Hindawi
Complexity
Volume 2020, Article ID 5129450, 9 pages
https://doi.org/10.1155/2020/5129450

Research Article

A Kind of Quaternary Sequences of Period $2p^m q^n$ and Their Linear Complexity

Qiuyan Wang,[1,2] **Chenhuang Wu**,[2,3] **Minghui Yang**,[4] **and Yang Yan**[2,5]

[1]*School of Computer Science and Technology, Tiangong University, Tianjin 300387, China*
[2]*Provincial Key Laboratory of Applied Mathematics, Putian University, Putian, Fujian 351100, China*
[3]*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731, China*
[4]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100195, China*
[5]*School of Information Technology Engineering, Tianjin University of Technology and Education, Tianjin 300222, China*

Correspondence should be addressed to Yang Yan; yanyangucas@126.com

Received 8 August 2019; Accepted 9 December 2019; Published 17 March 2020

Academic Editor: Mohamed Boutayeb

Sequences with high linear complexity have wide applications in cryptography. In this paper, a new class of quaternary sequences over $\mathbb{F}_4$ with period $2p^m q^n$ is constructed using generalized cyclotomic classes. Results show that the linear complexity of these sequences attains the maximum.

1. Introduction

Stream ciphers divide the plain text into characters and encipher each character with a time-varying function. It is known that the stream cipher plays a dominant role in cryptographic practice and remains a crucial role in military and commercial secrecy systems. The security of stream ciphers now depends on the "randomness" of the key stream [1]. For the system to be secure, the key stream must have a series of properties: balance, long period, low correlation, and so on.

A necessary requirement for unpredictability is a large linear complexity of the key stream, which is defined to be the length of the shortest linear-feedback shift register able to produce the key stream. Let $\mathbb{F}_l$ denote a finite field with l elements, where l is a prime power. A sequence $S = \{s_i\}$ is periodic if there exists a positive integer T such that $s_{j+T} = s_j$ for all $j \geq 0$. Let $S = \{s_i\}$ be a periodic sequence over $\mathbb{F}_l$. The linear complexity of S, denoted by $LC(S)$, is the least integer L of a linear recurrence relation over $\mathbb{F}_l$ satisfied by S:

$$-c_0 s_{i+L} = c_1 s_{i+L-1} + \cdots + c_L s_i, \quad \text{for } i \geq 0, \tag{1}$$

where $c_0 \neq 0$ and $c_0, c_1, \ldots, c_{L-1}, c_L \in \mathbb{F}_l$. By B-M algorithm [2], if $LC(S) \geq (N/2)$ (N is the least period of S), then S is considered to be good from the viewpoint of linear complexity.

Periodic sequences have been intensively studied in the past few years since they are widely used in CDMA (code-division multiple access), global position systems, and stream ciphers. As special cases, cyclotomic and generalized cyclotomic sequences of different periods and orders have attracted many researchers to deeply explore due to their good pseudorandom cryptographic properties [3–5]. In particular, the linear complexity of Legendre sequences and cyclotomic sequences of order r was studied in [6, 7], respectively. Generalized cyclotomy, as a natural generalization of cyclotomy, was presented by Whiteman [8] and Ding and Helleseth [9]. It should be noted that Whiteman's generalized cyclotomy is not in accordance with the classic cyclotomy. Ding–Helleseth cyclotomy includes the classic cyclotomy as a special case. Whereafter, the linear complexity of generalized cyclotomic sequences has been determined [10–15].

Quaternary sequences are also important from the point of many practical applications; please refer to [16]. Owing to the nice algebraic structure, quaternary sequences also have received a lot of attention. For instance, a kind of almost quaternary cyclotomic sequences was defined in [17] and was proved to have an ideal autocorrelation property [17]. A new class of quaternary sequences of length pq, constructed by the inverse Gray mapping, was studied in [18]. A family of quaternary sequences of period $2p$ over $\mathbb{F}_4$ was presented and showed to possess high linear complexity [19].

Motivated by the idea in [20, 21], we constructed a new class of quaternary sequences over $\mathbb{F}_4$ with period $2p^m q^n$ by using the generalized cyclotomic classes in this paper. From the definition of S in (11), we can easily see that the newly proposed sequences have longer period contrast to those in [21]. The linear complexity of these sequences is computed, and the results show that the proposed sequences have high linear complexity.

This paper is organized as follows. In Section 2, the periodic sequence S with period $2p^m q^n$ is given. Section 3 determines the linear complexity of the constructed sequence. Finally, we give some remarks on this paper.

2. Preliminaries

For a positive integer $a \geq 2$, use $\mathbb{Z}_a$ to denote the ring $\mathbb{Z}_a = \{0, 1, 2, \ldots, a-1\}$ with integer addition modulo a and integer multiplication modulo a. Usually, we use $\mathbb{Z}_a^*$ to denote all invertible elements of $\mathbb{Z}_a$, i.e., all elements b in $\mathbb{Z}_a$ satisfying $\gcd(a, b) = 1$. Obviously, the group $\mathbb{Z}_a^*$ has cardinality $\phi(a)$, where $\phi(\cdot)$ denotes the Euler function.

For a subset $A \subset \mathbb{Z}_a$ and an element $b \in \mathbb{Z}_a$, define

$$b + A = A + b = \{a + b\colon a \in A\}, \quad bA = \{ab\colon a \in A\}, \tag{2}$$

where addition and multiplication refer to those in $\mathbb{Z}_a$.

Let p and q be two distinct odd primes. Let m and n denote two positive integers. Suppose that g_1 is a primitive element of $\mathbb{Z}_{p^2}^*$. Then, g_1 is a primitive root of $\mathbb{Z}_{p^m}^*$ for $m \geq 1$ [22]. Without loss of generality, assume g_1 is an odd integer. It is known that g_1 is also a primitive root of $\mathbb{Z}_{2p^m}^*$ [22]. Obviously, g_1 is a common primitive root of $\mathbb{Z}_{p^i}$ and $\mathbb{Z}_{2p^i}$ for all $1 \leq i \leq m$. By the same argument, there exists an integer g_2 such that g_2 is a common primitive root of $\mathbb{Z}_{q^j}$ and $\mathbb{Z}_{2q^j}$ for any $1 \leq j \leq n$.

Lemma 1 (see [23]). *Let $m_1, \ldots, m_t$ be positive integers. For a set of integers $a_1, \ldots, a_t$, the system of congruences*

$$x \equiv a_i \bmod m_i, \quad i = 1, \ldots, t, \tag{3}$$

has solutions if and only if

$$a_i \equiv a_j \bmod \gcd(m_i, m_j), \quad i \neq j,\ 1 \leq i,\ j \leq t. \tag{4}$$

If (4) is satisfied, the solution is unique modulo $l\,\mathrm{cm}(m_1, \ldots, m_t)$.

Let g be the unique solution of the following congruence equations:

$$\begin{cases} g \equiv g_1 \pmod{2p^m}, \\ g \equiv g_2 \pmod{2q^n}. \end{cases} \tag{5}$$

Lemma 1 guaranteed the existence and uniqueness of the common primitive root g of p^i, $2p^i$, p^j, and $2p^j$. Similarly, there exists a unique integer y satisfying the following system of congruences:

$$\begin{cases} y \equiv g \pmod{2p^m}, \\ y \equiv 1 \pmod{2q^n}. \end{cases} \tag{6}$$

Assume that $e_{i,j} = \gcd(p^{i-1}(p-1), q^{j-1}(q-1))$ and $d_{i,j} = ((p-1)p^{i-1}(q-1)q^{j-1}/e_{i,j})$. Then, $d_{i,j}$ is the least positive integer that satisfies $g^{d_{i,j}} \equiv 1 \bmod p^i q^j$ ([9], Lemma 2), i.e., $\mathrm{ord}_{p^i q^j}(g) = d_{i,j}$. In the sequel, let i and j be two integers with $1 \leq i \leq m$ and $1 \leq j \leq n$. The generalized cyclotomic classes with respect to $p^i q^j$, similar to Ding–Helleseth's generalized cyclotomic classes ([9]), are defined as follows:

$$D_0^{(p^i q^j)} = \left\{ g^{2t} y^k \bmod p^i q^j\colon t = 0, 1, \ldots, \left(\frac{d_{i,j}}{2}\right) - 1;\ k = 0, 1, \ldots, e_{i,j} - 1 \right\}, \tag{7}$$

$$D_1^{(p^i q^j)} = g D_0^{(p^i q^j)} \bmod p^i q^j. \tag{8}$$

By Lemma 7 in [8], we get $\mathbb{Z}_{p^i q^j}{}^* = D_0^{(p^i q^j)} \cup D_1^{(p^i q^j)}$. Let

$$D_0^{(2p^i q^j)} = \left\{ g^{2t} y^k \bmod 2p^i q^j\colon t = 0, 1, \ldots, \left(\frac{d_{i,j}}{2}\right) - 1;\ k = 0, 1, \ldots, e_{i,j} - 1 \right\},$$

$$D_1^{(2p^i q^j)} = g D_0^{(2p^i q^j)} \bmod 2p^i q^j. \tag{9}$$

Similarly, we have $\mathbb{Z}_{2p^i q^j}{}^* = D_0^{(2p^i q^j)} \cup D_1^{(2p^i q^j)}$. For abbreviation, denote $H_h^{(2p^i q^j)} = p^{m-i} q^{n-j} D_h^{(2p^i q^j)}$ and $H_h^{(p^i q^j)} = p^{m-i} q^{n-j} D_h^{(p^i q^j)}$ for $h = 0, 1$. With the above preparations, we get a partition of $\mathbb{Z}_{2p^m q^n}$ as follows:

$$\begin{aligned} \mathbb{Z}_{2p^m q^n} = {} & \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} \bigcup_{h=0}^{1} p^{m-i} q^{n-j} \left(D_h^{(2p^i q^j)} \cup 2D_h^{(p^i q^j)} \right) \\ & \cdot \bigcup_{j=1}^{n} \bigcup_{h=0}^{1} p^m q^{n-j} \left(D_h^{(2q^j)} \cup 2D_h^{(q^j)} \right) \\ & \cdot \bigcup_{i=1}^{m} \bigcup_{h=0}^{1} p^{m-i} q^n \left(D_h^{(2p^i)} \cup 2D_h^{(p^i)} \right) \\ & \cup \{0, p^m q^n\}. \end{aligned} \tag{10}$$

Let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ be the finite field with 4 elements, where α satisfies $\alpha^2 = \alpha + 1$. A class of quaternary sequence can be given by allocating each elements of $\mathbb{F}_4$ to each generalized cyclotomic class with respect to $2p^m q^n$. To ensure the constructed sequence has high linear complexity, we should technologically do with it.

Let $\{a,b,c,d\}$ be a set of four tuples over $\mathbb{F}_4$, and the elements in these tuples are pairwise distinct. A quaternary generalized cyclotomic sequence $S=\{s_i\}$ of period $2p^mq^n$ is defined as

$$t\ s_i=\begin{cases}0, & \text{if } i=0,\\ e, & \text{if } i=p^mq^n,\\ a, & \text{if } i\in\bigcup_{i=1}^{m}\bigcup_{j=1}^{n}H_0^{(2p^iq^j)}\bigcup_{i=1}^{m}H_0^{(2p^i)}\bigcup_{j=1}^{n}H_0^{(2q^j)},\\ b, & \text{if } i\in\bigcup_{i=1}^{m}\bigcup_{j=1}^{n}H_1^{(2p^iq^j)}\bigcup_{i=1}^{m}H_1^{(2p^i)}\bigcup_{j=1}^{n}H_1^{(2q^j)},\\ c, & \text{if } i\in\bigcup_{i=1}^{m}\bigcup_{j=1}^{n}2H_0^{(p^iq^j)}\bigcup_{i=1}^{m}2H_0^{(p^i)}\bigcup_{j=1}^{n}2H_0^{(q^j)},\\ d, & \text{if } i\in\bigcup_{i=1}^{m}\bigcup_{j=1}^{n}2H_1^{(p^iq^j)}\bigcup_{i=1}^{m}2H_1^{(p^i)}\bigcup_{j=1}^{n}2H_1^{(q^j)},\end{cases}\tag{11}$$

where $e\neq b+d$ and $e\in\mathbb{F}_4^*$ if $p\equiv\pm1\pmod 8$ and $e\notin\{b,b+c\}$ and $e\in\mathbb{F}_4^*$ if $p\equiv\pm3\pmod 8$. It is easily seen that the sequence $S=\{s_i\}$ is balanced.

3. Linear Complexity of the Constructed Sequences

In generating running keys, the linear feedback shift register (LFSR) is one of the most useful devices. Also, it is shown that every periodic sequence can be generated by using LFSR. For researchers, what they most concern is the shortest length of LFSR that could produce a given sequence S, which is referred to the linear complexity of S.

Let $S=\{s_i\}$ be a periodic sequence over the finite field $\mathbb{F}_l$ of period N. We first recall the definition of linear complexity of periodic sequences that is given in Section 1. The *linear complexity* of S over $\mathbb{F}_l$, denoted by $LC(S)$, is the smallest positive integer L satisfying the following linear recurrence relation:

$$-c_0s_{i+L}=c_1s_{i+L-1}+\cdots+c_Ls_i,\quad \text{for } i\geq 0,\tag{12}$$

where $c_0\neq 0$ and $c_0,c_1,\ \ldots,\ c_{L-1},c_L\in\mathbb{F}_l$. The polynomial

$$c(x)=c_Lx^L+c_{L-1}x^{L-1}+\cdots+c_1x+c_0\in\mathbb{F}_l[x],\tag{13}$$

associated with the linear recurrence relation (12) is called the characteristic polynomial of S. A characteristic polynomial with the smallest degree is called a *minimal polynomial* of S [2]. For the periodic sequence S, let $S(x)=s_0+s_1x+\cdots+s_{N-1}x^{N-1}\in\mathbb{F}_l[x]$, which is called the *generating polynomial* of S. The following lemma gives a method to compute the linear complexity of S by using the generating polynomial $S(x)$.

Lemma 2 (see [24]). *Let S be a sequence over $\mathbb{F}_l$ of period N. Then, the minimal polynomial $m(x)$ of S is*

$$m(x)=\frac{x^N-1}{\gcd(x^N-1,S(x))},\tag{14}$$

and the linear complexity $LC(S)$ of S is given by

$$N-\deg\left(\gcd\left(x^N-1,S(x)\right)\right),\tag{15}$$

where $S(x)$ is the generating polynomial of S.

Lemma 3 (Lemma 2, [10] and Lemma 1, [20]). *Let notations be defined as above. Then, for $1\leq i\leq m$ and $h=0,1$, we have*

$$\begin{aligned}D_h^{(p^i)}&=\left\{x+py\colon x\in D_h^{(p)},\quad y\in\mathbb{Z}_{p^{i-1}}\right\},\\ D_h^{(2p^i)}&=\left\{x+py+\delta_{x,y}\colon x\in D_h^{(p)},\quad y\in\mathbb{Z}_{p^{i-1}}\right\},\end{aligned}\tag{16}$$

where

$$\delta_{x,y}=\begin{cases}0, & \text{if } x+\text{py is odd},\\ p^i, & \text{otherwise}.\end{cases}\tag{17}$$

For the generalized cyclotomic classes $D_h^{(p^iq^j)}$ and $D_h^{(2p^iq^j)}$ corresponding to p^iq^j and $2p^iq^j$, we have the following lemma.

Lemma 4 (Lemma 1, [25]). *For $1\leq i\leq m$ and $1\leq j\leq n$, we have*

$$\begin{aligned}D_h^{(p^iq^j)}&=\left\{a+pqb\colon a\in D_h^{(pq)},\quad b\in\mathbb{Z}_{p^{i-1}q^{j-1}}\right\},\\ D_h^{(2p^iq^j)}&=\left\{a+pqb+\delta_{a,b}\colon a\in D_h^{(pq)},\quad b\in\mathbb{Z}_{p^{i-1}q^{j-1}}\right\},\end{aligned}\tag{18}$$

where

$$\delta_{a,b}=\begin{cases}0, & \text{if } a+\text{bpq is odd},\\ p^iq^j, & \text{otherwise}.\end{cases}\tag{19}$$

Lemma 5 (see [9]). *$2\in D_h^{(p)}$ if and only if $2\in D_h^{(p^i)}$ for $1\leq i\leq m$ and $h=0,1$.*

Lemma 6 (see [22]). *Let symbols be the same as before. Then, we have*

$$\begin{aligned}&2\in D_0^{(p)}\ \text{if and only if } p\equiv\pm1\pmod 8,\\ &2\in D_1^{(p)}\ \text{if and only if } p\equiv\pm3\pmod 8.\end{aligned}\tag{20}$$

Lemma 7. *Let symbols be the same as before. Then, we have*

$$\begin{aligned}&2\in D_0^{(pq)}\ \text{if and only if } q\equiv\pm1\pmod 8,\\ &2\in D_1^{(pq)}\ \text{if and only if } q\equiv\pm3\pmod 8.\end{aligned}\tag{21}$$

Proof. We only prove the first part of this lemma. □

Sufficiency. Since $\gcd(2,pq)=1$, then $2\in\mathbb{Z}_{pq}^*$. If $q\equiv\pm1\pmod 8$, by Lemma 6, $2\in D_0^{(q)}$. Since $D_0^{(q)}\subseteq D_0^{(pq)}$, we get $2\in D_0^{(pq)}$.

Necessity. If $2\in D_0^{(pq)}$, by the definitions of y in (6) and $D_0^{(pq)}$ in (7), we know $2\pmod q\in D_0^{(q)}$. It follows from Lemma 6 that $q\equiv\pm1\pmod 8$.

By the method analogous to that used above, we can get the second conclusion of this lemma.

Let $d = \operatorname{ord} p^m q^n$ (8). Assume that β is a primitive $p^m q^n$th root of unity in $\mathbb{F}_{4^d}$. It can be easily checked that

$$x^{p^m q^n} - 1 = (x-1)(x-\beta)\ldots\left(x-\beta^{p^m q^n - 1}\right). \tag{22}$$

By Lemma 2, in order to determine the linear complexity of S, we need to determine $\gcd(x^{2p^m q^n} - 1, S(x)) = \gcd((x^{p^m q^n} - 1)^2, S(x))$ over $\mathbb{F}_4[x]$. By (22), we should check whether β^i, $0 \le i \le p^m q^n - 1$, is a root of $S(x)$. If it is a root of $S(x)$, we need to verify whether it is a multiple root of $S(x)$.

Recall that $H_h^{(2p^i q^j)} = p^{m-i} q^{n-j} D_h^{(2p^i q^j)}$ and $H_h^{(p^i q^j)} = p^{m-i} q^{n-j} D_h^{(p^i q^j)}$ for $h = 0, 1$. Define

$$\begin{aligned} S_h^{(i,j)}(x) &= \sum_{t \in H_h^{(2p^i q^j)}} x^t, \\ S_h^{(i,0)}(x) &= \sum_{t \in H_h^{(2p^i)}} x^t, \\ S_h^{(0,j)}(x) &= \sum_{t \in H_h^{(2q^j)}} x^t, \end{aligned} \tag{23}$$

for $1 \le i \le m$, $1 \le j \le n$, and $0 \le h \le 1$. Let a and b be two integers with $0 \le a \le m-1$ and $0 \le b \le n-1$. For $1 \le k \le p^m q^n - 1$, suppose $k = p^a q^b l$ with $\gcd(l, pq) = 1$. It follows from Lemma 4 that

$$\begin{aligned} S_h^{(i,j)}\left(\beta^k\right) &= \sum_{t \in p^{m-i} q^{n-j} D_h^{(2p^i q^j)}} \beta^{kt} \\ &= \sum_{t \in p^{m+a-i} q^{n+b-j} l D_h^{(2p^i q^j)}} \beta^t \\ &= \sum_{t \in p^{m+a-i} q^{n+b-j} l D_h^{(p^i q^j)}} \beta^t \\ &= \sum_{t \in H_h^{(p^i q^j)}} \beta^{kt}. \end{aligned} \tag{24}$$

Similarly, we have

$$S_h^{(i,0)}\left(\beta^k\right) = \sum_{t \in H_h^{(p^i)}} \beta^{kt}, \tag{25}$$

$$S_h^{(0,j)}\left(\beta^k\right) = \sum_{t \in H_h^{(q^j)}} \beta^{kt}. \tag{26}$$

Combining (24)–(26), we have

$$\begin{aligned} S\left(\beta^k\right) &= \sum_{i=0}^{p^m q^n - 1} s_i x^i \\ &= e\beta^{p^m q^n} + a\left(\sum_{i=1}^m \sum_{j=1}^n S_0^{(i,j)}\left(\beta^k\right) + \sum_{i=1}^m S_0^{(i,0)}\left(\beta^k\right) + \sum_{j=1}^n S_0^{(0,j)}\left(\beta^k\right)\right) \\ &\quad + b\left(\sum_{i=1}^m \sum_{j=1}^n S_1^{(i,j)}\left(\beta^k\right) + \sum_{i=1}^m S_1^{(i,0)}\left(\beta^k\right) + \sum_{j=1}^n S_1^{(0,j)}\left(\beta^k\right)\right) \\ &\quad + c\left(\sum_{i=1}^m \sum_{j=1}^n S_0^{(i,j)}\left(\beta^k\right) + \sum_{i=1}^m S_0^{(i,0)}\left(\beta^k\right) + \sum_{j=1}^n S_0^{(0,j)}\left(\beta^k\right)\right)^2 \\ &\quad + d\left(\sum_{i=1}^m \sum_{j=1}^n S_1^{(i,j)}\left(\beta^k\right) + \sum_{i=1}^m S_1^{(i,0)}\left(\beta^k\right) + \sum_{j=1}^n S_1^{(0,j)}\left(\beta^k\right)\right)^2. \end{aligned} \tag{27}$$

Let

$$A\left(\beta^k\right) = \sum_{i=1}^m \sum_{j=1}^n S_0^{(i,j)}\left(\beta^k\right) + \sum_{i=1}^m S_0^{(i,0)}\left(\beta^k\right) + \sum_{j=1}^n S_0^{(0,j)}\left(\beta^k\right). \tag{28}$$

Then,

$$\begin{aligned} A\left(\beta^k\right) &= \sum_{i=1}^m \sum_{j=1}^n \sum_{t \in p^{m-i} q^{n-j} D_0^{(p^i q^j)}} \beta^{kt} + \sum_{i=1}^m \sum_{t \in q^n p^{m-i} D_0^{(p^i)}} \beta^{kt} \\ &\quad + \sum_{j=1}^n \sum_{t \in p^m q^{n-j} D_0^{(q^j)}} \beta^{kt} \\ &= \sum_{i=1}^m \sum_{j=1}^n \sum_{t \in p^{m+a-i} q^{n+b-j} l D_0^{(p^i q^j)}} \beta^t + \sum_{i=1}^m \sum_{t \in p^{m-i+a} q^{n+b} l D_0^{(p^i)}} \beta^t \\ &\quad + \sum_{j=1}^n \sum_{t \in p^{m+a} q^{n+b-j} l D_0^{(q^j)}} \beta^t. \end{aligned} \tag{29}$$

We first compute

$$S_0^{(i,j)}\left(\beta^k\right) = \sum_{t \in p^{m+a-i} q^{n+b-j} l D_0^{(p^i q^j)}} \beta^t, \tag{30}$$

where $k = p^a q^b l$ and $\gcd(pq, l) = 1$. The computation is divided into the following cases.

Case 1: $i \le a$ and $j \le b$. With simple derivation, we have

$$S_0^{(i,j)}\left(\beta^k\right) = \left|D_0^{(p^i q^j)}\right| = \frac{(p-1)(q-1)p^{i-1}q^{j-1}}{2}. \tag{31}$$

Case 2: $i = a + 1$ and $j = b + 1$. Then,

$$S_0^{(i,j)}\left(\beta^k\right) = \sum_{t\in D_0^{(pq)}} \zeta_{pq}^{lt}, \tag{32}$$

where $\zeta_{pq} = \beta^{p^{m-1}q^{n-1}}$ is a pqth primitive root of unity. Case 3: $i > a+1$ or $j > b+1$. Let $\eta = \beta^{p^{m+a-i}q^{n+b-j}}$, then $\eta^{pq} \neq 1$. It follows from Lemma 4 that

$$S_0^{(i,j)}\left(\beta^k\right) = \sum_{t\in D_0^{\left(p^iq^j\right)}} \eta^t = \sum_{t_1\in D_0^{(pq)}} \eta^{t_1} \sum_{t_2\in \mathbb{Z}_{p^{i-1}q^{j-1}}} \eta^{pqt_2} = 0. \tag{33}$$

Case 4: $i \le a$ and $j = b+1$. Let $\zeta_q = \beta^{p^{m+a-i}q^{n-1}}$, then ζ_q is a qth primitive root of unity. Hence, we obtain

$$\begin{aligned} S_0^{(i,j)}\left(\beta^k\right) &= \sum_{t\in p^{m+a-i}q^{n+b-j}lD_0^{\left(p^iq^j\right)}} \beta^t \\ &= \sum_{t\in p^{m+a-i}q^{n-1}lD_0^{\left(p^iq^{b+1}\right)}} \beta^t \\ &= \sum_{t\in lD_0^{\left(p^iq^{b+1}\right)}} \zeta_q^t \\ &= (p-1)p^{i-1}q^b \sum_{t\in lD_0^{(q)}} \zeta_q^t \\ &= 0. \end{aligned} \tag{34}$$

Case 5: $i = a+1$ and $j \le b$. By Lemma 4, we get

$$\begin{aligned} S_0^{(i,j)}\left(\beta^k\right) &= \sum_{t\in p^{m+a-i}q^{n+b-j}lD_0^{\left(p^iq^j\right)}} \beta^t \\ &= \sum_{t\in p^{m-1}q^{n+b-j}lD_0^{\left(p^iq^j\right)}} \beta^t \\ &= \sum_{t\in lD_0^{\left(p^{a+1}q^b\right)}} \zeta_p^t \\ &= \frac{(q-1)p^aq^{j-1}}{2} \sum_{t\in \mathbb{Z}_p^*} \zeta_p^t \\ &= \frac{(q-1)p^aq^{j-1}}{2}, \end{aligned} \tag{35}$$

where $\zeta_p = \beta^{p^{m-1}q^{n+b-j}}$.

From the above discussions, we have proved the first part of the following lemma.

Lemma 8. *For $k = p^aq^bl$ with $gcd(l, pq) = 1, 0 \le a \le m-1$, and $0 \le b \le n-1$, we have*

$$S_0^{(i,j)}\left(\beta^k\right) = \begin{cases} \dfrac{(p-1)(q-1)p^{i-1}q^{j-1}}{2}, & if\ \mathrm{i} \le a\ and\ \mathrm{j} \le \mathrm{b}, \\ \displaystyle\sum_{t\in D_0^{(pq)}} \zeta_{pq}^{lt}, & if\ \mathrm{i} = \mathrm{a}+1\ and\ \mathrm{j} = \mathrm{b}+1, \\ 0, & if\ \mathrm{i} > \mathrm{a}+1\ or\ \mathrm{j} > \mathrm{b}+1, \\ 0, & if\ \mathrm{i} \le a\ and\ \mathrm{j} = \mathrm{b}+1, \\ \dfrac{q-1}{2}, & if\ \mathrm{i} = \mathrm{a}+1\ and\ \mathrm{j} \le \mathrm{b}, \end{cases} \tag{36}$$

$$S_1^{(i,j)}\left(\beta^k\right) = \begin{cases} \dfrac{(p-1)(q-1)p^{i-1}q^{j-1}}{2}, & if\ i \le a\ and\ j \le b, \\ \displaystyle\sum_{t\in D_1^{(pq)}} \zeta_{pq}^{lt}, & if\ i = a+1\ and\ j = b+1, \\ 0, & if\ i > a+1\ or\ j > b+1, \\ 0, & if\ i \le a\ and\ j = b+1, \\ \dfrac{q-1}{2}, & if\ i = a+1\ and\ j \le b, \end{cases} \tag{37}$$

where $\zeta_{pq} = \beta^{p^{m-1}q^{n-1}}$ is a pqth primitive root of unity and β is a p^mq^nth primitive root of unity.

Proof. The proof of the second conclusion of this lemma is similar to the first part and we omit it. □

Lemma 9. *For $k = p^aq^bl$ with $gcd(pq, l) = 1$, we obtain*

$$S_0^{(i,0)}\left(\beta^k\right) = \begin{cases} \dfrac{p^{i-1}(p-1)}{2}, & if\ i \le a, \\ \displaystyle\sum_{t\in D_0^{(p)}} \zeta_p^{lt}, & if\ i = a+1, \\ 0, & if\ i > a+1, \end{cases} \tag{38}$$

$$S_1^{(i,0)}\left(\beta^k\right) = \begin{cases} \dfrac{(p-1)p^{i-1}}{2}, & if\ i \le a, \\ \displaystyle\sum_{t\in D_1^{(p)}} \zeta_p^{lt}, & if\ i = a+1, \\ 0, & if\ i > a+1, \end{cases} \tag{39}$$

$$S_0^{(0,j)}\left(\beta^k\right)=\begin{cases}\dfrac{(q-1)q^{j-1}}{2}, & if\ j\le b,\\ \sum\limits_{t\in D_0^{(q)}}\zeta_q^{lt}, & if\ j=b+1,\\ 0, & if\ j>b+1,\end{cases}\tag{40}$$

$$S_1^{(0,j)}\left(\beta^k\right)=\begin{cases}\dfrac{(q-1)q^{j-1}}{2}, & if\ j\le b,\\ \sum\limits_{t\in D_1^{(q)}}\zeta_q^{lt}, & if\ j=b+1,\\ 0, & if\ j>b+1,\end{cases}\tag{41}$$

where $\zeta_p=\beta^{p^{m-1}q^{n+b}}$ *and* $\zeta_q=\beta^{p^{m+a}q^{n-1}}$.

Proof. Because (38)–(41) can be proved in a similar way, here we only prove (38). By notations and (25), we get

$$S_0^{(i,0)}\left(\beta^k\right)=\sum_{t\in p^{m-i}q^nD_0^{(2p^i)}}\beta^{kt}=\sum_{t\in p^{m+a-i}q^{n+b}lD_0^{(p^i)}}\beta^t,\tag{42}$$

where $k=p^aq^bl$ with $\gcd(pq,l)=1$.

If $i\le a$, for each $t\in p^{m+a-i}q^{n+b}lD_0^{(p^i)}$, it can be easily seen that $\beta^t=1$. Thus,

$$S_0^{(i,0)}\left(\beta^k\right)=\left|D_0^{(p^i)}\right|=\frac{p^{i-1}(p-1)}{2}.\tag{43}$$

If $i=a+1$, then $\beta^{p^{m-1}q^{n+b}}$ is a pth primitive root of unity and

$$S_0^{(i,0)}\left(\beta^k\right)=\sum_{t\in D_0^{(p)}}\zeta_p^{lt},\tag{44}$$

where $\zeta_p=\beta^{p^{m-1}q^{n+b}}$.

If $i>a+1$, we have $(\beta^{p^{m+a-i}q^{n+b}})^p\neq 1$ and $(\beta^{p^{m+a-i}q^{n+b}})^{p^i}=1$. By Lemma 3, we know

$$D_0^{(p^i)}=\left\{x+py\colon x\in D_0^{(p)},y\in\mathbb{Z}_{p^{i-1}}\right\}.\tag{45}$$

Therefore,

$$S_0^{(i,0)}\left(\beta^k\right)=\sum_{t\in D_0^{(p^i)}}\eta^t=\sum_{t_1\in D_0^{(p)}}\eta^{t_1}\sum_{t_2\in\mathbb{Z}_{p^{i-1}}}\eta^{t_2p}=\sum_{t_1\in D_0^{(p)}}\eta^{t_1}\cdot 0=0,\tag{46}$$

where $\eta=\beta^{p^{m+a-i}q^{n+b}l}$ and $\eta^p\neq 1$.

In the following, we will determine the terms with a,b,c,d as coefficients in (27), respectively.

First, we compute the terms with a as coefficient.

It follows from Lemmas 8 and 9 that

$$\begin{aligned}&a\left(\sum_{i=1}^m\sum_{j=1}^nS_0^{(i,j)}\left(\beta^k\right)+\sum_{i=1}^mS_0^{(i,0)}\left(\beta^k\right)+\sum_{j=1}^nS_0^{(0,j)}\left(\beta^k\right)\right)\\&a\left(\begin{array}{c}\sum\limits_{i=1}^m\sum\limits_{j=1}^bS_0^{(i,j)}\left(\beta^k\right)+\sum\limits_{i=1}^m\sum\limits_{j=b+1}S_0^{(i,b+1)}\left(\beta^k\right)+\sum\limits_{i=1}^m\sum\limits_{j>b+1}S_0^{(i,j)}\left(\beta^k\right)\\+\sum\limits_{i=1}^aS_0^{(i,0)}\left(\beta^k\right)+\sum\limits_{i=a+1}S_0^{(a+1,0)}\left(\beta^k\right)+0+\dfrac{q^{j-1}(q-1)}{2}+\sum\limits_{t\in D_0^{(q)}}\zeta_q^{lt}\end{array}\right)\\&a\left(\frac{q-1}{2}+\frac{(q-1)q^{j-1}}{2}+\frac{p^{i-1}(p-1)}{2}+\sum_{t\in D_0^{(pq)}}\zeta_{pq}^{lt}+\sum_{t\in D_0^{(p)}}\zeta_p^{lt}+\sum_{t\in D_0^{(q)}}\zeta_q^{lt}\right)\\&a\left(\frac{p-1}{2}+\sum_{t\in D_0^{(pq)}}\zeta_{pq}^{lt}+\sum_{t\in D_0^{(p)}}\zeta_p^{lt}+\sum_{t\in D_0^{(q)}}\zeta_q^{lt}\right).\end{aligned}\tag{47}$$

Similarly, we compute the terms with b as coefficients:

$$\begin{aligned}&b\left(\sum_{i=1}^m\sum_{j=1}^bS_1^{(i,j)}\left(\beta^k\right)+\sum_{i=1}^m\sum_{j=b+1}S_1^{(i,b+1)}\left(\beta^k\right)+0+\frac{p^{i-1}(p-1)}{2}\right.\\&\left.+\sum_{t\in D_1^{(p)}}\zeta_p^{lt}+0+\frac{q^{j-1}(q-1)}{2}+\sum_{t\in D_1^{(q)}}\zeta_q^{lt}+0\right)\\&=b\left(\frac{p-1}{2}+\sum_{t\in D_1^{(pq)}}\zeta_{pq}^{lt}+\sum_{t\in D_1^{(p)}}\zeta_p^{lt}+\sum_{t\in D_1^{(q)}}\zeta_q^{lt}\right).\end{aligned}\tag{48}$$

The terms with c as coefficient are

$$c\left(\left(\frac{p-1}{2}\right)^2+\sum_{t\in D_0^{(pq)}}\zeta_{pq}^{2lt}+\sum_{t\in D_0^{(p)}}\zeta_p^{2lt}+\sum_{t\in D_0^{(q)}}\zeta_q^{2lt}\right).\tag{49}$$

The terms with d as coefficient are

$$d\left(\left(\frac{p-1}{2}\right)^2+\sum_{t\in D_1^{(pq)}}\zeta_{pq}^{2lt}+\sum_{t\in D_1^{(p)}}\zeta_p^{2lt}+\sum_{t\in D_1^{(q)}}\zeta_q^{2lt}\right).\tag{50}$$

It can be easily checked that

$$S(1) = e + (a+b+c+d)\frac{(p-1)(q-1)p^{i-1}q^{j-1} + (p-1)p^{i-1} + (q-1)q^{j-1}}{2}. \\ = e \neq 0. \tag{51}$$

Next, we determine $S(\beta^k)$ according to the values of p and q, where $k = p^a q^b l$ with $\gcd(pq, l) = 1$.

(1) If $p \equiv \pm 1 \pmod 8$ and $q \equiv \pm 1 \pmod 8$, by Lemmas 6 and 7 we know $2 \in D_0^{(pq)}$, $2 \in D_0^{(p)}$, and $2 \in D_0^{(q)}$. Hence,

$$\begin{aligned} S(\beta^k) &= e + \frac{p-1}{2}(a+b+c+d) + (a+c)\sum_{t\in D_0^{(pq)}} \zeta_{pq}^{lt} \\ &\quad + (b+d)\sum_{t\in D_1^{(pq)}} \zeta_{pq}^{lt} \\ &\quad + (a+c)\sum_{t\in D_0^{(p)}} \zeta_p^{lt} + (b+d)\sum_{t\in D_1^{(p)}} \zeta_p^{lt} + (a+c) \\ &\quad \cdot \sum_{t\in D_0^{(q)}} \zeta_q^{lt} + (b+d)\sum_{t\in D_1^{(q)}} \zeta_q^{lt} \\ &= e + b + d. \end{aligned} \tag{52}$$

(2) If $p \equiv \pm 3 \pmod 8$ and $q \equiv \pm 1 \pmod 8$, then $2 \in D_0^{(pq)}$, $2 \in D_0^{(q)}$, and $2 \in D_1^{(p)}$. Hence,

$$\begin{aligned} S(\beta^k) &= e + (a+c)\sum_{t\in D_0^{(pq)}} \zeta_{pq}^{lt} + (b+d)\sum_{t\in D_1^{(pq)}} \zeta_{pq}^{lt} \\ &\quad + (a+c)\sum_{t\in D_0^{(q)}} \zeta_q^{lt} \\ &\quad + (b+d)\sum_{t\in D_1^{(q)}} \zeta_q^{lt} + (a+c+d)\sum_{t\in D_1^{(p)}} \zeta_p^{lt} \\ &\quad + b\left(1 + \sum_{t\in D_1^{(p)}} \zeta_p^{lt}\right) \\ &= e + b. \end{aligned} \tag{53}$$

(3) If $p \equiv \pm 1 \pmod 8$ and $q \equiv \pm 3 \pmod 8$, then $2 \in D_1^{(pq)}$, $2 \in D_1^{(q)}$, and $2 \in D_0^{(p)}$. Hence,

$$\begin{aligned} S(\beta^k) &= e + (a+d)\sum_{t\in D_0^{(pq)}} \zeta_{pq}^{lt} + (b+c)\sum_{t\in D_1^{(pq)}} \zeta_{pq}^{lt} \\ &\quad + (a+c)\sum_{t\in D_0^{(p)}} \zeta_p^{lt} \\ &\quad + (b+d)\sum_{t\in D_1^{(p)}} \zeta_p^{lt} + (a+d)\sum_{t\in D_0^{(q)}} \zeta_q^{lt} \\ &\quad + (b+c)\sum_{t\in D_1^{(q)}} \zeta_q^{lt} \\ &= e + b + d. \end{aligned} \tag{54}$$

(4) If $p \equiv \pm 3 \pmod 8$ and $q \equiv \pm 3 \pmod 8$, then $2 \in D_1^{(pq)}$, $2 \in D_1^{(q)}$, and $2 \in D_1^{(p)}$. Hence,

$$\begin{aligned} S(\beta^k) &= e + (a+d)\sum_{t\in D_0^{(pq)}} \zeta_{pq}^{lt} + (b+c)\sum_{t\in D_1^{(pq)}} \zeta_{pq}^{lt} \\ &\quad + (a+d)\sum_{t\in D_0^{(p)}} \zeta_p^{lt} \\ &\quad + (b+c)\sum_{t\in D_1^{(p)}} \zeta_p^{lt} + (a+d)\sum_{t\in D_0^{(q)}} \zeta_q^{lt} \\ &\quad + (b+c)\sum_{t\in D_1^{(q)}} \zeta_q^{lt} + (a+d) \\ &= e + b + c. \end{aligned} \tag{55}$$

From the choice of e, we know $e \neq b + d$ if $p \equiv \pm 1 \pmod 8$ and $e \notin \{b, b+c\}$ if $p \equiv \pm 3 \pmod 8$. By Lemma 2 and the above discussions, we obtain $LC(S) = 2p^m q^n$. □

Theorem 1. *Let $S = \{s_i\}$ be the quaternary sequence defined by (11). Then, the linear complexity of S is $2p^m q^n$.*

Example 1. Let $(p, q, m, n) = (3, 5, 1, 1)$ and $(a, b, c, d, e) = (\alpha, 1+\alpha, 1, 0, 1)$. Then,

$$\begin{aligned} D_0^{(2pq)} \cup qD_0^{(2p)} \cup D_0^{(2q)} &= \{1, 3, 5, 11, 19, 27, 29\}, \\ D_1^{(2pq)} \cup qD_1^{(2p)} \cup pD_1^{(2q)} &= \{7, 9, 13, 17, 21, 23, 25\}, \\ 2D_0^{(pq)} \cup 2qD_0^{(p)} \cup 2pD_0^{(q)} &= \{2, 6, 8, 10, 22, 24, 28\}, \\ 2D_1^{(2pq)} \cup 2qD_0^{(p)} \cup 2pD_0^{(q)} &= \{4, 12, 14, 16, 18, 20, 26\}. \end{aligned} \tag{56}$$

It can be checked by Magma that $\gcd(x^{15}-1, S(x)) = 1$ and $LC(S) = 30$.

Example 2. Let $(p,q,m,n) = (3,7,1,1)$ and $(a,b,c,d,e) = (\alpha, 1+\alpha, 1, 0, 1)$. Then,

$$\begin{aligned} D_0^{(2pq)} \cup qD_0^{(2p)} \cup D_0^{(2q)} &= \{1,3,7,11,23,25,27,29,33,37\}. \\ D_1^{(2pq)} \cup qD_1^{(2p)} \cup pD_1^{(2q)} &= \{5,9,13,15,17,19,31,35,39,41\}. \\ 2D_0^{(pq)} \cup 2qD_0^{(p)} \cup 2pD_0^{(q)} &= \{2,4,6,8,12,14,16,22,24,32\}. \\ 2D_1^{(2pq)} \cup 2qD_0^{(p)} \cup 2pD_0^{(q)} &= \{10,18,20,26,28,30,34,36,38,40\}. \end{aligned} \tag{57}$$

It can be checked by Magma that $\gcd(x^{21}-1, S(x)) = 1$ and $LC(S) = 42$.

Remark 1. For $1 \le k \le p^m q^n - 1$, let $k = p^a q^b l$ with $\gcd(l, ab) = 1$. In the case that $e = b + d \in \mathbb{F}_4^*$ if $p \equiv \pm 1 \pmod 8$ and the case that $e \in \{b, b+c\}$ if $p \equiv \pm 3 \pmod 8$, we know $S(\beta^k) = 0$ for $1 \le k \le p^m q^n - 1$. Hence, we need to check if β^k is a multiple root of $S(x)$. This means we should check if β^k is a root of the derivation polynomial $S'(x)$ of the generating polynomial $S(x)$ of S. By definitions, we have

$$\begin{aligned} \beta^k S'(\beta^k) = e + b + (a+b) \sum_{t \in D_0^{(pq)}} \zeta_{pq}^{lt} + (a+b) \sum_{t \in D_0^{(p)}} \zeta_p^{lt} \\ + (a+b) \sum_{t \in D_0^{(q)}} \zeta_q^{lt}, \end{aligned} \tag{58}$$

and

$$\begin{aligned} \beta^k S'(\beta^k) = e + (a+b) \sum_{t \in D_0^{(pq)}} \zeta_{pq}^{lt} + (a+b) \sum_{t \in D_0^{(p)}} \zeta_p^{lt} \\ + (a+b) \sum_{t \in D_0^{(q)}} \zeta_q^{lt}, \end{aligned} \tag{59}$$

respectively.

For the fixed a and b with $0 \le a \le m-1$ and $0 \le b \le n-1$, by the following equations,

$$\begin{aligned} \sum_{t \in D_0^{(pq)}} \zeta_{pq}^t + \sum_{t \in D_1^{(pq)}} \zeta_{pq}^t = 1, \\ \sum_{t \in D_0^{(p)}} \zeta_p^t + \sum_{t \in D_1^{(p)}} \zeta_p^t = 1, \\ \sum_{t \in D_0^{(q)}} \zeta_q^t + \sum_{t \in D_1^{(q)}} \zeta_q^t = 1, \end{aligned} \tag{60}$$

we know there are at least $1/2\phi(2p^{m-a}q^{n-b}) = ((p-1)(q-1)/2)p^{m-a-1}q^{n-b-1}$ many $k's$ satisfying $S'(\beta^k) \neq 0$. Hence, $S(\beta^k)$ will have at most

$$\begin{aligned} p^m q^n - 1 + \sum_{a=0}^{m} \sum_{b=0}^{n} \frac{(p-1)(q-1)p^{m-a-1}q^{n-b-1}}{2} \\ = \frac{3p^m q^n - p^m - q^n - 1}{2}, \end{aligned} \tag{61}$$

roots for $0 \le k \le p^m q^n - 1$. By Lemma 2, we obtain

$$\begin{aligned} LC(S) &\ge 2p^m q^n - \frac{3p^m q^n - p^m - q^n - 1}{2} \\ &= \frac{(p^m+1)(q^n+1)}{2}. \end{aligned} \tag{62}$$

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work was supported by the National Science Foundation of China (nos. 61602342 and 11701553), Natural Science Foundation of Tianjin (grant no. 18JCQNJC70300), Science and Technology Development Fund of Tianjin Education Commission for Higher Education (no. 2018KJ215, 2017KJ237), Key Laboratory of Applied Mathematics of Fujian Province University (Putian University) (nos. SX201804 and SX201904), China Scholarship Council (no. 201809345010), and Foundation of Science and Technology on Information Assurance Laboratory (no. 6142112010216211 2007).

References

[1] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, Berlin, Germany, 1986.

[2] C. Ding, G. Xiao, and W. Shan, "The stability theory of stream ciphers," *Lecture Notes in Computer Science*, Vol. 561, Springer-Verlag, Berlin, Germany, 1991.

[3] H. Aly and A. Winterhof, "On the k-error linear complexity over $\mathbb{F}_p$ of Legendre and Sidelnikov sequences," *Designs, Codes and Cryptography*, vol. 40, no. 3, pp. 369–374, 2006.

[4] Y. Cai and C. Ding, "Binary sequences with optimal autocorrelation," *Theoretical Computer Science*, vol. 410, no. 24-25, pp. 2316–2322, 2009.

[5] L. Hu, Q. Yue, and M. 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.

[6] C. Ding and T. Helleseth, "On cyclotomic generator of order r," *Information Processing Letters*, vol. 66, no. 1, pp. 21–25, 1998.

[7] C. Ding, T. Helleseth, and W. Shan, "On the linear complexity of Legendre sequences," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1276–1278, 1998.

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

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

[10] V. Edemskiy, "About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1}," *Designs, Codes and Cryptography*, vol. 61, no. 3, pp. 251–260, 2011.

[11] Y. J. Kim and H. Y. Song, "Linear complexity of prime n-square sequences," in *Proceedings of the 2008 IEEE International Symposium on Information Theory*, pp. 2405–2408, Toronto, ON, Canada, July 2008.

[12] T. Yan, X. Du, G. Xiao, and X. Huang, "Linear complexity of binary Whiteman generalized cyclotomic sequences of order 2^k," *Information Sciences*, vol. 179, no. 7, pp. 1019–1023, 2009.
[13] Q. Wang, Y. Jiang, and D. Lin, "Linear complexity of Ding-Helleseth sequences of order 2 over GF(l)," *Cryptography and Communications*, vol. 8, no. 1, pp. 33–49, 2016.
[14] Q. Wang, Y. Jiang, and D. Lin, "Linear complexity of binary generalized cyclotomic sequences over GF(q)," *Journal of Complexity*, vol. 31, no. 5, pp. 731–740, 2015.
[15] Q. Wang and D. Lin, "Generalized cyclotomic numbers of order two and their applications," *Cryptography and Communications*, vol. 8, no. 4, pp. 605–616, 2016.
[16] S. Krone and D. Sarwate, "Quadriphase sequences for spread-spectrum multiple-access communication," *IEEE Transactions on Information Theory*, vol. 30, no. 3, pp. 520–529, 1984.
[17] X. Tang and J. Lindner, "Almost quadriphase sequence with ideal autocorrelation property," *IEEE Signal Processing Letters*, vol. 16, no. 1, pp. 38–40, 2008.
[18] Z. Yang and P. Ke, "Construction of quaternary sequences of length pq with low autocorrelation," *Cryptography and Communications*, vol. 3, no. 2, pp. 55–64, 2011.
[19] X. Du and Z. Chen, "Linear complexity of quaternary sequences generated using generalized cyclotomic classes modulo $2p$," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E94-A, no. 5, pp. 1214–1217, 2011.
[20] P. Ke, J. Zhang, and S. Zhang, "On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^m$," *Designs, Codes and Cryptography*, vol. 67, no. 3, pp. 325–339, 2013.
[21] P. Ke and S. Zhang, "New classes of quaternary cyclotomic sequence of length $2p^m$ with high linear complexity," *Information Processing Letters*, vol. 112, no. 16, pp. 646–650, 2012.
[22] D. M. Burton, *Elementary Number Theory*, McGraw-Hill International Editions, New York, NY, USA, 4th edition, 1998.
[23] D. Pei, A. Salomaa, and C. Ding, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*, World Scientific, Singapore, 1996.
[24] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*, Gulf Professional Publishing, Houston, TX, USA, 2004.
[25] M. Yang, D. Lin, Q. Wang, and J. Gao, "On the linear complexity of binary generalized cyclotomic sequences of period $2p^{m+1}q^{n+1}$," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E102.A, no. 4, pp. 676–679, 2019.