^{(d,e)}\) with period \(4p^n\). To this end, we introduce the following notations. Let
\[
A(\tau) = \sum_{t \in \{0, p^n, 2p^n, 3p^n\}} (-1)^{s_{t+r} + s_{t}},
\]

\[
E_k(\tau) = \sum_{t \in H_i^{(4^k)} \cup H_j^{(4^k)}} (-1)^{s_{t+r} + s_{t}} + \sum_{t \in 2H_h^{(2^k)} \cup 2H_h^{(2^k)}} (-1)^{s_{t+r} + s_{t}} + \sum_{t \in 4H_h^{(p^k)} \cup 4H_h^{(p^k)}} (-1)^{s_{t+r} + s_{t}},
\]

\[
B(\tau) = \sum_{k=n-f+1}^{n} E_k(\tau), \quad C(\tau) = E_{n-f}(\tau), \quad D(\tau) = \sum_{k=1}^{n-f-1} E_k(\tau),
\]

where \(0 \leq f \leq n - 1\). Hence \(R_{S^{(d,e)}}(\tau) = A(\tau) + B(\tau) + C(\tau) + D(\tau)\) for \(0 \leq \tau \leq 4p^n - 1\).

**Theorem 4.8.** Let \(S^{(d,e)}\) be the generalized cyclotomic binary sequence with period \(4p^n\) defined by (1) and its defining vector be \(I = (i_1, i_2, \ldots, i_n) \in \mathbb{Z}_p^n\), where \(d, e \in \{0, 1\}\). Then, for \(0 \leq \tau \leq n - 1\), the autocorrelation of \(S^{(d,e)}\) is determined by the following cases:
where
\[ \Psi = \sum_{(n-1) \text{ is odd}} (-1)^{i_{n-1}} \varphi(p') \text{ and} \]
\[ \Delta_0 = \begin{cases} \sum_{l \in \Omega} (-1)^{i_{n-1}-i+l} \varphi(p') & \text{if } f \text{ is odd}, \\
\sum_{l \in \Omega} (-1)^{i_{n-1}-i} \varphi(p') & \text{if } f \text{ is even}; \end{cases} \]
\( \Omega = \{1, 2, \ldots, n - f - 1\} \), \( \Theta = \sum_{l \in \Omega} (-1)^{i_{n-1}-i} \varphi(p') \text{ and} \)

(II) when \( p \equiv 7 \pmod{8} \), \( e = 0 \) or \( p \equiv 3 \pmod{8} \), \( e = 1 \), we have

\[ R_{S(d,e)}(\tau) = \begin{cases} 4p^n, & \text{if } \tau = 0, \\
0, & \text{if } \tau \in \{p^n, 2p^n, 3p^n\}, \\
-4p^{n-1}(p-1) - 4\Psi, & \text{if } \tau \in 2p^f \mathbb{Z}_{2p^n-1}^*, \\
\kappa, & \text{if } \tau \in 4p^f \mathbb{Z}_{2p^n-1}^*; \end{cases} \]

where \( \kappa = 4p^n - 4p^{n-1} + 2p^{n-1}(p-3) - 4\Psi \), \( \Omega \) is defined in the case (I) and

(III) when \( p \equiv 5 \pmod{8} \), \( e = 0 \) or \( p \equiv 1 \pmod{8} \), \( e = 1 \), we have

\[ R_{S(d,e)}(\tau) = \begin{cases} 4p^n, & \text{if } \tau = 0, \\
-4p^n + 4, & \text{if } \tau = 2p^n, \\
0, & \text{if } \tau \in p^f \mathbb{Z}_{4p^n-1}^* \cup \{p^n, 3p^n\}, \\
-\omega + 4 \times (-1)^{i_{n-1}}, & \text{if } \tau \in 2p^f D_{0}^{(2p^n-1)}, \\
\omega + 4 \times (-1)^{i_{n-1}+1}, & \text{if } \tau \in \mathbb{Y}_0, \\
\omega + 4 \times (-1)^{i_{n-1}+1}, & \text{if } \tau \in \mathbb{Y}_1, \end{cases} \]

where \( \omega \) is defined in the case (I) and

\[ \mathbb{Y}_0 = \begin{cases} 4p^f D_{0}^{(p^n)}, & \text{if } p \equiv 5 \pmod{8} \text{ and } e = 0, \\
4p^f D_{1}^{(p^n)}, & \text{if } p \equiv 1 \pmod{8} \text{ and } e = 1, \end{cases} \]
\[ \mathbb{Y}_1 = \begin{cases} 4p^f D_{1}^{(p^n)}, & \text{if } p \equiv 5 \pmod{8} \text{ and } e = 0, \\
4p^f D_{0}^{(p^n)}, & \text{if } p \equiv 1 \pmod{8} \text{ and } e = 1; \end{cases} \]
(IV) when \( p \equiv 3 \pmod{8}, e = 0 \) or \( p \equiv 7 \pmod{8}, e = 1 \), we have

\[
R_{S(d,e)}(\tau) = \begin{cases} 
4p^n, & \text{if } \tau = 0, \\
0, & \text{if } \tau \in \{p^n, 3p^n\}, \\
-4p^n + 4, & \text{if } \tau = 2p^n; \\
(4p^n - f - 1 + 4\Psi) \times (-1)^d, & \text{if } \tau \in \Lambda_0, \\
(4p^n - f - 1 + 4\Psi) \times (-1)^{d+1}, & \text{if } \tau \in \Lambda_1, \\
-\kappa, & \text{if } \tau \in 2p^f\mathbb{Z}_p, \\
\kappa, & \text{if } \tau \in 4p^f\mathbb{Z}_p^n. 
\end{cases}
\]

where \( \kappa \) and \( \Psi \) are defined in the case (II), and

\[
\Lambda_0 = \begin{cases} 
p^fD_{0,0}^{(4p^n - f)} \cup p^fD_{1,0}^{(4p^n - f)}, & \text{if } p \equiv 3 \pmod{8} \text{ and } e = 0, \\
p^fD_{0,1}^{(4p^n - f)} \cup p^fD_{1,1}^{(4p^n - f)}, & \text{if } p \equiv 7 \pmod{8} \text{ and } e = 1,
\end{cases}
\]

\[
\Lambda_1 = \begin{cases} 
p^fD_{0,1}^{(4p^n - f)} \cup p^fD_{1,0}^{(4p^n - f)}, & \text{if } p \equiv 3 \pmod{8} \text{ and } e = 0, \\
p^fD_{0,0}^{(4p^n - f)} \cup p^fD_{1,1}^{(4p^n - f)}, & \text{if } p \equiv 7 \pmod{8} \text{ and } e = 1.
\end{cases}
\]

**Proof.** Similar to the proof of the case \( p \equiv 1 \pmod{8} \) and \( e = 0 \), others can be proved. So we only prove the case \( p \equiv 1 \pmod{8} \) and \( e = 0 \) here. By Lemma 3.1, we have \( 2 \in D^{(p)}_0 \). According to the value of \( \tau \), we discuss \( R_{S(d,e)}(\tau) \) with \( 0 \leq \tau < 4p^n \) in the following six cases.

**Case 1.** If \( \tau = 0 \), the result is trivial.

**Case 2.** If \( \tau = p^n \), then it can be verified that \( A(\tau) = 0 \). Since \( p \equiv 1 \pmod{8} \), it follows that \( p \equiv 1 \pmod{4} \). From (8) in Lemma 4.3, we have

\[
H_{(4p^n)}^2 + p^n = p^{n-k} \left(D_{i}^{(4p^n)} + p^n\right) = 2p^{n-k}D_{i}^{(2p^n)} = 2H_{i}^{(2p^n)}
\]

for any \( k \in \{0, 1, \cdots, n\} \) and \( i \in \{0, 1\} \). From (9)-(11) in Lemma 4.3, we get

\[
H_{1,0}^{(4p^n)} + p^n = 4H_{1,1}^{(2p^n)} + 2H_{1}^{(2p^n)} + p^n = 4H_{1}^{(4p^n)} + 4H_{1,i}^{(4p^n)} + p^n = H_{0,i}^{(4p^n)}
\]

for any \( k \in \{0, 1, \cdots, n\} \) and \( i \in \{0, 1\} \). Thus we obtain \( B(\tau) + C(\tau) + D(\tau) = 0 \) and \( R_{S(d,e)}(\tau) = 0 \) for \( \tau = p^n \). Similarly, \( R_{S(d,e)}(\tau) = 0 \) for \( \tau = 3p^n \) can be proved.

**Case 3.** If \( \tau = 2p^n \), it can be verified \( A(\tau) = 0 \). By (6), (7) and (12) in Lemma 4.3, we get

\[
2H_{1}^{(2p^n)} + 2p^n = 4H_{1}^{(4p^n)} + 4H_{1,i}^{(4p^n)} + 2p^n = 2H_{1}^{(2p^n)}, \quad H_{1}^{(4p^n)} + 2p^n = H_{1}^{(4p^n)}
\]

for any \( 1 \leq k \leq n \) and \( i = 0, 1 \). Then \( B(\tau) + C(\tau) + D(\tau) = -2(p^n - 1) + (p^n - 1) + (p^n - 1) = 0 \). Therefore, \( R_{S(d,e)}(\tau) = 0 \) for \( \tau = 2p^n \).

**Case 4.** If \( \tau \in p^fD_{0,0}^{(4p^n - f)} \) with \( 0 \leq f \leq n - 1 \), by (8) and (12) in Lemma 4.3, we have

\[
p^n + \tau \in H_{0,0}^{(4p^n - f)} + p^n = 2H_{0}^{(2p^n - f)} + 2p^n + \tau \in H_{1,0}^{(4p^n - f)} + 2p^n = H_{1,1}^{(4p^n - f)}, \quad 3p^n + \tau \in H_{1,0}^{(4p^n - f)} + 3p^n = 4H_{0}^{(p^n - f)}.
\]

Note that \( i_{n-f} = 1 \) and \( d = 0 \) here and others can be proved similarly. Hence, we get \( s_{y} = 0 \), \( s_{p^n - \tau} = 0 \), \( s_{2p^n - \tau} = 1 \) and \( s_{3p^n - \tau} = 0 \). Therefore, we have \( A(\tau) = 0 \). According to the value of \( k \), we further discuss \( R_{S(d,e)}(\tau) \) in several cases.

i) If \( k > n - f \), then \( H_{0}^{(4p^n)} + \tau = 2H_{0}^{(2p^n)} \cup 2H_{1}^{(2p^n)}, \quad H_{1}^{(4p^n)} + \tau = 4H_{0}^{(p^n)} \cup 4H_{1}^{(p^n)}, \quad \left(2H_{0}^{(2p^n)} \cup 2H_{1}^{(2p^n)}\right) + \tau = H_{1}^{(p^n)} \) and \( \left(4H_{0}^{(p^n)} \cup 4H_{1}^{(p^n)}\right) + \tau = H_{0}^{(4p^n)} \) by Lemma 4.5 (I). Thus \( B(\tau) = 0 \).
ii) If $k = n - f$, from Lemmas 4.5 (II) and 4.4 (i), we have

\begin{align}
&\left| H_0^{(4p^k)} + \tau \right| \cap 2H_j^{(2p^k)} = p^{k-1}[(0, j) + (1, j)], \left| H_1^{(4p^k)} + \tau \right| \cap 2H_j^{(2p^k)} = 0, \\
&\left| H_1^{(4p^k)} + \tau \right| \cap 4H_j^{(p^k)} = p^{k-1}[(0, j) + (1, j)], \left| H_0^{(4p^k)} + \tau \right| \cap 4H_j^{(p^k)} = 0, \\
&\left| 2H_j^{(2p^k)} + \tau \right| \cap H_1^{(4p^k)} = p^{k-1}[(j, 0) + (j, 1)], \left| 2H_j^{(2p^k)} + \tau \right| \cap H_1^{(4p^k)} = 0, \\
&\left| 4H_j^{(p^k)} + \tau \right| \cap H_0^{(4p^k)} = p^{k-1}[(j, 0) + (j, 1)], \left| 4H_j^{(p^k)} + \tau \right| \cap H_0^{(4p^k)} = 0,
\end{align}

where $j \in \{0, 1\}$. Note that $Z_{p^l}^* = D_0^{(p^l)} \cup D_1^{(p^l)}$, $Z_{2p^l}^* = D_0^{(2p^l)} \cup D_1^{(2p^l)}$ and $|H_0^{(4p^k)}| = |H_1^{(4p^k)}|$ for $1 \leq l \leq k$. Hence, from (19) and Lemma 4.1, we have

$$C(\tau) = (-1)^{s_{2p^n+s_\nu} + (-1)^{s_0+s_h} + (-1)^{s_{3p^n+s_e} + (-1)^{s_{p^n+s_d}}}} = 4,$$

where $2p^n = a + \tau \in H_0^{(4p^k)} + \tau$, $0 = b + \tau \in H_1^{(4p^k)} + \tau$, $3p^n = c + \tau \in 2H_0^{(2p^k)} + \tau$ and $p^n = d + \tau \in 4H_0^{(p^k)} + \tau$.

iii) If $k < n - f$, then $H_0^{(4p^k)} + \tau \subseteq 2H_0^{(2p^k-\tau)}$, $H_1^{(4p^k)} + \tau \subseteq 4H_0^{(p^k-\tau)}$, $\left(2H_0^{(2p^k)} + \tau\right) \cup \left(2H_1^{(2p^k)} + \tau\right) \subseteq H_1^{(4p^k)}$ and $\left(4H_0^{(p^k)} + \tau\right) \cup \left(4H_1^{(p^k)} + \tau\right) \subseteq H_0^{(4p^k)}$ by Lemma 4.5 (III). Then $D(\tau) = 0$.

Based on the above discussions, we get $R_{S(d, e)}(\tau) = 4$ for $\tau \in p^l D_{0,0}^{(4p^k-\tau)}$. Similarly, we can prove that $R_{S(d, e)}(\tau) = 4$ for $\tau \in p^l D_{1,1}^{(4p^k-\tau)}$ and $R_{S(d, e)}(\tau) = -4$ for $\tau \in p^l D_{0,1}^{(4p^k-\tau)}$ and $p^l D_{1,0}^{(4p^k-\tau)}$.

Case 5. If $\tau \in 2p^l D_{0,0}^{(4p^k)}$ with $0 \leq f \leq n - 1$, from (7) and (10) in Lemma 4.3, we get $p^n + \tau \in 2H_0^{(2p^k-\tau)}$, $p^n = H_1^{(4p^k-\tau)}$, $2p^n + \tau \in 2H_0^{(2p^k-\tau)} + 2p^n = 4H_0^{(p^k-\tau)}$ and $3p^n + \tau \in 2H_0^{(2p^k-\tau)} + 3p^n = H_0^{(4p^k-\tau)}$. Note that $s_\nu = 0$, $s_{p^n+\nu} = 1$, $s_{2p^n+\nu} = 0$ and $s_{3p^n+\nu} = 0$. Thus $A(\tau) = 0$. According to the value of $k$, we continue to discuss $R_{S(d, e)}(\tau)$ in the following three cases.

i) If $k > n - f$, from Lemma 4.6 (I), we have $H_1^{(4p^k)} + \tau = H_1^{(4p^k)}$, $2H_1^{(2p^k)} + \tau = 4H_1^{(p^k)}$ and $4H_1^{(p^k)} + \tau = 2H_1^{(2p^k)}$ for $i = 0, 1$. So $B(\tau) = -\left(2p^n - 2p^{n-\tau}\right) + \left(2p^n - 2p^{n-\tau}\right) = 0.$
ii) If \( k = n - f \), by Lemmas 4.6 (II) and 4.4 (i), we have
\[
\begin{aligned}
\left| \left( 2H_i^{(2p^k)} + \tau \right) \cap 4H_j^{(p^k)} \right| &= \left| \left( 4H_i^{(p^k)} + \tau \right) \cap 2H_j^{(2p^k)} \right| = p^{k-1}(i, j), \\
\left| \left( H_i^{(4p^k)} + \tau \right) \cap H_j^{(4p^k)} \right| &= \begin{cases} 
0, & \text{if } j = i, \\
p^{k-1}(p-2), & \text{if } j = i + 1,
\end{cases}
\end{aligned}
\]
(20)
\[
\begin{aligned}
\bigcup_{l=1}^{k-1} 4p^{n-l}z_{p^l}^* \cup \{0\} \subseteq 2H_0^{(2p^k)} + \tau, \quad \bigcup_{l=1}^{k-1} 2p^{n-l}z_{2p^l}^* \cup \{2p^l\} \subseteq 4H_0^{(p^k)} + \tau, \\
\bigcup_{l=1}^{k-1} H_0^{(4p^l)} \cup \{p^n\} \subseteq H_1^{(4p^k)} + \tau, \quad \bigcup_{l=1}^{k-1} H_1^{(4p^l)} \cup \{3p^n\} \subseteq H_0^{(4p^k)} + \tau,
\end{aligned}
\]
where \( i, j \in \{0, 1\} \). Note that \( z_{p^l}^* = D_0^{(p^l)} \cup D_1^{(p^l)} \), \( z_{2p^l}^* = D_0^{(2p^l)} \cup D_1^{(2p^l)} \) and \( |H_0^{(4p^l)}| = |H_1^{(4p^l)}| = \varphi(p') \) with \( 1 \leq l \leq k \). It follows from (20) and Lemma 4.1 that
\[
\begin{aligned}
C(\tau) &= -2p^{k-1}(p-2) + 2p^{k-1}[(0, 0) - (0, 1) - (1, 0) + (1, 1)] \\
&\quad + \sum_{l \in \Omega} 2(-1)^{i_1+\cdots+i_{k-1}} \varphi(p') \\
&= -2p^{k-1}(p-1) + 2 \sum_{i \in \Omega} (-1)^{i} \varphi(p'),
\end{aligned}
\]
where \( \Omega = \{1, 2, \cdots, k-1\} \).

iii) If \( k < n - f \), then \( H_1^{(4p^k)} + \tau \subseteq H_0^{(4p^{n-k})}, H_0^{(4p^k)} + \tau \subseteq H_1^{(4p^{n-k})}, \left( 2H_0^{(2p^k)} + \tau \right) \cup \left( H_1^{(2p^k)} + \tau \right) \subseteq 4H_0^{(p^k)} + \tau \), and \( \left( H_1^{(4p^k)} + \tau \right) \cup \left( H_1^{(4p^k)} + \tau \right) \subseteq 2H_0^{(2p^{n-k})} \) by (III) of Lemma 4.6. Note that \( 2|H_0^{(p^k)}| = 2|H_1^{(2p^k)}| = |H_1^{(4p^k)}| = \varphi(p^k) \) with \( 1 \leq k \leq n - f - 1 \) and \( i, j \in \{0, 1\} \). Hence we get \( D(\tau) = 2 \sum_{l \in \Omega} (-1)^{i_1+\cdots+i_{n-k-1}} \varphi(p') = 2 \sum_{l \in \Omega} (-1)^{i} \varphi(p') \), where \( \Omega = \{1, 2, \cdots, n - f - 1\} \).

Based on the above discussions, we get
\[
R_{S(d,e)}(\tau) = -2p^{n-f-1}(p-1) + 4 \sum_{i \in \Omega} (-1)^{i} \varphi(p') \quad \text{for } \tau \in 2p^f D_0^{(2p^{n-f})}.
\]
Similarly, \( R_{S(d,e)}(\tau) = -2p^{n-f-1}(p-1) + 4 \sum_{i \in \Omega} (-1)^{i} \varphi(p') \) with \( \tau \in 2p^f D_1^{(2p^{n-f})} \) can be proved.

Case 6. If \( \tau \in 4p^l z_{p^{n-f}}^* \) with \( 0 \leq l \leq n-1 \), by the same method as in the case 5, we get
\[
R_{S(d,e)}(\tau) = 4p^n - 4p^{n-f} + 2p^{n-f-1}(p-3) - 4 \sum_{i \in \Omega} (-1)^{i} \varphi(p')
\]
for \( i_{n-f} = 1 \) and \( d = 0 \), where \( \Omega = \{1, 2, \cdots, n - f - 1\} \). When \( i_{n-f} = 1, d = 1 \) or \( i_{n-f} = 0, d = 0, 1 \), the autocorrelation of \( S(d,e) \) can be obtained similarly.

As a result, when \( p \equiv 1 \pmod{8} \) and \( e = 0 \), we get the autocorrelation of \( S(d,e) \). The proof is completed. \( \Box \)

**Remark 1.** In Theorem 4.8, if \( \Omega = \emptyset \), then we set \( \Theta = \Psi = 0 \).
Remark 2. Let \( S^{(d,e)} = (s_0^{(d,e)}, s_1^{(d,e)}, \ldots, s_{4p^n-1}^{(d,e)}) \) be the binary sequence of period \( 4p^n \) defined by (1), where \( d, e \in \{0, 1\} \). Assume that the periodic sequence \( \tilde{S}^{(d,e)} = (\tilde{s}_0^{(d,e)}, \tilde{s}_1^{(d,e)}, \ldots, \tilde{s}_{4p^n-1}^{(d,e)}) \) satisfies

\[
\tilde{s}_i^{(d,e)} = \begin{dcases} 
1, & \text{if } i = 2p^n; \\
\tilde{s}_i^{(d,e)}, & \text{if } i \in \mathbb{Z}_{4p^n} \setminus \{2p^n\}.
\end{dcases}
\]

Obviously, the sequence \( \tilde{S}^{(d,e)} \) is balanced. Using the same method as in Theorem 4.8, we can present that these sequences also have high linear complexity, and an explicit formula of their autocorrelation.

To end this section, we provide an example to illustrate the results in Theorems 3.5 and 4.8.

Example 1. Let \( p = 3, g = 11, y = 65, n = 3, d = 1, e = 0 \) and \( \mathcal{I} = (0, 1, 1) \), we can obtain

\[
\begin{align*}
H_{0,0}^{(4p)} &= \{9\}, \\
H_{0,1}^{(4p)} &= \{45\}, \\
H_{1,0}^{(4p)} &= \{99\}, \\
H_{1,1}^{(4p)} &= \{63\}, \\
2H_{0}^{(2p)} &= \{18\}, \\
2H_{1}^{(2p)} &= \{90\}, \\
4H_{0}^{(p)} &= \{36\}, \\
4H_{1}^{(p)} &= \{72\}, \\
H_{0,0}^{(4p^2)} &= \{3, 39, 75\}, \\
H_{0,1}^{(4p^2)} &= \{15, 51, 87\}, \\
H_{1,0}^{(4p^2)} &= \{33, 69, 105\}, \\
H_{1,1}^{(4p^2)} &= \{21, 57, 93\}, \\
2H_{0}^{(2p^2)} &= \{6, 42, 78\}, \\
2H_{1}^{(2p^2)} &= \{30, 66, 102\}, \\
4H_{0}^{(p^2)} &= \{12, 48, 84\}, \\
4H_{1}^{(p^2)} &= \{24, 60, 96\}, \\
H_{0,0}^{(4p^2)} &= \{1, 13, 25, 37, 49, 61, 73, 85, 97\}, \\
H_{0,1}^{(4p^2)} &= \{5, 17, 29, 41, 53, 65, 77, 89, 101\}, \\
H_{1,0}^{(4p^2)} &= \{11, 23, 35, 47, 59, 71, 83, 95, 107\}, \\
H_{1,1}^{(4p^2)} &= \{7, 19, 31, 43, 55, 67, 79, 91, 103\}, \\
2H_{0}^{(2p^2)} &= \{2, 14, 26, 38, 50, 62, 74, 86, 98\}, \\
2H_{1}^{(2p^2)} &= \{10, 22, 34, 46, 58, 70, 82, 94, 106\}, \\
4H_{0}^{(p^2)} &= \{4, 16, 28, 40, 52, 64, 76, 88, 100\}, \\
4H_{1}^{(p^2)} &= \{8, 20, 32, 44, 56, 68, 80, 92, 104\}
\end{align*}
\]

and

\[
C_{1}^{(d,e)} = H_{1}^{(4p)} \cup 2H_{0}^{(2p)} \cup 4H_{0}^{(p)} \cup H_{0}^{(4p^2)} \cup 2H_{1}^{(2p^2)} \cup 4H_{1}^{(p^2)} \\
\cup H_{0}^{(4p^2)} \cup 2H_{1}^{(2p^2)} \cup 4H_{1}^{(p^2)} \cup \{0\}.
\]

Then the binary sequence \( S^{(d,e)} \) with support set \( C_{1}^{(d,e)} \) is

\[
(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, \ldots, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0).
\]
By computer experiment, its linear complexity is 108 and its autocorrelation distribution is given in Table 1.

| \(R_{S^{(d,e)}}(\tau)\) | \(\tau\) |
|----------------|--------|
| 68             | 1, 11, 13, 23, 25, 35, 37, 47, 49, 59, 61, 71, 73, 83, 85, 95, 97, 107 |
| 32             | 2, 10, 14, 22, 26, 34, 38, 46, 50, 58, 62, 70, 74, 82, 86, 94, 98, 106 |
| -4             | 3, 9, 33, 69, 75, 99, 105 |
| -32            | 4, 8, 16, 20, 28, 32, 40, 44, 52, 56, 64, 68, 76, 80, 88, 92, 100, 104 |
| 68             | 5, 7, 17, 19, 29, 31, 41, 43, 53, 55, 65, 67, 77, 79, 89, 91, 101, 103 |
| -80            | 6, 30, 42, 66, 78, 102 |
| 80             | 12, 24, 48, 60, 84, 96 |
| 4              | 15, 21, 45, 51, 57, 63, 87, 93, 99 |
| -96            | 18, 90 |
| 0              | 27, 81 |
| 96             | 36, 72 |
| -104           | 54 |

On the other hand, from Theorem 3.5, we have \(LC(S^{(d,e)}) = 4p^3 = 108\). From Theorem 4.8 (IV), we have that \(R_{S^{(d,e)}}(\tau) = 0\) if \(\tau \in \{p^3, 3p^3\}\) and \(R_{S^{(d,e)}}(\tau) = -4p^3 + 4 = -104\) if \(\tau = 2p^3\).

(i) when \(f = 0\), we have \(\Omega = \{1, 2\}\) and \(\Psi = (-1)^{i_3-i_1+1}\varphi(p) + (-1)^{i_3-i_2}\varphi(p^2) = 8\), and then

\[
R_{S^{(d,e)}}(\tau) = \begin{cases} 
(4p^2 + 4\Psi) \times (-1)^d = -68, & \text{if } \tau \in D_{0,0}^{(4p^3)} \cup D_{1,0}^{(4p^3)}, \\
(4p^2 + 4\Psi) \times (-1)^{d+1} = 68, & \text{if } \tau \in D_{0,1}^{(4p^3)} \cup D_{1,1}^{(4p^3)}, \\
-4p^3 + 4p^3 - 2p^2(p - 3) + 4\Psi = 32, & \text{if } \tau \in 2Z_{2p^3}^{*}, \\
4p^3 - 4p^3 + 2p^2(p - 3) - 4\Psi = -32, & \text{if } \tau \in 4Z_{p^3}^{*}.
\end{cases}
\]

(ii) when \(f = 1\), we have \(\Omega = \{1\}\) and \(\Psi = (-1)^{i_2-i_1}\varphi(p) = -2\), and then

\[
R_{S^{(d,e)}}(\tau) = \begin{cases} 
(4p + 4\Psi) \times (-1)^d = -4, & \text{if } \tau \in pD_{0,0}^{(4p^3)} \cup pD_{1,0}^{(4p^3)}, \\
(4p + 4\Psi) \times (-1)^{d+1} = 4, & \text{if } \tau \in pD_{0,1}^{(4p^3)} \cup pD_{1,1}^{(4p^3)}, \\
-4p^3 + 4p^2 - 2p(p - 3) + 4\Psi = -80, & \text{if } \tau \in 2pZ_{2p^3}^{*}, \\
4p^3 - 4p^2 + 2p(p - 3) - 4\Psi = 80, & \text{if } \tau \in 4pZ_{p^3}^{*}.
\end{cases}
\]

(iii) when \(f = 2\), we have \(\Omega = \emptyset\) and \(\Psi = 0\), and then

\[
R_{S^{(d,e)}}(\tau) = \begin{cases} 
(4 + 4\Psi) \times (-1)^d = -4, & \text{if } \tau \in p^2D_{0,0}^{(4p)} \cup p^2D_{1,0}^{(4p)}, \\
(4 + 4\Psi) \times (-1)^{d+1} = 4, & \text{if } \tau \in p^2D_{0,1}^{(4p)} \cup p^2D_{1,1}^{(4p)}, \\
-4p^3 + 4p - 2(p - 3) + 4\Psi = -96, & \text{if } \tau \in 2p^2Z_{2p^3}, \\
4p^3 - 4p + 2(p - 3) - 4\Psi = 96, & \text{if } \tau \in 4p^2Z_{p^3}.
\end{cases}
\]

Thus, these are consistent with the experimental results.

5. Conclusion

In this paper, a new class of almost balanced binary sequences of period \(4p^n\) was constructed via Ding-Helleseth’s generalized cyclotomy. The linear complexity
Moreover, we presented an explicit formula of their autocorrelation. To prove the assertion, one needs to determine the elements of $H_{i,j}^{(4p^k)} + \tau$, $2H_{i,j}^{(2p^k)} + \tau$ and $4H_{i,j}^{(p^k)} + \tau$ for each $k$ with $1 \leq k \leq n$ and $i = 0, 1$. Here we only investigate the structure of $H_{i,j}^{(4p^k)} + \tau$ and others can be proved similarly. According to the value of $k$, the following three cases are discussed.

(I) If $k > n - f$, then

$$H_{i,j}^{(4p^k)} + \tau = p^{n-k}f_{i,j}^{(4p^k)} + p^f \tau_1 = p^{n-k}\left(D_{i,j}^{(4p^k)} + p^{f-n+k}\tau_1\right).$$

Hence, to analyze the structure of $H_{i,j}^{(4p^k)} + \tau$, it suffices to investigate $D_{i,j}^{(4p^k)} + p^{f-n+k}\tau_1$. By (8) and (9) in Lemma 4.3, we have that

$$D_{i,j}^{(4p^k)} + p^{f-n+k}\tau_1 \mod 4p^k \begin{cases} 2D_{i,j}^{(2p^k)} + 1, & \text{if } \tau_1 \in D_{i,j}^{(4p^k)} \\ 4D_{i,j}^{(p^k)} + 1, & \text{if } \tau_1 \in D_{i,j}^{(2p^k)} \end{cases}$$

when $p \equiv 3 \mod 4$ and $f - n + k$ is even or $p \equiv 1 \mod 4$; and

$$D_{i,j}^{(4p^k)} + p^{f-n+k}\tau_1 \mod 4p^k \begin{cases} 2D_{i,j}^{(2p^k)} + 1, & \text{if } \tau_1 \in D_{i,j}^{(4p^k)} \\ 4D_{i,j}^{(p^k)} + 1, & \text{if } \tau_1 \in D_{i,j}^{(2p^k)} \end{cases}$$

when $p \equiv 3 \mod 4$ and $f - n + k$ is odd. Hence, (13) holds.

(II) If $k = n - f$, then

$$H_{i,h}^{(4p^k)} + \tau = p^{n-k}\left(D_{i,h}^{(4p^k)} + \tau_1\right) \mod 4p^k = p^{n-k}\left(D_{i,h}^{(4p^k)} + \tau_1\right) \mod 4p^k.$$ 

Hence, to investigate the structure of $H_{i,h}^{(4p^k)} + \tau_1$, it suffices to determine the elements of $D_{i,h}^{(4p^k)} + \tau_1$ for $\tau_1 = \tau_1 \mod 4p^k$. This is equivalent to calculating the number of solutions of the equation $u + \tau_1 = v \mod 4p^k$ with $u \in D_{i,h}^{(4p^k)}$ and $v \in \mathbb{Z}_{4p^k}$.

For abbreviation, let

$$T_0 = \bigcup_{l=1}^{k} p^{k-l}Z_{4p^l}^* \cup \{p^k, 3p^k\}, \quad T_1 = \bigcup_{l=1}^{k} 2p^{k-l}Z_{2p^l}^* \cup \{2p^k\}, \quad T_2 = \bigcup_{l=1}^{k} 4p^{k-l}Z_{p^l}^* \cup \{0\}.$$ 

Note that $\mathbb{Z}_{4p^k} = \bigcup_{l=1}^{k} p^{k-l} \left(\mathbb{Z}_{4p^l}^* \cup 2\mathbb{Z}_{2p^l}^* \cup 4\mathbb{Z}_{p^l}^*\right) \cup \{0, p^k, 2p^k, 3p^k\}$. It follows that $\mathbb{Z}_{4p^k} = T_0 \cup T_1 \cup T_2$. According to the value of $v \in T_t$, $0 \leq t \leq 2$, we discuss the number of solutions of $u + \tau_1 = v \mod 4p^k$ in the following three cases:
Case 1. $v \in T_0$. Note that $g \equiv 3 \pmod{4}$ and $y \equiv 1 \pmod{4}$. Then we have $u + \tau_1 = v \pmod{4p^k}$ has no solution if $\tau_1 \in \mathbb{Z}_{4p^k}^* = D_0^{(4p^k)} \cup D_1^{(4p^k)}$. Therefore

$$
\left(D_{i,h}^{(4p^k)} + \tau_1 \pmod{4p^k}\right) \cap T_0 = \emptyset \quad \text{if} \quad \tau_1 \in \mathbb{Z}_{4p^k}^*.
$$

Case 2. $v \in T_1$. Since $g \equiv 3 \pmod{4}$ and $y \equiv 1 \pmod{4}$, it follows that $u + \tau_1 = v \pmod{4p^k}$ has at least one solution when $\tau_1 \in D_1^{(4p^k)}$, and no solution when $\tau_1 \in D_{i+1}^{(4p^k)}$. That is,

$$
\left|\left(D_{i,h}^{(4p^k)} + \tau_1\right) \cap T_1\right| = \begin{cases} 
\tau_1 > 0, & \text{if} \ \tau_1 \in D_i^{(4p^k)}; \\
0, & \text{if} \ \tau_1 \in D_{i+1}^{(4p^k)}. 
\end{cases}
$$

Let $T_1 = 2\mathbb{Z}_{2p^k}$ and $T_i'' = \bigcup_{l=1}^{k-1} 2p^k - l \mathbb{Z}_{2p^l} \cup \{2p^k\}$, then $T_1 = T_1' \cup T_1''$. In order to further determine the value of $m$, we discuss it by the following two cases according to $v \in T_1'$ or $T_1''$:

(i) $v \in T_1'$. Due to $|D_{i,h}^{(4p^k)}| = |D_j^{(2p^k)}| = |D_j^{(p^k)}|$, then the number of the solutions of $u + \tau_1 = v \pmod{4p^k}$ with $u \in D_{i,h}^{(4p^k)}$, $v \in 2D_j^{(2p^k)}$ equals the number of the solutions of $u + \tau_1 = v \pmod{p^k}$ with $u \in D_{i,h}^{(p^k)}$, $v \in 2D_j^{(p^k)}$.

From Lemmas 3.2 (ii) and 4.2 (i), we get

$$
\left|\left(D_{i,h}^{(4p^k)} + \tau_1\right) \cap 2D_j^{(2p^k)}\right| = \left|\left(D_{i,h}^{(p^k)} + \tau_1 \pmod{p^k}\right) \cap D_j^{(p^k)}\right|
$$

if $\tau_1 \in D_{i,h}^{(4p^k)}$ and $2 \in D_j^{(p^k)}$. So (14) follows.

(ii) $v \in T_1''$. It follows that $u + \tau_1 \equiv 2 \pmod{4}$ and $u + \tau_1 \equiv 0 \pmod{p}$ are necessary conditions for the existence of $u + \tau_1 = v \pmod{4p^k}$. Hence, by Lemma 4.4, we have $u \in D_{i+1,h+1}^{(4p^k)}$ if $-\tau_1 \in D_{i,h}^{(4p^k)}$. To determine the number of solutions of $u + \tau_1 = v \pmod{4p^k}$, it suffices to study the structure of $D_{i+1,h+1}^{(4p^k)} + \tau_1$ for $-\tau_1 \in D_{i,h}^{(4p^k)}$. According to the value of the prime $p$, the following two cases are discussed:

1) $p \equiv 1 \pmod{4}$. Then we have $\tau_1 \in D_{i+1,h+1}^{(4p^k)}$ by Lemma 4.4 (i). Note that

$$
D_{i+1,h+1}^{(4p^k)} + \tau_1 = \left(D_{i+1,h+1}^{(4p^k)} + \lambda_i + \tau_1 + \lambda_i' \pmod{4p^k}\right),
$$

where $\lambda_i = p^i$ if $i = 0$, $\lambda_i = 3p^i$ otherwise, and $\lambda_i' = \lambda_i + 2p^k \pmod{4p^k}$. If $2 \in D_j^{(p^k)}$ with $r \in \{0, 1\}$, then for each $\tau_1 \in D_{i,h}^{(4p^k)}$, there exists only one $\tau''_1 \in D_{i,h+r}^{(2p^k)}$ satisfying $D_{i,h}^{(4p^k)} + \tau_1 = 4D_{i,h}^{(p^k)} + 2\tau''_1 \pmod{4p^k}$ by (8) and (9) in Lemma 4.3.

2) $p \equiv 3 \pmod{4}$. Then we obtain $\tau_1 \in D_{i+1,h}^{(4p^k)}$ by Lemma 4.4 (ii). If $2 \in D_j^{(p^k)}$ with $r \in \{0, 1\}$, then for each $\tau_1 \in D_{i+1,h}^{(4p^k)}$, we know that there exists a unique
element $\tau''_1 \in D_{i+1,h+r+1}^{(2p^k)}$ satisfying
\[
D_{i+1,h+1}^{(4p^k)} + \tau_1 = \begin{cases} 
(D_{i+1,h+1}^{(4p^k)} + \lambda'_i + (\tau_1 + \lambda'_i) \pmod{4p^k}), & \text{if } k \text{ is even;} \\
(D_{i+1,h+1}^{(4p^k)} + \lambda'_i + (\tau_1 + \lambda_i) \pmod{4p^k}), & \text{if } k \text{ is odd;}
\end{cases}
\]
by (8) and (9) in Lemma 4.3.

Hence, to determine the elements of
\[
D_{i+1,h+1}^{(4p^k)} + \tau_1 = 4D_{i+1}^{(p^k)} + 2\tau''_1 \pmod{4p^k}
\]
by Lemma 4.4. Hence, to analysis the structure of $D_{i+1,h+1}^{(4p^k)} + \tau_1$, it suffices to investigate $4D_{i+1}^{(p^k)} + 2\tau''_1 \pmod{4p^k}$. From Lemma 4.2 (ii), we have
\[
4 \left( \bigcup_{i=1}^{k-1} p^{k-i}Z_{p^i} \cup \{0\} \right) + 2p^k \subseteq 4D_{j}^{(p^k)} + (4\tau'_1 + 2p^k) \pmod{4p^k} \quad \text{for } \tau_1'' \in D_{j}^{(p^k)}.
\]

If $2 \in D_j^{(p)}$ for $r \in \{0,1\}$, then $4D_j^{(p)} + 2p^l \pmod{4p^l} = 2D_j^{(2p^l)}$ with $1 \leq l \leq k$ by (6) in Lemma 4.3. This combines with $Z_{p^i} = D_0^{(p^i)} \cup D_1^{(p^i)}$ and $Z_{2p^i} = D_0^{(2p^i)} \cup D_1^{(2p^i)}$, one obtains
\[
\bigcup_{i=1}^{k-1} 2p^{k-i}Z_{p^i} \cup \{2p^k\} \subseteq 4D_{j}^{(p^k)} + 2\tau''_1 \pmod{4p^k} \quad \text{for } \tau_1'' \in D_{j}^{(2p^k)}.
\]

Denote $j = i + h$, combining (21) with (22), we get
\[
T_j'' = \bigcup_{i=1}^{k-1} 2p^{k-i}Z_{p^i} \cup \{2p^k\} \subseteq D_{i+1,h+1}^{(4p^k)} + \tau_1 \pmod{4p^k} \quad \text{for } \tau_1 \in D_{i+1,h}^{(4p^k)}
\]
and (15) follows.

Case 3. $v \in T_2$. (16) and (17) can be proved by the same method as the case 2. So their proofs are omitted here.

(III) If $k < n - f$, we have
\[
H^{(4p^k)}_i + \tau = p^f \left( p^{n-f-k}D^{(4p^k)}_i + \tau_1 \right) \pmod{4p^n} = p^f \left( p^{n-f-k}D^{(4p^k)}_i + \tau_1 \pmod{4p^{n-f}} \right).
\]

Hence, to determine the elements of $H^{(4p^k)}_i + \tau$, it suffices to investigate $p^{n-f-k}D^{(4p^k)}_i + \tau_1$. Note that $Z_{4p^{n-f}} = \bigcup_{i=1}^{n-f} p^{n-f-i} \left( Z_{4p^i} \cup 2Z_{2p^i} \cup 4Z_{p^i} \right) \cup \{0, p^{n-f}, 2p^{n-f}, 3p^{n-f}\}$. Then it can be verified that
\[
p^{n-f-k}D^{(4p^k)}_i + \tau_1 \pmod{4p^{n-f}} \subseteq Z_{4p^{n-f}} \cup 2Z_{2p^{n-f}} \cup 4Z_{p^{n-f}}.
\]

According to the values of $p$ and $n - f - k$, we further explore $p^{n-f-k}D^{(4p^k)}_i + \tau_1 \pmod{4p^{n-f}}$ in following two cases:
i) \( p \equiv 3 \pmod{4} \) and \( n - f - k \) is even or \( p \equiv 1 \pmod{4} \). Since \( g \equiv 3 \pmod{4} \) and \( y \equiv 1 \pmod{4} \), we have

\[
p^{n-f-k}D_i^{(4p^k)} + \tau_1 \equiv \begin{cases} 2\mathbb{Z}_{2^{n-f}}^*, & \text{if } \tau_1 \in D_1^{D_i^{(4p^k)}}, \\
4\mathbb{Z}_{p^{n-f}}^*, & \text{if } \tau_1 \in D_1^{D_i^{(4p^k)}}.
\end{cases}
\]

Note that \( \mathbb{Z}_{2^{n-f}}^* = D_0^{(2^{n-f})} \cup D_1^{(2^{n-f})} \) and \( \mathbb{Z}_{p^{n-f}}^* = D_0^{(p^{n-f})} \cup D_1^{(p^{n-f})} \). Then we get

\[(23) \quad p^{n-f-k}D_i^{(4p^k)} + \tau_1 \equiv \begin{cases} 2D_1^{(2^{n-f})}, & \text{if } \tau_1 \in D_1^{(2^{n-f})}, \\
4D_1^{(p^{n-f})}, & \text{if } \tau_1 \in D_1^{(p^{n-f})}.
\end{cases}
\]

where \( j, j' \in \{0,1\} \). Next we determine the values of \( j \) and \( j' \) in (23). By the definitions of \( D_1^{(2^{n-f})}, D_i^{(2^{n-f})}, D_j^{(2^{n-f})} \) and \( D_{j'}^{(2^{n-f})} \), we have

\[
D_1^{(2^{n-f})} \equiv D_1^{(p)}, \quad D_i^{(2^{n-f})} \equiv D_i^{(p)}, \quad D_j^{(2^{n-f})} \equiv D_j^{(p)}.
\]

Hence, \( \tau_1 \equiv 2D_1^{(p)} \) when \( \tau_1 \in D_i^{(2^{n-f})} \), and \( \tau_1 \equiv 4D_1^{(p)} \) when \( \tau_1 \in D_i^{(2^{n-f})} \). If \( 2 \in D_i^{(p)} \) with \( r \in \{0,1\} \), then \( 4 \in D_0^{(p)} \). It follows that \( j = i + h + r \) and \( j' = i + h + 1 \). Therefore,

\[
p^{n-f-k}D_i^{(4p^k)} + \tau_1 \equiv \begin{cases} 2D_1^{(2^{n-f})}, & \text{if } \tau_1 \in D_1^{(2^{n-f})}, \\
4D_1^{(p^{n-f})}, & \text{if } \tau_1 \in D_1^{(p^{n-f})}.
\end{cases}
\]

ii) \( p \equiv 3 \pmod{4} \) and \( n - f - k \) is odd. If \( 2 \in D_i^{(p)} \) with \( r \in \{0,1\} \), using the same way as in i), we can prove

\[
p^{n-f-k}D_i^{(4p^k)} + \tau_1 \equiv \begin{cases} 4D_1^{(p^{n-f})}, & \text{if } \tau_1 \in D_1^{(4p^{n-f})}, \\
2D_1^{(2p^{n-f})}, & \text{if } \tau_1 \in D_1^{(2p^{n-f})}.
\end{cases}
\]

Based on the above discussions, (18) can be obtained. The proof is completed.

References

[1] E. Bai, X. Liu and G. Xiao, Linear complexity of new generalized cyclotomic sequences of order two of length \( pq \), IEEE Trans. Inf. Theory, 51 (2005), 1849–1853.

[2] D.M. Burton, Elementary Number Theory, McGram-Hill, New York, 1998.

[3] T. W. Cusick, C. Ding and A. Renvall, Stream Ciphers and Number Theory, Elsevier Science B. V., Amsterdam, 2004.

[4] C. Ding, Linear complexity of generalized cyclotomic binary sequences of order 2, Finite Fields Appl., 3 (1997), 159–174.

[5] C. Ding, Autocorrelation values of generalized cyclotomic sequences of order two, IEEE Trans. Inf. Theory, 44 (1998), 1699–1702.

[6] C. Ding and T. Helleseth, New generalized cyclotomy and its applications, Finite Fields Appl., 4 (1998), 140–166.

[7] C. Ding and T. Helleseth, Generalized cyclotomy codes of length \( p_1^{m_1}p_2^{m_2} \ldots p_t^{m_t} \), IEEE Trans. Inf. Theory, 45 (1999), 467–474.

[8] X. Dong, Linear complexity of generalized cyclotomic binary sequences of length \( 4p^n \), Inf. Sci. Lett., 4 (2015), 67–70.

[9] V. Edemskiy, about computation of the linear complexity of generalized cyclotomic sequences with period \( p^{n+1} \), Des. Codes Cryptogr., 61 (2011), 251–260.
[10] V. Edemskiy and O. Antonova, The evaluation of the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2^np^m$, *International Journal of Mathematical Models and Methods in Applied Sciences*, 9 (2015), 512–517.

[11] V. Edemskiy, C. Li, X. Zeng and T. Helleseth, The linear complexity of generalized cyclotomic binary sequences of period $p^m$, *Des. Codes Cryptogr.*, 87 (2018), 1183–1197.

[12] V. Edemskiy and C. Wu, On the linear complexity of binary sequences derived from generalized cyclotomic classes modulo $2^np^m$, *WSEAS Transactions on Mathematics*, 18 (2019), 197–202.

[13] C. Fan and G. Ge, A unified approach to Whiteman’s and Ding-Helleseth’s generalized cyclotomy over residue class rings, *IEEE Trans. Inf. Theory*, 60 (2014), 1326–1336.

[14] S. W. Golomb and G. Gong, *Signal Design for Good Correlation, for Wireless Communications, Cryptography and Radar Applications*, Cambridge University Press, Cambridge, 2005.

[15] P. Ke, J. Zhang and S. Zhang, On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^m$, *Des. Codes Cryptogr.*, 67 (2013), 325–339.

[16] Y. J. Kim, S. Y. Jin and H. Y. Song, Linear complexity and autocorrelation of prime cube sequences, *AAECC, LNCS*, 4851 (2007), 188–197.

[17] J. L. Massey, Shift-register synthesis and BCH decoding, *IEEE Trans. Inf. Theory*, 15 (1969), 122–127.

[18] M. B. Nathnson, *Elementary Methods in Number Theory*, Springer, Berlin, GTM 195, 2003.

[19] A. L. Whiteman, A family of difference sets, *Illinois J. Math.*, 6 (1962), 107–121.

[20] Z. Xiao, X. Zeng, C. Li and T. Helleseth, New generalized cyclotomic binary sequences of period $p^2$, *Des. Codes Cryptogr.*, 86 (2018), 1483–1497.

[21] T. Yan, B. Huang and G. Xiao, Cryptographic properties of some binary generalized cyclotomic sequences with length $p^2$, *Inf. Sci.*, 178 (2008), 1078–1086.

[22] T. Yan, S. Li and G. Xiao, On the linear complexity of generalized cyclotomic sequences with period $p^m$, *Appl. Math. Lett.*, 21 (2008), 187–193.

[23] T. Yan and X. Li, Some notes on the generalized cyclotomic binary sequences of length $2p^m$ and $pm$, *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, 96 (2013), 2049–2051.

[24] T. Yan, R. Sun and G. Xiao, Autocorrelation and linear complexity of the new generalized cyclotomic sequences, *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, 90 (2007), 857–864.

[25] X. Zeng, H. Cai, X. Tang and Y. Yang, Optimal frequency hopping sequences of odd length, *IEEE Trans. Inf. Theory*, 59 (2013), 3237–3248.

[26] J. Zhang, C. Zhao and X. Ma, Linear complexity of generalized cyclotomic binary sequences of length $2p^m$, *Applicable Algebra in Engineering Communication and Computing*, 21 (2010), 93–108.

Received January 2021; revised April 2021.

E-mail address: linyi2017@aliyun.com
E-mail address: xiangyongzeng@aliyun.com
E-mail address: zmsun@hubu.edu.cn
E-mail address: amushasha@163.com