AIMS Mathematics, 7(8): 13790–13802.
DOI: 10.3934/math.2022760
Received: 28 February 2022
Revised: 03 May 2022
Accepted: 10 May 2022
Published: 23 May 2022

http://www.aimspress.com/journal/Math

Research article

Linear complexity and 2-adic complexity of binary interleaved sequences with optimal autocorrelation magnitude

Yan Wang[1], Ying Cao[1,*], Ziling Heng[2] and Weiqiong Wang[2]

[1] School of Science, Xi'an University of Architecture and Technology, Xi'an 710055, China
[2] School of Science, Chang'an University, Xi'an 710064, China

* **Correspondence:** Email: caoying@xauat.edu.cn; Tel: 17629276014.

Abstract: A construction of binary sequences with period $4N$ and optimal autocorrelation magnitude has been investigated based on sampling and interleaving technique. We determine the exact value of the linear complexity of the constructed sequences according to the deep relationship among the characteristic polynomials, and show it is $2N + 2$. Moreover, we determine the 2-adic complexity of these sequences by the autocorrelation function, and show it can attain the maximum value. Results show that such sequences can resist both the Berlekamp-Massey attack and the Rational Approximation Algorithm, in addition are good for communication.

Keywords: binary sequences; interleaved sequences; linear complexity; 2-adic complexity; autocorrelation
Mathematics Subject Classification: 94A60, 11T22

1. Introduction

Sequences with good cryptographic properties such as optimal autocorrelation, large linear complexity and high 2-adic complexity are widely used in cryptography and communication systems [1]. The interleaved structure of sequences was introduced by Gong [2]. It is shown that the interleaving technique is effective to analyze and design sequences [3]. Linear complexity of a sequence is the length of the shortest linear feedback shift register generating the sequence, which is the criterion of the ability to resist the Berlekamp-Massey attack. Li [5] determined the linear complexity of a class of optimal autocorrelation sequences with period $4N$ based on interleaving technique. Edemskiy [6] proved that the linear complexity of interleaved sequences with period $4p$ based on Hall sequences and Legendre sequences is maximal. Fan [7] proved that this class of sequences has a large linear complexity. Zhang [8] discussed the linear complexity of two classes of binary interleaved sequences with period $4N$ with low autocorrelation. Liu [9] proved binary interleaved sequences with

period $4n$ have high linear complexity.

In 2010, Tian and Qi determined the 2-adic complexity of the m-sequence [10]. Xiong [11] proposed a new method to compute 2-adic complexity of binary sequence, and proved the 2-adic complexity of all the ideal 2-level autocorrelation sequences attained the maximum, such as twin-prime sequences, Legendre sequences etc. Hu [12] used a simpler way to prove that the 2-adic complexity of binary sequences achieves the maximum. Moreover, the 2-adic complexity of a class of binary sequences with interleaved structure optimal autocorrelation magnitude were studied in [13, 14]. Yu-Gong sequences with optimal autocorrelation magnitude of interleaved structure have been constructed by Sun [15]. Zhang [16] determined the 2-adic complexity of a class of sequences utilizing Gauss periods and quadratic Gauss sums. Qiang [17] studied the 2-adic complexity of GMW sequences and two-prime sequences with interleaved structure. Xiao [18] calculated the 2-adic complexity of binary sequences with optimal autocorrelation magnitude constructed by Tang and Gong [19]. Edemskiy [20] studied the symmetric 2-adic complexity of sequences with period $8q$ with optimal autocorrelation magnitude.

In this paper, we investigate the linear complexity and the 2-adic complexity of binary sequences with optimal autocorrelation magnitude constructed by reference [21] and show that the linear complexity of sequences with period $4N$ is $2N + 2$. Furthermore, we determine the 2-adic complexity of such sequences, and show it does reach the maximum value. The rest of the paper is organized as follows. In Section 2, we introduce some necessary notations and definitions. In Section 3, we determine the linear complexity of sequences. In Section 4, we discuss the 2-adic complexity of sequences. Section 5 concludes this paper.

2. Preliminaries

2.1. Autocorrelation function

Let N be a positive integer, $\mathbb{Z}_N = \{0, 1, \cdots, N-1\}$ be the residue class ring modulo N, and $s = (s_0, s_1, \cdots, s_{N-1})$ be a binary sequence red with period N. The autocorrelation function of binary sequence s with period N is defined by

$$AC_s(\tau) = \sum_{i=0}^{N-1} (-1)^{s_i + s_{i+\tau}} \quad (0 \le \tau \le N-1). \tag{2.1}$$

It is easy to see $AC_s(0) = N$.

A sequence s is said to have optimal autocorrelation if when $N \equiv 0, 1, 2, 3 \pmod 4$ the corresponding autocorrelation functions have range as $\{0, -4\}, \{1, -3\}, \{2, -2\}, \{-1\}$ separately for any $\tau \neq 0$.

2.2. Linear complexity

Let p be an odd prime and m be a positive integer, $\mathbb{F}_{p^m}$ be the extension field of p^m elements with characteristic p. Let $s = (s_0, s_1, \cdots, s_{N-1})$ be a sequence with period N. The linear complexity of s, denoted by $LC(s)$, is the length of the shortest feedback shift register generating s that is, the smallest positive integer L which satisfies the following recurrence relation

$$s_{t+L} = c_{L-1}s_{t+L-1} + \cdots c_1 s_{t+1} + c_0 s_t$$

for $t \geq 0, c_0, c_1, \cdots, c_{L-1} \in \mathbb{F}_{p^m}$. The minimal polynomial of s is

$$m(x) = x^L - \sum_{i=0}^{L-1} c_i x^i,$$

and the generating polynomial of s is

$$S(x) = \sum_{t=0}^{N-1} s_t x^t. \tag{2.2}$$

The following equation relates the minimal polynomial and the generating polynomial [7] of s

$$m(x) = \frac{x^N - 1}{\gcd(x^N - 1, S(x))}. \tag{2.3}$$

Moerover, the linear complexity of s can also be given by

$$LC(s) = \deg(m(x)) = N - \deg(\gcd(x^N - 1, S(x))). \tag{2.4}$$

2.3. 2-Adic complextiy

Let $s = (s_0, s_1, \cdots, s_{N-1})$ be a binary sequence with period N and put $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$. If $S(x) \neq 0$, write

$$\frac{S(2)}{2^N - 1} = \frac{\sum_{i=0}^{N-1} s_i 2^i}{2^N - 1} = \frac{a}{q}$$

with integer $1 \leq a \leq q$ and $\gcd(a, q) = 1$, then the 2-adic complexity $\Phi(s)$ of s is the real number $\lfloor \log_2 q \rfloor$. If $\gcd(S(2), 2^N - 1) = 1$, then the 2-adic complexity $\Phi(s)$ of s achieves the maximum value N.

Clearly, when $M_N = 2^N - 1$ is prime, which is called Mersenne prime, we have $\gcd(S(2), 2^N - 1) = 1$, the 2-adic complexity of such sequences is maximum. For the common situation, it is interesting to find which kind of sequence satisfies $\gcd(S(2), 2^N - 1) = 1$ or a small number.

Xiong [11] utilized the determinant of the circulant matrix sequence s to decide whether $\Phi(s) = N$.

Lemma 1. [11] Let $s = (s_0, s_1, \ldots, s_{N-1})$ be a binary sequence with period N and $P_s(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$. Put $\mathbf{A} = (a_{i,j})_{N \times N}$ be the matrix defined by $a_{i,j} = s_{(i-j) \bmod N}$, and view $\mathbf{A}$ as a matrix over the rational number set $\mathbb{Q}$. If $\det(\mathbf{A}) \neq 0$ and $\gcd(1 - 2^N, \det(\mathbf{A})) = 1$, then $\Phi(s) = N$.

By Lemma 1, we only need to compute the determinate of the circulant matrix constructed from the sequence and then verify whether $\gcd(1 - 2^N, \det(\mathbf{A})) = 1$.

Lemma 2. [12] Let $s = (s_0, s_1, \ldots, s_{N-1})$ be an ideal two-level autocorrelation sequence with period N, $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$ and $P(x) = \sum_{i=0}^{N-1} (-1)^{s_i} x^i \in \mathbb{Z}[x]$. Then

$$S(2)P(2^{-1}) \equiv -\frac{N+1}{2} \pmod{2^N - 1}$$

This shows $\gcd(S(2), 2^N - 1) = 1$, and means the 2-adic complexity of two-level autocorrelation sequence is maximum. Moreover, Hu shows that the 2-adic complexity of ideal two-level autocorrelation sequences is maximum.

2.4. Interleaved sequences

Let N be a positive integer and $s_i = (s_i(0), s_i(1), \cdots, s_i(N-1))$, $0 \le i \le T-1$ be T binary sequences with period N. Based on these T binary sequences, an $N \times T$ matrix $\mathbf{u} = \left(u_{i,j}\right)$ can be given by

$$\mathbf{u} = \begin{bmatrix} s_0(0) & s_1(0) & \cdots & s_{T-1}(0) \\ s_0(1) & s_1(1) & \cdots & s_{T-1}(1) \\ \vdots & \vdots & \ddots & \vdots \\ s_0(N-1) & s_1(N-1) & \cdots & s_{T-1}(N-1) \end{bmatrix}. \tag{2.5}$$

An interleaved sequence which is also denoted by $\mathbf{u}$ is defined by placing the sequence s_i on the ith column and concatenate the successive rows of the matrix $\mathbf{u}$. For simplicity, the interleaved sequence $\mathbf{u}$ can be written as $\mathbf{u} = I(s_0, s_1, \cdots, s_{T-1})$ where I denotes the interleaved operator and $s_0, s_1, \cdots, s_{T-1}$ are called the column sequences of $\mathbf{u}$.

The cyclic left shift operator of $\mathbf{u}$ is defined by $L^e(\mathbf{u})$, where $0 \le e \le N-1$, which means shifting e bits to the left on sequences $\mathbf{u}$.

Let $s = (s_0, s_1, \ldots, s_{N-1})$ be a binary sequence with period N with ideal autocorrelation, where $N \equiv 3 \pmod 4$. Define the interleaved sequence $\mathbf{u}$ as follows

$$\mathbf{u} = \mathbf{u}(\mathbf{a}, \mathbf{b}) = I\left(\mathbf{a}, L^{\frac{N+1}{4}}(\mathbf{b}), L^{\frac{N+1}{2}}(\overline{\mathbf{a}}), L^{\frac{3(N+1)}{4}}(\mathbf{b})\right) \tag{2.6}$$

where $\mathbf{a}$ is the even decimated sequence of binary ideal autocorrelation sequence s with period N, $\mathbf{b}$ is the odd decimated sequence of the sequence s, $\overline{\mathbf{a}}$ is the complement sequences of $\mathbf{a}$.

Let N be an odd prime. $\mathbb{Z}_N = \{0, 1, \cdots, N-1\}$ is the integer residue ring and $\mathbb{Z}_N^* = \mathbb{Z}_N \backslash \{0\}$. Let $Q_N = \left\{x^2 \bmod N | \, x \in \mathbb{Z}_N^*\right\}$ and $\overline{Q}_N = \mathbb{Z}_N^* \backslash Q_N$. There are two types of Legendre sequence l and l' with period N defined by [21]

$$l(i) = l'(i) = \begin{cases} 1, \text{if } i \in Q_N, \\ 0, \text{if } i \in \bar{Q}_N, \end{cases}$$

and $l(0) = 1$, $l'(0) = 0$.

3. Linear complexity of optimal autocorrelation sequences with period $4N$

Lemma 3. [4] Let $\mathbf{a}$ be a binary sequence with period N, and define $S_{\mathbf{a}}(x)$ to be the polynomial $S_{\mathbf{a}}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1}$.

(1) If $\mathbf{b} = L^\tau(\mathbf{a})$, then $S_{\mathbf{b}}(x) = x^{N-\tau} S_{\mathbf{a}}(x) \mod x^N - 1$.

(2) If $\mathbf{b}$ is the complement sequence of $\mathbf{a}$, then $S_{\mathbf{b}}(x) = S_{\mathbf{a}}(x) + \frac{x^N-1}{x-1}$.

(3) If $\mathbf{u} = I(\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d})$, then $S_{\mathbf{u}}(x) = S_{\mathbf{a}}(x^4) + xS_{\mathbf{b}}(x^4) + x^2 S_{\mathbf{c}}(x^4) + x^3 S_{\mathbf{d}}(x^4)$.

Lemma 4. Let N be an odd integer, and $\mathbf{a} = (s_{2i})_{i=0}^{N-1}$ and $\mathbf{b} = (s_{2i+1})_{i=0}^{N-1}$ be the even decimated sequence and odd decimated sequence of binary ideal autocorrelation sequences s respectively, where $2i$ and $2i+1$ are performed modulo N. Denote

$$\mathbf{u} = \mathbf{u}(\mathbf{a}, \mathbf{b}) = I\left(\mathbf{a}, L^{\frac{N+1}{4}}(\mathbf{b}), L^{\frac{N+1}{2}}(\overline{\mathbf{a}}), L^{\frac{3(N+1)}{4}}(\mathbf{b})\right)$$

as a binary interleaved sequence with period $4N$, and $S_{\mathbf{u}}(x) = \sum_{i=0}^{4N-1} u_i x^i \in \mathbb{F}_2[x]$. Then

$$S_{\mathbf{u}}(x) = \sum_{i=0}^{4N-1} u_i x^i = \left(1 + x^{2N}\right) \sum_{i=0}^{N-1} s_{2i} x^{4i} + \left(x^N + x^{3N}\right) \sum_{i=0}^{N-1} s_{2i+1} x^{4i} + x^{2N} \frac{x^{4N} - 1}{x^4 - 1} \pmod{x^{4N} - 1}.$$

Theorem 1. Let β be a primitive Nth root of unity in an extension field K of $\mathbb{F}_2$. Denote $S_{\mathbf{a}}(x) = \sum_{i=0}^{N-1} a_{2i} x^i$, $S_{\mathbf{b}}(x) = \sum_{i=0}^{N-1} b_{2i+1} x^i$, $S_{\mathbf{a}+\mathbf{b}}(x) = S_{\mathbf{a}}(x) + S_{\mathbf{b}}(x)$, $M_{\mathbf{a}} = \left\{1 \le \lambda \le N-1 : S_{\mathbf{a}}(\beta^\lambda) = 0\right\}$, $M_{\mathbf{b}} = \left\{1 \le \lambda \le N-1 : S_{\mathbf{b}}(\beta^\lambda) = 0\right\}$ and $M_{\mathbf{a}+\mathbf{b}} = \left\{1 \le \lambda \le N-1 : S_{\mathbf{a}+\mathbf{b}}(\beta^\lambda) = 0\right\}$. Then the linear complexity of the interleaved sequence $\mathbf{u} = \mathbf{u}(\mathbf{a}, \mathbf{b})$ is

$$LC(\mathbf{u}) = 2N + 2 - \deg\left(\gcd\left(S_{\mathbf{a}}(x), S_{\mathbf{b}}(x), \frac{x^N - 1}{x - 1}\right)\right) - \deg\left(\gcd\left(S_{\mathbf{a}+\mathbf{b}}(x), \frac{x^N - 1}{x - 1}\right)\right).$$

Proof. Since K is the splitting field of $x^N - 1$ and has characteristic 2, we have

$$x^{4N} - 1 = (x^N - 1)^4 = \prod_{\lambda=0}^{N-1} (x - \beta^\lambda)^4 = (x-1)^4 \prod_{\lambda=1}^{N-1} (x - \beta^\lambda)^4.$$

By Lemma 4 we have

$$S_{\mathbf{u}}(x) = \sum_{i=0}^{4N-1} u_i x^i = \left(\frac{x^N - 1}{x - 1}\right)^2 \left[(x-1)^2 S_{\mathbf{a}}\left(x^4\right) + x^N (x-1)^2 S_{\mathbf{b}}\left(x^4\right) + x^{2N} \left(\frac{x^N - 1}{x - 1}\right)^2\right].$$

Therefore,

$$\gcd(S_{\mathbf{u}}(x), x^{4N} - 1) = \left(\frac{x^N - 1}{x - 1}\right)^2 \cdot \gcd\left((x-1)^2 S_{\mathbf{a}}\left(x^4\right) + x^N (x-1)^2 S_{\mathbf{b}}\left(x^4\right) + x^{2N} \left(\frac{x^N - 1}{x - 1}\right)^2, \left(x^N - 1\right)^2 (x-1)^2\right).$$

Denote

$$F(x) = (x-1)^2 S_{\mathbf{a}}\left(x^4\right) + x^N (x-1)^2 S_{\mathbf{b}}\left(x^4\right) + x^{2N} \left(\frac{x^N - 1}{x - 1}\right)^2.$$

Since $F(x) \equiv x^{2N} \left(\frac{x^N - 1}{x - 1}\right)^2 \equiv N^2 x^{2N} \equiv 1 \pmod{x - 1}$, we have $\gcd(F(x), x - 1) = 1$. Then

$$\gcd(S_{\mathbf{u}}(x), x^{4N} - 1) = \left(\frac{x^N - 1}{x - 1}\right)^2 \cdot \gcd\left(F(x), \left(\frac{x^N - 1}{x - 1}\right)^2\right) = \left(\frac{x^N - 1}{x - 1}\right)^2 \gcd\left(S_{\mathbf{a}}\left(x^4\right) + x^N S_{\mathbf{b}}\left(x^4\right), \left(\frac{x^N - 1}{x - 1}\right)^2\right).$$

Denote

$$q(x) = \gcd\left(F(x), \left(\frac{x^N - 1}{x - 1}\right)^2\right) = \gcd\left(S_{\mathbf{a}}\left(x^4\right) + x^N S_{\mathbf{b}}\left(x^4\right), \left(\frac{x^N - 1}{x - 1}\right)^2\right),$$

and

$$f(x) = S_{\mathbf{a}}\left(x^4\right) + x^N S_{\mathbf{b}}\left(x^4\right),$$

then $f'(x) = N x^{N-1} S_{\mathbf{b}}\left(x^4\right) = x^{N-1} S_{\mathbf{b}}\left(x^4\right)$. Since $\left(\frac{x^N - 1}{x - 1}\right)^2 = \prod_{\lambda=1}^{N-1} \left(x - \beta^\lambda\right)^2$, then $q(x) = \prod_{\lambda=1}^{N-1} \left(x - \beta^\lambda\right)^{q_\lambda}$, $0 \le q_\lambda \le 2$. For $1 \le \lambda \le N-1$, we have $f(\beta^\lambda) = S_{\mathbf{a}}\left(\beta^{4\lambda}\right) + \beta^{\lambda N} S_{\mathbf{b}}\left(\beta^{4\lambda}\right) = S_{\mathbf{a}+\mathbf{b}}\left(\beta^{4\lambda}\right)$, we discuss the result by the following.

(1) If $S_{\mathbf{a+b}}\left(\beta^{\lambda}\right) \neq 0$, then $f(\beta^{\lambda}) \neq 0$ and $q(\beta^{\lambda}) \neq 0$, we obtain $q_{\lambda} = 0$.

(2) If $S_{\mathbf{a+b}}\left(\beta^{\lambda}\right) = 0$ and $S_{\mathbf{b}}(\beta^{\lambda}) \neq 0$, then $S_{\mathbf{a}}\left(\beta^{\lambda}\right) \neq 0$ and $f(\beta^{\lambda}) = 0$. Since $f'(\beta^{\lambda}) \neq 0$, we have $q_{\lambda} = 1$.

(3) If $S_{\mathbf{a+b}}\left(\beta^{\lambda}\right) = S_{\mathbf{b}}\left(\beta^{\lambda}\right) = 0$, then $S_{\mathbf{a}}\left(\beta^{\lambda}\right) = 0$ and $\left(x-\beta^{\lambda}\right)^2 \Big| f(x)$, we have $q_{\lambda} = 2$. Then we obtain

$$q(x) = \prod_{\substack{\lambda=1 \\ S_{\mathbf{a}}(\beta^{\lambda})=S_{\mathbf{b}}(\beta^{\lambda})=0}}^{N-1} \left(x-\beta^{\lambda}\right)^2 \cdot \prod_{\substack{\lambda=1 \\ S_{\mathbf{a}}(\beta^{\lambda})=S_{\mathbf{b}}(\beta^{\lambda})\neq 0}}^{N-1} \left(x-\beta^{\lambda}\right).$$

Then

$$\begin{aligned} LC(\mathbf{u}) &= 4N - \deg \gcd\left(S_{\mathbf{u}}(x), x^{4N}-1\right) \\ &= 4N - \deg\left(\tfrac{x^N-1}{x-1}\right)^2 \gcd\left(S_{\mathbf{a}}\left(x^4\right) + x^N S_{\mathbf{b}}\left(x^4\right), \left(\tfrac{x^N-1}{x-1}\right)^2\right) \\ &= 4N - 2(N-1) - \deg q(x) \\ &= 2N + 2 - 2|M_{\mathbf{a}} \cap M_{\mathbf{b}}| - |M_{\mathbf{a+b}} \backslash (M_{\mathbf{a}} \cap M_{\mathbf{b}})| \\ &= 2N + 2 - |M_{\mathbf{a}} \cap M_{\mathbf{b}}| - |M_{\mathbf{a+b}}| \\ &= 2N + 2 - \deg \gcd\left(S_{\mathbf{a}}(x), S_{\mathbf{b}}(x), \tfrac{x^N-1}{x-1}\right) - \deg \gcd\left(S_{\mathbf{a+b}}(x), \tfrac{x^N-1}{x-1}\right). \end{aligned}$$

Since $M_{\mathbf{a}} \cap M_{\mathbf{b}} = \left\{1 \leq \lambda \leq N-1 : S_{\mathbf{a}}(\beta^{\lambda}) = S_{\mathbf{b}}(\beta^{\lambda}) = 0\right\}$, $M_{\mathbf{a+b}} = \left\{1 \leq \lambda \leq N-1 : S_{\mathbf{a+b}}(\beta^{\lambda}) = 0\right\}$. So we have $|M_{\mathbf{a}} \cap M_{\mathbf{b}}| = \deg \gcd\left(S_{\mathbf{a}}(x), S_{\mathbf{b}}(x), \frac{x^N-1}{x-1}\right)$ and $|M_{\mathbf{a+b}}| = \deg \gcd\left(S_{\mathbf{a+b}}(x), \frac{x^N-1}{x-1}\right)$. This completes the proof of Theorem 1.

□

From Theorem 1 we obtain $LC(\mathbf{u}) \leq 2N+2$. Moreover, $LC(\mathbf{u}) = 2N+2$ if and only if $M_{\mathbf{a}} \cap M_{\mathbf{b}}$ and $M_{\mathbf{a+b}}$ are empty. It is easy to see that $M_{\mathbf{a}} \cap M_{\mathbf{b}} \subset M_{\mathbf{a+b}}$.

Theorem 2. Let $N \equiv 3 \pmod 4$ be a prime number, l_1 be the even decimated of the first type Legendre sequence, $c = L^r(l')$, $1 \leq r \leq N-1$, $\mathbf{u} = \mathbf{u}(l_1, c)$, then $LC(\mathbf{u}) = 2N+2$.

Proof. $S_l(x) = \sum_{i=1}^{N-1} x^i$, $S_{l_1} = \sum_{i=0}^{N-1} l_{2i} x^i$, $S_{l'}(x) = 1 + S_l(x)$, $S_c = x^{N-r} S_{l'}(x) (\text{mod } x^{N-1})$, $S_{l_1+c} \equiv S_{l_1} + x^{N-r}(S_l(x)+1) \pmod{x^{N-1}}$. So

$$\gcd\left(S_{l_1}(x) + x^{N-r}(S_l(x)+1), \frac{x^N-1}{x-1}\right) = 1,$$

for each λ, $1 \leq \lambda \leq N-1$,

$$S_{l_1}(\beta^{\lambda}) + \beta^{-r\lambda}(S_l(\beta^{\lambda})+1) \neq 0.$$

Therefore

$$LC(\mathbf{u}) = 2N+2.$$

□

Example 1. Let $N = 19$ and $r = 3$, the even decimated of Legendre sequence is

$$l_1 = (1,0,1,1,0,0,0,0,1,0,1,0,1,1,1,1,0,0,1),$$

and the modified Legendre sequence is

$$c = \mathrm{L}^3(l') = (0,1,1,1,1,0,1,0,1,0,0,0,0,1,1,0,0,1,0).$$

Then the new binary interleaved sequence

$$\mathbf{u} = I(l_1, L^{\frac{N+1}{4}}(c), L^{\frac{N+1}{2}}(\overline{l_1}), L^{\frac{3(N+1)}{4}}(c))$$

with period $4N = 76$ defined in Theorem 1 is

$$\mathbf{u} = (1,0,0,0,0,1,1,0,1,0,0,1,1,1,0,0,0,0,0,0,0,0,0,1,0,0,1,1,0,0,1,1,1,1,0,1,0,\\ 1,0,0,1,0,1,1,0,0,0,0,1,1,0,1,1,0,1,0,1,0,1,0,1,1,1,0,0,1,1,0,0,1,0,1,1,1,1,1).$$

By Magma program, the linear complexity of this sequence is $LC(\mathbf{u}) = 40$, which are compatible with the results given by Theorem 2.

Table 1 shows the comparison of linear complexity of binary interleaved sequences with period $T \equiv 0 (\mathrm{mod}\ 4)$.

Table 1. Comparison of linear complexity.

Sequence	Period	Linear complexity
$a = I(s^1, L^d(\overline{s^1}), s^2, L^d(\overline{s^2}))$[8]	$4N$	$2N$
$a = I(s^1, L^d(\overline{s^1}), \overline{s^2}, L^d(s^2))$[8]	$4N$	$2N+1$
$w = I(a, L^m(b), L^{2m}(a), L^{3m}(\overline{b}))$[9]	$4n$	$2n+2$
$\mathbf{u} = I(\mathbf{a}, L^{\frac{N+1}{4}}(\mathbf{b}), L^{\frac{N+1}{2}}(\overline{\mathbf{a}}), L^{\frac{3(N+1)}{4}}(\mathbf{b}))$[this paper]	$4N$	$2N+2$

4. 2-Adic complexity of optimal autocorrelation sequences with period $4N$

Lemma 5. [23] Let $\mathbf{u} = I\left(\mathbf{a}, L^{\frac{N+1}{4}}(\mathbf{b}), L^{\frac{N+1}{2}}(\overline{\mathbf{a}}), L^{\frac{3(N+1)}{4}}(\mathbf{b})\right)$ be binary interleaved sequence. For $\tau = 4\tau_1 + \tau_2$ where $0 \le \tau_2 < 4$ and $0 \le \tau_1 < N$, the autocorrelation value of the sequence $\mathbf{u}$ is

$$AC(\tau) = \begin{cases} 4N, \tau_1 = 0, \tau_2 = 0, \\ -4, 0 < \tau_1 < N, \tau_2 = 0, \\ 0, 0 \le \tau_1 < N, \tau_2 = 1,2,3. \end{cases}$$

Lemma 6. [22] Let s be a binary sequence with period N, $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$, $P(x) = \sum_{i=0}^{N-1} (-1)^{s_i} x^i \in \mathbb{Z}[x]$. Then

$$-2S(x)P\left(x^{-1}\right) \equiv N + \sum_{\tau=1}^{N-1} AC(\tau)x^{\tau} - P\left(x^{-1}\right)\sum_{i=0}^{N-1} x^i \left(\mathrm{mod}\ x^N - 1\right).$$

Lemma 7. Let $\mathbf{u}$ be a binary sequence with period $4N$, $U(x) = \sum_{i=0}^{4N-1} u_i x^i \in \mathbb{Z}[x]$ and $T(x) = \sum_{i=0}^{4N-1} (-1)^{u_i} x^i \in \mathbb{Z}[x]$. Then

$$U(2)\,T\left(2^{-1}\right) \equiv -2\left(N+1-\frac{2^{4N}-1}{15}\right)\left(\mathrm{mod}\ 2^{4N}-1\right).$$

Proof. From Lemma 6, we obtain

$$\begin{aligned}-2U(2)\,T\left(2^{-1}\right) &\equiv 4N+\sum_{\tau=1}^{4N-1} AC(\tau)2^{\tau}-T\left(2^{-1}\right)\sum_{i=0}^{4N-1}2^{i}\\ &\equiv 4N+\sum_{\tau=1}^{4N-1} AC(\tau)2^{\tau}\left(\mathrm{mod}\ 2^{4N}-1\right).\end{aligned}$$

Since $\gcd\left(2,2^{4N}-1\right)=1$, the equation above can be simplified into

$$U(2)\,T\left(2^{-1}\right) \equiv -2N-\tfrac{1}{2}\sum_{\tau=1}^{4N-1} AC(\tau)2^{\tau}\left(\mathrm{mod}\ 2^{4N}-1\right).$$

By utilizing Lemma 5, we obtain

$$\begin{aligned}\sum_{\tau=1}^{4N-1} AC(\tau)\,2^{\tau} &= \sum_{\tau_1=1}^{N-1}\sum_{\tau_2=1}^{3} AC(\tau)2^{4\tau_1+\tau_2}\\ &= -4\sum_{\tau_1=1}^{N-1}2^{4\tau_1}\\ &= -4\left(\tfrac{1-2^{4N}}{1-2^{4}}-1\right).\end{aligned}$$

Thus,

$$\begin{aligned}U(2)\,T\left(2^{-1}\right) &= -2N+2\left(\tfrac{2^{4N}-1}{2^{4}-1}-1\right)\\ &\equiv -2(N+1)+2\tfrac{2^{4N}-1}{2^{4}-1}\left(\mathrm{mod}\ 2^{4N}-1\right)\\ &\equiv -2\left(N+1-\tfrac{2^{4N}-1}{15}\right)\left(\mathrm{mod}\ 2^{4N}-1\right).\end{aligned}$$

□

Lemma 8. Let N be an odd prime.

(1) If $N\neq 3$, then $3|\,2^{N}+1$, $9\nmid 2^{N}+1$.

(2) If $N>3$, then $15|\,2^{4N}-1$, $9\nmid 2^{4N}-1$; if $N>5$, then $25\nmid 2^{4N}-1$.

Proof. (1) Obviously, $3|\,2^{N}+1$, it follows that $2^{N}\equiv -1\,(\mathrm{mod}\ 3)$. Since

$$\frac{2^{N}+1}{3}=\frac{3\left(1-2+2^{2}-2^{3}+\cdots-2^{N-1}\right)}{3}\equiv N\,(\mathrm{mod}\ 3),$$

we have $\gcd\left(\frac{2^{N}+1}{3},3\right)=\gcd(N,3)=1$, if $N\neq 3$, which shows $9\nmid 2^{N}+1$.

(2) $3|\,2^{4N}-1$ and $5|\,2^{4N}-1$ are easily derived by $15|\,2^{4N}-1$. Since

$$\frac{2^{4N}-1}{3}\equiv\frac{\left(2^{2}-1\right)\left(2^{2}+1\right)\left(1+2^{4}+2^{4\cdot 2}+\cdots+2^{4\cdot(N-1)}\right)}{2^{2}-1}\equiv 5N\,(\mathrm{mod}\ 3),$$

we have $\gcd\left(\frac{2^{4N}-1}{3},3\right)=\gcd(5N,3)=1$, when $N>3$. Therefore $\gcd\left(2^{4N}-1,9\right)=3$ and $9\nmid 2^{4N}-1$. Since $5\left|2^{4N}-1\right.$, it follows that $2^{4N}\equiv 1\,(\mathrm{mod}\ 5)$.

Similarly,

$$\frac{2^{4N}-1}{5} \equiv \frac{\left(2^2-1\right)\left(2^2+1\right)\left(1+2^4+2^{4\cdot 2}+\cdots+2^{4\cdot(N-1)}\right)}{2^2+1} \equiv 3N \,(\mathrm{mod}\, 5),$$

we have $\gcd\left(\frac{2^{4N}-1}{5}, 5\right) = 1$, $\gcd\left(2^{4N}-1, 25\right) = 1$ and $25 \nmid 2^{4N}-1$ when $N > 5$.

□

Lemma 9. Let N be a prime satisfying $N \equiv 3 \,(\mathrm{mod}\, 4)$, and $T = 4N$. Then $\gcd\left(N+1-\frac{2^{4N}-1}{15}, 2^{2N}-1\right) = 1$.

Proof. It is clear that

$$\gcd\left(N+1-\frac{2^{4N}-1}{15}, 2^{4N}-1\right) = \gcd\left(N+1-\frac{2^{4N}-1}{15}, 2^{2N}-1\right)\gcd\left(N+1-\frac{2^{4N}-1}{15}, 2^{2N}+1\right).$$

Since $\frac{2^{4N}-1}{15} = \frac{2^{2N}+1}{5} \cdot \frac{2^N+1}{3} \cdot \left(2^N-1\right)$, we have $2^N-1 \Big| \frac{2^{4N}-1}{15}$ and $2^N+1 \Big| \frac{2^{4N}-1}{5}$. Thus

$$N+1-\frac{2^{4N}-1}{15} \equiv \begin{cases} N+1 \left(\mathrm{mod}\ 2^N-1\right), \\ N+1-\frac{2^{4N}-1}{15} \left(\mathrm{mod}\ 2^N+1\right). \end{cases}$$

Firstly, $\gcd\left(N+1, 2^{2N}-1\right) = 1$, which suggests both $\gcd\left(N+1, 2^N-1\right) = 1$ and $\gcd\left(N+1, 2^N+1\right) = 1$. Now we show that $\gcd\left(N+1, 2^N-1\right) = 1$. Let r be an odd prime factor of $\gcd\left(N+1, 2^N-1\right)$. Since $r \mid 2^N-1$, we get $2^N \equiv 1 \bmod r$, which is only possible if $\mathrm{ord}_r 2 = N$. Moreover, we have $N \mid r-1$ by the Fermat's little theorem. However $r \mid N+1$, we have a contradiction. Therefore, $\gcd\left(N+1, 2^N-1\right) = 1$. Then show that $\gcd\left(N+1-\frac{2^{4N}-1}{15}, 2^N+1\right) = 1$. If $N = 3$, by a simple calculation, we can verify that $3 \nmid N+1-\frac{2^{4N}-1}{15}$. On the other hard, we have $3 \mid 2^N+1$ and $\frac{2^N+1}{3} \Big| \frac{2^{4N}-1}{15}$, so we get

$$\gcd\left(N+1-\frac{2^{4N}-1}{15}, 2^N+1\right) = \gcd\left(N+1-\frac{2^{4N}-1}{15}, \frac{2^N+1}{3}\right) = \gcd\left(N+1, \frac{2^N+1}{3}\right).$$

Suppose r is an odd prime factor of $\gcd\left(N+1, \frac{2^N+1}{3}\right)$. Since $r \mid \frac{2^N+1}{3}$, it follows that $2^N \equiv -1 \,(\mathrm{mod}\, r)$. Then we have $2^{2N} \equiv 1 \,(\mathrm{mod}\, r)$, which suggests $\mathrm{ord}_r 2 = 2$ or $2N$. If $\mathrm{ord}_r 2 = 2$, then $r = 3$. Since $3 \mid \frac{2^N+1}{3}$, $9 \mid 2^N+1$, which contradicts to Lemma 8. If $\mathrm{ord}_r 2 = 2N$, then $2N \mid r-1$ by the Fermat's little theorem, so $N \le \frac{r-1}{2}$. While $r \mid N+1$, we deduce a contradiction. Therefore, $\gcd\left(N+1-\frac{2^{4N}-1}{15}, 2^{2N}-1\right) = 1$.

□

Lemma 10. Let N be a prime satisfying $N \equiv 3 \,(\mathrm{mod}\, 4)$, and $T = 4N$. Then $\gcd\left(N+1-\frac{2^{4N}-1}{15}, 2^{2N}+1\right) = 1$.

Proof. Firstly, note that $3 \nmid 2^{2N}+1$, hence 3 is not an odd prime factor of $\gcd\left(N+1-\frac{2^{4N}-1}{15}, 2^{2N}+1\right)$. Let m be a common prime factor of both $N+1-\frac{2^{4N}-1}{15}$ and $2^{2N}+1$. If $m = 5$, we claim that for any prime N we have $5 \nmid N+1-\frac{2^{4N}-1}{15}$. Then we will show that $\gcd\left(N+1-\frac{2^{4N}-1}{15}, 2^{2N}+1\right)$ has no prime factors greater than 5.

Let $m > 5$ be a common prime factor of both $N+1-\frac{2^{4N}-1}{15}$ and $2^{2N}+1$. From $m \mid 2^{2N}+1$ it follows that $m \mid 2^{4N}-1$. And since $m > 5$, we obtain $m \mid \frac{2^{4N}-1}{15}$ and hence $m \mid N+1$. Moreover, since $m \left| 2^{2N}+1 \right.$,

we get $2^{2N} \equiv -1 (\text{mod } m)$ and $2^{4N} \equiv 1 (\text{mod } m)$, which suggests $\text{ord}_m 2 = 4$ or $4N$. If $\text{ord}_m 2 = 4$, we have $m = 5$, which contradicts to $m > 5$. If $\text{ord}_m 2 = 4N$, then we have $4N \,|m-1$, i.e., $N \leq \frac{m-1}{4}$. Since we have showed $m \,|N+1$, then $N \leq \frac{m-1}{4}$, we arrive a contradiction. The proof is completed.

□

Theorem 3. Let $\mathbf{u} = I\left(\mathbf{a}, L^{\frac{N+1}{4}}(\mathbf{b}), L^{\frac{N+1}{2}}(\overline{\mathbf{a}}), L^{\frac{3(N+1)}{4}}(\mathbf{b})\right)$ be the sequence with period $4N$ defined in (2.6). Then the 2-adic complexity $\Phi(\mathbf{u})$ of sequence $\mathbf{u}$ is given by

$$\Phi(\mathbf{u}) = \log_2(2^{4N} - 1).$$

Proof. To obtain the 2-adic complexity of sequences $\mathbf{u}$, it suffices to determine $\gcd\left(U(2), 2^{4N} - 1\right)$. Since

$$\gcd\left(U(2), 2^{4N} - 1\right) \Big| \gcd\left(U(2) T\left(2^{-1}\right), 2^{4N} - 1\right),$$

from Lemmas 9 and 10, we have

$$\gcd\left(N + 1 - \frac{2^{4N} - 1}{15}, 2^{2N} - 1\right) = 1$$

and

$$\gcd\left(N + 1 - \frac{2^{4N} - 1}{15}, 2^{2N} + 1\right) = 1.$$

It follows that $\gcd\left(U(2) T\left(2^{-1}\right), 2^{4N} - 1\right) = 1$ and we have $\gcd\left(U(2), 2^{4N} - 1\right) = 1$.

□

Example 2. Let

$$l = (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$$

be a sequence with period $N = 19$. Then the binary interleaved sequence $\mathbf{u} = I\left(\mathbf{a}, L^{\frac{N+1}{4}}(\mathbf{b}), L^{\frac{N+1}{2}}(\overline{\mathbf{a}}), L^{\frac{3(N+1)}{4}}(\mathbf{b})\right)$ with period $4N$ is

$$\begin{aligned}\mathbf{u} = (&1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1,\\ &0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1,\\ &0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1).\end{aligned}$$

By Magma, $\gcd\left(U(2), 2^{76} - 1\right) = 1$ and the 2-adic complexity of $\mathbf{u}$ is $\Phi(\mathbf{u}) = \log_2 \frac{2^{76}-1}{\gcd\left(U(2), 2^{76}-1\right)} = \log_2\left(2^{76} - 1\right)$, which is consistent with the Theorem 1.

Example 3. Let

$$\begin{aligned}l = (&1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1,\\ &0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)\end{aligned}$$

be a sequence with period $N = 59$. Then the binary interleaved sequence $\mathbf{u} =$

$I\left(\mathbf{a}, L^{\frac{N+1}{4}}(\mathbf{b}), L^{\frac{N+1}{2}}(\overline{\mathbf{a}}), L^{\frac{3(N+1)}{4}}(\mathbf{b})\right)$ with period $4N$ is

$$\begin{aligned}\mathbf{u} = (&1,0,1,0,1,0,0,0,1,0,1,1,1,1,1,0,1,0,1,0,0,0,0,1,0,0,1,0,1,0,\\ &0,1,1,1,1,0,1,1,0,1,1,0,0,1,0,0,1,1,1,0,0,0,1,0,0,1,1,0,1,1,\\ &0,1,1,0,0,1,1,1,1,1,0,0,0,1,1,0,0,1,1,0,1,0,1,1,0,0,1,0,1,1,\\ &0,1,0,1,0,0,1,1,1,1,1,1,1,1,1,0,1,0,0,1,1,1,1,1,1,1,1,1,0,0,\\ &0,0,0,0,1,0,0,0,0,1,0,1,0,0,0,0,0,0,1,0,1,1,1,0,0,0,0,0,1,1,\\ &0,1,0,0,0,1,1,1,0,0,1,1,1,0,0,1,0,0,1,0,0,0,1,1,0,0,0,1,1,1,\\ &0,0,1,1,0,1,0,1,1,0,1,1,0,0,1,1,0,0,0,0,0,1,1,0,0,0,0,1,1,1,\\ &1,1,1,0,0,1,0,1,0,1,0,1,0,0,0,0,1,1,0,1,0,1,0,1,0,1)\,.\end{aligned}$$

By Magma, $\gcd\left(U(2), 2^{236}-1\right) = 1$ and the 2-adic complexity of $\mathbf{u}$ is $\Phi(\mathbf{u}) = \log_2 \frac{2^{236}-1}{\gcd\left(U(2),2^{236}-1\right)} = \log_2\left(2^{236}-1\right)$, which is consistent with the Theorem 1.

5. Conclusions

In this paper, we investigate the linear complexity and 2-adic complexity of a class of binary sequences with period $4N$ and optimal autocorrelation magnitude. This sequence is obtained by even and odd sampling from Legendre sequence. We show that the linear complexity of binary sequences with period $4N$ is $2N + 2$. Our results show that these sequences are safe enough to resist the attacks by the Rational Approximation algorithm and the Berlekamp-Massey algorithm. By discussing some great common divisors according to Hu [12], we determine that the 2-adic complexity of the sequence can reach the maximum value $\log_2(2^{4N} - 1)$. Our results show that these sequences are safe enough to resist attacks of the rational approximation algorithm.

Acknowledgments

The work of Y. Wang was supported by the National Natural Science Foundation of China under Grant 61902304. The work of Z. Heng was supported by the National Natural Science Foundation of China under Grant 11901049.

Conflict of interest

The authors declare no conflict of interest.

References

1. T. W. Cusick, C. Ding, A. Renvall, *Stream ciphers and number theory*, Amsterdam: Elsevier, 2004.
2. G. Guang, Theory and applications of q-ary interleaved sequences, *IEEE T. Inform. Theory*, **41** (1995), 400–411. https://doi.org/10.1109/18.370141
3. S. W. Golomb, G. Gong, *Signal design for good correlation: For wireless communication, cryptography, and radar*, Cambridge: Cambridge University Press, 2005.

4. Q. Wang, X. Du, The linear complexity of binary sequences with optimal autocorrelation, *IEEE T. Inform. Theory*, **56** (2010), 6388–6397. https://doi.org/10.1109/TIT.2010.2079550
5. N. Li, X. Tang, On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation value/magnitude, *IEEE T. Inform. Theory*, **57** (2011), 7597–7604. https://doi.org/10.1109/TIT.2011.2159575
6. V. Edemskiy, On the linear complexity of interleaved binary sequences of period $4p$ obtained from Hall sequences or Legendre and Hall sequences, *Electron. Lett.*, **50** (2014), 604–605. https://doi.org/10.1049/el.2014.0568
7. C. Fan, The linear complexity of a class of binary sequences with optimal autocorrelation, *Design. Code. Cryptogr.*, **86** (2018), 2441–2450. https://doi.org/10.1007/s10623-018-0456-7
8. S. Zhang, T. Yan, Y. Sun, L. Wang, Linear complexity of two classes of binary interleaved sequences with low autocorrelation, *Int. J. Netw. Secur.*, **22** (2020), 150–154.
9. Q. Liu, S. Qiang, M. Yang, K. Feng, Linear complexity of binary interleaved sequences of period $4n$, *arXiv preprint*, 2021. https://doi.org/10.48550/arXiv.2105.13777
10. T. Tian, W. F. Qi, 2-Adic complexity of binary m-sequences, *IEEE T. Inform. Theory*, **56** (2009), 450–454. https://doi.org/10.1109/TIT.2009.2034904
11. H. Xiong, L. Qu, C. Li, A new method to compute the 2-adic complexity of binary sequences, *IEEE T. Inform. Theory*, **60** (2014), 2399–2406. https://doi.org/10.1109/TIT.2014.2304451
12. H. Hu, Comments on "a new method to compute the 2-adic complexity of binary sequences", *IEEE T. Inform. Theory*, **60** (2014), 5803–5804. https://doi.org/10.1109/TIT.2014.2336843
13. Y. Sun, T. Yan, Z. Chen, L. Wang, The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude, *Cryptogr. Commun.*, **12** (2020), 675–683. https://doi.org/10.1007/s12095-019-00411-4
14. M. Yang, L. Zhang, K. Feng, On the 2-adic complexity of a class of binary sequences of period $4p$ with optimal autocorrelation magnitude, *2020 IEEE Int. Sym. Inform. Theory*, 2020, 2915–2920. https://doi.org/10.1109/ISIT44484.2020.9174142
15. Y. Sun, T. Yan, Q. Wang, The 2-adic complexity of Yu-Gong sequences with interleaved structure and optimal autocorrelation magnitude, *Design. Code. Cryptogr.*, **89** (2021), 695–707. https://doi.org/10.1007/s10623-020-00841-9
16. L. Zhang, J. Zhang, M. Yang, K. Feng, On the 2-adic complexity of the Ding-Helleseth-Martinsen binary sequences, *IEEE T. Inform. Theory*, **66** (2020), 4613–4620. https://doi.org/10.1109/TIT.2020.2964171
17. S. Qiang, X. Jing, M. Yang, The 2-adic complexity of two classes of binary sequences with interleaved structure, *arXiv preprint*, 2020. https://doi.org/10.48550/arXiv.2011.12080
18. Z. Xiao, X. Zeng, 2-Adic complexity of two constructions of binary sequences with period $4N$ and optimal autocorrelation magnitude, *Cryptogr. Commun.*, **13** (2021), 865–885. https://doi.org/10.1007/s12095-021-00498-8
19. X. Tang, G. Gong, New constructions of binary sequences with optimal autocorrelation value/magnitude, *IEEE T. Inform. Theory*, **56** (2010), 1278–1286. https://doi.org/10.1109/TIT.2009.2039159

20. V. Edemskiy, Y. Sun, The symmetric 2-adic complexity of sequences with optimal autocorrelation magnitude and length 8q, *Cryptogr. Commun.*, **14** (2021), 183–199. https://doi.org/10.1007/s12095-021-00503-0

21. X. Tang, C. Ding, New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value, *IEEE T. Inform. Theory*, **56** (2010), 6398–6405. https://doi.org/10.1109/TIT.2010.2081170

22. W. Su, Y. Yang, C. Fan, New optimal binary sequences with period 4p via interleaving Ding-Helleseth-Lam sequences, *Design. Code. Cryptogr.*, **86** (2018), 1329–1338. https://doi.org/10.1007/s10623-017-0398-5

23. J. Wang, Structure and properties of binary and quaternary sequence analysis, *Huaibei Normal Univ.*, 2021.