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 Yan5

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

Abstract

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 encrypt 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 $F_l$ 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 $F_l$. The linear complexity of $S$, denoted by $LC(S)$, is the least integer $L$ of a linear recurrence relation over $F_l$ satisfied by $S$:

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

where $c_0 \neq 0$ and $c_0, c_1, \ldots, c_{L-1}, c_L \in F_l$. 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 \( \mathbb{F}_q \) 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 \( \mathbb{F}_q \) with period \( 2pq^4 \) 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 \( 2pq^4 \) 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 \( \varphi(a) \), where \( \varphi(\cdot) \) denotes the Euler function.

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

\[
b + A = \{a + b: a \in A\}, \quad bA = \{ab: a \in A\},
\]

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 \( \mathbb{Z}_p^* \). Then, \( g_1 \) is a primitive root of \( \mathbb{Z}_q^* \) 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 \( \mathbb{Z}^*_q \) [22]. Obviously, \( g_1 \) is a common primitive root of \( \mathbb{Z}_p \) and \( \mathbb{Z}_q \) 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 \( \mathbb{Z}_q^* \) and \( \mathbb{Z}_q^* \) 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

\[
x \equiv a_i \mod m_j, \quad i = 1, \ldots , t,
\]

has solutions if and only if

\[
a_i \equiv a_j \mod \gcd(m_j, m_j), \quad i \neq j, \quad 1 \leq i, j \leq t.
\]

If (4) is satisfied, the solution is unique modulo \( \text{lcm}(m_1, \ldots , m_t) \).

Let \( g \) be the unique solution of the following congruence equations:

\[
\begin{align*}
g & \equiv g_1 \mod 2p^m, \\
g & \equiv g_2 \mod 2q^n.
\end{align*}
\]

**Lemma 1** guaranteed the existence and uniqueness of the common primitive root \( g \) of \( 2p^m \), \( 2q^n \), and \( 2pq^4 \). Similarly, there exists a unique integer \( y \) satisfying the following system of congruences:

\[
\begin{align*}
y & \equiv g \mod 2p^m, \\
y & \equiv 1 \mod 2q^n.
\end{align*}
\]

Assume that \( e_{ij} = \gcd(p^{-1}(p - 1), q^{-1}(q - 1)) \) and \( d_{ij} = ((p - 1)p^{-1}(q - 1)q^{-1}e_{ij}) \). Then, \( d_{ij} \) is the least positive integer that satisfies \( g^{d_{ij}} \equiv 1 \mod p^iq^j \) \((9), \text{Lemma 2})\), i.e., \( \text{ord}_{p^iq^j}(g) = d_{ij} \). 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 \( p^iq^j \), similar to Ding-Helleseth’s generalized cyclotomic classes \((9)\), are defined as follows:

\[
D_0(p^iq^j) = \left\{ g^{2i}y^k \mod p^i q^j : t = 0, 1, \ldots , \left(\frac{d_{ij}}{2}\right) - 1; \right. \\
\left. \quad k = 0, 1, \ldots , e_{ij} - 1 \right\},
\]

\[
D_1(p^iq^j) = gD_0(p^iq^j) \mod p^i q^j.
\]

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

\[
D_0(2pq^4) = \left\{ g^{2i}y^k \mod 2p^4 q^4 : t = 0, 1, \ldots , \left(\frac{d_{ij}}{2}\right) - 1; \right. \\
\left. \quad k = 0, 1, \ldots , e_{ij} - 1 \right\},
\]

\[
D_1(2pq^4) = gD_0(2pq^4) \mod 2p^4 q^4.
\]

Similarly, we have \( \mathbb{Z}_{2pq^4} = D_0(2pq^4) \cup D_1(2pq^4) \). For abbreviation, denote \( H_0h(2pq^4) = p^{m-i}q^{n-j}D_0(2pq^4) \) and \( H_1h(2pq^4) = p^{m-i}q^{n-j}D_0(2pq^4) \) for \( h = 0, 1 \). With the above preparations, we get a partition of \( \mathbb{Z}_{2pq^4} \) as follows:

\[
\mathbb{Z}_{2pq^4} = \bigcup_{i=1}^{m} \bigcup_{j=0}^{n} \bigcup_{h=0}^{1} p^{-i}q^{-j} \left( D_h(2pq^4) \cup 2D_h(2pq^4) \right)
\]

\[
\cup \bigcup_{i=1}^{m} \bigcup_{j=0}^{n} p^{m-i}q^{n-j} D_h(2pq^4) \cup 2D_h(2pq^4)
\]

\[
\cup \left\{ 0, p^{m}q^{n} \right\}.
\]

Let \( \mathbb{F}_4 = \{0, 1, a, a^2\} \) be the finite field with 4 elements, where \( a \) satisfies \( a^2 = a + 1 \). A class of quaternary sequence can be given by allocating each elements of \( \mathbb{F}_4 \) to each generalized cyclotomic class with respect to \( 2pq^4 \). 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 \( 2p^mq^r \) is defined as

\[
 t_{s_i} = \begin{cases} 
 0, & \text{if } i = 0, \\
 e, & \text{if } i = p^mq^r, \\
 a, & \text{if } i = \sum_{j=1}^{m} n_{H_0}^i, \\
 b, & \text{if } i = \sum_{j=1}^{m} n_{H_1}^i, \\
 c, & \text{if } i = \sum_{j=1}^{m} 2H_0^i, \\
 d, & \text{if } i = \sum_{j=1}^{m} 2H_1^i,
\end{cases}
\]

where \( e \neq b + d \) and \( e \in \mathbb{F}_4 \) if \( p \equiv \pm 1 \pmod{8} \) and \( e \notin \{b, b + c\} \) and \( e \notin \mathbb{F}_4 \) if \( p \equiv \pm 3 \pmod{8} \). 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 \( \mathbb{F}_4 \) 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 \( \mathbb{F}_4 \), denoted by \( LC(S) \), is the smallest positive integer \( L \) satisfying the following linear recurrence relation:

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

(12)

where \( c_0 \neq 0 \) and \( c_0, c_1, \ldots, c_{L-1}, c_L \in \mathbb{F}_4 \). The polynomial

\[
c(x) = c_L x^L + c_{L-1} x^{L-1} + \cdots + c_1 x + c_0 \in \mathbb{F}_4[x],
\]

(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 \( S(x) = s_0 + s_1 x + \cdots + s_{N-1} x^{N-1} \in \mathbb{F}_4[x] \), 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 \( \mathbb{F}_4 \) of period \( N \). Then, the minimal polynomial \( m(x) \) of \( S \) is

\[
m(x) = \frac{x^N - 1}{\gcd(x^N - 1, S(x))},
\]

(14)

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

\[
N - \deg(\gcd(x^N - 1, S(x))),
\]

(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

\[
D_h(p^m) = \{x + py : x \in D_h(p), \ y \in \mathbb{Z}_{p^m}\},
\]

(16)

where \( D_h(p^m) = \{x + py + \delta_{x,y} \ : \ x \in D_h(p), \ y \in \mathbb{Z}_{p^m}\} \),

(17)

where

\[
\delta_{x,y} = \begin{cases} 
 0, & \text{if } x + py \text{ is odd}, \\
 p', & \text{otherwise}.
\end{cases}
\]

(18)

For the generalized cyclotomic classes \( D_h(p^m) \) and \( D_h(2p^m) \) corresponding to \( p^m \) and \( 2p^m \), we have the following lemma.

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

\[
D_h(p^m) = \{a + pqb : a \in D_h(p), \ b \in \mathbb{Z}_{p^m}\},
\]

(19)

where

\[
\delta_{a,b} = \begin{cases} 
 0, & \text{if } a + bpq \text{ is odd}, \\
 p', & \text{otherwise}.
\end{cases}
\]

(20)

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

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

\[
2 \in D_0(\phi) \text{ if and only if } p \equiv \pm 1 \pmod{8},
\]

(21)

\[
2 \in D_1(\phi) \text{ if and only if } p \equiv \pm 3 \pmod{8}.
\]

**Proof.** We only prove the first part of this lemma. \( \Box \)

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

**Necessity.** If \( 2 \notin D_0(\phi) \), by the definitions of \( y \) in (6) and \( D_0(\phi) \) in (7), we know \( 2 \notin D_0(\phi) \). It follows from Lemma 6 that \( q \equiv \pm 1 \pmod{8} \).
By the method analogous to that used above, we can get the second conclusion of this lemma.

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

\[
\alpha^{p^m q^n - 1} = (x - 1) (x - \beta) \cdots (x - \beta^{p^m q^n - 1}).
\]

(22)

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

Recall that \( H^{(2p^n q^n)} \) is divided into the following cases. \( H \) divided into the following cases. Let \( A(x) \) be two integers with \( 0 \leq a \leq m - 1 \) and \( 0 \leq b \leq n - 1 \). For \( 1 \leq k \leq p^m q^n - 1 \), suppose \( k = p^n q^m \), with \( \gcd (l, pq) = 1 \). It follows from Lemma 4 that

\[
S_h^{(i,j)}(\beta^k) = \sum_{\tau \in \mathbb{F}_q^m} \beta^{\tau x}.
\]

(23)

Similarly, we have

\[
S_h^{(0,j)}(\beta^k) = \sum_{\tau \in \mathbb{F}_q^m} \beta^{\tau x}.
\]

(24)

Combining (24)-(26), we have

\[
S(\beta^k) = \sum_{i=0}^{d} b_i x^i = e^{p^m q^n} + a \left( \sum_{i=1}^{m} \sum_{j=1}^{n} S_{i,j}^{(i,j)}(\beta^k) + \sum_{i=1}^{m} S_{0,i}^{(i,j)}(\beta^k) + \sum_{j=1}^{n} S_{0,j}^{(i,j)}(\beta^k) \right)
\]

(27)

Let

\[
A(\beta^k) = \sum_{i=1}^{m} \sum_{j=1}^{n} S_{i,j}^{(0,0)}(\beta^k) + \sum_{i=1}^{m} S_{0,j}^{(0,0)}(\beta^k) + \sum_{j=1}^{n} S_{0,j}^{(0,0)}(\beta^k)
\]

(28)

Then,

\[
A(\beta^k) = \sum_{i=1}^{m} \sum_{j=1}^{n} \sum_{\tau \in \mathbb{F}_q^m} \beta^{\tau x} + \sum_{i=1}^{m} \sum_{\tau \in \mathbb{F}_q^m} \beta^{\tau x}.
\]

(29)

We first compute

\[
S_0^{(i,j)}(\beta^k) = \sum_{\tau \in \mathbb{F}_q^m} \beta^{\tau x},
\]

(30)

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

Case 1: \( i \leq a \) and \( j \leq b \). With simple derivation, we have

\[
S_0^{(i,j)}(\beta^k) = \left| D_0^{(\rho^l q^m)} \right| = \frac{(P - 1) \cdot (q - 1) \cdot p^{a-1} q^{b-1}}{2}.
\]

(31)

Case 2: \( i = a + 1 \) and \( j = b + 1 \). Then,
\[ S_{0}^{(i,j)}(\beta^{k}) = \sum_{t \in D_{0}^{(n)}} \zeta_{pq}^{t} (\rho t)^{p^{-1}q^{i+j}} \]  

where \( \zeta_{pq} = \beta^{p^{-1}q^{i+j}} \) is a \( pq \)-th primitive root of unity.

Case 3: \( i > a + 1 \) or \( j > b + 1 \). Let \( \eta = \beta^{p^{m-i-1}q^{n-j-1}} \), then \( \eta^{pq} \neq 1 \). It follows from Lemma 4 that

\[ S_{0}^{(i,j)}(\beta^{k}) = \sum_{t \in D_{0}^{(n)}} \eta t = \sum_{t \in D_{0}^{(n)}} \eta^{|t|} \sum_{t \in \mathbb{Z}/p^{m-i-1} \mathbb{Z}} \eta^{pq}t = 0. \]  

Case 4: \( i \leq a \) and \( j = b + 1 \). Let \( \zeta_{pq} = \beta^{p^{m-i}q^{n-j-1}} \), then \( \zeta_{pq} \) is a \( pq \)-th primitive root of unity. Hence, we obtain

\[ S_{0}^{(i,j)}(\beta^{k}) = \sum_{t \in p^{m-i}q^{n-j-1}ID_{0}^{(n)}} \beta^{t} = \sum_{t \in p^{m-i}q^{n-j-1}ID_{0}^{(n)}} \beta^{t} \left( \frac{p-1}{2} \right) q^{j} \sum_{t \in \mathbb{Z}/p^{m-i-1} \mathbb{Z}} \zeta_{pq}^{t} = (p-1)p^{i-1}q^{j} \sum_{t \in \mathbb{Z}/p^{m-i-1} \mathbb{Z}} \zeta_{pq}^{t} = 0. \]

Case 5: \( i = a + 1 \) and \( j \leq b \). By Lemma 4, we get

\[ S_{0}^{(i,j)}(\beta^{k}) = \sum_{t \in p^{m-i}q^{n-j-1}ID_{0}^{(n)}} \beta^{t} = \sum_{t \in p^{m-i}q^{n-j-1}ID_{0}^{(n)}} \beta^{t} = \sum_{t \in \mathbb{Z}/p^{m-i} \mathbb{Z}} \zeta_{p}^{t} = (p-1)p^{i-1}(p-1)q^{j} \sum_{t \in \mathbb{Z}/p^{m-i-1} \mathbb{Z}} \zeta_{p}^{t} = (q-1)p^{n-1}q^{j} \sum_{t \in \mathbb{Z}/p^{m-i-1} \mathbb{Z}} \zeta_{p}^{t} = \left( \frac{p-1}{2} \right) q^{j} \sum_{t \in \mathbb{Z}/p^{m-i-1} \mathbb{Z}} \zeta_{p}^{t} \]

where \( \zeta_{p} = \beta^{p^{m-i}q^{n-j-1}} \).

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

**Lemma 8.** For \( k = p^{m}q^{l} \) with \( \gcd(l, pq) = 1, 0 \leq a \leq m - 1 \), and \( 0 \leq b \leq n - 1 \), we have

\[ S_{0}^{(i,j)}(\beta^{k}) = \begin{cases} 
\frac{(p-1)(q-1)p^{i-1}q^{j-1}}{2}, & \text{if } i \leq a \text{ and } j \leq b, \\
\sum_{t \in D_{0}^{(n)}} \zeta_{pq}^{t}, & \text{if } i = a + 1 \text{ and } j = b + 1,
\end{cases} \]

**Lemma 9.** For \( k = p^{m}q^{l} \) with \( \gcd(pq, l) = 1 \), we obtain

\[ S_{0}^{(i,0)}(\beta^{k}) = \begin{cases} 
\frac{p^{i-1}(p-1)}{2}, & \text{if } i \leq a, \\
0, & \text{if } i > a + 1,
\end{cases} \]

\[ S_{1}^{(i,0)}(\beta^{k}) = \begin{cases} 
\frac{(p-1)p^{i-1}}{2}, & \text{if } i \leq a, \\
0, & \text{if } i > a + 1,
\end{cases} \]
Proof. Because (38)–(41) can be proved in a similar way, where \( \zeta = \beta^{p^{m-1}q^{a-1}} \) and \( \zeta_2 = \beta^{p^{m+1}q^{a}} \),

\[
S_0^{(i,j)}(\beta^k) = \begin{cases} 
\frac{(q-1)q^{j-1}}{2}, & \text{if } j \leq b, \\
\sum_{t \in D_0^{(i)}} \beta_k^t, & \text{if } j = b + 1, \\
0, & \text{if } j > b + 1,
\end{cases}
\]

(40)

\[
S_1^{(i,j)}(\beta^k) = \begin{cases} 
\frac{(q-1)q^{j-1}}{2}, & \text{if } j \leq b, \\
\sum_{t \in D_1^{(i)}} \beta_k^t, & \text{if } j = b + 1, \\
0, & \text{if } j > b + 1,
\end{cases}
\]

(41)

where \( \zeta_1 = \beta^{p^{m+1}q^{a-1}} \) and \( \zeta_2 = \beta^{p^{m+1}q^{a}} \).

If \( i \leq a \), for each \( t \in \beta^{p^{m-a-1}q^{b+1}D_0^{(r)}} \), it can be easily seen that \( \beta^k = 1 \). Thus,

\[
a \left( \sum_{i=1}^{m} \sum_{j=1}^{n} S_0^{(i,j)}(\beta^k) + \sum_{i=1}^{m} S_0^{(i)}(\beta^k) + \sum_{i=1}^{m} S_1^{(i,j)}(\beta^k) \right)
\]

\[
a \left( \sum_{i=1}^{m} \sum_{j=1}^{n} S_0^{(i,j)}(\beta^k) + \sum_{i=1}^{m} S_0^{(i,b+1)}(\beta^k) + \sum_{i=1}^{m} \sum_{j=b+1}^{j(b+1)} S_0^{(i,j)}(\beta^k) \right)
\]

\[
a \left( \sum_{i=1}^{m} \sum_{j=1}^{n} S_1^{(i,j)}(\beta^k) + \sum_{i=1}^{m} S_1^{(i,b+1)}(\beta^k) + \sum_{i=1}^{m} \sum_{j=b+1}^{j(b+1)} S_1^{(i,j)}(\beta^k) \right)
\]

\[
a \left( \sum_{i=1}^{m} \sum_{j=1}^{n} S_0^{(i,j)}(\beta^k) + \sum_{i=1}^{m} \sum_{j=b+1}^{j(b+1)} S_0^{(i,j)}(\beta^k) + \sum_{i=1}^{m} \sum_{j=b+1}^{j(b+1)} S_1^{(i,j)}(\beta^k) \right)
\]

\[
a \left( \frac{q-1}{2} + \frac{(q-1)q^{j-1}}{2} + \frac{p^{j-1}(p-1)}{2} + \sum_{t \in D_0^{(r)}} \zeta_t^p + \sum_{t \in D_1^{(r)}} \zeta_t^p + \sum_{t \in D_0^{(r)}} \zeta_t^q \right)
\]

(47)

Similarly, we compute the terms with \( b \) as coefficients:

\[
b \left( \sum_{i=1}^{m} \sum_{j=1}^{n} S_1^{(i,j)}(\beta^k) + \sum_{i=1}^{m} \sum_{j=b+1}^{j(b+1)} S_1^{(i,b+1)}(\beta^k) + \sum_{t \in D_0^{(r)}} \zeta_t^p + \sum_{t \in D_1^{(r)}} \zeta_t^p + \sum_{t \in D_0^{(r)}} \zeta_t^q \right)
\]

(48)

The terms with \( c \) as coefficient are

\[
c \left( \frac{p-1}{2} + \sum_{t \in D_0^{(r)}} \zeta_t^p + \sum_{t \in D_1^{(r)}} \zeta_t^p + \sum_{t \in D_0^{(r)}} \zeta_t^q \right).
\]

(49)

The terms with \( d \) as coefficient are

\[
d \left( \frac{p-1}{2} + \sum_{t \in D_0^{(r)}} \zeta_t^p + \sum_{t \in D_1^{(r)}} \zeta_t^p + \sum_{t \in D_0^{(r)}} \zeta_t^q \right).
\]

(50)

It can be easily checked that
Next, we determine $S(p^k)$ according to the values of $p$ and $q$, where $k = p^aq^b$ 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 $2 \in D_0^{(pq)}$, $2 \in D_1^{(pq)}$, and $2 \in D_0^{(q)}$. Hence,

\[
S(p^k) = e + \frac{p - 1}{2}(a + b + c + d) + (a + c) \sum_{t \in D_1^{(pq)}} \zeta_{t},
\]

\[
= e + b + d.
\]

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

\[
S(p^k) = e + (a + c) \sum_{t \in D_1^{(pq)}} \zeta_{t} + (b + d) \sum_{t \in D_1^{(pq)}} \zeta_{t} + (a + c) \sum_{t \in D_1^{(q)}} \zeta_{t},
\]

\[
+ (a + c) \sum_{t \in D_1^{(q)}} \zeta_{t},
\]

\[
= e + b + c.
\]

(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 $2 \in D_0^{(q)}$. Hence,

\[
S(p^k) = e + (a + b + c + d) \frac{(p - 1)(q - 1)p^{q - 1}q^{p - 1} + (p - 1)p^{q - 1} + (q - 1)q^{p - 1}}{2}
\]

\[
= e + b.
\]

(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 $2 \in D_1^{(q)}$. Hence,

\[
S(p^k) = e + (a + d) \sum_{t \in D_1^{(pq)}} \zeta_{t},
\]

\[
+ (a + c) \sum_{t \in D_1^{(pq)}} \zeta_{t},
\]

\[
+ (b + d) \sum_{t \in D_1^{(pq)}} \zeta_{t} + (a + d) \sum_{t \in D_1^{(q)}} \zeta_{t},
\]

\[
+ (b + c) \sum_{t \in D_1^{(q)}} \zeta_{t} + (a + d) \sum_{t \in D_1^{(q)}} \zeta_{t},
\]

\[
= e + b + c.
\]

From the choice of $c$, 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 $LC(S) = 2p^n q^n$. □

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

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

\[
D_0^{(2pq)} \cup qD_0^{(2p)} \cup D_0^{(2q)} = \{1, 3, 5, 11, 19, 27, 29\},
\]

\[
D_1^{(2pq)} \cup qD_1^{(2p)} \cup pD_1^{(2q)} = \{7, 9, 13, 17, 21, 23, 25\},
\]

\[
2D_0^{(pq)} \cup 2qD_0^{(p)} \cup 2pD_0^{(q)} = \{2, 6, 8, 10, 22, 24, 28\},
\]

\[
2D_1^{(pq)} \cup 2qD_1^{(p)} \cup 2pD_1^{(q)} = \{4, 12, 14, 16, 18, 20, 26\}.
\]
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,

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

(57)

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

**Remark 1.** For \( 1 \leq k \leq p^m q^n - 1 \), let \( k = p^m d^k \) with \( \gcd(l, ab) = 1 \). In the case that \( e = b + d \in F_{a}^{*} \) 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 \( 1 \leq k \leq p^m q^n - 1 \). Hence, we need to check if \( \beta^k \) is a multiple root of \( S(x) \). This means we should check if \( \beta^k \) is a root of the derivation polynomial \( S'(x) \) of the generating polynomial \( S(x) \) of \( S \). By definitions, we have

\[
\begin{align*}
\beta^k S'(\beta^k) &= e + b + (a + b) \sum_{t \in D_1^{(p)}} \zeta_{p}^{bt} + (a + b) \sum_{t \in D_1^{(p)}} \zeta_{p}^{bt} \\
&\quad + (a + b) \sum_{t \in D_0^{(p)}} \zeta_{q}^{bt},
\end{align*}
\]

(58)

and

\[
\begin{align*}
\beta^k S'(\beta^k) &= e + (a + b) \sum_{t \in D_1^{(p)}} \zeta_{p}^{bt} + (a + b) \sum_{t \in D_1^{(p)}} \zeta_{p}^{bt} \\
&\quad + (a + b) \sum_{t \in D_0^{(p)}} \zeta_{q}^{bt},
\end{align*}
\]

(59)

respectively.

For the fixed \( a \) and \( b \) with \( 0 \leq a \leq m - 1 \) and \( 0 \leq b \leq n - 1 \), by the following equations,

\[
\begin{align*}
\sum_{t \in D_1^{(p)}} \zeta_{p}^{bt} + \sum_{t \in D_1^{(p)}} \zeta_{p}^{bt} &= 1, \\
\sum_{t \in D_0^{(p)}} \zeta_{q}^{bt} + \sum_{t \in D_0^{(p)}} \zeta_{q}^{bt} &= 1, \\
\sum_{t \in D_1^{(p)}} \zeta_{p}^{bt} + \sum_{t \in D_1^{(p)}} \zeta_{p}^{bt} &= 1,
\end{align*}
\]

(60)

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

\[
p^m q^n - 1 + \sum_{a=0}^{m} \sum_{b=0}^{n} \frac{(p - 1)(q - 1)p^{m-a-1} q^{n-b-1}}{2}
\]

(61)

roots for \( 0 \leq k \leq p^m q^n - 1 \). By Lemma 2, we obtain

\[
LC(S) \geq \frac{2p^m q^n - 3p^m q^n - p^m - q^n - 1}{2}
\]

(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. 61421120102162121007).

**References**


