IMPROVEMENTS ON THE 4-ADIC COMPLEXITY OF A CLASS OF QUATERNARY SEQUENCES

Ting Jiang¹,* and Fang-Wei Fu²

Abstract. Yang and Ke proposed a new class of quaternary sequences with low autocorrelation of period \(pq\) by using the inverse Gray mapping and the pair of two generalized cyclotomic sequences (Cryptography and Communications, vol. 3, pp. 55–64, 2011). In this paper, we aim to study and determine the 4-adic complexity of this class of quaternary sequences, and our results show that the 4-adic complexity of this class of quaternary sequences is quite large, and it can reach the maximum in particular cases.

Mathematics Subject Classification. 94A55, 94A60, 65C10.

Received September 2, 2022. Accepted November 16, 2023.

1. Introduction

In stream cipher, the feedback with carry shift register (FCSR) proposed by Klapper and Goresky [7] is an important kind of generator to generate nonlinear periodic sequences fast. Quaternary periodic sequences with low nontrivial autocorrelation have attracted considerable attention and have widely been applied for communication systems since they can be easily implemented [1, 5, 8, 9].

For a \(m\)-ary periodic sequence \(s\) over \(\mathbb{Z}_m\), the \(m\)-adic complexity \(\Phi_m(s)\) measures the smallest length of the FCSR which generates the sequence \(s\) [10, 12]. It is well-known that a quaternary sequence \(s\) can be decoded with \(6\Phi_4(s) + 16\) consecutive bits in the view of the rational approximation algorithm (RAA) [11, 12]. In order to avoid safety risks in communication and cryptography systems, it thus demands that the 4-adic complexity of a safe sequence \(s\) with period \(N\) should exceed \(\frac{N-16}{6}\), otherwise this sequence is so insecure that it can be decrypted by the RAA. In recent ten years, the research results of the 2-adic complexity of binary periodic sequences are rich [3, 4, 6, 15–20, 25]. To the best of our knowledge, there are few literatures to study the 4-adic complexity of quaternary periodic sequences [2, 13, 14, 21, 22].

Recently, there are some new constructions of quaternary sequences used the method of the inverse Gray mapping and two binary period sequences pairs (see [1, 5, 8, 9, 23]). For example, Yang and Ke [23] proposed a new class of quaternary sequences with low autocorrelation of period \(pq\) by using the inverse Gray mapping. Later, Zhao and Wen studied the linear complexity of this class of quaternary sequences, and their results showed that the linear complexity of this class of quaternary sequences is large [24]. This paper contributes to compute the 4-adic complexity of this class of quaternary sequences with low autocorrelation.

Keywords and phrases: Quaternary sequences, 4-adic complexity, generalized cyclotomic sequences, inverse Gray mapping, stream cipher.

1 School of Mathematics and Big Data, Chaohu University, Hefei 238024, PR China.
2 Chern Institute of Mathematics and LPMC, Nankai University, Tianjin 300071, PR China.
* Corresponding author: ahjiangting@126.com

© The authors. Published by EDP Sciences, 2024

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.
The remainder of this paper is organized as follows. Some concepts and notations are introduced in Section 2. In Section 3, we give some auxiliary lemmas which are very useful to determine the 4-adic complexity of a class of quaternary sequences with low autocorrelation of period $pq$. In Section 4, we give the exact values of 4-adic complexity of this class of quaternary sequences with low autocorrelation of period $pq$, and list some examples to illustrate our results. Finally, we summarize the paper in Section 5.

2. Preliminaries

In this section, we will introduce some concepts and notations. Throughout this paper, we denote $N = pq$.

Let $p$ and $q$ be two distinct odd primes. Define

$$P = \{p, 2p, \cdots, (q-1)p\}, \quad Q = \{q, 2q, \cdots, (p-1)q\}.$$ 

Then a partition of the integer residue class ring $\mathbb{Z}_N$ modulo $N$ is

$$\mathbb{Z}_N = \mathbb{Z}_N^* \cup P \cup Q \cup \{0\},$$

where $\mathbb{Z}_N^*$ denotes the all invertible elements of $\mathbb{Z}_N$. Note that $\mathbb{Z}_N^*$ can be also expressed in the following form:

$$\mathbb{Z}_N^* = \{e \pmod{pq} : \gcd(e, pq) = 1\} = \{ip + jq \pmod{pq} : 1 \leq i \leq q-1, 1 \leq j \leq p-1\}.$$ 

For two integer $x$ and $y$, $\gcd(x, y)$ denotes the greatest common divisor of $x$ and $y$. Denote $\left(\frac{x}{p}\right)$ the Legendre symbol, that is

$$\left(\frac{\ell}{p}\right) = \begin{cases} 1, & \text{if } \ell = d^2 \text{ for some } d \in \mathbb{F}_p^*; \\ -1, & \text{otherwise}, \end{cases}$$

where $\mathbb{F}_p^*$ denotes all the nonzero elements of finite field $\mathbb{F}_p$.

Let $\phi$ be the inverse Gray mapping $\mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_4$ defined by

$$\phi[0, 0] = 0, \phi[0, 1] = 1, \phi[1, 1] = 2, \phi[1, 0] = 3.$$ 

It is easy to show that

$$\phi[a, b] = 2a - a(b - 1) - (a - 1)b, \quad (2.1)$$

where $a, b \in \{0, 1\}$. By the inverse Gray mapping, we can build a quaternary sequence from two binary sequences. Define

$$u = \phi[x, y] \quad (2.2)$$

as a quaternary sequence of period $n$, where $x$ and $y$ are two binary sequences of period $n$. Here the binary sequences $x$ and $y$ are called component sequences of $u$. The components of the sequence $u$ are given as

$$u(t) = \phi[x(t), y(t)],$$
where $0 \leq t \leq n - 1$. Let $s = \{s(i)\}_{i=0}^{n-1}$ be a quaternary sequence of period $n$, where $s(i) \in \mathbb{Z}_4$. The sequence polynomial of the quaternary sequence $s$ is defined by

$$S(x) = s(0) + s(1)x + s(2)x^2 + \cdots + s(n-1)x^{n-1}. $$

**Definition 2.1.** Let $s = \{s(i)\}_{i=0}^{n-1}$ be a quaternary sequence of period $n$, $S(4) = \sum_{i=0}^{n-1} s(i)4^i$, where $s(i) \in \mathbb{Z}_4$. The 4-adic complexity of the quaternary sequence $s$, denoted by $\Phi_4(s)$, is defined by

$$\Phi_4(s) = \log_4 \left( \frac{4^n - 1}{\gcd(S(4), 4^n - 1)} \right),$$

where $\gcd(S(4), 4^n - 1)$ denotes the greatest common divisor of $S(4)$ and $4^n - 1$.

For a quaternary periodic sequence $s$, the smallest length of FCSR which generates the quaternary sequence $s$ is $\lceil \Phi_4(s) + 1 \rceil$, where $\lceil x \rceil$ denotes the greatest integer that is less than or equal to $x$. By the above definition, it is easily seen that the 4-adic complexity achieves the maximum value $\log_4(4^n - 1)$ when $\gcd(S(4), 4^n - 1) = 1$. It is also clear to observe that we need to determine $d = \gcd(S(4), 4^n - 1)$ in order to compute the 4-adic complexity of a quaternary sequence of period $n$.

**Definition 2.2.** [23, Definition 3.1] Let $p$ and $q$ be two distinct odd primes, and let $s_1 = \{s_1(i)\}_{i=0}^{pq-1}$ and $s_2 = \{s_2(i)\}_{i=0}^{pq-1}$ be two binary generalized cyclotomic sequences of period $pq$ defined by

$$s_1(t) = \begin{cases} 
1, & \text{if } t \in P; \\
0, & \text{if } t \in Q \cup \{0\}; \\
\frac{1-(\frac{t}{p})(\frac{t}{q})}{2}, & \text{if } t \in \mathbb{Z}_*^{pq}.
\end{cases}$$

(2.3)

and

$$s_2(t) = \begin{cases} 
0, & \text{if } t \in P; \\
1, & \text{if } t \in Q \cup \{0\}; \\
\frac{1-(\frac{t}{p})(\frac{t}{q})}{2}, & \text{if } t \in \mathbb{Z}_*^{pq}.
\end{cases}$$

(2.4)

The quaternary sequence $s = \{s(i)\}_{i=0}^{pq-1}$ of period $pq$ is defined by

$$s = \phi[s_1, s_2].$$

3. **Some auxiliary lemmas**

In this section, we will present some auxiliary lemmas in order to determine the 4-adic complexity of the quaternary sequence defined by Definition 2.2 in the next section.

For the convenience of writing, we denote

$$G_p = \sum_{j=1}^{p-1} \left( \frac{jq}{p} \right) 4^{jq}$$

and

$$G_q = \sum_{i=1}^{q-1} \left( \frac{ip}{q} \right) 4^{ip}.$$
Lemma 3.1. Let \( p \) and \( q \) be two distinct odd primes, and let \( s \) be the quaternary sequence of period \( pq \) defined by Definition 2.2, then we have

\[
S(4) = \frac{(4^p - 1)(4^q - 1)}{(4p - 1)(4q - 1)} + \frac{2(4^p - 1)}{4p - 1} - 2 - G_pG_q \pmod{4^p - 1}.
\]

Proof. By Definition 2.2 and equation (2.1), we have

\[
S(4) = \sum_{t=0}^{pq-1} \phi[s_1(t), s_2(t)] \cdot 4^t
\]

\[
= \sum_{t \in P^*} \phi[s_1(t), s_2(t)] \cdot 4^t + \sum_{t \in \mathbb{Z}_{p^*}^+} \phi[s_1(t), s_2(t)] \cdot 4^t + \sum_{t \in \mathbb{Z}_{q^*}^+} \phi[s_1(t), s_2(t)] \cdot 4^t
\]

\[
= \sum_{t \in P^*} \phi[0, 1] \cdot 4^t + \sum_{t \in \mathbb{Z}_{p^*}^+} \phi[s_1(t), s_2(t)] \cdot 4^t + \sum_{t \in \mathbb{Z}_{q^*}^+} \phi[s_1(t), s_2(t)] \cdot 4^t
\]

\[
= 3 \cdot \sum_{t=1}^{pq-1} 4^{ip} + \sum_{t=0}^{p-1} 4^{iq} + \sum_{t \in \mathbb{Z}_{pq}^*} \left[ 1 - \left( \frac{t}{p} \right) \left( \frac{t}{q} \right) \right] \cdot 4^t
\]

\[
= 3 \cdot \left( \frac{4^p - 1}{4p - 1} - 1 \right) + \left( \frac{4^q - 1}{4q - 1} \right) + \sum_{t \in \mathbb{Z}_{pq}^*} 4^t - \sum_{t \in \mathbb{Z}_{pq}^*} \left( \frac{t}{p} \right) \left( \frac{t}{q} \right) \cdot 4^t
\]

\[
= 3 \cdot \left( \frac{4^p - 1}{4p - 1} - 1 \right) + \left( \frac{4^q - 1}{4q - 1} \right) + \sum_{i=1}^{q-1} \sum_{j=1}^{p-1} 4^{ip+jq}
\]

\[
- \sum_{i=1}^{q-1} \sum_{j=1}^{p-1} \left( \frac{ip + jq}{p} \right) \left( \frac{ip + jq}{q} \right) \cdot 4^{ip+jq}
\]

\[
= 3 \cdot \left( \frac{4^p - 1}{4p - 1} - 1 \right) + \left( \frac{4^q - 1}{4q - 1} \right) + \left( \sum_{i=1}^{q-1} 4^{ip} \right) \cdot \left( \sum_{j=1}^{p-1} \frac{jq}{p} \right) 4^{jq}
\]

\[
- \left( \sum_{i=1}^{q-1} \frac{ip}{q} \right) 4^{ip} \cdot \left( \sum_{j=1}^{p-1} \frac{jq}{p} \right) 4^{jq}
\]

\[
= 3 \cdot \left( \frac{4^p - 1}{4p - 1} - 1 \right) + \left( \frac{4^q - 1}{4q - 1} \right) + \left( \frac{4^q - 1}{4q - 1} \right) \left( \frac{4^p - 1}{4p - 1} - 1 \right) - G_pG_q
\]

\[
\equiv \frac{(4^p - 1)(4^q - 1)}{(4p - 1)(4q - 1)} + \frac{2(4^p - 1)}{4p - 1} - 2 - G_pG_q \pmod{4^p - 1}.
\]

Hence we complete the proof of this lemma.

\[\square\]

Lemma 3.2. Let the symbols be the same as before, then we have

(i) \( G_p \equiv 0 \pmod{4^q - 1} \);

(ii) \( G_q \equiv 0 \pmod{4p - 1} \).
Proof. (i) By the definition of $G_p$, then we have

$$G_p = \sum_{j=1}^{p-1} \left( \frac{jq}{p} \right) 4^j q \equiv \sum_{j=1}^{p-1} \left( \frac{jq}{p} \right) = 0 \pmod{4^q - 1}. $$

(ii) Similarly, we have $G_q \equiv 0 \pmod{4^p - 1}$. □

From Lemmas 3.1 and 3.2, we have

$$S(4) \equiv \frac{(4pq - 1)(4pq - 1)}{(4p - 1)(4q - 1)} + \frac{2(4pq - 1)}{4p - 1} - 2 - G_pG_q \pmod{4^{pq} - 1}$$

$$\equiv q \cdot \frac{4p - 1}{3} + 2q - 2 \pmod{4^p - 1}. \quad (3.1)$$

In the above formula, we can apply the following equation.

$$\frac{4pq - 1}{4q - 1} \equiv \frac{4p - 1}{3} \pmod{4^p - 1}. $$

Similarly, we have

$$S(4) \equiv p \cdot \frac{4^q - 1}{3} + 2 \cdot \frac{4^q - 1}{3} - 2 \pmod{4^q - 1}$$

$$\equiv (4^q - 1)(p + 2) - 2 \pmod{4^q - 1}. \quad (3.2)$$

Lemma 3.3. Keep the symbols as before, then we have

(i) $S(4) \equiv 0 \pmod{3}$, if $p = 3, q \equiv 1 \pmod{3}$ or $p \equiv 2 \pmod{3}, q \equiv 2 \pmod{3}$;

(ii) $S(4) \not\equiv 0 \pmod{3}$, otherwise.

Proof. From Lemma 3.1, we have

$$S(4) \equiv \frac{(4pq - 1)(4pq - 1)}{(4p - 1)(4q - 1)} + \frac{2(4pq - 1)}{4p - 1} - 2 - G_pG_q \pmod{4^{pq} - 1}$$

$$\equiv pq + 2(q - 1) \pmod{3}. $$

If $p = 3, q \equiv 1 \pmod{3}$ or $p \equiv 2 \pmod{3}, q \equiv 2 \pmod{3}$, then $3 \mid S(4)$. Otherwise, then $3 \nmid S(4)$. Hence the conclusions are proved directly. □

Lemma 3.4. Keep the symbols as before.

(i) If $q = 3$ or $q \equiv 1 \pmod{3}, p \not\equiv 3$ or $q \equiv 2 \pmod{3}, p \not\equiv 2 \pmod{3}$, then we have

$$\gcd(S(4), 4^p - 1) = 1.$$ 

(ii) If $q \equiv 1 \pmod{3}, p = 3$ or $q \equiv 2 \pmod{3}, p \equiv 2 \pmod{3}$, then we have

$$\gcd(S(4), 4^p - 1) = 3.$$
Proof. It is easy to verify that
\[ \gcd(a + kb, b) = \gcd(a, b), \]
where \(a, b, k \in \mathbb{Z}\), and \(\mathbb{Z}\) denotes the integer ring. From equation (3.1), we have
\[ S(4) \equiv q \cdot \frac{4^p - 1}{3} + 2q - 2 \pmod{4^p - 1}. \]

(1) If \(q = 3\), then
\[ \gcd \left( q \cdot \frac{4^p - 1}{3} + 2q - 2, 4^p - 1 \right) = \gcd(4, 4^p - 1) = 1. \]

(2) If \(q \equiv 1 \pmod{3}\), then
\[
\begin{align*}
\gcd \left( q \cdot \frac{4^p - 1}{3} + 2q - 2, 4^p - 1 \right) &= \gcd \left( \frac{4^p - 1}{3} + 2q - 2, 4^p - 1 \right) \\
&= \gcd \left( \frac{4^p - 1}{3} + 2q - 2, 6(q - 1) \right) = \gcd \left( \frac{4^p - 1}{3} + 2q - 2, 3(q - 1) \right) \\
&= \gcd \left( \frac{4^p - 1}{3} - (q - 1), 3(q - 1) \right).
\end{align*}
\]
Furthermore, if \(p = 3\), we have
\[ \gcd \left( q \cdot \frac{4^p - 1}{3} + 2q - 2, 4^p - 1 \right) = 3, \]
and if \(p \neq 3\), we have
\[ \gcd \left( q \cdot \frac{4^p - 1}{3} + 2q - 2, 4^p - 1 \right) = 1. \]

(3) If \(q \equiv 2 \pmod{3}\), then
\[
\begin{align*}
\gcd \left( q \cdot \frac{4^p - 1}{3} + 2q - 2, 4^p - 1 \right) &= \gcd \left( \frac{2(4^p - 1)}{3} + 2q - 2, 4^p - 1 \right) \\
&= \gcd \left( \frac{4^p - 1}{3} + q - 1, 4^p - 1 \right) = \gcd \left( \frac{4^p - 1}{3} + q - 1, -3(q - 1) \right) \\
&= \gcd \left( \frac{4^p - 1}{3} + q - 1, 3(q - 1) \right).
\end{align*}
\]
Furthermore, if \(p \equiv 2 \pmod{3}\), we have
\[ \gcd \left( q \cdot \frac{4^p - 1}{3} + 2q - 2, 4^p - 1 \right) = 3, \]
and if \( p \not\equiv 2 \pmod{3} \), we have

\[
gcd \left( q \cdot \frac{4^p - 1}{3} + 2q - 2, 4^p - 1 \right) = 1.
\]

Hence we complete the proof of the lemma. \( \square \)

**Lemma 3.5.** Keep the symbols as before. Then we have

\[
gcd \left( S(4), \frac{4^q - 1}{3} \right) = 1.
\]

**Proof.** From equation (3.2), we have

\[
S(4) \equiv \frac{(4^q - 1)(p + 2)}{3} - 2 \pmod{4^q - 1}
\]

\[
\equiv -2 \pmod{\frac{4^q - 1}{3}}.
\]

Hence,

\[
gcd \left( S(4), \frac{4^q - 1}{3} \right) = \gcd \left( 2, \frac{4^q - 1}{3} \right) = 1.
\]

\( \square \)

**Lemma 3.6.** Let \( p \) be an odd prime, then

(i) \( 4^p \equiv 1 \pmod{9} \) for \( p = 3 \);
(ii) \( 4^p \not\equiv 1 \pmod{9} \) for \( p > 3 \).

**Proof.** (i) It is easy to show that \( 4^p - 1 = 4^3 - 1 = 63 \equiv 0 \pmod{9} \).
(ii) Assume that \( 4^p \equiv 1 \pmod{9} \), then \( p \) divides the value of the Euler’s totient function \( \varphi(9) = 6 \). This is a contradiction. \( \square \)

**Lemma 3.7.** Keep the symbols as before. If \( p = 3 \), then

(i) \( \gcd(S(4), 9) = 9 \) if and only if \( q \equiv 4 \pmod{9} \);
(ii) \( \gcd(S(4), 9) = 3 \) if and only if \( q \equiv 1, 7 \pmod{9} \);
(iii) \( \gcd(S(4), 9) = 1 \) if and only if \( q \equiv 2, 5, 8 \pmod{9} \).

**Proof.** From Lemma 3.6 and equation (2.4), we have

\[
S(4) \equiv q \cdot \frac{4^p - 1}{3} + 2q - 2 \pmod{4^p - 1}
\]

\[
\equiv 21q + 2(q - 1) \pmod{9}.
\]

It then follows that

\[
\gcd(S(4), 9) = \gcd(21q + 2(q - 1), 9) = \gcd(2q + 1, 9).
\]

Thus, it is easy to show that \( \gcd(2q + 1, 9) = 9 \) if and only if \( q \equiv 4 \pmod{9} \), \( \gcd(2q + 1, 9) = 3 \) if and only if \( q \equiv 1, 7 \pmod{9} \), and \( \gcd(2q + 1, 9) = 1 \) if and only if \( q \equiv 2, 5, 8 \pmod{9} \). Hence the lemma is completely proved. \( \square \)
4. 4-Adic Complexity of a Class of Quaternary Sequences

In this section, we mainly determine the 4-adic complexity of the quaternary sequence $s$ defined by Definition 2.2.

Denote

$$d_1 = \gcd \left( S(4), \frac{3(4^{pq} - 1)}{(4^p - 1)(4^q - 1)} \right),$$

$$d_2 = \gcd (S(4), 4^p - 1),$$

and

$$d_3 = \gcd \left( S(4), \frac{4^q - 1}{3} \right).$$

Conjecture 4.1. Keep the symbols as before, then

$$\gcd \left( S(4), \frac{3(4^{pq} - 1)}{(4^p - 1)(4^q - 1)} \right) = 1.$$

Remark 4.2. To the best of our knowledge, it is very hard to determine the greatest common divisor of $S(4)$ and $\frac{3(4^{pq} - 1)}{(4^p - 1)(4^q - 1)}$. But, by the calculation using the Magma program, we find that the above conjecture is correct.

Based on Conjecture 4.1, we will directly present our main results as below.

Theorem 4.3. If $p = 3$ and $q \equiv 4 \pmod{9}$, then we have

$$\Phi_4(s) = \log_4 \left( \frac{4^{pq} - 1}{9} \right).$$

Theorem 4.4. If $p = 3$, $q \equiv 1, 7 \pmod{9}$ or $p \equiv 2 \pmod{3}$, $q \equiv 2 \pmod{3}$, then we have

$$\Phi_4(s) = \log_4 \left( \frac{4^{pq} - 1}{3} \right).$$

Theorem 4.5. For $p$ and $q$ are not the form as above, then we have

$$\Phi_4(s) = \log_4 (4^{pq} - 1).$$

Next, we will give the comprehensive proofs of Theorems 4.3–4.5.

The proofs of Theorems 4.3–4.5:

It is easy to show that the 4-adic complexity of the quaternary sequence $s$ defined by Definition 2.2 is given by

$$\Phi_4(s) = \log_4 \left( \frac{4^{pq} - 1}{r} \right),$$

where $r$ is determined by the specific conditions of $p$ and $q$. For instance, in Theorem 4.3, $r = 9$ when $q \equiv 4 \pmod{9}$, and in Theorem 4.4, $r = 3$ when $q \equiv 1, 7 \pmod{9}$ or $q \equiv 2 \pmod{3}$. For other conditions, $r$ is determined accordingly to ensure that the complexity is well-defined and consistent with the given theorems.
where

\[ r = \gcd \left( \frac{q \cdot (4^p - 1)}{3} + 2(q - 1), 4^p - 1 \right). \]

In what follows, we will mainly determine the value of \( r \). It is easy to verify that

\[ \gcd \left( 4^p - 1, \frac{4^q - 1}{3} \right) = \begin{cases} 1, & \text{if } q \neq 3; \\ 3, & \text{if } q = 3. \end{cases} \]

Next we divide into the following two cases to prove the theorems.

Case 1: For \( q \neq 3 \). Since \( \gcd \left( 4^p - 1, \frac{4^q - 1}{3} \right) = 1 \), we then have \( \gcd(d_2, d_3) = 1 \). Next, we prove that

\[ \gcd(d_1, d_2) = 1. \]

Note that

\[ \frac{3(4^{pq} - 1)}{(4^p - 1)(4^q - 1)} \not\equiv 0 \pmod{3}. \]

Assume that \( \mu > 3 \) is an odd prime with \( \mu \mid d_1 \). Since \( \mu \) is a divisor of \( \frac{3(4^{pq} - 1)}{(4^p - 1)(4^q - 1)} \), we easily show that \( \mu \) is a divisor of \( \frac{3(4^{pq} - 1)}{4^p - 1} = 3(1 + 4^p + \cdots + 4^{(p-1)q}), \)

from which we derive

\[ 1 + 4^p + \cdots + 4^{(p-1)q} \equiv 0 \pmod{\mu}. \]

If \( 4^p \equiv 1 \pmod{\mu} \), we have

\[ 0 \equiv 1 + 4^p + \cdots + 4^{(p-1)q} \equiv q \pmod{\mu}. \]

This implies that \( q = \mu \) since \( \mu > 3 \) is an odd prime. Together with \( \mu \mid S(4) \) and \( \mu \mid (4^p - 1) \), then we have \( q \mid \gcd(S(4), 4^p - 1) \). This means that \( q \mid 2(q - 1) \) since

\[ \gcd(S(4), 4^p - 1) = \gcd \left( \frac{q \cdot (4^p - 1)}{3} + 2(q - 1), 4^p - 1 \right). \]

This is a contradiction.

Similarly, we have

\[ \gcd(d_1, d_3) = 1. \]

It is easy to know that

\[ 4^{pq} - 1 = (4^p - 1) \cdot \frac{4^q - 1}{3} \cdot \frac{3(4^{pq} - 1)}{(4^p - 1)(4^q - 1)}. \]
Hence

$$\gcd(S(4), 4^{pq} - 1) = \gcd\left(S(4), \frac{3(4^{pq} - 1)}{(4^p - 1)(4^q - 1)}\right) \cdot \gcd\left(S(4), \frac{4^q - 1}{3}\right).$$

The results then follow by Lemmas 3.3–3.5 and 3.7.

Case 2: For $q = 3$. By Lemma 3.3, we have $\gcd(S(4), \frac{4^q - 1}{3}) = 1$. Hence we have

$$\gcd(d_2, d_3) = 1.$$ 

The remaining proofs are similar to Case 1.

**Remark 4.6.** For a quaternary sequence $u$ of period $N$, it demands that the 4-adic complexity $\Phi_4(u)$ should exceed $\frac{N-16}{6}$ to resist the rational approximation algorithm. The results of Theorems 4.3–4.5 show that the 4-adic complexity $\Phi_4(s)$ of the quaternary sequence $s$ defined by Definition 2.2 is larger than $\frac{pq-16}{6}$. Thus the quaternary sequence $s$ is safe to resist the attack of the rational approximation algorithm effectively.

In the following, we give some examples to illustrate the results of Theorems 4.3–4.5, respectively.

**Example 4.7.** Let $p = 3$ and $q = 13$, then the pair of two generalized cyclotomic sequences is given as

$$s_1 = \{0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1\}$$

and

$$s_2 = \{1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1\}.$$ 

By the inverse Gray mapping, then we have

$$s = \{1, 0, 0, 3, 0, 0, 3, 2, 0, 3, 0, 3, 0, 3, 1, 2, 3, 0, 2, 3, 2, 0, 3, 0, 2, 3, 0, 1, 3, 0, 1, 0, 0, 0, 2, 3, 2, 2\}.$$ 

By the Magma program, we obtain that $\gcd(S(4), 4^P - 1) = 9$. Hence the 4-adic complexity of the quaternary sequence $s$ is

$$\Phi_4(s) = \log_4 \left(\frac{4^{pq} - 1}{9}\right).$$

**Example 4.8.** Let $p = 5$ and $q = 11$, then the pair of two generalized cyclotomic sequences is given as

$$s_1 = \{0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0\}$$

and

$$s_2 = \{1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1\}.$$
By the inverse Gray mapping, then we have
\[ s = \{1, 0, 0, 2, 0, 3, 2, 0, 0, 0, 3, 1, 2, 0, 0, 0, 2, 3, 2, 1, 2, 2, 3, 0, 2, 0, 2, 3, 0, \\
0, 1, 0, 3, 0, 2, 2, 3, 2, 2, 0, 1, 3, 2, 2, 0, 3, 2, 0, 2, 2 \}. \]

By the Magma program, we obtain that \( \gcd(S(4), 4^p - 1) = 3 \). Hence the 4-adic complexity of the quaternary sequence \( s \) is
\[ \Phi_4(s) = \log_4 \left( \frac{4^p q - 1}{3} \right). \]

**Example 4.9.** Let \( p = 7 \) and \( q = 5 \), then the pair of two generalized cyclotomic sequences is given as
\[ s_1 = \{0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, \\
1, 0, 0, 1, 1, 0, 1\} \]
and
\[ s_2 = \{1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, \\
0, 1, 0, 1, 1, 0, 1\}. \]

By the inverse Gray mapping, then we have
\[ s = \{1, 0, 2, 0, 0, 1, 2, 3, 2, 0, 1, 0, 0, 0, 3, 1, 0, 0, 2, 2, 1, 2, 2, 2, 1, 2, 0, \\
3, 0, 1, 2, 2, 0, 2\}. \]

By the Magma program, we obtain that \( \gcd(S(4), 4^p - 1) = 1 \). Hence the 4-adic complexity of the quaternary sequence \( s \) is
\[ \Phi_4(s) = \log_4 (4^p q - 1). \]

**5. Conclusion**

In this paper, we devote to study the 4-adic complexity of a class of quaternary sequences with low autocorrelation of period \( pq \) that presented in [23]. It turns out that the 4-adic complexity of this class of quaternary sequences is quite large. As a consequence, this class of quaternary sequences is safe enough to resist the attack of the rational approximation algorithm.

**Acknowledgements.** The authors sincerely thank the reviewers for their helpful comments and valuable suggestion, which have improved the presentation of this paper.

**Funding.** This research of Ting Jiang is supported in part by High-level Talents Research Project of Chaohu University under Grant KYQD-2023064. This research of Fang-Wei Fu is supported by the National Key Research and Development Program of China (Grant No. 2018YFA0704703), the National Natural Science Foundation of China (Grant Nos. 12226336, 62371259), the Fundamental Research Funds for the Central Universities of China (Nankai University).

**References**


---

Please help to maintain this journal in open access!

This journal is currently published in open access under the Subscribe to Open model (S2O). We are thankful to our subscribers and supporters for making it possible to publish this journal in open access in the current year, free of charge for authors and readers. Check with your library that it subscribes to the journal, or consider making a personal donation to the S2O programme by contacting subscribers@edpsciences.org.

More information, including a list of supporters and financial transparency reports, is available at https://edpsciences.org/en/subscribe-to-open-s2o.