A Family of Pseudorandom Binary Sequences Derived from Generalized Cyclotomic Classes Modulo $p^{m+1}q^{n+1}$

Xiaolin Chen[1], Zhixiong Chen[2], and Huaning Liu[1]
(Corresponding author: Huaning Liu)

School of Mathematics, Northwest University[1]
Xi'an 710127, Shaanxi, P. R. China
Provincial Key Laboratory of Applied Mathematics, Putian University[2]
Putian 351100, Fujian, P. R. China
(Email: hnliu@nwu.edu.cn)

(Received Feb. 22, 2019; Revised and Accepted Sept. 6, 2019; First Online Feb. 29, 2020)

Abstract

Let p, q be two distinct odd primes, and let m, n be non-negative integers. We consider a family of binary sequences defined by generalized cyclotomic classes modulo $p^{m+1}q^{n+1}$. The first contribution is to determine their linear complexity, which improves certain results of Hu, Yue and Wang. The second contribution is to compute the autocorrelation values. Results obtained indicate that such sequences are 'good' from the viewpoint of cryptography.

Keywords: Autocorrelation Value; Generalized Cyclotomy; Generalized Cyclotomic Sequence; Linear Complexity; Stream Cipher

1 Introduction

The theory of cyclotomy is widely applied in cryptography. A typical application is the design of pseudorandom sequences or numbers. By defining the (generalized) cyclotomic classes modulo an integer, families of pseudorandom sequences can be designed with the desired cryptographic features. The classical examples are the Legendre sequences that derived from cyclotomic classes modulo an odd prime and the Jacobi sequences that derived from generalized cyclotomic classes modulo the product of two odd distinct primes. Attention is also paid to the generalized cyclotomic classes modulo a general number in the literature, see *e.g.*, [1–5, 9, 11, 12].

At the beginning of this decade, Hu, Yue and Wang [6] introduced families of binary sequences via defining generalized cyclotomic classes modulo N, where $N = p^{m+1}q^{n+1}$ for two distinct odd primes p and q and non-negative integers m and n. Let

$$\begin{aligned} d &= (p-1, q-1) = \left(\phi\left(p^{m+1}\right), \phi\left(q^{n+1}\right)\right), \\ e &= \frac{\phi\left(p^{m+1}\right)\phi\left(q^{n+1}\right)}{d}, \end{aligned}$$

where ϕ denotes the Euler function. Let g be a common primitive root of p^{m+1} and q^{n+1}, and let x be an integer satisfying

$$x \equiv g \pmod{p^{m+1}}, \quad x \equiv 1 \pmod{q^{n+1}}.$$

Define

$$G_i = \left\{g^s x^i : s = 0, 1, \cdots, e-1\right\}, \quad i = 0, 1, \cdots, d-1.$$

Then

$$\mathbb{Z}^*_{p^{m+1}q^{n+1}} = \bigcup_{i=0}^{d-1} G_i$$

For $0 \le a \le m+1$ and $0 \le b \le n+1$, let

$$G_i^{(a,b)} = \begin{cases} p^a q^b G_i, & \text{if } a \le m,\ b \le n,\ 0 \le i \le d-1, \\ p^a q^{n+1}\mathbb{Z}_N^*, & \text{if } a \le m,\ b = n+1,\ i = 0, \\ p^{m+1}q^b\mathbb{Z}_N^*, & \text{if } a = m+1,\ b \le n,\ i = 0, \\ \{0\}, & \text{if } a = m+1,\ b = n+1,\ i = 0. \end{cases}$$

Then Hu, Yue and Wang [6] introduced the binary sequence s^∞ of period N by setting

$$s_j = \begin{cases} 1, & \text{if } (j \bmod N) \in \Omega, \\ 0, & \text{otherwise}, \end{cases} \tag{1}$$

where Ω, usually called the *characteristic set* or *support set* of s^∞, is selected as

$$\Omega = \bigcup_{a=0}^{m+1} \bigcup_{b=0}^{n+1} \bigcup_{i \in I_{a,b}} G_i^{(a,b)},$$

for

$$I_{a,b} \subset \begin{cases} \{0,1,\cdots,d-1\}, & \text{if } a \le m,\ b \le n, \\ \{0\}, & \text{otherwise.} \end{cases} \quad (2)$$

They developed a way to compute the *linear complexity* (see the notion below) of s^∞. However, it seems difficult to determine the exact values due to the choice of $I_{a,b}$, see [6, Thm.2.5]. Motivated by this reason, we will only choose a special $I_{a,b}$ as follows and consider the linear complexity and *autocorrelation* (see the notion below) of the special binary sequence:

$$I_{a,b} = \begin{cases} \{1,3,5,\cdots,d-1\}, \\ \qquad \text{if } 0 \le a \le m \text{ and } 0 \le b \le n, \\ \emptyset, \\ \qquad \text{if } 0 \le a \le m+1 \text{ and } b = n+1, \\ \{0\}, \\ \qquad \text{if } a = m+1 \text{ and } 0 \le b \le n. \end{cases} \quad (3)$$

We remark that, results of autocorrelation of such sequences have not been reported in the literature. We organise this work as follows. In Section 2 we prove the linear complexity of sequence defined in Equation (1) with $I_{a,b}$ in Equation (3) and compute its autocorrelation values in Section 3. Finally we draw a conclusion in Section 4. We conclude this section by introducing the notions of linear complexity and autocorrelation of sequences.

The linear complexity is an important cryptographic characteristic of sequences and provides information on predictability and thus unsuitability for cryptography. Let $\mathbb{F}$ be a field. For a T-periodic sequence s^∞ over $\mathbb{F}$, the *linear complexity* $L(s^\infty)$ of the sequence s^∞ is defined to be the length of the shortest linear feedback shift register that can generate the sequence, which is the smallest nonnegative integer L satisfying

$$s_t = c_1 s_{t-1} + c_2 s_{t-2} + \cdots + c_L s_{t-L} \text{ for all } t \ge L,$$

where constants $c_1, \cdots, c_L \in \mathbb{F}$. Let

$$s(X) = s_0 + s_1 X + \cdots + s_{T-1} X^{T-1} \in \mathbb{F}[X],$$

which is called the *generating polynomial* of s^∞. Then the linear complexity over $\mathbb{F}$ of s^∞ can be computed as

$$L(s^\infty) = T - \deg\left(\gcd(X^T - 1,\ s(X))\right), \quad (4)$$

which is the degree of the *characteristic polynomial*, $\frac{X^T-1}{\gcd(X^T-1,\ s(X))}$, of the sequence. Moreover, the *autocorrelation value* $C_s(w)$ of the sequence s^∞ at shift w is defined by

$$C_s(w) = \sum_{i=0}^{T-1} (-1)^{s_{i+w}+s_i},$$

where $1 \le w \le T-1$. See, *e.g.*, [3] for details.

2 Linear Complexity

In this section, we will determine the exact values of the linear complexity of the binary sequences defined in Equation (1) with $I_{a,b}$ in Equation (3). Our result is the following.

Theorem 1. *Let s^∞ be the N-periodic binary sequence defined as in Equation (1) with $I_{a,b}$ in Equation (3) for defining Ω. Then the linear complexity of s^∞ satisfies*

$$L(s^\infty) = p^{m+1}q^{n+1} - \frac{(p^{m+1}-1)(q^{n+1}-1)}{2} - A_{p,m}(q^{n+1}-1) - A_{q,n}(p^{m+1}-1) - 1$$

if $p \equiv \pm 1 \pmod 8$, $q \equiv \pm 1 \pmod 8$ or $p \equiv \pm 3 \pmod 8$, $q \equiv \pm 3 \pmod 8$, and otherwise

$$L(s^\infty) = p^{m+1}q^{n+1} - A_{p,m}(q^{n+1}-1) - A_{q,n}(p^{m+1}-1) - 1,$$

where

$$A_{q,n} = \begin{cases} 1, & \text{if } \frac{(n+1)(q-1)}{2} \equiv 0 \pmod 2, \\ 0, & \text{if } \frac{(n+1)(q-1)}{2} \equiv 1 \pmod 2, \end{cases}$$

$$A_{p,m} = \begin{cases} 1, & \text{if } 1 + \frac{(m+1)(p-1)}{2} \equiv 0 \pmod 2, \\ 0, & \text{if } 1 + \frac{(m+1)(p-1)}{2} \equiv 1 \pmod 2. \end{cases}$$

2.1 Properties of the Generalized Cyclotomic Classes

Lemma 1. *Let α be a primitive N-th root of unity in the field $\mathbb{F}_{2^\delta}$ for $\delta = \mathrm{ord}_N(2)$. Let $(t, pq) = 1$, $0 \le u \le m+1$, $0 \le v \le n+1$.*

1) *Suppose that $0 \le a \le m$ and $0 \le b \le n$. Then we have*

$$\sum_{l \in G_0^{(a,b)}} \alpha^{tp^u q^v l} = \begin{cases} 0, & \text{if } u < m-a \text{ or } v < n-b, \\ \sum_{l \in G_0^{(m,n)}} \alpha^{tl}, & \text{if } u = m-a,\ v = n-b, \\ \frac{q-1}{d}, & \text{if } u = m-a,\ v > n-b, \\ \frac{p-1}{d}, & \text{if } u > m-a,\ v = n-b, \\ 0, & \text{if } u > m-a,\ v > n-b. \end{cases}$$

2) *Suppose that $0 \le a \le m$ and $b = n+1$. Then we have*

$$\sum_{l \in G_0^{(a,n+1)}} \alpha^{tp^u q^v l} = \begin{cases} 1, & \text{if } u = m-a, \\ 0, & \text{if } u \ne m-a. \end{cases}$$

3) *Suppose that $a = m+1$ and $0 \le b \le n$. Then we have*

$$\sum_{l \in G_0^{(m+1,b)}} \alpha^{tp^u q^v l} = \begin{cases} 1, & \text{if } v = n-b, \\ 0, & \text{if } v \ne n-b. \end{cases}$$

Proof. See Lemma 2.4 in [6]. □

According to [10], Whiteman's generalized cyclotomic classes of order d are defined by

$$D_i = \left\{ g^s x^i : s = 0, 1, \cdots, \frac{(p-1)(q-1)}{d} - 1 \right\},$$

where $i = 0, 1, \cdots, d-1$. Clearly,

$$\mathbb{Z}_{pq}^* = \cup_{i=0}^{d-1} D_i, \qquad D_i \cap D_j = \emptyset \text{ for } i \neq j.$$

Lemma 2. $D_i D_j = D_{(i+j) \bmod d}$, *where* $i, j = 0, 1, \cdots, d-1$.

Proof. This is Lemma 1 of [13]. □

Lemma 3. $2 \in \bigcup_{j=0}^{\frac{d}{2}-1} D_{2j}$ *if and only if* $p \equiv \pm 1 \pmod 8$, $q \equiv \pm 1 \pmod 8$ *or* $p \equiv \pm 3 \pmod 8$, $q \equiv \pm 3 \pmod 8$; $2 \in \bigcup_{j=0}^{\frac{d}{2}-1} D_{2j+1}$ *if and only if* $p \equiv \pm 1 \pmod 8$, $q \equiv \pm 3 \pmod 8$ *or* $p \equiv \pm 3 \pmod 8$, $q \equiv \pm 1 \pmod 8$.

Proof. See Theorem 5 in [13]. □

2.2 Proof of Theorem 1

According to Equation (4), the linear complexity of s^∞ can be computed by

$$L(s^\infty) = N - \left| \left\{ t : s(\alpha^t) = 0,\ 0 \le t < N \right\} \right|,$$

where α is a primitive N-th root of unity in the field $\mathbb{F}_{2^\delta}$ for $\delta = \mathrm{ord}_N(2)$.

We note that $G_k^{(a,b)} = p^a q^b G_k = p^a q^b x^k G_0 = x^k G_0^{(a,b)}$ for $0 \le a \le m$, $0 \le b \le n$, and

$$\Omega = \bigcup_{a=0}^{m+1} \bigcup_{b=0}^{n+1} \bigcup_{i \in I_{a,b}} G_i^{(a,b)} = \bigcup_{b=0}^{n+1} G_0^{(m+1,b)} \bigcup_{a=0}^{m} \bigcup_{b=0}^{n} \bigcup_{i=0}^{\frac{d}{2}-1} G_{2i+1}^{(a,b)}.$$

Hence

$$\begin{aligned} s(\alpha^t) &= \sum_{j \in \Omega} \alpha^{tj} \\ &= \sum_{j \in \bigcup_{b=0}^{n} G_0^{(m+1,b)} \bigcup_{a=0}^{m} \bigcup_{b=0}^{n} \bigcup_{i=0}^{\frac{d}{2}-1} G_{2i+1}^{(a,b)}} \alpha^{tj} \\ &= \sum_{b=0}^{n} \sum_{l \in G_0^{(m+1,b)}} \alpha^{tl} + \sum_{a=0}^{m} \sum_{b=0}^{n} \sum_{i=0}^{\frac{d}{2}-1} \sum_{l \in G_0^{(a,b)}} \alpha^{x^{2i+1} tl}. \end{aligned}$$

Since

$$\mathbb{Z}_N = \bigcup_{a=0}^{m} \bigcup_{b=0}^{n} \bigcup_{k=0}^{d-1} p^a q^b G_k \bigcup_{a=0}^{m} p^a q^{n+1} \mathbb{Z}_N^* \bigcup_{b=0}^{n+1} p^{m+1} q^b \mathbb{Z}_N^*,$$

any $t \in \mathbb{Z}_N$ can be written as $t = p^u q^v x^k g^h$ for $0 \le u \le m+1$, $0 \le v \le n+1$, $0 \le k \le d-1$ and $0 \le h \le e-1$. Then by Lemma 1 we have

$$\begin{aligned} s(\alpha^t) &= \sum_{b=0}^{n} \sum_{l \in G_0^{(m+1,b)}} \alpha^{p^u q^v x^k g^h l} \\ &\quad + \sum_{a=0}^{m} \sum_{b=0}^{n} \sum_{i=0}^{\frac{d}{2}-1} \sum_{l \in G_0^{(a,b)}} \alpha^{x^{2i+1} p^u q^v x^k g^h l} \\ &= \sum_{b=0}^{n} \sum_{l \in G_0^{(m+1,b)}} \alpha^{p^u q^v l} \\ &\quad + \sum_{a=0}^{m} \sum_{b=0}^{n} \sum_{i=0}^{\frac{d}{2}-1} \sum_{l \in G_0^{(a,b)}} \alpha^{x^{2i+1+k} p^u q^v l} \\ &= \sum_{\substack{b=0 \\ b=n-v}}^{n} 1 + \sum_{\substack{a=0 \\ a=m-u}}^{m} \sum_{\substack{b=0 \\ b=n-v}}^{n} \sum_{i=0}^{\frac{d}{2}-1} \sum_{l \in G_0^{(m,n)}} \alpha^{x^{2i+1+k} l} \\ &\quad + \frac{q-1}{d} \sum_{\substack{a=0 \\ a=m-u}}^{m} \sum_{\substack{b=0 \\ b>n-v}}^{n} \sum_{i=0}^{\frac{d}{2}-1} 1 \\ &\quad + \frac{p-1}{d} \sum_{\substack{a=0 \\ a>m-u}}^{m} \sum_{\substack{b=0 \\ b=n-v}}^{n} \sum_{i=0}^{\frac{d}{2}-1} 1. \end{aligned} \tag{5}$$

Case I: For $0 \le u \le m$ and $0 \le v \le n$, from Equation (5) we have

$$\begin{aligned} s(\alpha^t) &= 1 + \sum_{i=0}^{\frac{d}{2}-1} \sum_{l \in G_0^{(m,n)}} \alpha^{x^{2i+1+k} l} + \frac{q-1}{2} \sum_{\substack{b=0 \\ b>n-v}}^{n} 1 \\ &\quad + \frac{p-1}{2} \sum_{\substack{a=0 \\ a>m-u}}^{m} 1 \\ &= 1 + \sum_{i=0}^{\frac{d}{2}-1} \sum_{r=0}^{\frac{(p-1)(q-1)}{d}-1} \alpha^{x^{2i+1+k} p^m q^n g^r} \\ &\quad + \frac{v(q-1)}{2} + \frac{u(p-1)}{2} \\ &= 1 + \sum_{i=0}^{\frac{d}{2}-1} \sum_{l \in D_{(2i+1+k) \bmod d}} \alpha^{p^m q^n l} \\ &\quad + \frac{v(q-1)}{2} + \frac{u(p-1)}{2}, \end{aligned}$$

which implies that

$$\begin{aligned} s(\alpha^t) = 0 \iff & \sum_{i=0}^{\frac{d}{2}-1} \sum_{l \in D_{(2i+1+k) \bmod d}} \alpha^{p^m q^n l} \\ & \equiv 1 + \frac{v(q-1)}{2} + \frac{u(p-1)}{2} \pmod 2. \end{aligned}$$

Hence we get

$$\left|\left\{t : s(\alpha^t) = 0,\ t \in \bigcup_{a=0}^{m}\bigcup_{b=0}^{n}\bigcup_{k=0}^{d-1} p^a q^b G_k\right\}\right| = \sum_{a=0}^{m}\sum_{b=0}^{n} A_{p,q,a,b}\frac{p^{m-a}q^{n-b}(p-1)(q-1)}{d},$$

where

$$A_{p,q,a,b} = \begin{cases} E, & \text{if } 1+\frac{b(q-1)}{2}+\frac{a(p-1)}{2} \equiv 0 \pmod 2, \\ F, & \text{if } 1+\frac{b(q-1)}{2}+\frac{a(p-1)}{2} \equiv 1 \pmod 2, \end{cases}$$

for

$$E = |\{k : \sum_{i=0}^{\frac{d}{2}-1}\sum_{l\in D_{(2i+1+k) \bmod d}} \alpha^{p^m q^n l} = 0, k = 0,\cdots,d-1\}|,$$

$$F = |\{k : \sum_{i=0}^{\frac{d}{2}-1}\sum_{l\in D_{(2i+1+k) \bmod d}} \alpha^{p^m q^n l} = 1, k = 0,\cdots,d-1\}|.$$

On the other hand, since $s(X) \in \mathbb{F}_2[X]$, it follows that $s(\alpha^t)^2 = s(\alpha^{2t})$. If $2 \in \cup_{j=0}^{\frac{d}{2}-1} D_{2j}$, then by Lemma 2 we have

$$\begin{aligned} s(\alpha^t)^2 &= s(\alpha^{2t}) \\ &= 1 + \sum_{i=0}^{\frac{d}{2}-1}\sum_{l\in D_{(2i+1+k) \bmod d}} \alpha^{2p^m q^n l} \\ &\quad + \frac{v(q-1)}{2} + \frac{u(p-1)}{2} \\ &= s(\alpha^t). \end{aligned}$$

In this case $s(\alpha^t) \in \{0,1\}$.

Note that $\alpha^{p^m q^n}$ is a primitive pq-th root of unity in an extension field of $\mathbb{F}_2$ and

$$\sum_{i=0}^{\frac{d}{2}-1}\sum_{l\in D_{2i}} \alpha^{p^m q^n l} + \sum_{i=0}^{\frac{d}{2}-1}\sum_{l\in D_{2i+1}} \alpha^{p^m q^n l} = 1.$$

If $2 \in \bigcup_{j=0}^{\frac{d}{2}-1} D_{2j+1}$, then by Lemma 2 we have

$$\begin{aligned} s(\alpha^t)^2 &= s(\alpha^{2t}) \\ &= 1 + \sum_{i=0}^{\frac{d}{2}-1}\sum_{l\in D_{(2i+1+k) \bmod d}} \alpha^{2p^m q^n l} \\ &\quad + \frac{v(q-1)}{2} + \frac{u(p-1)}{2} \\ &= s(\alpha^t) + 1. \end{aligned}$$

Thus $s(\alpha^t) \notin \{0,1\}$.

By Lemma 3, if $p \equiv \pm 1 \pmod 8$, $q \equiv \pm 1 \pmod 8$ or $p \equiv \pm 3 \pmod 8$, $q \equiv \pm 3 \pmod 8$, then $E = F = \frac{d}{2}$ and hence $A_{p,q,a,b} = \frac{d}{2}$ and

$$\begin{aligned} &\left|\left\{t : s(\alpha^t) = 0,\ t \in \bigcup_{a=0}^{m}\bigcup_{b=0}^{n}\bigcup_{k=0}^{d-1} p^a q^b DG_k\right\}\right| \\ &= \sum_{a=0}^{m}\sum_{b=0}^{n} \frac{p^a q^b (p-1)(q-1)}{2} \\ &= \frac{(p^{m+1}-1)(q^{n+1}-1)}{2}. \end{aligned}$$

If $p \equiv \pm 1 \pmod 8$, $q \equiv \pm 3 \pmod 8$ or $p \equiv \pm 3 \pmod 8$, $q \equiv \pm 1 \pmod 8$, then $E = F = 0$ and hence $A_{p,q,a,b} = 0$ and

$$\left|\left\{t : s(\alpha^t) = 0,\ t \in \bigcup_{a=0}^{m}\bigcup_{b=0}^{n}\bigcup_{k=0}^{d-1} p^a q^b G_k\right\}\right| = 0.$$

Case II: For $u = m+1$ and $0 \le v \le n$, from Equation (5) we have

$$s(\alpha^t) = 1 + \frac{(m+1)(p-1)}{2},$$

and

$$s(\alpha^t) = 0 \Longleftrightarrow 1 + \frac{(m+1)(p-1)}{2} \equiv 0 \pmod 2.$$

So we conclude that

$$\begin{aligned} &\left|\left\{t : s(\alpha^t) = 0,\ t \in \bigcup_{b=0}^{n} p^{m+1} q^b \mathbb{Z}_N^*\right\}\right| \\ &= A_{p,m}\sum_{b=0}^{n} q^{n-b}(q-1) = A_{p,m}(q^{n+1}-1). \end{aligned}$$

Case III: For $0 \le u \le m$ and $v = n+1$, from Equation (5) we have

$$s(\alpha^t) = \frac{(n+1)(q-1)}{2},$$

from which we obtain

$$s(\alpha^t) = 0 \Longleftrightarrow \frac{(n+1)(q-1)}{2} \equiv 0 \pmod 2.$$

Therefore

$$\begin{aligned} &\left|\left\{t : s(\alpha^t) = 0,\ t \in \bigcup_{a=0}^{m} p^a q^{n+1} \mathbb{Z}_N^*\right\}\right| \\ &= A_{q,n}\sum_{a=0}^{m} p^{m-a}(p-1) = A_{q,n}(p^{m+1}-1). \end{aligned}$$

Case IV: For $u = m+1$ and $v = n+1$, from Equation (5) we have

$$s(\alpha^t) = s(\alpha^0) = s(1) = 0.$$

Putting everything together, we complete the proof of Theorem 1. □

Remark 1. *It is not hard to show that*

$$A_{q,0} = \begin{cases} 1, & \text{if } q \equiv 1 \pmod 4, \\ 0, & \text{if } q \equiv 3 \pmod 4, \end{cases}$$
$$A_{p,0} = \begin{cases} 1, & \text{if } p \equiv 3 \pmod 4, \\ 0, & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

It is obvious that our results are entirely consistent with those in [13].

3 Autocorrelations

Let $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol modulo p, and $\left(\frac{\cdot}{q}\right)$ the Legendre symbol modulo q. In this section, we determine the exact values of autocorrelation of s^∞.

Theorem 2. *Let s^∞ be the N-periodic binary sequence defined as in Equation (1) with $I_{a,b}$ in Equation (3) for defining Ω. For $1 \le w \le p^{m+1}q^{n+1} - 1$ with $(w, p^{m+1}q^{n+1}) = p^{a_0}q^{b_0}$, the autocorrelation of s^∞ satisfies*

$$C_s(w) = \begin{cases} p^m q^n + \left(1 - (-1)^{\frac{p+q}{2}}\right) \cdot \left(\frac{w}{p}\right)\left(\frac{w}{q}\right) - 2, \\ \quad \text{if } a_0 = 0,\ b_0 = 0, \\ q^n(1 - p^{m+1}) + q^{n+1} - 4, \\ \quad \text{if } a_0 = m+1,\ b_0 = 0, \\ p^m(1 - q^{n+1}) + p^{m+1}, \\ \quad \text{if } a_0 = 0,\ b_0 = n+1, \\ p^m q^{n-b_0} + p^m q^{n-b_0+1}(1 - q^{b_0}) \\ \quad + \left(1 - (-1)^{\frac{p+q}{2}}\right) \cdot \left(\frac{\frac{w}{q^{b_0}}}{p}\right)\left(\frac{\frac{w}{q^{b_0}}}{q}\right) - 2, \\ \quad \text{if } a_0 = 0,\ 1 \le b_0 \le n, \\ p^{m-a_0} q^n + q^n p^{m-a_0+1}(1 - p^{a_0}) \\ \quad + \left(1 - (-1)^{\frac{p+q}{2}}\right) \cdot \left(\frac{\frac{w}{p^{a_0}}}{p}\right)\left(\frac{\frac{w}{p^{a_0}}}{q}\right) - 2, \\ \quad \text{if } 1 \le a_0 \le m,\ b_0 = 0, \\ q^{n-b_0}(1 - p^{m+1}) \\ \quad + q^{n-b_0+1}(1 - q^{b_0})(1 - p^{m+1}) + q^{n+1} - 4, \\ \quad \text{if } a_0 = m+1,\ 1 \le b_0 \le n, \\ p^{m-a_0}(1 - q^{n+1}) \\ \quad + p^{m-a_0+1}(1 - p^{a_0})(1 - q^{n+1}) + p^{m+1}, \\ \quad \text{if } 1 \le a_0 \le m,\ b_0 = n+1, \\ p^{m-a_0} q^{n-b_0} + p^{m-a_0} q^{n-b_0+1}(1 - q^{b_0}) \\ \quad + q^{n-b_0} p^{m-a_0+1}(1 - p^{a_0}) \\ \quad + p^{m-a_0+1} q^{n-b_0+1}(1 - p^{a_0})(1 - q^{b_0}) \\ \quad + \left(1 - (-1)^{\frac{p+q}{2}}\right) \cdot \left(\frac{\frac{w}{p^{a_0}q^{b_0}}}{p}\right)\left(\frac{\frac{w}{p^{a_0}q^{b_0}}}{q}\right) - 2, \\ \quad \text{if } 1 \le a_0 \le m,\ 1 \le b_0 \le n. \end{cases}$$

Remark 2. *Theorem 2 shows that the autocorrelation values of s^∞ are quite good.*

3.1 Certain Identities Involving Character Sums

To prove Theorem 2, we need the following identities.

Lemma 4. *Assume that $1 \le w \le p^{m+1}q^{n+1} - 1$. Then we have*

$$\sum_{\substack{k=0 \\ q^{n+1}|k \\ q^{n+1}|k+w}}^{p^{m+1}q^{n+1}-1} 1 - \sum_{\substack{k=1 \\ p^{m+1}|k \\ q^{n+1}|k+w}}^{p^{m+1}q^{n+1}-1} 1 - \sum_{\substack{k=0 \\ q^{n+1}|k \\ p^{m+1}|k+w \\ p^{m+1}q^{n+1}\nmid k+w}}^{p^{m+1}q^{n+1}-1} 1 + \sum_{\substack{k=1 \\ p^{m+1}|k \\ p^{m+1}|k+w \\ p^{m+1}q^{n+1}\nmid k+w}}^{p^{m+1}q^{n+1}-1} 1 = \begin{cases} q^{n+1} - 4, & \text{if } p^{m+1} \mid w, \\ p^{m+1}, & \text{if } q^{n+1} \mid w, \\ -2, & \text{if } p^{m+1} \nmid w \text{ and } q^{n+1} \nmid w. \end{cases}$$

Proof. It is not hard to show that

$$\sum_{\substack{k=0 \\ q^{n+1}|k \\ q^{n+1}|k+w}}^{p^{m+1}q^{n+1}-1} 1 = \begin{cases} p^{m+1}, & q^{n+1} \mid w, \\ 0, & q^{n+1} \nmid w, \end{cases}$$

$$\sum_{\substack{k=1 \\ p^{m+1}|k \\ q^{n+1}|k+w}}^{p^{m+1}q^{n+1}-1} 1 = \begin{cases} 0, & q^{n+1} \mid w, \\ 1, & q^{n+1} \nmid w, \end{cases}$$

$$\sum_{\substack{k=0 \\ q^{n+1}|k \\ p^{m+1}|k+w \\ p^{m+1}q^{n+1}\nmid k+w}}^{p^{m+1}q^{n+1}-1} 1 = \begin{cases} 0, & q^{n+1} \mid w, \\ 1, & q^{n+1} \nmid w, \end{cases}$$

$$\sum_{\substack{k=1 \\ p^{m+1}|k \\ p^{m+1}|k+w \\ p^{m+1}q^{n+1}\nmid k+w}}^{p^{m+1}q^{n+1}-1} 1 = \begin{cases} q^{n+1} - 2, & p^{m+1} \mid w, \\ 0, & p^{m+1} \nmid w. \end{cases}$$

Lemma 4 is thus established. □

Lemma 5. *Assume that $1 \le w \le p^{m+1}q^{n+1} - 1$ with $(w, p^{m+1}q^{n+1}) = p^{a_0}q^{b_0}$. Then we have*

$$\sum_{a=0}^{m}\sum_{b=0}^{n} \sum_{\substack{k=0 \\ (k,p^{m+1}q^{n+1})=p^a q^b \\ q^{n+1}|k+w}}^{p^{m+1}q^{n+1}-1} \left(\frac{\frac{k}{p^a q^b}}{p}\right)\left(\frac{\frac{k}{p^a q^b}}{q}\right)$$
$$-\sum_{a=0}^{m}\sum_{b=0}^{n} \sum_{\substack{k=0 \\ (k,p^{m+1}q^{n+1})=p^a q^b \\ p^{m+1}|k+w \\ p^{m+1}q^{n+1}\nmid k+w}}^{p^{m+1}q^{n+1}-1} \left(\frac{\frac{k}{p^a q^b}}{p}\right)\left(\frac{\frac{k}{p^a q^b}}{q}\right)$$

$$+\sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k=0\\ q^{n+1}|k\\ (k+w,p^{m+1}q^{n+1})=p^aq^b}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k+w}{p^aq^b}}{p}\right)\left(\frac{\frac{k+w}{p^aq^b}}{q}\right)$$
$$-\sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k=1\\ p^{m+1}|k\\ (k+w,p^{m+1}q^{n+1})=p^aq^b}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k+w}{p^aq^b}}{p}\right)\left(\frac{\frac{k+w}{p^aq^b}}{q}\right)$$
$$=\begin{cases}\left(1-(-1)^{\frac{p+q}{2}}\right)\cdot\left(\frac{\frac{w}{p^{a_0}q^{b_0}}}{p}\right)\left(\frac{\frac{w}{p^{a_0}q^{b_0}}}{q}\right), \\ \qquad \textit{if } \ a_0\leq m, \ b_0\leq n, \\ 0, \\ \qquad \textit{if } \ a_0=m+1 \ \ \textit{or} \ \ b_0=n+1.\end{cases}$$

Proof. By the properties of the Legendre symbols and complete residue systems we get

$$\sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k=0\\ (k,p^{m+1}q^{n+1})=p^aq^b\\ q^{n+1}|k+w}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^aq^b}}{p}\right)\left(\frac{\frac{k}{p^aq^b}}{q}\right)$$
$$=\sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k=0\\ (k,pq)=1\\ q^{n+1}|p^aq^bk+w}}^{p^{m+1-a}q^{n+1-b}-1}\left(\frac{k}{p}\right)\left(\frac{k}{q}\right)$$
$$=\sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k=0\\ q^{n+1}|p^aq^bk+w}}^{p^{m+1-a}q^{n+1-b}-1}\left(\frac{k}{p}\right)\left(\frac{k}{q}\right)$$
$$=\sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k_1=0\\ q^{n+1}|p^{m+1}q^bk_1+w}}^{q^{n+1-b}-1}\left(\frac{k_1p^{m+1-a}}{q}\right)$$
$$\times\sum_{k_2=0}^{p^{m+1-a}-1}\left(\frac{k_2q^{n+1-b}}{p}\right)$$
$$=0, \tag{6}$$

and

$$\sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k=0\\ (k,p^{m+1}q^{n+1})=p^aq^b\\ p^{m+1}|k+w\\ p^{m+1}q^{n+1}\nmid k+w}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^aq^b}}{p}\right)\left(\frac{\frac{k}{p^aq^b}}{q}\right)$$
$$=\sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k=0\\ (k,p^{m+1}q^{n+1})=p^aq^b\\ p^{m+1}|k+w}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^aq^b}}{p}\right)\left(\frac{\frac{k}{p^aq^b}}{q}\right)$$
$$-\sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k=0\\ (k,p^{m+1}q^{n+1})=p^aq^b\\ p^{m+1}|k+w\\ p^{m+1}q^{n+1}|k+w}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^aq^b}}{p}\right)\left(\frac{\frac{k}{p^aq^b}}{q}\right)$$
$$=\begin{cases}\displaystyle\sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k=0\\ p^{m+1}|p^aq^bk+w}}^{p^{m+1-a}q^{n+1-b}-1}\left(\frac{k}{p}\right)\left(\frac{k}{q}\right) \\ \quad -\left(\frac{\frac{-w}{p^{a_0}q^{b_0}}}{p}\right)\left(\frac{\frac{-w}{p^{a_0}q^{b_0}}}{q}\right), \\ \quad \text{if } \ a_0\leq m, \ b_0\leq n, \\ \displaystyle\sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k=0\\ p^{m+1}|p^aq^bk+w}}^{p^{m+1-a}q^{n+1-b}-1}\left(\frac{k}{p}\right)\left(\frac{k}{q}\right), \\ \quad \text{if } \ a_0=m+1 \ \text{ or } \ b_0=n+1,\end{cases}$$
$$=\begin{cases}-\left(\frac{\frac{-w}{p^{a_0}q^{b_0}}}{p}\right)\left(\frac{\frac{-w}{p^{a_0}q^{b_0}}}{q}\right), \\ \quad \text{if } \ a_0\leq m, \ b_0\leq n, \\ 0, \\ \quad \text{if } \ a_0=m+1 \ \text{ or } \ b_0=n+1.\end{cases} \tag{7}$$

Similarly, we have

$$\sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k=0\\ q^{n+1}|k\\ (k+w,p^{m+1}q^{n+1})=p^aq^b}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k+w}{p^aq^b}}{p}\right)\left(\frac{\frac{k+w}{p^aq^b}}{q}\right)=0, \tag{8}$$

and

$$\sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k=1\\ p^{m+1}|k\\ (k+w,p^{m+1}q^{n+1})=p^aq^b}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k+w}{p^aq^b}}{p}\right)\left(\frac{\frac{k+w}{p^aq^b}}{q}\right)$$
$$=\begin{cases}-\left(\frac{\frac{w}{p^{a_0}q^{b_0}}}{p}\right)\left(\frac{\frac{w}{p^{a_0}q^{b_0}}}{q}\right), \\ \quad \text{if } \ a_0\leq m, \ b_0\leq n, \\ 0, \\ \quad \text{if } \ a_0=m+1 \ \text{ or } \ b_0=n+1.\end{cases} \tag{9}$$

From Equation (6), Equation (7), Equation (8), and Equation (9), we can get the conclusion of Lemma 5 directly. □

Lemma 6. *Assume that* $1\leq w\leq p^{m+1}q^{n+1}-1$ *with* $(w,p^{m+1}q^{n+1})=p^{a_0}q^{b_0}$*. Then we have*

$$\sum_{a_1=0}^{m}\sum_{b_1=0}^{n}\sum_{a_2=0}^{m}\sum_{b_2=0}^{n}\sum_{\substack{k=0\\ (k,p^{m+1}q^{n+1})=p^{a_1}q^{b_1}\\ (k+w,p^{m+1}q^{n+1})=p^{a_2}q^{b_2}}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{p}\right)$$
$$\times\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{q}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{q}\right)$$

$$
= \begin{cases}
p^m q^n, \\
\qquad if \ \ a_0 = 0, \ b_0 = 0, \\
q^n(1 - p^{m+1}), \\
\qquad if \ \ a_0 = m+1, \ b_0 = 0, \\
p^m(1 - q^{n+1}), \\
\qquad if \ \ a_0 = 0, \ b_0 = n+1, \\
p^m q^{n-b_0} + p^m q^{n-b_0+1}(1 - q^{b_0}), \\
\qquad if \ \ a_0 = 0, \ 1 \le b_0 \le n, \\
p^{m-a_0} q^n + q^n p^{m-a_0+1}(1 - p^{a_0}), \\
\qquad if \ \ 1 \le a_0 \le m, \ b_0 = 0, \\
q^{n-b_0}(1 - p^{m+1}) + q^{n-b_0+1}(1 - q^{b_0})(1 - p^{m+1}), \\
\qquad if \ \ a_0 = m+1, \ 1 \le b_0 \le n, \\
p^{m-a_0}(1 - q^{n+1}) + p^{m-a_0+1}(1 - p^{a_0})(1 - q^{n+1}), \\
\qquad if \ \ 1 \le a_0 \le m, \ b_0 = n+1, \\
p^{m-a_0} q^{n-b_0} + p^{m-a_0} q^{n-b_0+1}(1 - q^{b_0}) \\
\quad + q^{n-b_0} p^{m-a_0+1}(1 - p^{a_0}) \\
\quad + p^{m-a_0+1} q^{n-b_0+1}(1 - p^{a_0})(1 - q^{b_0}), \\
\qquad if \ \ 1 \le a_0 \le m, \ 1 \le b_0 \le n.
\end{cases}
$$

Proof. By the properties of character sums, greatest common divisors and complete residue systems we have

$$
\sum_{\substack{a_1=0\\a_1>a_2}}^{m}\sum_{a_2=0}^{m}\sum_{\substack{b_1=0\\b_1>b_2}}^{n}\sum_{b_2=0}^{n}\sum_{\substack{k=0\\(k,p^{m+1}q^{n+1})=p^{a_1}q^{b_1}\\(k+w,p^{m+1}q^{n+1})=p^{a_2}q^{b_2}}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{p}\right)
\times\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{q}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{q}\right)
$$

$$
= \sum_{\substack{a_1=0\\a_1>a_2}}^{m}\sum_{a_2=0}^{m}\sum_{\substack{b_1=0\\b_1>b_2}}^{n}\sum_{b_2=0}^{n}\sum_{\substack{k=0\\(p^{a_1}q^{b_1}k+w,p^{m+1}q^{n+1})=p^{a_2}q^{b_2}}}^{p^{m+1-a_1}q^{n+1-b_1}-1}\left(\frac{k}{p}\right)
\times\left(\frac{k}{q}\right)\left(\frac{\frac{p^{a_1}q^{b_1}k+w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{p^{a_1}q^{b_1}k+w}{p^{a_2}q^{b_2}}}{q}\right)
$$

$$
= \sum_{\substack{a_1=0\\a_1>a_2\\p^{a_2}q^{b_2}\|w}}^{m}\sum_{a_2=0}^{m}\sum_{\substack{b_1=0\\b_1>b_2}}^{n}\sum_{b_2=0}^{n}\sum_{k=0}^{p^{m+1-a_1}q^{n+1-b_1}-1}\left(\frac{k}{p}\right)
\times\left(\frac{k}{q}\right)\left(\frac{\frac{w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{w}{p^{a_2}q^{b_2}}}{q}\right)
$$

$$
= \sum_{\substack{a_1=0\\a_1>a_2\\p^{a_2}q^{b_2}\|w}}^{m}\sum_{a_2=0}^{m}\sum_{\substack{b_1=0\\b_1>b_2}}^{n}\sum_{b_2=0}^{n}\sum_{k_1=0}^{q^{n+1-b_1}-1}\sum_{k_2=0}^{p^{m+1-a_1}}\left(\frac{k_2}{p}\right)
\times\left(\frac{k_1}{q}\right)\left(\frac{\frac{w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{w}{p^{a_2}q^{b_2}}}{q}\right) = 0.
$$

In the same way we obtain

$$
\sum_{\substack{a_1=0\\a_1>a_2}}^{m}\sum_{a_2=0}^{m}\sum_{\substack{b_1=0\\b_1<b_2}}^{n}\sum_{b_2=0}^{n}\sum_{\substack{k=0\\(k,p^{m+1}q^{n+1})=p^{a_1}q^{b_1}\\(k+w,p^{m+1}q^{n+1})=p^{a_2}q^{b_2}}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{p}\right)
\times\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{q}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{q}\right) = 0,
$$

$$
\sum_{\substack{a_1=0\\a_1>a_2}}^{m}\sum_{a_2=0}^{m}\sum_{\substack{b_1=0\\b_1=b_2}}^{n}\sum_{b_2=0}^{n}\sum_{\substack{k=0\\(k,p^{m+1}q^{n+1})=p^{a_1}q^{b_1}\\(k+w,p^{m+1}q^{n+1})=p^{a_2}q^{b_2}}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{p}\right)
\times\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{q}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{q}\right) = 0,
$$

$$
\sum_{\substack{a_1=0\\a_1<a_2}}^{m}\sum_{a_2=0}^{m}\sum_{\substack{b_1=0\\b_1<b_2}}^{n}\sum_{b_2=0}^{n}\sum_{\substack{k=0\\(k,p^{m+1}q^{n+1})=p^{a_1}q^{b_1}\\(k+w,p^{m+1}q^{n+1})=p^{a_2}q^{b_2}}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{p}\right)
\times\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{q}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{q}\right) = 0,
$$

$$
\sum_{\substack{a_1=0\\a_1<a_2}}^{m}\sum_{a_2=0}^{m}\sum_{\substack{b_1=0\\b_1>b_2}}^{n}\sum_{b_2=0}^{n}\sum_{\substack{k=0\\(k,p^{m+1}q^{n+1})=p^{a_1}q^{b_1}\\(k+w,p^{m+1}q^{n+1})=p^{a_2}q^{b_2}}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{p}\right)
\times\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{q}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{q}\right) = 0,
$$

$$
\sum_{\substack{a_1=0\\a_1<a_2}}^{m}\sum_{a_2=0}^{m}\sum_{\substack{b_1=0\\b_1=b_2}}^{n}\sum_{b_2=0}^{n}\sum_{\substack{k=0\\(k,p^{m+1}q^{n+1})=p^{a_1}q^{b_1}\\(k+w,p^{m+1}q^{n+1})=p^{a_2}q^{b_2}}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{p}\right)
\times\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{q}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{q}\right) = 0,
$$

$$
\sum_{\substack{a_1=0\\a_1=a_2}}^{m}\sum_{a_2=0}^{m}\sum_{\substack{b_1=0\\b_1<b_2}}^{n}\sum_{b_2=0}^{n}\sum_{\substack{k=0\\(k,p^{m+1}q^{n+1})=p^{a_1}q^{b_1}\\(k+w,p^{m+1}q^{n+1})=p^{a_2}q^{b_2}}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{p}\right)
\times\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{q}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{q}\right) = 0,
$$

$$
\sum_{\substack{a_1=0\\a_1=a_2}}^{m}\sum_{a_2=0}^{m}\sum_{\substack{b_1=0\\b_1>b_2}}^{n}\sum_{b_2=0}^{n}\sum_{\substack{k=0\\(k,p^{m+1}q^{n+1})=p^{a_1}q^{b_1}\\(k+w,p^{m+1}q^{n+1})=p^{a_2}q^{b_2}}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{p}\right)
\times\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{q}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{q}\right) = 0.
$$

Summarizing the results of the eight cases we obtain

$$
\sum_{a_1=0}^{m}\sum_{b_1=0}^{n}\sum_{a_2=0}^{m}\sum_{b_2=0}^{n}\sum_{\substack{k=0\\(k,p^{m+1}q^{n+1})=p^{a_1}q^{b_1}\\(k+w,p^{m+1}q^{n+1})=p^{a_2}q^{b_2}}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{p}\right)
$$

$$
\begin{aligned}
&\times \left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{q}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{q}\right)\\
&= \sum_{\substack{a_1=0\\a_1=a_2}}^{m}\sum_{a_2=0}^{m}\sum_{b_1=0}^{n}\sum_{\substack{b_2=0\\b_1=b_2}}^{n}\sum_{\substack{k=0\\(k,p^{m+1}q^{n+1})=p^{a_1}q^{b_1}\\(k+w,p^{m+1}q^{n+1})=p^{a_2}q^{b_2}}}^{p^{m+1}q^{n+1}-1}\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{p}\right)\\
&\times \left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{q}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{q}\right)\\
&= \sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k=0\\(p^aq^bk+w,p^{m+1}q^{n+1})=p^aq^b}}^{p^{m+1-a}q^{n+1-b}-1}\left(\frac{k}{p}\right)\left(\frac{k}{q}\right)\\
&\times \left(\frac{k+\frac{w}{p^aq^b}}{p}\right)\left(\frac{k+\frac{w}{p^aq^b}}{q}\right)\\
&= \sum_{a=0}^{m}\sum_{b=0}^{n}\sum_{\substack{k_1=0\\q^b\|k_1p^{m+1}q^b+w}}^{q^{n+1-b}-1}\sum_{\substack{k_2=0\\p^a\|k_2p^aq^{n+1}+w}}^{p^{m+1-a}-1}\left(\frac{k_2q^{n+1-b}}{p}\right)\\
&\times \left(\frac{k_1p^{m+1-a}}{q}\right)\left(\frac{k_2q^{n+1-b}+\frac{w}{p^aq^b}}{p}\right)\\
&\times \left(\frac{k_1p^{m+1-a}+\frac{w}{p^aq^b}}{q}\right)\\
&= \sum_{\substack{a=0\\p^a\|w,}}^{m}\sum_{\substack{b=0\\q^b\|w}}^{n}\sum_{\substack{k_1=0\\q\nmid k_1p^{m+1}+\frac{w}{q^b}}}^{q^{n+1-b}-1}\sum_{\substack{k_2=0\\p\nmid k_2q^{n+1}+\frac{w}{p^a}}}^{p^{m+1-a}-1}\left(\frac{k_2q^{n+1-b}}{p}\right)\\
&\times \left(\frac{k_1p^{m+1-a}}{q}\right)\left(\frac{k_2q^{n+1-b}+\frac{w}{p^aq^b}}{p}\right)\\
&\times \left(\frac{k_1p^{m+1-a}+\frac{w}{p^aq^b}}{q}\right)\\
&+ \sum_{\substack{a=0\\p^a\|w,}}^{m}\sum_{\substack{b=0\\q^{b+1}|w}}^{n}\sum_{\substack{k_1=0\\(k_1,q)=1}}^{q^{n+1-b}-1}\sum_{\substack{k_2=0\\p\nmid k_2q^{n+1}+\frac{w}{p^a}}}^{p^{m+1-a}-1}\left(\frac{k_2q^{n+1-b}}{p}\right)\\
&\times \left(\frac{k_1p^{m+1-a}}{q}\right)\left(\frac{k_2q^{n+1-b}+\frac{w}{p^aq^b}}{p}\right)\left(\frac{k_1p^{m+1-a}}{q}\right)\\
&+ \sum_{\substack{a=0\\p^{a+1}|w,}}^{m}\sum_{\substack{b=0\\q^b\|w}}^{n}\sum_{\substack{k_1=0\\q\nmid k_1p^{m+1}+\frac{w}{q^b}}}^{q^{n+1-b}-1}\sum_{\substack{k_2=0\\(k_2,p)=1}}^{p^{m+1-a}-1}\left(\frac{k_2q^{n+1-b}}{p}\right)\\
&\times \left(\frac{k_1p^{m+1-a}}{q}\right)\left(\frac{k_2q^{n+1-b}}{p}\right)\left(\frac{k_1p^{m+1-a}+\frac{w}{p^aq^b}}{q}\right)\\
&+ \sum_{\substack{a=0\\p^{a+1}|w,}}^{m}\sum_{\substack{b=0\\q^{b+1}|w}}^{n}\sum_{\substack{k_1=0\\(k_1,q)=1}}^{q^{n+1-b}-1}\sum_{\substack{k_2=0\\(k_2,p)=1}}^{p^{m+1-a}-1}\left(\frac{k_2q^{n+1-b}}{p}\right)\\
&\times \left(\frac{k_1p^{m+1-a}}{q}\right)\left(\frac{k_2q^{n+1-b}}{p}\right)\left(\frac{k_1p^{m+1-a}}{q}\right)
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{\substack{a=0\\p^a\|w,}}^{m}\sum_{\substack{b=0\\q^b\|w}}^{n}\sum_{k_1=0}^{q^{n+1-b}-1}\left(\frac{k_1}{q}\right)\left(\frac{k_1+\frac{w}{p^aq^b}}{q}\right)\\
&\quad\times \sum_{k_2=0}^{p^{m+1-a}-1}\left(\frac{k_2}{p}\right)\left(\frac{k_2+\frac{w}{p^aq^b}}{p}\right)\\
&\quad+ \sum_{\substack{a=0\\p^a\|w,}}^{m}\sum_{\substack{b=0\\q^{b+1}|w}}^{n} q^{n-b}(q-1)\\
&\quad\times \sum_{k_2=0}^{p^{m+1-a}-1}\left(\frac{k_2}{p}\right)\left(\frac{k_2+\frac{w}{p^aq^b}}{p}\right)\\
&\quad+ \sum_{\substack{a=0\\p^{a+1}|w,}}^{m}\sum_{\substack{b=0\\q^b\|w}}^{n} p^{m-a}(p-1)\\
&\quad\times \sum_{k_1=0}^{q^{n+1-b}-1}\left(\frac{k_1}{q}\right)\left(\frac{k_1+\frac{w}{p^aq^b}}{q}\right)\\
&\quad+ \sum_{\substack{a=0\\p^{a+1}|w,}}^{m}\sum_{\substack{b=0\\q^{b+1}|w}}^{n} p^{m-a}q^{n-b}(p-1)(q-1)\\
&= \sum_{\substack{a=0\\p^a\|w,}}^{m}\sum_{\substack{b=0\\q^b\|w}}^{n} (-q^{n-b})\cdot(-p^{m-a})\\
&\quad+ \sum_{\substack{a=0\\p^a\|w,}}^{m}\sum_{\substack{b=0\\q^{b+1}|w}}^{n} q^{n-b}(q-1)\cdot(-p^{m-a})\\
&\quad+ \sum_{\substack{a=0\\p^{a+1}|w,}}^{m}\sum_{\substack{b=0\\q^b\|w}}^{n} p^{m-a}(p-1)\cdot(-q^{n-b})\\
&\quad+ \sum_{\substack{a=0\\p^{a+1}|w,}}^{m}\sum_{\substack{b=0\\q^{b+1}|w}}^{n} p^{m-a}q^{n-b}(p-1)(q-1)\\
&= \begin{cases}
p^mq^n, & \text{if } a_0=0,\ b_0=0,\\
q^n(1-p^{m+1}), & \text{if } a_0=m+1,\ b_0=0,\\
p^m(1-q^{n+1}), & \text{if } a_0=0,\ b_0=n+1,\\
p^mq^{n-b_0}+p^mq^{n-b_0+1}(1-q^{b_0}), & \text{if } a_0=0,\ 1\le b_0\le n,\\
p^{m-a_0}q^n+q^np^{m-a_0+1}(1-p^{a_0}), & \text{if } 1\le a_0\le m,\ b_0=0,\\
q^{n-b_0}(1-p^{m+1})+q^{n-b_0+1}(1-q^{b_0})(1-p^{m+1}), & \text{if } a_0=m+1,\ 1\le b_0\le n,\\
p^{m-a_0}(1-q^{n+1})+p^{m-a_0+1}(1-p^{a_0})(1-q^{n+1}), & \text{if } 1\le a_0\le m,\ b_0=n+1,\\
p^{m-a_0}q^{n-b_0}+p^{m-a_0}q^{n-b_0+1}(1-q^{b_0}) \\
\quad +q^{n-b_0}p^{m-a_0+1}(1-p^{a_0}) \\
\quad +p^{m-a_0+1}q^{n-b_0+1}(1-p^{a_0})(1-q^{b_0}), & \text{if } 1\le a_0\le m,\ 1\le b_0\le n.
\end{cases}
\end{aligned}
$$

□

3.2 Proof of Theorem 2

For integer k, suppose that $\gcd(k,N)=p^aq^b$, $0\le a\le m$, $0\le b\le n$. Write $k=p^aq^bk'$, where $\gcd(k',N)=1$. Note that $\Omega=\bigcup_{a=0}^{m+1}\bigcup_{b=0}^{n+1}\bigcup_{i\in I_{a,b}}G_i^{(a,b)}$, we have

$$\begin{aligned}
k\in\Omega &\iff \text{there exists } i\in I_{a,b} \text{ such that } k\in p^aq^bG_i\\
&\iff \text{there exists } i\in I_{a,b} \text{ such that } k'\in G_i\\
&\iff \text{there exist } i\in I_{a,b},\ 0\le s\le e-1\\
&\qquad \text{such that } k'\equiv g^sx^i \pmod N\\
&\iff \frac{1}{\phi(N)}\sum_{i\in I_{a,b}}\sum_{s=0}^{e-1}\sum_{\chi \bmod N}\chi(k')\overline{\chi}(g^sx^i)=1\\
&\iff \frac{1}{d}\sum_{\substack{\chi \bmod N\\ \chi(g)=1}}\chi(k')\sum_{i\in I_{a,b}}\overline{\chi}(x^i)=1,
\end{aligned}$$

where $\sum_{\chi \bmod N}$ denotes the summation of all the multiplicative characters χ modulo N. Hence,

$$(-1)^{s_k}=-\frac{2}{d}\sum_{\substack{\chi \bmod N\\ \chi(g)=1\\ \chi\ne\chi_0}}\left(\sum_{i\in I_{a,b}}\overline{\chi}(x^i)\right)\chi(k'). \qquad (10)$$

Every character $\chi \bmod N$ can be factored in the form $\chi=\chi_1\chi_2$, where χ_1 is a character mod p^{m+1} and χ_2 is a character mod q^{n+1}. Therefore we have

$$\begin{aligned}
&\sum_{\substack{\chi \bmod N\\ \chi(g)=1\\ \chi\ne\chi_0}}\left(\sum_{i\in I_{a,b}}\overline{\chi}(x^i)\right)\chi(k')\\
&=\sum_{\substack{\chi_1 \bmod p^{m+1}\\ \chi_1(g)\chi_2(g)=1\\ \chi_1\chi_2\ne\chi_0}}\sum_{\chi_2 \bmod q^{n+1}}\left(\sum_{i\in I_{a,b}}\overline{\chi}_1(x^i)\overline{\chi}_2(x^i)\right)\\
&\quad\times\chi_1(k')\chi_2(k')\\
&=\sum_{\substack{\chi_1 \bmod p^{m+1}\\ \chi_1(g)\chi_2(g)=1\\ \chi_1\chi_2\ne\chi_0}}\sum_{\chi_2 \bmod q^{n+1}}\left(\sum_{i\in I_{a,b}}\overline{\chi}_1(g^i)\right)\chi_1(k')\chi_2(k').
\end{aligned}$$

Write

$$\chi_1(k')=\begin{cases} e\left(\frac{k_1\mathrm{ind}_{g,p^{m+1}}(k')}{p^m(p-1)}\right), & (k',p)=1,\\ 0, & (k',p)>1,\end{cases}$$

$$\chi_2(k')=\begin{cases} e\left(\frac{k_2\mathrm{ind}_{g,q^{n+1}}(k')}{q^n(q-1)}\right), & (k',q)=1,\\ 0, & (k',q)>1,\end{cases}$$

where $e(y)=\mathrm{e}^{2\pi iy}$, $\mathrm{ind}_{g,p^{m+1}}(k')$ is the unique integer with $k'\equiv g^{\mathrm{ind}_{g,p^{m+1}}(k')} \pmod{p^{m+1}}$, $0\le \mathrm{ind}_{g,p^{m+1}}(k')\le p^m(p-1)-1$, and $\mathrm{ind}_{g,q^{n+1}}(k')$ denotes the unique integer with $k'\equiv g^{\mathrm{ind}_{g,q^{n+1}}(k')} \pmod{q^{n+1}}$, $0\le \mathrm{ind}_{g,q^{n+1}}(k')\le q^n(q-1)-1$. Then we have

$$\begin{aligned}
&\sum_{\substack{\chi \bmod N\\ \chi(g)=1\\ \chi\ne\chi_0}}\left(\sum_{i\in I_{a,b}}\overline{\chi}(x^i)\right)\chi(k')\\
&=\sum_{\substack{k_1=0\\ e\left(\frac{k_1}{p^m(p-1)}\right)e\left(\frac{k_2}{q^n(q-1)}\right)=1\\ k_1^2+k_2^2>0}}^{p^m(p-1)-1}\sum_{k_2=0}^{q^n(q-1)-1}\left(\sum_{i\in I_{a,b}}e\left(-\frac{ik_1}{p^m(p-1)}\right)\right)\\
&\quad\times e\left(\frac{k_1\mathrm{ind}_{g,p^{m+1}}(k')}{p^m(p-1)}\right)e\left(\frac{k_2\mathrm{ind}_{g,q^{n+1}}(k')}{q^n(q-1)}\right).
\end{aligned}$$

It is not hard to show that

$$\begin{aligned}
&\mathrm{e}\left(\frac{k_1}{p^m(p-1)}\right)\mathrm{e}\left(\frac{k_2}{q^n(q-1)}\right)=1\\
&\iff \mathrm{e}\left(\frac{k_1q^n(q-1)+k_2p^m(p-1)}{p^mq^n(p-1)(q-1)}\right)=1\\
&\iff p^mq^n(p-1)(q-1)\mid k_1q^n(q-1)+k_2p^m(p-1)\\
&\iff \frac{p^mq^n(p-1)(q-1)}{d}\Big| k_1\frac{q^n(q-1)}{d}+k_2\frac{p^m(p-1)}{d}.
\end{aligned}$$

Then we deduce

$$\frac{p^m(p-1)}{d}\Big| k_1,\qquad \frac{q^n(q-1)}{d}\Big| k_2.$$

Hence,

$$\begin{aligned}
&\sum_{\substack{\chi \bmod N\\ \chi(g)=1\\ \chi\ne\chi_0}}\left(\sum_{i\in I_{a,b}}\overline{\chi}(x^i)\right)\chi(k')\\
&=\sum_{\substack{0\le t_1\le d-1\\ t_1+t_2\equiv 0 \pmod d\\ t_1^2+t_2^2>0}}\sum_{0\le t_2\le d-1}\sum_{i\in I_{a,b}}\left(e\left(-\frac{it_1}{d}\right)\right)\\
&\quad\times e\left(\frac{t_1\mathrm{ind}_{g,p^{m+1}}(k')}{d}\right)e\left(\frac{t_2\mathrm{ind}_{g,q^{n+1}}(k')}{d}\right)\\
&=\sum_{t=1}^{d-1}\left(\sum_{i\in I_{a,b}}e\left(-\frac{it}{d}\right)\right)e\left(\frac{t\mathrm{ind}_{g,p^{m+1}}(k')}{d}\right)\\
&\quad\times e\left(-\frac{t\mathrm{ind}_{g,q^{n+1}}(k')}{d}\right).
\end{aligned}\qquad (11)$$

By Equation (10) and Equation (11), together with the definition of $I_{a,b}$ we obtain

$$\begin{aligned}(-1)^{s_k} &= -\frac{2}{d}\sum_{t=1}^{d-1}\left(\sum_{i=0}^{\frac{d}{2}-1} e\left(-\frac{(2i+1)t}{d}\right)\right)\\ &\quad \times e\left(\frac{t\mathrm{ind}_{g,p^{m+1}}(k')}{d}\right) e\left(-\frac{t\mathrm{ind}_{g,q^{n+1}}(k')}{d}\right)\\ &= e\left(\frac{\mathrm{ind}_{g,p^{m+1}}(k')}{2}\right) e\left(-\frac{\mathrm{ind}_{g,q^{n+1}}(k')}{2}\right)\\ &= \left(\frac{k'}{p}\right)\left(\frac{k'}{q}\right).\end{aligned}$$

Then for $0 \le k \le p^{m+1}q^{n+1}-1$, we have

$$(-1)^{s_k} = \begin{cases} \left(\frac{k'}{p}\right)\left(\frac{k'}{q}\right), \text{ if } k = p^a q^b k', \\ \qquad 0 \le a \le m,\ 0 \le b \le n,\ (k', pq) = 1, \\ 1, \\ \qquad \text{if } q^{n+1} \mid k, \\ -1, \\ \qquad \text{if } p^{m+1} \mid k,\ k > 0. \end{cases}$$

For $1 \le w \le p^{m+1}q^{n+1}-1$ with $\left(w, p^{m+1}q^{n+1}\right) = p^{a_0}q^{b_0}$, we get

$$\begin{aligned} C_s(w) &= \sum_{k=0}^{p^{m+1}q^{n+1}-1} (-1)^{s_{k+w}+s_k} \\ &= \sum_{a_1=0}^{m}\sum_{b_1=0}^{n}\sum_{a_2=0}^{m}\sum_{b_2=0}^{n} \sum_{\substack{k=0 \\ (k,p^{m+1}q^{n+1})=p^{a_1}q^{b_1} \\ (k+w,p^{m+1}q^{n+1})=p^{a_2}q^{b_2}}}^{p^{m+1}q^{n+1}-1} \\ &\quad \left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{p}\right)\left(\frac{\frac{k}{p^{a_1}q^{b_1}}}{q}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{p}\right)\left(\frac{\frac{k+w}{p^{a_2}q^{b_2}}}{q}\right) \\ &\quad + \sum_{a=0}^{m}\sum_{b=0}^{n} \sum_{\substack{k=0 \\ (k,p^{m+1}q^{n+1})=p^aq^b \\ q^{n+1}\mid k+w}}^{p^{m+1}q^{n+1}-1} \left(\frac{\frac{k}{p^aq^b}}{p}\right)\left(\frac{\frac{k}{p^aq^b}}{q}\right) \\ &\quad - \sum_{a=0}^{m}\sum_{b=0}^{n} \sum_{\substack{k=0 \\ (k,p^{m+1}q^{n+1})=p^aq^b \\ p^{m+1}\mid k+w \\ p^{m+1}q^{n+1}\nmid k+w}}^{p^{m+1}q^{n+1}-1} \left(\frac{\frac{k}{p^aq^b}}{p}\right)\left(\frac{\frac{k}{p^aq^b}}{q}\right) \\ &\quad + \sum_{a=0}^{m}\sum_{b=0}^{n} \sum_{\substack{k=0 \\ q^{n+1}\mid k \\ (k+w,p^{m+1}q^{n+1})=p^aq^b}}^{p^{m+1}q^{n+1}-1} \left(\frac{\frac{k+w}{p^aq^b}}{p}\right)\left(\frac{\frac{k+w}{p^aq^b}}{q}\right) \\ &\quad - \sum_{a=0}^{m}\sum_{b=0}^{n} \sum_{\substack{k=1 \\ p^{m+1}\mid k \\ (k+w,p^{m+1}q^{n+1})=p^aq^b}}^{p^{m+1}q^{n+1}-1} \left(\frac{\frac{k+w}{p^aq^b}}{p}\right)\left(\frac{\frac{k+w}{p^aq^b}}{q}\right) \\ &\quad + \sum_{\substack{k=0 \\ q^{n+1}\mid k \\ q^{n+1}\mid k+w}}^{p^{m+1}q^{n+1}-1} 1 - \sum_{\substack{k=1 \\ p^{m+1}\mid k \\ q^{n+1}\mid k+w}}^{p^{m+1}q^{n+1}-1} 1 \\ &\quad - \sum_{\substack{k=0 \\ q^{n+1}\mid k \\ p^{m+1}\mid k+w \\ p^{m+1}q^{n+1}\nmid k+w}}^{p^{m+1}q^{n+1}-1} 1 + \sum_{\substack{k=1 \\ p^{m+1}\mid k \\ p^{m+1}\mid k+w \\ p^{m+1}q^{n+1}\nmid k+w}}^{p^{m+1}q^{n+1}-1} 1. \end{aligned}$$

The statements of Theorem 2 then follows from Lemma 4-Lemma 6.

4 Conclusions

In this paper we have proven the linear complexity and autocorrelation values of a family of generalized cyclotomic sequences of period N with any order d. The result of linear complexity improves certain statement of [6] and the result of autocorrelation is new.

In 2012 Hu, Yue and Wang [6] gave a method for computing the linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$ $(m, n \ge 0)$ with any order d. The method is applied to computing the exact linear complexity of Whiteman's generalized cyclotomic sequences of period pq with order 4 and period $p^{m+1}q^{n+1}$ $(m, n \ge 0)$ with order 4, respectively. In fact, it is difficult to compute the exact value of $A_{u,v}$ for $0 \le u \le m$ and $0 \le v \le n$ in the calculation formula [6]. In this paper we determine the exact linear complexity and the exact values of autocorrelation of Whiteman's generalized cyclotomic binary sequences of any order d and period $p^{m+1}q^{n+1}$ $(m, n \ge 0)$ due to the different definitions of the support set, which makes it easier to ensure the balance of these sequences.

The autocorrelation values of generalized cyclotomic sequences with respect to p^n for any $n > 0$ are calculated in [7] by using formulas for the generalized cyclotomic numbers of order 2. We can use the proof method of Theorem 2 to calculate the autocorrelation values of these sequences.

It seems more difficult to calculate the autocorrelation values of generalized cyclotomic sequences. By making a more detailed division on $p^iq^{n+1}\mathbb{Z}_N^*$ and $p^{m+1}q^j\mathbb{Z}_N^*$, Ke, Li and Zhang [8] determined the linear complexity of a new class of generalized cyclotomic binary sequences of period $p^{m+1}q^{n+1}$ $(m, n > 0)$. However, the exact values of autocorrelation of these sequences have not been calculated by now.

We will further study the autocorrelations of quaternary cyclotomic sequences over $\mathbb{F}_4$ of length $2p^m$.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

Z.X.C. was partially supported by the National Natural Science Foundation of China under grant No. 61772292, by the Projects of International Cooperation and Exchanges NSFC-RFBR No. 61911530130, by the Provincial Natural Science Foundation of Fujian under grant No. 2018J01425 and by the Program for Innovative Research Team in Science and Technology in Fujian Province University under grant No. 2018-49.

H.N.L was was partially supported by National Natural Science Foundation of China under Grant No. 11571277, and the Science and Technology Program of Shaanxi Province of China under Grant No. 2016GY-080 and 2016GY-077.

References

[1] N. Brandstätter and A. Winterhof, "Some notes on the two-prime generator of order 2," *IEEE Transactions on Information Theory*, vol. 51, no. 10, pp. 3654–3657, 2005.

[2] Z. X. Chen and V. Edemskiy, "Linear complexity of quaternary sequences over $\mathbb{Z}_4$ derived from generalized cyclotomic classes modulo $2p$," *International Journal of Network Security*, vol. 19, no. 4, pp. 613–622, 2017.

[3] T. W. Cusick, C. S. Ding, and A. Renvall, *Stream Ciphers and Number Theory*. Amsterdam: Elsevier, 2004.

[4] C. S. Ding, *Codes from Difference Sets*. Singapore: World Scientific, 2014.

[5] C. S. Ding and T. Helleseth, "New generalized cyclotomy and its applications," *Finite Fields and Their Applications*, vol. 4, no. 2, pp. 140–166, 1998.

[6] L. Q. Hu, Q. Yue, and M. H. Wang, "The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$," *IEEE Transactions on Information Theory*, vol. 58, no. 8, pp. 5534–5543, 2012.

[7] S.-Y. Jin, Y.-J. Kim, and H.-Y. Song, "Autocorrelation of new generalized cyclotomic sequences of period p^n," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 93, no. 11, pp. 2345–2348, 2010.

[8] P. H. Ke, R. F. Li, and S. Y. Zhang, "The linear complexity of a new class of generalized cyclotomic binary sequences of length $p^{m+1}q^{n+1}$ (in Chinese)," *Acta Electronica Sinica*, vol. 42, no. 5, pp. 1009–1013, 2014.

[9] L. F. Liu, X. Y. Yang, X. N. Du, and B. Wei, "On the linear complexity of new generalized cyclotomic binary sequences of order two and period pqr," *Tsinghua Science and Technology*, vol. 21, no. 3, pp. 295–301, 2016.

[10] A. L. Whiteman, "A family of difference sets," *Illinois Journal of Mathematics*, vol. 6, no. 1, pp. 107–121, 1962.

[11] C. H. Wu, X. N. Du, and Z. T. Jiang, "Linear complexity of a family of pseudorandom discrete logarithm threshold sequences," *International Journal of Network Security*, vol. 18, no. 3, pp. 487–492, 2016.

[12] Z. B. Xiao, X. Y. Zeng, C. L. Li, and T. Helleseth, "New generalized cyclotomic binary sequences of period p^2," *Designs, Codes and Cryptography*, vol. 86, no. 7, pp. 1483–1497, 2018.

[13] T. J. Yan, K. Fan, X. N. Du, and G. Z. Xiao, "Linear complexity of binary Whiteman generalized cyclotomic sequences (in Chinese)," *Journal of Xidian University*, vol. 33, no. 4, 2006.

Biography

Xiaolin Chen was born in 1992. She is a Ph.D. student of Northwest University. She received the M.S. degree in Mathematics from Northwest University in 2017. Her research interests include number theory and information security.

Zhixiong Chen was born in 1972. He received the M.S. degree in Mathematics from Fujian Normal University in 1999 and Ph.D. degree in Cryptography from Xidian University in 2006, respectively. Now he is a professor of Putian University. He worked as a visiting scholar supervised by Prof. Arne Winterhof in Austrian Academy of Sciences (Linz) in 2013 and by Prof. Andrew Klapper in University of Kentucky (Lexington) during 2014-2015, respectively. His research interests include stream cipher, elliptic curve cryptography and digital signatures.

Huaning Liu was born in 1979. He received the M.S. degree in Mathematics from Northwest University in 2004 and Ph.D. degree in Mathematics from Northwest University in 2007, respectively. He was the recipient of the Zhong Jiaqing Mathematics Award in 2005. He worked as a post-doctoral fellow at School of Mathematics, Shandong University during 2007-2011. He worked as a post-doctoral fellow at Department of Pure Mathematics and Mathematical Statistics, University of Cambridge during 2012-2013. Now he is a professor of Northwest University. His research interests include number theory and information security.