RAIRO-Theor. Inf. Appl. 59 (2025) 9
https://doi.org/10.1051/ita/2025004

RAIRO - Theoretical Informatics and Applications
www.rairo-ita.org

LINEAR COMPLEXITY AND 2-ADIC COMPLEXITY OF NEW CYCLOTOMIC BINARY SEQUENCES OF ORDER FOUR WITH LOW AUTOCORRELATION

Xiaoyan Jing, Chaoran Zhang and Zhefeng Xu*

Abstract. A new family of binary sequences with low 4-value autocorrelation of length $4p$ based on cyclotomic classes of order four is proposed, as well as the linear complexity and 2-adic complexity of these sequences are determined. The results show that the linear complexity of s is $LC(s) = 4p - 1$, and the 2-adic complexity of s is $\Phi_2(s) = \log_2(\frac{2^{4p}-1}{3})$, both of which are greater than half of the period. The sequences are safe enough to resist Berlekamp–Massey algorithm attacks and rational approximation algorithm attacks, which indicate that they are good sequences in communication.

Mathematics Subject Classification. 94A55, 94A60.

Received August 25, 2023. Accepted July 11, 2025.

1. Introduction

Binary sequences play an important role in encrypting communications, synchronous communications, radar monitoring and other fields. In practical applications, binary sequences are required to have low autocorrelation, large linear complexity and large 2-adic complexity to resist various attacks. For a binary sequence $s = \{s_i\}_{i=0}^{N-1}$ with period N, the autocorrelation value is defined by

$$AC_s(\tau) = \sum_{i=0}^{N-1} (-1)^{s_i + s_{i+\tau}} \in \mathbb{Z} \ (0 \le \tau \le N-1).$$

If $\tau \neq 0$, we say that $AC_s(\tau)$ is nontrivial autocorrelation of s. The binary sequence s is called perfect sequence if $AC_s(\tau) = 0$ for $N \equiv 0 \pmod 4$, and the only known perfect sequence is (0111) with period of $N = 4$. The other three types of smallest possible values of the nontrivial autocorrelation are as follows:
(1). $AC_s(\tau) = -1$ for $N \equiv 3 \pmod 4$;
(2). $AC_s(\tau) \in \{1, -3\}$ for $N \equiv 1 \pmod 4$;
(3). $AC_s(\tau) \in \{2, -2\}$ for $N \equiv 2 \pmod 4$.
The binary sequences s of type (1) are called ideal sequences and the type (2) and type (3) are called the optimal sequences. There have been a lot of work on the construction of ideal autocorrelation sequences and

Keywords and phrases: Autocorrleation, binary sequences, cyclotomic classes of order four, linear complexity, 2-adic complexity.

Research Center for Number Theory and Its Applications Northwest University, Xi'an 710127, China

* Corresponding author: zfxu@nwu.edu.cn

optimal autocorrelation sequences, which we will not repeat here, but there are also a great deal of literature on the linear complexity and 2-adic complexity of these sequences, which can be seen [1–17].

The linear complexity and 2-adic complexity of a binary sequence s are defined as the length of the shortest linear feedback shift register (LFSR) and the shift feedback register with carry (FCSR) to generate the sequence, respectively. According to the Berlekamp–Massey (BM) algorithm [18] and rational approximation algorithm (RAA) [19, 20], binary sequences with linear complexity and 2-adic complexity greater than half of the period are safe in practical applications. Therefore, it is of great significance to construct binary sequences with good autocorrelation properties, large linear complexity and 2-adic complexity.

The cyclotomic classes of order four [21] is an important tool for constructing binary sequences. Let $p = 4f + 1$ be a prime, for a primitive element θ of $\mathbb{F}_p$, define $D_\theta = \langle \theta^4 \rangle$, then the cyclotomic classes of order four is defined as

$$D_j = \theta^j D_\theta = \{\theta^{j+4a} : 0 \le a \le f-1\} (0 \le j \le 3). \tag{1.1}$$

In 2001, Ding, Helleseth and Martinsen constructed two families of optimal autocorrelation binary sequences using cyclotomic classes of order four [22]. Zhang *et al.* [16] determined their linear complexity in 2015 and the results showed that the sequences have high linear complexity. After that, Zhang *et al.* [17] calculated their 2-adic complexity and explained that it exceeds half of the period. Su *et al.* [7] constructed several optimal binary sequences *via* Ding-Helleseth-Lam sequences, which were given by Ding, Helleseth and Lam based on cyclotomic classes of order four in 1999 [23]. Subsequently, Fan *et al.* [3] and Sun *et al.* [9] determined their linear complexity and 2-adic complexity, respectively, and demonstrated that the sequences are safe enough to resist BM algorithm attacks and RAA attacks.

In this paper, we propose a new family of binary sequences s with low autocorrelation of length $4p$, as well as determine their linear complexity and 2-adic complexity. The results show that the linear complexity of s is $LC(s) = 4p - 1$, and the 2-adic complexity of s is $\Phi_2(s) = \log_2(\frac{2^{4p}-1}{3})$, both of which are greater than half of the period. The following section introduces some background information and defines the sequence s. In Sections 3-5, we determine the autocorrelation values, linear complexity, and 2-adic complexity of the sequence, respectively, and provide examples to illustrate the correctness of the conclusions. The last section is a summary of the paper.

2. Preliminaries

Let $p = 4f + 1 = x^2 + 4y^2$ be a prime and f be an odd number. For $N = 4p$, we have the following isomorphism of ring by the Chinese Remainder Theorem

$$\begin{aligned} \varphi : \mathbb{Z}_4 \times \mathbb{Z}_p &\cong \mathbb{Z}_N, \\ (\alpha, \beta) &\mapsto \alpha p + (3p+1)\beta, \end{aligned}$$

and the inverse mapping of φ is $\varphi^{-1}(m) = (m \pmod 4, m \pmod p)$.

Let $a, b, c, d \in \{0, 1, 2, 3\}$ be four distinct numbers and $a \not\equiv b + 2 \pmod 4$, $a \not\equiv c + 2 \pmod 4$, $C_0 = D_a \cup D_b \cup \{0\}$, $C_1 = D_a \cup D_c \cup \{0\}$, $C_2 = D_a \cup D_b$, $C_3 = D_b \cup D_d$,

$$C = \{0\} \times C_0 \cup \{1\} \times C_1 \cup \{2\} \times C_2 \cup \{3\} \times C_3,$$

where D_j is the cyclotomic classes of order four given by (1.1). Then for $a \in C$, it is easy to see $\varphi(a) = \alpha p + (3p + 1)\beta$, where $\alpha = 0$, $\beta \in D_a \cup D_b \cup \{0\}$, $\alpha = 1$, $\beta \in D_a \cup D_c \cup \{0\}$, $\alpha = 2$, $\beta \in D_a \cup D_b$, or $\alpha = 3$, $\beta \in D_b \cup D_d$.

Definition 2.1. Let $p \equiv 5 \pmod 8$ be a prime, $p = x^2 + 4y^2$ and $y = \pm 1$. The binary sequence s with period $N = 4p$ is defined by

$$s_i = \begin{cases} 1, & \text{if } i \in \varphi(C), \\ 0, & \text{otherwise.} \end{cases} \tag{2.1}$$

In the above definition, let $C' = \varphi(C)$, then we say C' is the support of s .

Following that, we introduce the relevant lemmas for the cyclotomic numbers of order four. The cyclotomic numbers of order four in $\mathbb{F}_p$ are defined by

$$(i,j) = \mid (D_i + 1) \bigcap D_j \mid = \sharp\{(g,k) : g \in D_i, k \in D_j, g + 1 \equiv k \pmod p\} (0 \le i, j \le 3).$$

There are only five different values for the cyclotomic numbers of order four, which have been determined.

Lemma 2.2. *[21, 24] Let $p = x^2 + 4y^2 \equiv 5 \pmod 8$ be a prime with $x, y \in \mathbb{Z}$, $x \equiv 1 \pmod 4$. We have*

$$\begin{aligned}
&(0,0) = (2,2) = (2,0) = \frac{p - 7 + 2x}{16}, \\
&(0,1) = (1,3) = (3,2) = \frac{p + 1 + 2x - 8y}{16}, \\
&(1,2) = (0,3) = (3,1) = \frac{p + 1 + 2x + 8y}{16}, \\
&(0,2) = \frac{p + 1 - 6x}{16}, \\
&(1,0) = (1,1) = (2,1) = (3,0) = (3,3) = (2,3) = \frac{p - 3 - 2x}{16}.
\end{aligned}$$

3. Autocorrelation

In this section, we determine the autocorrelation of the binary sequence s defined by (2.1). First of all, we give another way to describe the autocorrelation function.

Lemma 3.1. *[25] Let $s = (s_i)_{i=0}^{N-1}$ be a binary sequence of length N with support C. Then*

$$AC_s(\tau) = N - 4(k - d_C(\tau)),$$

where $k = |C|$ and $d_C(\tau) = \mid (C + \tau) \bigcap C \mid = \sharp\{(g,k) : g \in C, k \in C, g \equiv k + \tau \pmod p\}$.

Next, we determine $d_{C'}(\tau)$.

Lemma 3.2. *Let the symbols as the same before. For $(a,b,c,d) = (0,1,3,2)$, we have*

$$d_{C'}(\tau) = \begin{cases} 2p, & \text{if } \alpha = 0,\ \beta = 0, \\ p - 2y, & \text{if } \alpha = 2,\ \beta \in D_0 \cup D_2, \\ p + 2y, & \text{if } \alpha = 2,\ \beta \in D_1 \cup D_3 \\ p - 1, & \text{if } \alpha = 0,\ \text{or } \alpha = 2,\ \beta = 0,\ \text{or } \alpha = 1,3,\ \beta \in D_2 \cup D_3, \\ p + 1, & \text{if } \alpha = 1,3,\ \beta \in D_0 \cup D_1, \\ p, & \text{if } \alpha = 1,3,\ \beta = 0. \end{cases}$$

Proof. From the definition of $d_{C'}(\tau)$ we know that

$$\begin{aligned}
d_{C'}(\tau) = d_C(\alpha,\beta) =& \mid C \cap (C+(\alpha,\beta)) \mid \\
=& \mid \{0\}\cap\{\alpha\} \mid\mid C_0\cap(C_0+\beta)\mid + \mid \{0\}\cap\{\alpha+1\}\mid\mid C_0\cap(C_1+\beta)\mid \\
&+ \mid \{0\}\cap\{\alpha+2\}\mid\mid C_0\cap(C_2+\beta)\mid + \mid \{0\}\cap\{\alpha+3\}\mid\mid C_0\cap(C_3+\beta)\mid \\
&+ \mid \{1\}\cap\{\alpha\}\mid\mid C_1\cap(C_0+\beta)\mid + \mid \{1\}\cap\{\alpha+1\}\mid\mid C_1\cap(C_1+\beta)\mid \\
&+ \mid \{1\}\cap\{\alpha+2\}\mid\mid C_1\cap(C_2+\beta)\mid + \mid \{1\}\cap\{\alpha+3\}\mid\mid C_1\cap(C_3+\beta)\mid \\
&+ \mid \{2\}\cap\{\alpha\}\mid\mid C_2\cap(C_0+\beta)\mid + \mid \{2\}\cap\{\alpha+1\}\mid\mid C_2\cap(C_1+\beta)\mid \\
&+ \mid \{2\}\cap\{\alpha+2\}\mid\mid C_2\cap(C_2+\beta)\mid + \mid \{2\}\cap\{\alpha+3\}\mid\mid C_2\cap(C_3+\beta)\mid \\
&+ \mid \{3\}\cap\{\alpha\}\mid\mid C_3\cap(C_0+\beta)\mid + \mid \{3\}\cap\{\alpha+1\}\mid\mid C_3\cap(C_1+\beta)\mid \\
&+ \mid \{3\}\cap\{\alpha+2\}\mid\mid C_3\cap(C_2+\beta)\mid + \mid \{3\}\cap\{\alpha+3\}\mid\mid C_3\cap(C_3+\beta)\mid \\
=& \begin{cases}
\mid C_0\cap(C_0+\beta)\mid + \mid C_1\cap(C_1+\beta)\mid + \mid C_2\cap(C_2+\beta)\mid + \mid C_3\cap(C_3+\beta)\mid, & \text{if } \alpha=0,\\
\mid C_0\cap(C_3+\beta)\mid + \mid C_1\cap(C_0+\beta)\mid + \mid C_2\cap(C_1+\beta)\mid + \mid C_3\cap(C_2+\beta)\mid, & \text{if } \alpha=1,\\
\mid C_0\cap(C_2+\beta)\mid + \mid C_1\cap(C_3+\beta)\mid + \mid C_2\cap(C_0+\beta)\mid + \mid C_3\cap(C_1+\beta)\mid, & \text{if } \alpha=2,\\
\mid C_0\cap(C_1+\beta)\mid + \mid C_1\cap(C_2+\beta)\mid + \mid C_2\cap(C_3+\beta)\mid + \mid C_3\cap(C_0+\beta)\mid, & \text{if } \alpha=3.
\end{cases}
\end{aligned}$$

If $\beta = 0$, we have

$$\begin{aligned}
d_{C'}(\alpha,0) =& \begin{cases}
\mid C_0\mid + \mid C_1\mid + \mid C_2\mid + \mid C_3\mid, & \text{if } \alpha=0,\\
\mid C_0\cap C_3\mid + \mid C_1\cap C_0\mid + \mid C_2\cap C_1\mid + \mid C_3\cap C_2\mid, & \text{if } \alpha=1,\\
2(\mid C_0\cap C_2\mid + \mid C_1\cap C_3\mid), & \text{if } \alpha=2,\\
\mid C_0\cap C_1\mid + \mid C_1\cap C_2\mid + \mid C_2\cap C_3\mid + \mid C_3\cap C_0\mid, & \text{if } \alpha=3,
\end{cases}\\
=& \begin{cases}
2p, & \text{if } \alpha=0,\\
p, & \text{if } \alpha=1,\\
p-1, & \text{if } \alpha=2,\\
p, & \text{if } \alpha=3.
\end{cases}
\end{aligned}$$

If $\alpha = 0,\ \beta \in D_0$ and $(a,b,c,d) = (0,1,3,2)$, combining with Lemma 3.1 we obtain

$$\begin{aligned}
& d_{C'}(\alpha,\beta)\\
=& \mid C_0\cap(C_0+\beta)\mid + \mid C_1\cap(C_1+\beta)\mid + \mid C_2\cap(C_2+\beta)\mid + \mid C_3\cap(C_3+\beta)\mid\\
=& \mid (\beta^{-1}C_0+1)\cap\beta^{-1}C_0\mid + \mid (\beta^{-1}C_1+1)\cap\beta^{-1}C_1\mid + \mid (\beta^{-1}C_2+1)\cap\beta^{-1}C_2\mid + \mid (\beta^{-1}C_3+1)\cap\beta^{-1}C_3\mid\\
=& \mid (\beta^{-1}(D_0\cap D_1\cap\{0\})+1)\cap\beta^{-1}(D_0\cap D_1\cap\{0\})\mid + \mid (\beta^{-1}(D_0\cap D_3\cap\{0\})+1)\cap\beta^{-1}(D_0\cap D_3\cap\{0\})\mid\\
&+ \mid (\beta^{-1}(D_0\cap D_1)+1)\cap\beta^{-1}(D_0\cap D_1)\mid + \mid (\beta^{-1}(D_1\cap D_2)+1)\cap\beta^{-1}(D_1\cap D_2)\mid\\
=& 2[(0,0)+(0,1)+(1,0)+(1,1)]+(0,0)+(0,3)+(3,0)+(3,3)+(1,1)+(1,2)+(2,1)+(2,2)\\
&+ \mid \{1\}\cap(D_0\cup D_1)\mid + \mid (D_0\cup D_1+1)\cap\{0\}\mid + \mid \{1\}\cap(D_0\cup D_3)\mid + \mid (D_0\cup D_3+1)\cap\{0\}\mid\\
=& p-1,
\end{aligned}$$

since $1\in D_0$ and $-1\in D_2$. The rest cases are similarly provable. □

From Lemmas 3.1 and 3.2, the following theorem is obtained.

Theorem 3.3. *Let p be a prime with $p\equiv 5 \pmod 8$, $p = x^2+4y^2$ and $y=\pm 1$. Then the autocorrelation of the binary sequence s with period $4p$ defined by (2.1) is*

$$AC_s(\tau) = \{0, \pm 4, -y8\}.$$

Example 3.4. Let $p = 5,\ (a, b, c, d) = (0, 1, 3, 2),\ \theta = 2$, the binary sequence of period $N = 20$ is

$$s = (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1).$$

Computed by Magma, we have the autocorrelation $AC_s(\tau) \in \{0, \pm 4, \pm 8\}$ as follows:

TABLE 1. Autocorrelation of s with period 20 and $(a, b, c, d) = (0, 1, 3, 2)$.

τ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$AC_s(\tau)$	4	–8	–4	–4	0	8	4	–4	–4	–4	–4	–4	4	8	0	–4	–4	–8	4

which is consist of the Theorem 3.3.

Let $(a, b, c, d) = (1, 2, 0, 3)$, then we have

$$s = (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1).$$

Computed by Magma, we have the autocorrelation $AC_s(\tau) \in \{0, \pm 4, \pm 8\}$ as follows:

TABLE 2. Autocorrelation of s with period 20 and $(a, b, c, d) = (1, 2, 0, 3)$.

τ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$AC_s(\tau)$	4	8	4	–4	0	–8	–4	–4	–4	–4	–4	–4	–4	–8	0	–4	4	8	4

which is consist of the Theorem 3.3.

4. Linear complexity

Let $s = (s_i)_{i=0}^{N-1}$ be a binary sequence with period N. The linear complexity $LC(s)$ of the sequence s is the smallest positive integer L satisfying $s_{i+L} = c_{L-1}s_{i+L-1} + \cdots + c_1 s_{i+1} + c_0 s_i$ for $L < i < N$, where the coefficients $c_0,\ c_1,\ \cdots,\ c_{L-1} \in \mathbb{F}_2$. The characteristic polynomial of s is defined as $C(x) = x^L + c_{L-1}x^{L-1} + \cdots + c_0 \in \mathbb{F}_2[x]$, where $c_0 \neq 0$. The generating polynomial of s is defined by $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{F}_2[x]$. It is well known that

$$C(x) = \frac{x^N - 1}{\gcd(x^N - 1,\ S(x))} \tag{4.1}$$

and the linear complexity of s is

$$LC(s) = N - \deg(\gcd(x^N - 1,\ S(x))). \tag{4.2}$$

By the definition of the linear complexity of binary sequences, we need to consider the greatest common divisor of generating polynomial

$$S(x) = \sum_{v \in C} x^v = \Big(\sum_{v \in \phi^{-1}(\{0\} \times C_0)} + \sum_{v \in \phi^{-1}(\{1\} \times C_1)} + \sum_{v \in \phi^{-1}(\{2\} \times C_2)} + \sum_{v \in \phi^{-1}(\{3\} \times C_3)} \Big) x^v \tag{4.3}$$

and $x^{4p} - 1$ over $\mathbb{F}_2$. In the rest of this section, we denote $S'(x)$ by the formal derivative of $S(x)$.

Lemma 4.1. *Let ξ be a primitive $p-$th root of unity in an extension field of $\mathbb{F}_p$. Then we have*

$$\sum_{v\in\cup_{i=0}^{3}D_i}\xi^v=1$$

Proof. See [16], Lemma 1. □

Lemma 4.2. *Let the symbols as the same before, then we have*

$$\sum_{v\in\varphi(\{k\}\times C_i)}\xi^v=\sum_{v\in C_i}\xi^v,$$

where $k=0,1,2,3$.

Proof. By the definition of the mapping φ and $\xi^p=1$, we have

$$\sum_{v\in\varphi(\{k\}\times C_i)}\xi^v=\sum_{t\in C_i}\xi^{kp+t(3p+1)}=\sum_{t\in C_i}\xi^t.$$

□

Lemma 4.3. *The generating polynomial $S(x)$ of s has no repeated root 1.*

Proof. To prove this lemma, we need to show that $S(1)=S'(1)=0$. By the definition of $S(x)$ and Lemma 4.2 we have

$$\begin{aligned}S(1)&=(\sum_{v\in\varphi(\{0\}\times C_0)}+\sum_{v\in\varphi(\{1\}\times C_1)}+\sum_{v\in\varphi(\{2\}\times C_2)}+\sum_{v\in\varphi(\{3\}\times C_3)})1^v\\&=\frac{p-1}{4}\times 8+1+1=2p\\&\equiv 0\pmod 2.\end{aligned}$$

From

$$\begin{aligned}S'(x)&=(\sum_{v\in\varphi(\{0\}\times C_0)}+\sum_{v\in\varphi(\{1\}\times C_1)}+\sum_{v\in\varphi(\{2\}\times C_2)}+\sum_{v\in\varphi(\{3\}\times C_3)})v\cdot x^{v-1}\\&=\sum_{v\in\varphi(\{1\}\times C_1)}x^{v-1}+\sum_{v\in\varphi(\{3\}\times C_3)}x^{v-1},\end{aligned}\tag{4.4}$$

we derive $S'(1)=\frac{p-1}{4}\times 4+1=p\equiv 1\pmod 2$ and we know that 1 is not a repeated root. □

Lemma 4.4. *Let ξ be a primitive p-th root of unity defined before. Then we have $S(\xi^u)\equiv 1\pmod 2$, where $u\in\mathbb{Z}_p^*$.*

Proof. Let $u\in\mathbb{Z}_p^*=\cup_{h=0}^{3}D_h$. If $u\in D_h$, we then infer from the definition of $S(x)$ and Lemma 4.2 that

$$\begin{aligned}S(\xi^u)&=(\sum_{v\in\varphi(\{0\}\times C_0)}+\sum_{v\in\varphi(\{1\}\times C_1)}+\sum_{v\in\varphi(\{2\}\times C_2)}+\sum_{v\in\varphi(\{3\}\times C_3)})\xi^{uv}\\&=2(\sum_{v\in D_a}+\sum_{v\in D_b})\xi^{uv}+(\sum_{v\in D_a}+\sum_{v\in D_b}+\sum_{v\in D_c}+\sum_{v\in D_d})\xi^{uv}\end{aligned}$$

$$= (\sum_{uv\in D_{a+h}} + \sum_{uv\in D_{b+h}} + \sum_{uv\in D_{c+h}} + \sum_{uv\in D_{d+h}})\xi^{uv}$$
$$= 1 \pmod 2.$$

□

Theorem 4.5. *Let p be a prime with $p \equiv 5 \pmod 8$, $p = x^2 + 4y^2$ and $y = 1$. Then the linear complexity of the binary sequence s with period $4p$ defined by (2.1) is $4p - 1$.*

Example 4.6. Let $p = 5$, $(a, b, c, d) = (0, 1, 3, 2)$, $\theta = 2$, then we have

$$s = (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1).$$

Computed by $\gcd(x^{20} - 1,\ S(x)) = x + 1$, we have linear complexity $L = 20 - 1 = 19$, which is same as Theorem 4.5.

5. 2-Adic complexity

In this section, we calculate the 2-adic complexity of the sequence s.

Let $s = (s_i)_{i=0}^{N-1}$ be a binary sequence with period N and $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$. The 2-adic complexity of s is defined as

$$\Phi_2(s) = \log_2 \left(\frac{2^N - 1}{\gcd(S(2), 2^N - 1)} \right).$$

Before the calculation, we introduce some relevant knowledge to use. Similar to the introduction in [17], let $N = 4p$, we have the following homomorphism of groups from $(\mathbb{Z}_p, +)$ to $(\mathbb{Z}^*_{2^N-1}, \cdot)$,

$$f : (\mathbb{Z}_p, +) \to (\mathbb{Z}_{2^N-1}, \times),\ f(a) = 2^{4a},$$

which can be viewed as an additive character of finite field $\mathbb{Z}_p = \mathbb{F}_p$ valued in $\mathbb{Z}^*_{2^N-1}$. As well as we have the "Gauss periods" of order four

$$\eta_j = \sum_{i\in D_j} 2^{4i} \pmod{2^N - 1}\ (j = 0, 1, 2, 3)$$

and quadratic "Gauss sums"

$$G = \sum_{i\in\mathbb{F}_p^*} 2^{4i}\chi(i) = \eta_0 - \eta_1 + \eta_2 - \eta_3 \pmod{2^N - 1},$$

where χ is the quadratic multiplicative character of $\mathbb{F}_p^*$, that is,

$$\chi(i) = \begin{cases} 1, & \text{if } i \in D_0 \cup D_2, \\ -1, & \text{if } i \in D_1 \cup D_3. \end{cases}$$

Then we have the following lemma.

Lemma 5.1. *Let the symbols as the same before, then we have*
(1). $G^2 \equiv p - \frac{2^N-1}{15} \pmod{2^N - 1}$.

(2). For $0 \le e \le 3$,

$$16\eta_e^2 \equiv (\frac{2^N-1}{15}-1)p+(-7+2x)\eta_e+(1+2x-8y)\eta_{e+1}+(1-6x)\eta_{e+2}+(1+2x+8y)\eta_{e+3} \pmod{2^N-1},$$
$$16\eta_e\eta_{e+1} \equiv (\frac{2^N-1}{15}-1)p+(-3-2x)(\eta_e+\eta_{e+1})+(1+2x+8y)\eta_{e+2}+(1+2x-8y)\eta_{e+3} \pmod{2^N-1},$$
$$16\eta_e\eta_{e+2} \equiv (\frac{2^N-1}{15}-1)p+(-7+2x)(\eta_e+\eta_{e+2})+(-3-2x)(\eta_{e+1}+\eta_{e+3})+4(q-1) \pmod{2^N-1}.$$

(3). $(\eta_0+\eta_1-\eta_2-\eta_3)^2 \equiv 2yG-p+\frac{2^N-1}{15} \pmod{2^N-1}$,
$(\eta_0-\eta_1-\eta_2+\eta_3)^2 \equiv -2yG-p+\frac{2^N-1}{15} \pmod{2^N-1}$.

Proof. The proof is similar to Lemmas 2–4 in [17], we omit it here. □

By the definition of $S(2)$ and s, we have

$$\begin{aligned}
S(2) &= \sum_{i=0}^{N-1} s_i \cdot 2^i \pmod{2^{4p}-1} \\
&= \sum_{i\in\varphi(\{0\}\times C_0\cup\{1\}\times C_1\cup\{2\}\times C_2\cup\{3\}\times C_3)}^{4p-1} 2^i \pmod{2^{4p}-1} \\
&= \sum_{\beta\in D_a\cup D_b\cup\{0\}}^{4p-1} 2^{(3p+1)\beta} + \sum_{\beta\in D_a\cup D_c\cup\{0\}}^{4p-1} 2^{(3p+1)\beta+p} + \sum_{\beta\in D_a\cup D_b}^{4p-1} 2^{(3p+1)\beta+2p} + \sum_{\beta\in D_b\cup D_d}^{4p-1} 2^{(3p+1)\beta+3p} \pmod{2^{4p}-1}.
\end{aligned}$$

Since $p \equiv 5 \pmod 8$ *i.e.* $2 \in D_1 \cup D_3$, we have $4 \in D_2$. Therefore

$$\begin{aligned}
S(2) &= \sum_{4\beta\in D_a\cup D_b}^{4p-1} 2^{4(3p+1)\beta} + \sum_{4\beta\in D_a\cup D_c}^{4p-1} 2^{4(3p+1)\beta+p} \\
&\quad + \sum_{4\beta\in D_a\cup D_b}^{4p-1} 2^{4(3p+1)\beta+2p} + \sum_{4\beta\in D_b\cup D_d}^{4p-1} 2^{4(3p+1)\beta+3p} + 1 + 2^p \pmod{2^{4p}-1} \\
&= \sum_{4\beta\in D_a\cup D_b}^{4p-1} 2^{4\beta} + \sum_{4\beta\in D_a\cup D_c}^{4p-1} 2^{4\beta+p} + \sum_{4\beta\in D_a\cup D_b}^{4p-1} 2^{4\beta+2p} + \sum_{4\beta\in D_b\cup D_d}^{4p-1} 2^{4\beta+3p} + 1 + 2^p \pmod{2^{4p}-1} \\
&= \sum_{\beta\in D_{a+2}\cup D_{b+2}}^{4p-1} 2^{4\beta} + 2^p \cdot \sum_{\beta\in D_{a+2}\cup D_{c+2}}^{4p-1} 2^{4\beta} + 2^{2p} \cdot \sum_{\beta\in D_{a+2}\cup D_{b+2}}^{4p-1} 2^{4\beta} + 2^{3p} \cdot \sum_{\beta\in D_{b+2}\cup D_{d+2}}^{4p-1} 2^{4\beta} + 1 + 2^p \pmod{2^{4p}-1}
\end{aligned} \tag{5.1}$$

$$\begin{aligned}
&= \begin{cases}
(\eta_{a+2}+\eta_{b+2})+(\eta_{a+2}+\eta_{c+2})+(\eta_{a+2}+\eta_{b+2})+(\eta_{b+2}+\eta_{d+2})+2 \pmod{2^p-1}, \\
(\eta_{a+2}+\eta_{b+2})-(\eta_{a+2}+\eta_{c+2})+(\eta_{a+2}+\eta_{b+2})-(\eta_{b+2}+\eta_{d+2}) \pmod{2^p+1}, \\
(\eta_{a+2}+\eta_{b+2})+2^p(\eta_{a+2}+\eta_{c+2})-(\eta_{a+2}+\eta_{b+2})-2^p(\eta_{b+2}+\eta_{d+2})+2^p+1 \pmod{2^{2p}+1},
\end{cases} \\
&= \begin{cases}
\eta_{a+2}+\eta_{b+2}-\eta_{c+2}-\eta_{d+2}+\frac{2^{4p}-1}{15} \pmod{2^p-1}, \\
\eta_{a+2}+\eta_{b+2}-\eta_{c+2}-\eta_{d+2} \pmod{2^p+1}, \\
2^p(\eta_{a+2}-\eta_{b+2}+\eta_{c+2}-\eta_{d+2})+2^p+1 \pmod{2^{2p}+1}.
\end{cases}
\end{aligned} \tag{5.2}$$

Theorem 5.2. *Let p be a prime with $p \equiv 5 \pmod 8$, $p = x^2 + 4y^2$, $y = \pm 1$. Then the 2-adic complexity of the binary sequence s with period $4p$ defined by (2.1) is*

$$\Phi_2(s) = \log_2(\frac{2^{4p} - 1}{3}).$$

Proof. Let $d_1 = \gcd(S(2), 2^p - 1)$, $d_2 = \gcd(S(2), 2^p + 1)$ and $d_3 = \gcd(S(2), 2^{2p} + 1)$. Since $\gcd(2^p - 1,\ 2^p + 1) = 1, \gcd(2^{2p} - 1,\ 2^{2p} + 1) = 1$. We have $d = \gcd(S(2),\ 2^{4p} - 1) = d_1 \cdot d_2 \cdot d_3$.

Firstly, we determine d_1, from (5.2) and Lemma 5.1 (3) we have

$$S(2) \equiv \eta_{a+2} + \eta_{b+2} - \eta_{c+2} - \eta_{d+2} + \frac{2^{4p} - 1}{15} \equiv -2yG - p + 2 \cdot \frac{2^N - 1}{15} \equiv -2yG - p \pmod{2^p - 1}.$$

Assume that π is an odd prime divisor of $\gcd(S(2),\ 2^p - 1)$. We obtain

$$0 \equiv -2yG - p \pmod \pi.$$

Then we derive

$$p^2 \equiv 4yG^2 \equiv 4p - 4 \cdot \frac{2^{4p} - 1}{15} \equiv 4p \pmod \pi.$$

Since $y = \pm 1$, we have $\pi \mid p^2 - 4p$, namely $\pi = p$ or $\pi \mid p - 4$. If $\pi = p$, we have $2^p \equiv 2 \pmod \pi$, which contradicts $\pi \mid 2^p + 1$. If $\pi \mid p - 4$, from $2^p \equiv -1 \pmod \pi$ we obtain the order of 4 mod π is p. Therefore $p \mid \pi - 1$, which contradicts $\pi \mid p - 4$. In conclusion, $\gcd(S(2),\ 2^p - 1) = 1$, so we have $d_1 = 1$.

Next, we will determine d_2. On the one hand, from (5.1) we have

$$\begin{aligned} S(2) &\equiv \sum_{\substack{i=0 \\ \beta \in D_2 \cup D_3}}^{4p-1} 1 + 2 \cdot \sum_{\substack{i=0 \\ \beta \in D_0 \cup D_1}}^{4p-1} 1 + \sum_{\substack{i=0 \\ \beta \in D_0 \cup D_3}}^{4p-1} 1 \cdot \sum_{\substack{i=0 \\ \beta \in D_1 \cup D_2}}^{4p-1} 1 \pmod 3 \\ &\equiv \frac{p-1}{2} + 2 \cdot \frac{p-1}{2} + \frac{p-1}{2} + 2 \cdot \frac{p-1}{2} \pmod 3 \\ &\equiv 0 \pmod 3. \end{aligned} \tag{5.3}$$

On the other hand, assume that π is an odd prime divisor of $\gcd(S(2),\ \frac{2^p+1}{3})$. From (5.2) and Lemma 5.1 (3) we have

$$0 \equiv \eta_{a+2} + \eta_{b+2} - \eta_{c+2} - \eta_{d+2} + 2 \equiv -2yG - p + \frac{2^N - 1}{15} + 2 \equiv -2yG - p + 2 \pmod{\frac{2^p + 1}{3}}.$$

Then we obtain

$$(p-2)^2 \equiv 4yG^2 \equiv 4p - 4 \cdot \frac{2^{4p} - 1}{15} \equiv 4p \pmod \pi.$$

Thus we have $\pi \mid p^2 - 8p + 4$. Assume that π' is an odd prime divisor of $\gcd(p^2 - 8p + 4,\ \frac{2^p+1}{3})$, we have $p \mid \pi' - 1$, and so $\pi' = 2kp + 1$ $(k \geq 1)$. From $2kp \equiv -1 \pmod{\pi'}$, we obtain $0 \equiv 2k(p^2 - 8p + 4) \equiv -p + 8 + 8k \pmod{\pi'}$, which imply $p = 8(k + 1)$. This is a contradiction. Therefore $\gcd(p^2 - 8p + 4,\ \frac{2^p+1}{3}) = 1$ and $d_2 = 3$.

In the last part, we determine $d_3 = \gcd(S(2),\ 2^{2p}+1)$. Assume that π is an odd prime divisor of $\gcd(S(2),\ \frac{2^{2p}+1}{5})$. We have

$$0 \equiv S(2) \equiv 2^p \cdot G + 1 + 2^p \pmod{\pi},$$

which leads to $2^{p+1} \equiv (1+2^p)^2 \equiv 2^{2p} \cdot G^2 \equiv -G^2 \equiv -p + \frac{2^{4p}-1}{15} \equiv -p \pmod{\pi}$. This is a contradiction, thus we have $\gcd(S(2),\ \frac{2^{2p}+1}{5}) = 1$.

In addition, from (5.1) we have

$$\begin{aligned} S(2) &\equiv \sum_{\substack{i=0 \\ \beta \in D_2 \cup D_3}}^{4p-1} 1 + 2 \cdot \sum_{\substack{i=0 \\ \beta \in D_0 \cup D_1}}^{4p-1} 1 - \sum_{\substack{i=0 \\ \beta \in D_0 \cup D_3}}^{4p-1} 1 - 2 \cdot \sum_{\substack{i=0 \\ \beta \in D_1 \cup D_2}}^{4p-1} 1 + 1 + 2^p \pmod 5 \\ &\equiv \frac{p-1}{2} + 2 \cdot \frac{p-1}{2} - \frac{p-1}{2} - 2 \cdot \frac{p-1}{2} + 1 + 2^p \pmod 5 \\ &\equiv 2^{4f+1} + 1 \equiv 3 \pmod 5, \end{aligned}$$

Therefore we have $d_3 = 1$.

To sum up, we have $\Phi_2(s) = \log_2(\frac{2^{4p}-1}{3})$. □

At the end of this section, we also provide an example to demonstrate the Theorem 5.2.

Example 5.3. Let $p = 29 = 5^2 + 4 \cdot 1$ and $\theta = 2$, we have

$$\begin{aligned} D_0 &= \{1, 16, 24, 7, 25, 23, 20\},\ D_1 = \{2, 3, 19, 14, 21, 17, 11\}, \\ D_2 &= \{4, 6, 9, 28, 13, 5, 22\},\ D_3 = \{8, 12, 18, 27, 26, 10, 15\}. \end{aligned}$$

Then for $(a, b, c, d) = (0, 1, 3, 2)$,

$$\begin{aligned} C = \{&0, 1, 2, 3, 11, 14, 16, 19, 20, 24, 25, 29, 30, 31, 32, 35, 36, 37, 40, 41, 43, 45, 46, 48, 49, 50, 51, 52, 53, 54, 60, \\ &63, 65, 67, 71, 72, 73, 74, 75, 78, 79, 81, 82, 85, 88, 90, 91, 94, 97, 98, 104, 105, 106, 108, 110, 112, 113, 115\}. \end{aligned}$$

The binary sequence s with period $N = 4p$ is

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

Computed by Magma program, we have $\gcd(S(2),\ 2^{4p}-1) = 3$, the 2-adic complexity of sequence s is $\Phi_2(s) = \log_2 \frac{2^N-1}{3}$, the result is consistent with the Theorem 5.2.

6. Conclusion

In this paper, we construct a new family of binary sequences s with period $4p$ based on cyclotomic classes of order four, and determine their autocorrelation, linear complexity and 2-adic complexity. The results show that the sequences s have low 4-value autocorrelation. The linear complexity $LC(s)$ of s is $4p-1$, and the 2-adic complexity of s is $\Phi_2(s) = \log_2(\frac{2^{4p}-1}{3})$, both greater than $2p$, indicating that the sequences are safe enough to resist BM algorithm attacks and RAA attacks, and thus have good properties in communication applications.

Acknowledgments

This work is supported by National Natural Science Foundation of China(12471006, 12371007) and Shaanxi Fundamental Science Research Project for Mathematics and Physics(Grant No. 22JSY007).

Conflict of interest

The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] 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.

[2] V. Edemskiy and A. Palvinskiy, The linear complexity of binary sequences of length $2p$ with optimal three-level autocorrelation. *Inf. Process. Lett.* **116** (2016) 153–156.

[3] C. Fan, The linear complexity of a class of binary sequences with optimal autocorrelation. *Des. Codes Cryptogr.* **86** (2018) 2441–2450.

[4] R. Hofer and A. Winterhof, On the 2-adic complexity of the two-prime generator. *IEEE Trans. Inf. Theory* **64** (2018) 5957–5960.

[5] H. Hu, Comments on a new method to compute the 2-adic complexity of binary sequences. *IEEE Trans. Inf. Theory* **60** (2004) 5803–5804.

[6] N. Li and X. Tang, On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation value/magnitude. *IEEE Trans. Inf. Theory* **57** (2011) 7597–7604.

[7] W. Su, Y. Yang and C. Fan, New optimal binary sequences with period $4p$ via interleaving Ding–Helleseth-Lam sequences. *Des. Codes Cryptogr.* **86** (2018) 1329–1338.

[8] Y. Sun, Q. Wang and T. Yan, A lower bound on the 2-adic complexity of modified Jacobi sequences. *Cryptogr. Commun.* **11** (2019) 337–349.

[9] 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. *Cryptogr. Commun.* **10** (2018) 467–477.

[10] Y. Sun, T. Yan and H. Li, The linear complexity of a class of binary sequences with three-level autocorrelation. *IEICE Trans. Fundam.* **E96-A** (2013) 1586–1592.

[11] T. Tian and W. Qi, 2-adic complexity of binary m-sequences. *IEEE Trans. Inf. Theory* **56** (2010) 450–454.

[12] Q. Wang and X. Du, The linear complexity of binary sequences with optimal autocorrelation. *IEEE Trans. Inf. Theory* **56** (2010) 6388–6397.

[13] Q. Wang, The linear complexity of some binary sequences with three-level autocorrelation. *IEEE Trans. Inf. Theory* **57** (2010) 4046–4052.

[14] H. Xiong, L. Qu and C. Li, A new method to compute the 2-adic complexity of binary sequences. *IEEE Trans. Inf. Theory* **60** (2014) 2399–2406.

[15] H. Xiong, L. Qu and C. Li, 2-adic complexity of binary sequences with interleaved structure. *Finite Fields Appl.* **33** (2015) 14–28.

[16] J. Zhang and C. Zhao, The linear complexity of a class of binary sequences with period $2p$. *Algebra Eng. Commun. Comput.* **26** (2015) 475–491.

[17] L. Zhang, J. Zhang, M. Yang and K. Feng, On the 2-adic complexity of the Ding–Helleseth–Martinsen binary sequences. *IEEE Trans. Inf. Theory* **66** (2020) 4613–4620.

[18] J.L. Massey, Shift-register synthesis and BCH decoding. *IEEE Trans. Inf. Theory* **15** (1969) 122–127.

[19] A. Klapper and M. Goresky, Cryptanalysis based on 2-adic rational approximation. In: *CRYPTO 1995, LNCS* **963** (1995) 262–273.

[20] A. Klapper and M. Goresky, Feedback shift registers, 2-adic span, and combiners with memory. *J. Cryptol.* **10** (1997) 111–147.

[21] T. Storer, Cyclotomy and Difference Sets. Markham, Chicago, IL (1967).

[22] C. Ding, T.H. Helleseth and H. Martinsen, New families of binary sequences with optimal three-level autocorrelation. *IEEE Trans. Inf. Theory* **47** (2001) 428–433.

[23] C. Ding, T.H. Helleseth and K.Y. Lam, Several classes of sequences with three-level autocorrelation. *IEEE Trans. Inf. Theory* **45** (1999) 2606–2612.

[24] B. Berndt, R. Evans and K. Williams, Gauss and Jacobi Sums. John Wiley and Sons Inc. (1998).

[25] T.W. Cusick, C. Ding and A. Renvall, Stream Ciphers and Number Theory. North-Holland Mathematical Library 55. North-Holland/Elsevier, Amsterdam, The Netherlands (1998).