On the 2-adic complexity of a class of binary sequences of period $4p$ with optimal autocorrelation magnitude *

Minghui Yang, Lulu Zhang, Keqin Feng

Abstract-Via interleaving Ding-Helleseth-Lam sequences, a class of binary sequences of period $4p$ with optimal autocorrelation magnitude was constructed in [8]. Later, Fan showed that the linear complexity of this class of sequences is quite good [3]. Recently, Sun et al. determined the upper and lower bounds of the 2-adic complexity of such sequences [11]. We determine the exact value of the 2-adic complexity of this class of sequences. The results show that the 2-adic complexity of this class of binary sequences is close to the maximum.
keywords-2-adic complexity, optimal autocorrelation magnitude, binary sequences.

1 Introduction

Sequences with good randomness such as long period, low autocorrelation and large linear complexity are widely used in cryptography, communication, etc. Feedback with carry shift registers (FCSRs) are a class of nonlinear pseudo random sequence generators. Due to the rational approximation algorithm [17], 2-adic complexity has become an important security criteria. Hence, it is interesting to investigate the 2-adic complexity of some well-known sequences with optimal autocorrelation and large linear complexity.

The autocorrelation function of binary sequence $s = (s_0, s_1, \dots, s_{N-1})$ with period N is defined by

$$C_s(\tau) = \sum_{i=0}^{N-1} (-1)^{s_i + s_{i+\tau}}, \quad \tau \in \mathbb{Z}/N\mathbb{Z}.$$

A sequence s with period N is called an optimal autocorrelation sequence [1] if for any $\tau \neq 0$,

* Minghui Yang was supported by NSFC under Grant 11701553. Lulu Zhang was supported by the National Natural Science Foundation of China (NSFC) under Grant 11601350. Keqin Feng was supported by NSFC under Grant 11571007 and 11471178.

Minghui Yang is with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China, email: (yangminghui6688@163.com).

Lulu Zhang is with Capital Normal University, Beijing 100048, China, (e-mail: 840375411@qq.com).

Keqin Feng is with the department of Mathematical Sciences, Tsinghua University, Beijing, 100084, China, email: (fengkq@tsinghua.edu.cn).

(1) $C_s(\tau) = -1$ for $N \equiv 3 \pmod 4$; or
(2) $C_s(\tau) \in \{1, -3\}$ for $N \equiv 1 \pmod 4$; or
(3) $C_s(\tau) \in \{2, -2\}$ for $N \equiv 2 \pmod 4$; or
(4) $C_s(\tau) = 0$ for $N \equiv 0 \pmod 4$.

Up to equivalence, the only known binary sequence in Type (4) is (0, 0, 0, 1). Hence, for a sequence with period $N \equiv 0 \pmod 4$, it is natural to consider the case $C_s(\tau) \in \{0, \pm 4\}$. When τ ranges from 1 to $N-1$, s is referred to as a sequence with optimal autocorrelation value if $C_s(\tau) \in \{0, -4\}$ or $\{0, 4\}$ [12], and s is referred to as a sequence with optimal autocorrelation magnitude if $C_s(\tau) \in \{0, \pm 4\}$ [18].

Interleaved operator that was originally presented by Gong [4] is a powerful tool to construct sequences with optimal autocorrelation and large period.

Let $s^t = (s_0^t, s_1^t, \ldots, s_{N-1}^t)$ be a binary sequence of period N, where $0 \le t \le M-1$. An $N \times M$ matrix is obtained from these M binary sequences and given by

$$U = \begin{pmatrix} s_0^0 & s_0^1 & \cdots & s_0^{M-1} \\ s_1^0 & s_1^1 & \cdots & s_1^{M-1} \\ \vdots & \vdots & \ddots & \vdots \\ s_{N-1}^0 & s_{N-1}^1 & \cdots & s_{N-1}^{M-1} \end{pmatrix}.$$

An interleaved sequence $u = (u_h)$ of period MN is obtained by concatenating the successive rows and defined by

$$u_{iM+j} = U_{i,j}, 0 \le i < N, 0 \le j < M.$$

The sequence u is denoted by

$$u = I(s^0, s^1, \ldots, s^{M-1})$$

for simplicity.

Recently, using Ding-Helleseth-Lam sequences defined in [2] and a binary sequence $\mathbf{b} = (b(0), b(1), b(2), b(3))$ with $b(0) = b(2)$, $b(1) = b(3)$, Su et al. [8] constructed a new class of binary sequences of period $4p$ with optimal autocorrelation magnitude by interleaving operator. Later, Fan [3] proved that the linear complexity of these sequences is close to the maximum.

The 2-adic complexity of binary sequences with good autocorrelation has not been studied so fully as the linear complexity. The 2-adic complexity of sequences in Type (1) was studied in [6, 13, 15]. Very recently, the 2-adic complexity of Ding-Helleseth-Martinsen sequence with period $2p$ in Type (3) was determined in [19] by using "Gauss periods" and "Gauss sum" on finite field $\mathbb{F}_q$ valued in the ring $\mathbb{Z}_{2^{2p}-1}$. The 2-adic complexity of some other sequences with good autocorrelation was studied in [5, 9, 10, 11, 14, 16]. Specially, Sun et al. [11] presented the 2-adic complexity of the upper and lower bounds of interleaved sequence u constructed from [8] when $\mathbf{b} = (b(0), b(1), b(2), b(3)) = (0, 1, 0, 1)$ by using Hu's method [6] that associates with the autocorrelation function. In the conclusion of their paper, they guessed the upper bound can be arrived which means $\gcd(u(2), 2^{2p}+1) = 5$ where $u(x) = u_0 + u_1 x + \cdots + u_{4p-1}x^{4p-1}$.

In this paper, we prove the guess in [11] is right inspired by [19]. Furthermore, we determine the exact value of the 2-adic complexity of other interleaved sequences constructed in [8] with binary sequence $\mathbf{b} = (b(0), b(1), b(2), b(3))$ satisfying $b(0) = b(2)$, $b(1) = b(3)$.

2 Preliminaries

In this section, we will introduce some notations and well-known results.

From now on, we adopt the following notation without special explanation.

• Let $u = (u_0, u_1, \ldots, u_{N-1})$ be a binary sequence of period N. The set

$$B_u = \{t \in \mathbb{Z}_N : u_t = 1\}$$

is called the support of u.

• $U(x) = \sum_{i=0}^{N-1} u_i x^i \in \mathbb{Z}[x]$, $T(x) = \sum_{i=0}^{N-1} (-1)^{u_i} x^i$.

• $u + 1$ is defined by $u + 1 = (u_0 + 1, u_1 + 1, \ldots, u_{N-1} + 1)$.

• The cyclic left shift operator of u is defined by

$$L^e(u) = (u_e, u_{e+1}, \ldots, u_{N-1}, u_0, \ldots, u_{e-1}),$$

where $0 \le e \le N - 1$.

• d is a positive integer satisfying $4d \equiv 1 \pmod{p}$.

• Let g be a primitive root of p. Define $D_j = \{g^{j+4i} : 0 \le i \le \frac{p-1}{4} - 1\}$ for $0 \le j \le 3$.

• Let s^1, s^2, s^3 be the Ding-Helleseth-Lam sequences of period p with supports $D_0 \cup D_1$, $D_0 \cup D_3$, $D_1 \cup D_2$, respectively, where $p = 4f + 1 = x^2 + 4y^2$ is a prime number, f is odd and $y = \pm 1$.

• "gcd" denotes the greatest common divisor.

By using the interleaved operator, Su, Yang and Fan [8] designed binary sequence of period $4p$ with autocorrelation magnitude. The following result was given by them.

Lemma 2.1([8]) Let $\mathbf{b} = (b(0), b(1), b(2), b(3))$ be a binary sequence with $b(0) = b(2), b(1) = b(3)$. Then the binary sequence of period $4p$ constructed by

$$u = I(s^3 + b(0), L^d(s^2) + b(1), L^{2d}(s^1) + b(2), L^{3d}(s^1) + b(3))$$

is optimal with respect to the autocorrelation magnitude, i.e., $C_u(\tau) \in \{0, \pm 4\}$ for all $0 < \tau < 4p$.

Assume that

$$\frac{U(2)}{2^N-1} = \frac{\sum_{i=0}^{N-1} u_i 2^i}{2^N-1} = \frac{a}{e}, 0 \le a \le e, \gcd(a,e) = 1.$$

Then the 2-adic complexity $\Phi_2(u)$ [17] is defined by $\log_2 \frac{2^N-1}{\gcd(2^N-1, U(2))}$. Therefore, determining $\Phi_2(u)$ is equivalent to determining $\gcd(2^N-1, U(2))$.

3 Main result

In this section, we study the 2-adic complexity of the binary sequence u with optimal autocorrelation magnitude in Lemma 2.1. Firstly, for a sequence u constructed with $\mathbf{b} = (b(0), b(1), b(2), b(3)) = (0,1,0,1)$, we prove that the guess $\gcd(U(2), 2^{2p}+1) = 5$ proposed by Sun et al. in [11] is right. Then we determine the exact value of the 2-adic complexity of the sequence u defined in Lemma 2.1.

The following lemma is useful in our paper.

Lemma 3.1 $(\sum_{i\in\mathbb{F}_p^*} (\frac{i}{p}) 2^{4i})^2 \equiv p \pmod{\frac{2^{2p}+1}{5}}$, where $(\frac{i}{p})$ is the Legendre symbol defined by

$$(\frac{i}{p}) = \begin{cases} 0, & \text{if } i \equiv 0 \pmod{p}, \\ 1, & \text{if } i \not\equiv 0 \pmod{p} \text{ and } i \text{ is the square of an element of } \mathbb{F}_p^*, \\ -1, & \text{otherwise.} \end{cases}$$

Proof. Since $(\frac{i}{p})$ is a multiplicative character, we have

$$\begin{aligned}
(\sum_{i\in\mathbb{F}_p^*} (\frac{i}{p}) 2^{4i})^2 &= \sum_{a,b=1}^{p-1} (\frac{ab}{p}) 2^{4(a+b)} \\
&\equiv \sum_{a,c=1}^{p-1} (\frac{a^2 c}{p}) 2^{4a(1+c)} \text{ (let } b = ac) \\
&\equiv \sum_{a,c=1}^{p-1} (\frac{c}{p}) 2^{4a(1+c)} \\
&\equiv \sum_{c=1}^{p-1} (\frac{c}{p}) \sum_{a=1}^{p-1} 2^{4a(1+c)} \pmod{2^{4p}-1}
\end{aligned} \tag{3.1}$$

Since $p \equiv 1 \pmod 4$, we have $(\frac{-1}{p}) = 1$ and then the contribution of $c = p-1$ to the right hand side of (3.1) is

$$\sum_{a=1}^{p-1} 2^{4ap} \equiv p-1 \bmod (2^{4p}-1).$$

From $(\frac{-1}{p})=1$ we know $\sum_{c=1}^{p-2}(\frac{c}{p})=-1$ and then

$$\begin{aligned}
(\sum_{i\in\mathbb{F}_p^*}(\frac{i}{p})2^{4i})^2 &\equiv p-1+\sum_{c=1}^{p-2}(\frac{c}{p})(-1+\sum_{a=0}^{p-1}2^{4a(1+c)}) \pmod{2^{4p}-1}\\
&\equiv p-1-\sum_{c=1}^{p-2}(\frac{c}{p})+\sum_{c=1}^{p-2}(\frac{c}{p})\sum_{a=0}^{p-1}2^{4a(1+c)} \pmod{2^{4p}-1}\\
&\equiv\ p-\sum_{a=0}^{p-1}2^{4a} \pmod{2^{4p}-1}\\
&\equiv p \pmod{\frac{2^{2p}+1}{5}}.
\end{aligned}$$

□

Remark : The proof of Lemma 3.1 is similar to Lemma 2.4(1) in [19]. For the completeness of the paper, we give a proof here.

Let $\overline{\mathbf{b}}=(\overline{b(0)},\overline{b(1)},\overline{b(2)},\overline{b(3)})$ be the complement of $\mathbf{b}=(b(0),b(1),b(2),b(3))$. Let $\overline{u}$ and u be constructed with $\overline{\mathbf{b}}$ and $\mathbf{b}$ respectively in Lemma 2.1. Then $\overline{u}$ is the complement of u, i.e., $\overline{u}=u+1$. Therefore we have

$$\begin{aligned}
\overline{U}(2)=&u_0+1+(u_1+1)\cdot 2+\cdots+(u_{N-1}+1)2^{N-1}\\
=&U(2)+2^N-1\equiv U(2) \pmod{2^N-1}.
\end{aligned}$$

Thus $\gcd(\overline{U}(2),2^N-1)=\gcd(U(2),2^N-1)$ and then $\Phi_2(\overline{U})=\Phi_2(U)$.

There are four cases for $\mathbf{b}$ satisfying $b(0)=b(2),b(1)=b(3)$, i.e., $\mathbf{b}=(b(0),b(1),b(2),b(3))=(1,0,1,0),(0,1,0,1),(0,0,0,0),(1,1,1,1)$. In order to determine the 2-adic complexity of the sequence with optimal autocorrelation magnitude in Lemma 2.1, we only need to consider the 2-adic complexity of u' and u'' constructed with $\mathbf{b}=(b(0),b(1),b(2),b(3))=(0,1,0,1)$ and $(0,\ 0,\ 0,\ 0)$, respectively.

In the following, we will denote by u' and u'' the sequence constructed with $\mathbf{b}=(b(0),b(1),b(2),b(3))=(0,1,0,1)$, and $(0,\ 0,\ 0,\ 0)$ in Lemma 2.1, respectively. Denote $U(x),T(x)$ by $U'(x),T'(x)$ and $U''(x),T''(x)$ for u' and u'', respectively.

We determine the 2-adic complexity of u'. The following two lemmas have been proved by Sun et al. in [11].

Lemma 3.2 ([11]) Let the symbols be the same as before. Then

$$\begin{aligned}
&U'(2)T'(2^{-1})\\
&\equiv 2\left[\frac{2^{4p}-1}{2^4-1}+(2^{2p}+1)(2^p-1)-2^p(2^{2p}-1)y\sum_{i\in\mathbb{F}_p^*}(\frac{i}{p})2^{4i}-p\right] \pmod{2^{4p}-1}.
\end{aligned}$$

Lemma 3.3([11]) $\gcd(U'(2), 2^{2p}-1) = 1$ and $5|\gcd(U'(2), 2^{2p}+1)$.

The following theorem shows that the guess of Sun et al. in [11] is right.

Theorem 3.4 For the sequence u', we have $\gcd(U'(2), 2^{2p}+1) = 5$.

Proof. (i) Assume that $p \neq 5$.

From Lemma 3.2 we get

$$U'(2)T'(2^{-1}) \equiv 2[-2^p(2^{2p}-1)y\sum_{i\in\mathbb{F}_p^*}(\frac{i}{p})2^{4i} - p] \pmod{\frac{2^{2p}+1}{5}}.$$

Suppose that $U'(2)$ and $\frac{2^{2p}+1}{5}$ have a common prime factor l. Then

$$\begin{aligned} 0 \equiv U'(2)T'(2^{-1}) &\equiv 2[-2^p(2^{2p}-1)y\sum_{i\in\mathbb{F}_p^*}(\frac{i}{p})2^{4i} - p] \pmod{l} \\ &\equiv 2[-2^p(-2)y\sum_{i\in\mathbb{F}_p^*}(\frac{i}{p})2^{4i} - p] \pmod{l}. \end{aligned}$$

Therefore $2^{p+1}y\sum_{i\in\mathbb{F}_p^*}(\frac{i}{p})2^{4i} - p \equiv 0 \pmod{l}$. From $y = \pm 1$ we get

$$2^{2p+2}(\sum_{i\in\mathbb{F}_p^*}(\frac{i}{p})2^{4i})^2 - p^2 \equiv 0 \pmod{l}.$$

From Lemma 3.1 we get $0 \equiv 2^{2p+2}p - p^2 \equiv -4p - p^2 \pmod{l}$ which implies that $l = p$ or $l|p+4$. If $l = p$, by Fermat's Little Theorem, we get $0 \equiv 2^{2p}+1 \equiv 5 \pmod{p}$ which contradicts to the assumption $p \neq 5$. If $l|p+4$, from $2^{2p} \equiv -1 \pmod{l}$ we know that $l \neq 3$ and the order D of $2 \pmod{l}$ is 4 or $4p$. From $D|l-1$ and $l|p+4$ we know that $D \neq 4p$. From $p \neq 5$ and

$$\frac{2^{2p}+1}{5} = [1 + (-2^2) + \cdots + (-2^2)^{p-2} + (-2^2)^{p-1}] \equiv p \pmod{5},$$

we have $\gcd(\frac{2^{2p}+1}{5}, 5) = 1$ which implies that $l \neq 5$. If $D = 4$, then $0 \equiv 2^4 - 1 \equiv 15 \pmod{l}$ which contradicts to $l \neq 3, 5$. Therefore $\gcd(U'(2), \frac{2^{2p}+1}{5}) = 1$. From Lemma 3.3, we get

$$\gcd(U'(2), 2^{2p}+1) = \gcd(U'(2), \frac{2^{2p}+1}{5})\gcd(U'(2), 5) = 5.$$

(ii) Assume that $p = 5$.

From $\mathbb{F}_5^* = \langle 2 \rangle$, we know the cyclotomic classes of order 4 in $\mathbb{F}_5$ are $D_0 = \langle 1 \rangle$, $D_1 = \langle 2 \rangle$, $D_2 = \langle 4 \rangle$, $D_3 = \langle 3 \rangle$. Since s^2 is a binary sequence with support $B_{s^2} = D_0 \cup D_3$, we have $B_{L^d(s^2)} = (D_0 \cup D_3) - d$ and $B_{L^d(s^2)+1} = (D_1 \cup D_2 \cup \{0\}) - d$. From $4d \equiv 1 \pmod{p}$, we have $-d \equiv \frac{p-1}{4} \pmod{p}$. Then by the definition of u', we get

$$\begin{aligned}
U'(2) &= \sum_{i \in D_1 \cup D_2} 2^{4i} + \sum_{i \in \{\frac{p-1}{4}\} \cup (D_1 \cup D_2) + \frac{p-1}{4}} 2^{4i+1} \\
&\quad + \sum_{i \in (D_0 \cup D_1) + \frac{p-1}{2}} 2^{4i+2} + \sum_{i \in \{\frac{3(p-1)}{4}\} \cup ((D_2 \cup D_3) + \frac{3(p-1)}{4})} 2^{4i+3} \\
&= \sum_{i \in \{2,4\}} 2^{4i} + \sum_{i \in \{1,3,5\}} 2^{4i+1} + \sum_{i \in \{3,4\}} 2^{4i+2} + \sum_{i \in \{3,2,1\}} 2^{4i+3} \\
&= 2484640 \\
&\equiv \begin{cases} 15, & \pmod{25}, \\ 40, & \pmod{41}. \end{cases}
\end{aligned}$$

Then we have $\gcd(U'(2), 2^{2p}+1) = \gcd(U'(2), 2^{10}+1) = \gcd(U'(2), 25 \cdot 41) = 5$. □

Theorem 3.5 For $\mathbf{b} = (b(0), b(1), b(2), b(3)) = (0, 1, 0, 1)$ or $(1, 0, 1, 0)$, the 2-adic complexity of the sequence u defined in Lemma 2.1 is

$$\Phi_2(u) = \log_2 \frac{2^{4p}-1}{5}.$$

Proof. We need to determine $\Phi_2(u')$ only. From the definition of the 2-adic complexity, we have $\Phi_2(u') = \log_2 \frac{2^{4p}-1}{\gcd(2^{4p}-1, U'(2))}$. Since $\gcd(2^{2p}+1, 2^{2p}-1) = 1$, we know $\Phi_2(u') = \log_2 \frac{2^{4p}-1}{\gcd(2^{2p}+1, U'(2))\gcd(2^{2p}-1, U'(2))}$. From Lemma 3.3 and Theorem 3.4, we get

$$\Phi_2(u') = \log_2 \frac{2^{4p}-1}{\gcd(2^{2p}+1, U'(2))\gcd(2^{2p}-1, U'(2))} = \log_2 \frac{2^{4p}-1}{5}.$$

□

In the following, we will determine the 2-adic complexity of u'', the following two Lemmas are useful.

Lemma 3.6 ([6, 11]) Let $U(x)$ and $T(x)$ be defined in Section 2. Then for a binary sequence u with period N, we have

$$-2U(x)T(x^{-1}) \equiv N + \sum_{\tau=1}^{N-1} C_u(\tau)x^\tau - T(x^{-1})(\sum_{i=0}^{N-1} x^i) \pmod{x^N - 1}.$$

Lemma 3.7 [8] Let $\tau=\tau_1+4\tau_2$, where $\tau_1=0, 1\le\tau_2\le p-1$ or $1\le\tau_1\le 3, 0\le \tau_2\le p-1$. Then the autocorrelation function of u'' is

$$C_{u''}(\tau)=\begin{cases}-4, & \tau_1=0, \tau_2\neq 0,\\ 4, & \tau_1=1, \tau_2+d\equiv 0 \pmod p,\\ 4y, & \tau_1=1, \tau_2+d \pmod p\in D_0\cup D_2,\\ -4y, & \tau_1=1, \tau_2+d \pmod p\in D_1\cup D_3,\\ 4, & \tau_1=2, \tau_2+2d\equiv 0 \pmod p,\\ 0, & \tau_1=2, \tau_2+2d\not\equiv 0 \pmod p,\\ 4, & \tau_1=3, \tau_2+3d\equiv 0 \pmod p,\\ -4y, & \tau_1=3, \tau_2+3d \pmod p\in D_0\cup D_2,\\ 4y, & \tau_1=3, \tau_2+3d \pmod p\in D_1\cup D_3.\end{cases}$$

Lemma 3.8 Let the symbols be the same as before. Then

$$\begin{aligned}&U''(2)T''(2^{-1})\\ &\equiv 2\left[\frac{2^{4p}-1}{2^4-1}-(2^{2p}+1)(2^p+1)+2^p(2^{2p}-1)y\sum_{i\in\mathbb{F}_p^*}(\frac{i}{p})2^{4i}-p\right] \pmod{2^{4p}-1}.\end{aligned}$$

Proof. From $-d\equiv\frac{p-1}{4} \pmod p$ and Lemma 3.7, we have

$$\begin{aligned}&\sum_{\tau=1}^{4p-1}C_{u''}(\tau)2^{4\tau}\\ &=\sum_{\tau_2=1}^{p-1}C_{u''}(4\tau_2)2^{4\tau_2}+\sum_{\tau_1=1}^{3}\sum_{\tau_2=0}^{p-1}C_{u''}(\tau_1+4\tau_2)2^{\tau_1+4\tau_2}\\ &=-4\sum_{\tau_2=1}^{p-1}2^{4\tau_2}+4\cdot 2^{1+4\cdot\frac{p-1}{4}}+4y\sum_{\tau_2\in(D_0\cup D_2)+\frac{p-1}{4}}2^{1+4\tau_2}-4y\sum_{\tau_2\in(D_1\cup D_3)+\frac{p-1}{4}}2^{1+4\tau_2}\\ &\quad+4\cdot 2^{2+4\cdot\frac{p-1}{2}}+4\cdot 2^{3+4\cdot\frac{3(p-1)}{4}}-4y\sum_{\tau_2\in(D_0\cup D_2)+\frac{3(p-1)}{4}}2^{3+4\tau_2}+4y\sum_{\tau_2\in(D_1\cup D_3)+\frac{3(p-1)}{4}}2^{3+4\tau_2}\\ &\equiv -4\left[\frac{2^{4p}-1}{2^4-1}-(1+2^{2p})(2^p+1)-2^py\sum_{i\in\mathbb{F}_p^*}(\frac{i}{p})2^{4i}+2^{3p}y\sum_{i\in\mathbb{F}_p^*}(\frac{i}{p})2^{4i}\right] \pmod{2^{4p}-1}.\end{aligned}$$

From Lemma 3.6 we get

$$\begin{aligned}&U''(2)T''(2^{-1})\\ &\equiv 2\left[\frac{2^{4p}-1}{2^4-1}-(2^{2p}+1)(2^p+1)+2^p(2^{2p}-1)y\sum_{i\in\mathbb{F}_p^*}(\frac{i}{p})2^{4i}-p\right] \pmod{2^{4p}-1}.\end{aligned}$$

$\square$

Lemma 3.9 $\gcd(U''(2), 2^{2p}-1) = 3$.

Proof. From Lemma 3.8 we know

$$\begin{aligned} U''(2)T''(2^{-1}) \equiv& 2[-(1+2^{2p})(2^p+1)-p] \pmod{\frac{2^{2p}-1}{3}} \\ \equiv& 2[-2(2^p+1)-p] \pmod{\frac{2^{2p}-1}{3}}. \end{aligned}$$

Then $U''(2)T''(2^{-1}) \equiv 2(-4-p) \pmod{2^p-1}$ and $U''(2)T''(2^{-1}) \equiv -2p \pmod{\frac{2^p+1}{3}}$.

(1). We prove $\gcd(U''(2), 2^p-1) = 1$ firstly. Let l_1 be a prime divisor of $\gcd(2^p-1, -4-p)$. Then $2^p \equiv 1 \pmod{l_1}$. From Fermat's theorem, we know that $p|l_1-1$ which contradicts to $l_1|-p-4$. Therefore $\gcd(U''(2)T''(2^{-1}), 2^p-1) = \gcd(-4-p, 2^p-1) = 1$ which implies that $\gcd(U''(2), 2^p-1) = 1$.

(2). Next we prove that $\gcd(U''(2), \frac{2^p+1}{3}) = 1$. Suppose that l is a common prime divisor of $U''(2)$ and $\frac{2^p+1}{3}$. Then, by Lemma 3.8, $0 \equiv U''(2)T''(2^{-1}) \equiv -2p \pmod{l}$ so that $l = p$. From $-1 \equiv 2^p \equiv 2 \pmod{p}$ we get $p = 3$ which contradicts to $p \equiv 1 \pmod{4}$. Therefore $\gcd(U''(2), \frac{2^p+1}{3}) = 1$.

(3). At last, we prove $3|U''(2)$. By the definition of $U''(2)$, we get

$$\begin{aligned} U''(2) =& \sum_{i\in D_1\cup D_2} 2^{4i} + \sum_{i\in D_0\cup D_3} 2^{4(i+\frac{p-1}{4})+1} + \sum_{i\in D_0\cup D_1} 2^{4(i+\frac{p-1}{2})+2} + \sum_{i\in D_0\cup D_1} 2^{4(i+\frac{3(p-1)}{4})+3} \\ =& \sum_{i\in D_1\cup D_2} 2^{4i} + 2^p \sum_{i\in D_0\cup D_3} 2^{4i} + 2^{2p} \sum_{i\in D_0\cup D_1} 2^{4i} + 2^{3p} \sum_{i\in D_0\cup D_1} 2^{4i} \\ \equiv& \frac{p-1}{2} - \frac{p-1}{2} + \frac{p-1}{2} - \frac{p-1}{2} \pmod{3} \\ \equiv& 0 \pmod{3}. \end{aligned}$$

From (1)-(3) we get

$$\gcd(U''(2), 2^{2p}-1) = 3 \cdot \gcd\left(\frac{U''(2)}{3}, \frac{2^p+1}{3}\right) \cdot \gcd\left(U''(2), 2^p-1\right) = 3.$$

$\square$

Lemma 3.10 $\gcd(U''(2), \frac{2^{2p}+1}{5}) = 1$ for $p \neq 5$.

The proof of this lemma is similar to Theorem 3.4, we omit it.

Lemma 3.11 $\gcd(U''(2), 2^{2p}+1) = 25$ for $p = 5$.

Proof. From $\mathbb{F}_5^* = \langle 2 \rangle$, we know the four cyclotomic classes of order four are $D_0 = \{1\}$, $D_1 = \{2\}$, $D_2 = \{4\}$ and $D_3 = \{3\}$. For a binary periodic sequence s, we have $B_{L^d(s)} = B_s - d$. From the definition of u'' we have

$$\begin{aligned}
U''(2) &= \sum_{i \in D_1 \cup D_2} 2^{4i} + \sum_{i \in D_0 \cup D_3} 2^{4(i+\frac{p-1}{4})+1} + \sum_{i \in D_0 \cup D_1} 2^{4(i+\frac{p-1}{2})+2} + \sum_{i \in D_0 \cup D_1} 2^{4(i+\frac{3(p-1)}{4})+3} \\
&= \sum_{i \in \{2,4\}} 2^{4i} + \sum_{i \in \{2,4\}} 2^{4i+1} + \sum_{i \in \{3,4\}} 2^{4i+2} + \sum_{i \in \{4,5\}} 2^{4i+3} \\
&= 9388800 \\
&\equiv \begin{cases} 0, & (\bmod\ 25), \\ 5, & (\bmod\ 41). \end{cases}
\end{aligned}$$

Then we have $25 | U''(2)$ and then from $2^{2p} + 1 = 5^2 \times 41$, we get $\gcd(U''(2), 2^{2p} + 1) = 25$. □

Theorem 3.12 For $\mathbf{b} = (b(0), b(1), b(2), b(3)) = (0, 0, 0, 0)$ or $(1, 1, 1, 1)$, the 2-adic complexity of the sequence u defined in Lemma 2.1 is

$$\Phi_2(u) = \begin{cases} \log_2 \frac{2^{4p}-1}{75}, p = 5 \\ \log_2 \frac{2^{4p}-1}{15}, p \neq 5 \end{cases}.$$

Proof. From $p \equiv 1 \pmod 4$ and $2^4 \equiv 1 \pmod 5$ we get $2^p \equiv 2 \pmod 5$. Then by the definition of u'',

$$\begin{aligned}
U''(2) &= \sum_{i \in D_1 \cup D_2} 2^{4i} + \sum_{i \in D_0 \cup D_3} 2^{4(i+\frac{p-1}{4})+1} + \sum_{i \in D_0 \cup D_1} 2^{4(i+\frac{p-1}{2})+2} + \sum_{i \in D_0 \cup D_1} 2^{4(i+\frac{3(p-1)}{4})+3} \\
&\equiv \sum_{i \in D_0 \cup D_2} 1 + \sum_{i \in D_0 \cup D_3} 2 + \sum_{i \in D_0 \cup D_1} (4 + 8) \equiv 15 \cdot \frac{p-1}{2} \equiv 0 \pmod 5.
\end{aligned}$$

If $p \neq 5$, by Lemma 3.9 and 3.10 we get $\Phi_2(u'') = \log_2(\frac{2^{4p}-1}{C})$ where

$$D = \gcd(U''(2), 2^{4p} - 1) = 5 \cdot \gcd\left(\frac{U''(2)}{5}, \frac{2^{2p}+1}{5}\right) \cdot \gcd\left(U''(2), 2^p - 1\right) = 15.$$

For $p = 5$, by Lemma 3.11 and 3.9 we get $C = \gcd(U''(2), 2^{2p}+1) \cdot \gcd(U''(2), 2^{2p}-1) = 75$. □

At the end of this section we give an example to illustrate our main results.

Example Let $q = 13 = 3^2 + 4 \cdot 1^2$, $\mathbb{F}_{13}^* = \langle 2 \rangle$. The cyclotomic classes of order 4 in $\mathbb{F}_{13}$ are $D_0 = \{1, 3, 9\}$, $D_1 = \{2, 5, 6\}$, $D_2 = \{4, 10, 12\}$, $D_3 = \{7, 8, 11\}$. Let

$\mathbf{b} = (b(0), b(1), b(2), b(3)) = (0, 1, 0, 1)$. From the definition of the sequence u in Lemma 2.1, we have

$$
\begin{aligned}
U'(2) = & \sum_{i\in D_1\cup D_2} 2^{4i} + \sum_{i\in\{\frac{p-1}{4}\}\cup((D_1\cup D_2)+\frac{p-1}{4})} 2^{4i+1} \\
& + \sum_{i\in(D_0\cup D_1+\frac{p-1}{2})} 2^{4i+2} + \sum_{i\in\{\frac{3(p-1)}{4}\}\cup((D_2\cup D_3)+\frac{3(p-1)}{4})} 2^{4i+3} \\
= & \sum_{i\in\{2,5,6,4,10,12\}} 2^{4i} + \sum_{i\in\{3,5,8,9,7,0,2\}} 2^{4i+1} + \sum_{i\in\{7,9,2,8,11,12\}} 2^{4i+2} + \sum_{i\in\{9,0,6,8,3,4,7\}} 2^{4i+3}.
\end{aligned}
$$

Let $\mathbf{b} = (b(0), b(1), b(2), b(3)) = (0, 0, 0, 0)$. From the definition of the sequence u in Lemma 2.1, we have

$$
\begin{aligned}
U''(2) = & \sum_{i\in D_1\cup D_2} 2^{4i} + \sum_{i\in D_0\cup D_3} 2^{4(i+\frac{p-1}{4})+1} + \sum_{i\in D_0\cup D_1} 2^{4(i+\frac{p-1}{2})+2} + \sum_{i\in D_0\cup D_1} 2^{4(i+\frac{3(p-1)}{4})+3} \\
= & \sum_{i\in D_1\cup D_2} 2^{4i} + \sum_{i\in D_0\cup D_3} 2^{4(i+3)+1} + \sum_{i\in D_0\cup D_1} 2^{4(i+6)+2} + \sum_{i\in D_0\cup D_1} 2^{4(i+9)+3} \\
= & \sum_{i\in\{2,4,5,6,10,12\}} 2^{4i} + \sum_{i\in\{1,3,9,7,8,11\}} 2^{4(i+3)+1} + \sum_{i\in\{1,3,9,2,5,6\}} 2^{4(i+6)+2} \\
& + \sum_{i\in\{1,3,9,2,5,6\}} 2^{4(i+9)+3}.
\end{aligned}
$$

Computing with magma, we have $\gcd(U'(2), 2^{52}-1) = 5$ and $\gcd(U''(2), 2^{52}-1) = 15$. Then we get $\Phi_2(u') = \log_2 \frac{2^{4p-1}}{5}$ and $\Phi_2(u'') = \log_2 \frac{2^{4p-1}}{15}$ which coincides with Theorem 3.5 and 3.12, respectively.

References

[1] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar, H. Martinsen, Almost difference sets and their sequences with optimal autocorrealtion, IEEE Trans. Inf. Theory, vol. 47, no. 7, pp. 2934-2943, 2001.

[2] C. Ding, T. Helleseth, K. Y. Lam, Several classes of sequecnes with three-level autocorrelation, IEEE Trans. Inf. Theory, vol. 45, no. 7, pp. 2606-2612, 1999.

[3] C. Fan, The linear complexity of a class of binary sequences with optimal autocorrelation, Designs, Codes and Cryptography, https://doi.org/10.1007/s10623-018-0456-7, 2018.

[4] G. Gong, Theory and applications of q-ary interleaved sequences, IEEE Trans. Inf. Theory, vol. 41, no. 2, pp. 400-411, 1995.

[5] R. Hofer, A. Winterhof, On the 2-adic complexity of the two-prime generator, IEEE Trans. Inf. Theory, vol. 64, no. 8, pp. 5957-5960, 2018.

[6] H. Hu, Comments on A new method to compute the 2-adic complexity of binary sequences, IEEE Trans. Inf. Theory, vol. 60, no. 9, pp. 5803-5804, 2014.

[7] A. Klapper and M. Goresky, Cryptanalysis based on 2-adic rational approximation, in Advances in CryptologyCRYPTO'95, vol. 963, pp. 262-273, 1995.

[8] W. Su, Y. Yang, C. Fan, New optimal binary sequences with period $4p$ via interleaving Ding-Helleseth-Lam sequences, Designs, Codes and Cryptography, http://doi.org/10.1007/s10623-017-0398-5, 2017.

[9] Y. Sun, Q. Wang and T. Yan, A lower bound on the 2-adic complexity of modified Jacobi Sequences, arXiv: 1704.01685, 2017.

[10] Y. Sun, Q. Wang and T. Yan, The exact autocorrelation distribution and 2-adic complexity of a class of binary sequences with almost optimal autocorrelation, Cryptography and Communications, vol. 10, no. 3, pp. 467-477, 2018.

[11] Y. Sun, T. Yan, Z. Chen, The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude, The 10th conference on Sequences and Their Applications, Hongkong, 2018./arXiv: 1805.0199021, 2018.

[12] X. Tang, G. Gong, New constructions of binary seqeucnes with optimal autocorrelation value/magnitue, IEEE Trans. Inf. Theory, vol. 56, no. 13, pp. 1278-1286, 2010.

[13] T. Tian, W. F. Qi, 2-Adic complexity of binary m-sequences, IEEE Trans. Inf. Theory, vol. 56, no. 1, pp. 450-454, 2010.

[14] Z. Xiao, X. Zeng, Z. Sun, 2-Adic complexity of two classes of generalized cyclotomic binary sequences, Internationl Journal of Foundations of Comput. Sci., vol. 27, no. 7, pp. 879-893, 2016.

[15] H. Xiong, L. Qu, C. Li, A new method to compute 2-adic complexity of binary sequences, IEEE Trans. Inf. Theory, vol. 60, no. 4, pp. 2399-2406, 2014.

[16] H. Xiong, L. Qu, C. Li, 2-Adic complexity of binary sequnces with interleaved structure, Finite Fields Appl., vol. 33, pp. 14-28, 2015.

[17] A. Klapper, M. Goresky, Feedback shift registers, 2-adic span, and combiners with memory, J. Cryptology, vol. 10, no. 2, pp. 111-147, 1997.

[18] N. Y. Yu, G. Gong, New binary sequences with optimal autocorrelation magnitude, IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4771-4779, 2008.

[19] L. Zhang, J. Zhang, M. Yang, K. Feng, On the 2-adic complexity of the Ding-Helleseth-Martinsen binary sequences, arXiv: 1904.05499v1, 2019.