Linear Complexity of \( n \)-Periodic Cyclotomic Sequences over \( \mathbb{F}_p \)

Quiyuan WANG\(^{a)}\), Member and Yang YAN\(^{b)}\), Nonmember

SUMMARY Periodic sequences, used as keys in cryptosystems, play an important role in cryptography. Such periodic sequences should possess high linear complexity to resist B-M algorithm. Sequences constructed by cyclotomic cosets have been widely studied in the past few years. In this paper, the linear complexity of \( n \)-periodic cyclotomic sequences of order 2 and 4 over \( \mathbb{F}_p \) has been calculated, where \( n \) and \( p \) are two distinct odd primes. The conclusions reveal that the presented sequences have high linear complexity in many cases, which indicates that the sequences can resist the linear attack.

key words: Legendre sequences, cyclotomic sequences, linear complexity, Gauss periods

1. Introduction

Periodic sequences used for stream ciphers are required to have qualities of unpredictability. The linear complexity is shown to have valuable properties as a measure for the randomness (or equivalently the unpredictability) of periodic sequences. Let \( c = (c_i)_{i=0}^{\infty} \) be a sequence of period \( n \) over the finite field \( \mathbb{F}_p \). The linear complexity (also called linear span) of \( c \) over \( \mathbb{F}_p \), denoted by \( L_p(c) \), is defined to be the smallest positive integer \( \lambda \) such that there are constants \( a_0 \neq 0, a_1, \ldots, a_{\lambda-1} \in \mathbb{F}_p \) satisfying \(-a_0c_i + a_1c_{i-1} + a_2c_{i-2} + \cdots + a_{\lambda-1}c_{i-\lambda+1} = 0 \) for all \( i \geq \lambda \). The Berlekamp-Massey algorithm \([1],[10]\) states that if \( L_p(c) > n/2 \), then \( c \) is considered good with respect to its linear complexity.

For an odd prime \( n \), let \( n-1 = ek (e \geq 2) \) and \( \mathbb{F}_p \) be the finite field with \( n \) elements. Suppose \( \theta \) is a primitive element of \( \mathbb{F}_p^* \), \( \mathbb{F}_p = \mathbb{F}_n \). Let

\[
C_\lambda = C_\lambda^\theta = \theta^\lambda C_0, \quad (0 \leq \lambda \leq e-1),
\]

where \( C_0 = (\theta^0) \) is the subgroup of \( \mathbb{F}_p^* \) generated by \( \theta^e \) and \( C_\lambda (0 \leq \lambda \leq e-1) \) are the cosets of \( C_0 \) in \( \mathbb{F}_p^* \). Let \( S \) be a subset of \( \{0, 1, \ldots, e-1\} \) and

\[
\Sigma_S = \bigcup_{\lambda \in S} C_\lambda.
\]

We define the following binary periodic sequence \( c_S = (c_i)_{i=0}^{\infty} \) with period \( n \) by

\[
c_i = \begin{cases} 1, & \text{if } (i \mod n) \in \Sigma_S, \\ 0, & \text{otherwise,}
\end{cases}
\]

Such sequences are called binary cyclotomic sequences of order \( e \) and used as keys in cryptography since they have good pseudo-random properties and correlation properties \([6],[8],[11]–[13]\). The linear complexity of such sequences over \( \mathbb{F}_2 \) has been determined by Ding et al. \([5]\) for order 2 case (Legendre sequences) and Edemskii \([7]\) for order 4 case. Since \( c_i \) is either 0 or 1, such sequences can be viewed over \( \mathbb{F}_q \), where \( q = p^m \) and \( p \) is a prime number. When \((n-1)/4 \equiv 0 \pmod{p}\), Ding \([4]\) has determined the linear complexity of cyclotomic sequences of order 4 over \( \mathbb{F}_{p^m} \) from the viewpoint of coding theory. In this paper, our first contribution is to give a general formula on the linear complexity of cyclotomic sequences by using Gauss periods. Our second contribution is to determine the linear complexity of binary \( n \)-periodic cyclotomic sequences of order 2 and 4 over a finite field \( \mathbb{F}_{p^m} \), where \( p \) and \( n \) are two distinct odd primes. The results show that the linear complexity of \( c \) over \( \mathbb{F}_{p^m} \) is nearly equal to the period \( n \) in many cases so that they can resist the linear attack in cryptography.

This paper is organized as follows. Section 2 contains the definitions and formulas of linear complexity of periodic sequences and Gauss periods. In Sect. 3, we determine the linear complexity of the binary cyclotomic sequences of order 2 and 4 over \( \mathbb{F}_q \).

2. Preliminaries

Firstly, we introduce the definition and formula of linear complexity of periodic sequences over a finite field. See \([3]\) or \([9]\) for more details.

Let \( q \) be a power of a prime \( p \) and let \( c = (c_i)_{i=0}^{\infty} \) be a periodic sequence over \( \mathbb{F}_q \) with period \( n \), where \( c_i \in \mathbb{F}_q (i \geq 0) \). The sequence \( c \) can be viewed as a power series

\[
c^\infty(x) = \sum_{n=0}^{\infty} c_n x^n = \frac{u(x)}{1 - x^n},
\]

where \( u(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x] \) in the power series ring \( \mathbb{F}_q[x] \).

Let \( h(x) = \gcd(u(x), 1 - x^n) \), then

\[
c^\infty(x) = \frac{u(x)}{v(x)}, \quad v(x) = \frac{1 - x^n}{h(x)}, \quad w(x) = \frac{u(x)}{h(x)}
\]

where \( u(x), v(x), h(x) \in \mathbb{F}_q[x] \).
Definition 2.1 ([9]) The polynomial \( v(x) \) is called the minimal polynomial of the periodic sequence \( c \) over \( \mathbb{F}_q \). The \( \deg v(x) = n - \deg h(x) \) is called the linear complexity of the sequence \( c \) over \( \mathbb{F}_q \), which is denoted by \( L_q(c) \).

Indeed, \( L_q(c) \) is the length of the shortest linear feedback shift register which generates the sequence \( c \).

If \( \gcd(n, p) = 1 \), then \( 1 - x^a \) has \( n \) distinct zeros \( \zeta_a^i \) \( (0 \leq i \leq n-1) \) in the algebraic closure \( \Omega_q \) of \( \mathbb{F}_q \). Let

\[
m = \#\{i : 0 \leq i \leq n - 1, \mu(c_a^i) = 0\}.
\]

Then it is easy to see that \( \deg h(x) = m \) and \( L_q(c) = n - m \).

In order to determine \( L_q(c) \) for the binary cyclotomic sequences, we introduce Gauss periods.

Definition 2.2 ([2]) For a prime power \( q = p^m \) \( (p \neq n) \), let \( \zeta_n \) be a primitive \( n \)-th root of unity in the algebraic closure \( \Omega_q \) of \( \mathbb{F}_q \). The Gauss periods of order \( e \) are defined by

\[
\eta_i = \sum_{x \in S} \zeta_n^{x^e} \quad (0 \leq A \leq e - 1).
\]

The following Lemma states some basic properties on Gauss periods which can be derived from the definition directly.

Lemma 2.3 ([2]) Let symbols be the same as before. Then we have

1. \( \sum_{A=0}^{e-1} \eta_i = -1; \)
2. For \( a = \theta^e \), \( \sum_{x \in S} \zeta_n^x = \eta_{
 \theta^e+i}; \)
3. For \( 0 \leq A \leq e - 1 \), let

\[
g_A = \sum_{x=0}^{n-1} \zeta_n^{x^e\theta^i}.
\]

Then

\[
g_A = 1 + e\eta_A;
\]

4. For \( p \in C_i \),

\[
r^p_A = r^A_{\theta^p+i}.
\]

The values of Gauss periods of order 2 and 4 can be determined explicitly (see [2] or [9]) by Gauss sums. In this paper, we need the following results on the modified period polynomial

\[
f(x) = (x - g_0)(x - g_1) \cdots (x - g_{e-1}).
\]

For \( e = 2 \) and \( n - 1 = 2k \), it is well known that [2]

\[
(x - g_0)(x - g_1) = x^2 - \left( \frac{1}{n} \right) n.
\]

For \( e = 4 \), \( n = 4k + 1 \) can be expressed by

\[
n = a^2 + b^2, \quad a, b \in \mathbb{Z},
\]

where \( a \) is determined by \( a = -\left( \frac{2}{n} \right) \) \( \pmod{4} \), the even integer \( b \) is determined up to sign and \( \left( \frac{2}{n} \right) \) is the Legendre symbol ([2], Theorem 3.2.1).

Lemma 2.4 ([2], Theorem 4.2.1, Corollary 4.2.2)

1. For \( e = 4 \) and \( n - 1 = 4k \),

\[
f(x) = \prod_{\lambda=0}^{3}(x - g_{\lambda}) = x^4 - 2n\left[1 + 2\left( \frac{2}{n} \right) \right]x^2 - 8\left( \frac{2}{n} \right) anx + \left[1 - 4\left( \frac{2}{n} \right) \right]n^2 + 4b^2n,
\]

where

\[
\left( \frac{2}{n} \right) = \begin{cases} 1, & \text{if } n \equiv 1 \pmod{8}, \\ -1, & \text{if } n \equiv 5 \pmod{8}. \end{cases}
\]

2. The discriminant of \( f(x) \) is

\[
\Delta = 2^{14}b^2n^3 \left[ n\left(1 - 2\left( \frac{2}{n} \right) \right) + a^2 \right]^2.
\]

Therefore, \( f(x) \) has multiple zeros in \( \Omega_q \) if and only if

\[
2bn\left[n(1 - 2\left( \frac{2}{n} \right) + a^2)\right] \equiv 0 \pmod{p}.
\]

3. For \( g_0 \), we have

\[
g_0 = \sqrt{n} \pm 2\left( \frac{2}{n} \right)(n + a\sqrt{n})^{1/2}.
\]

3. Results and Proofs

Let \( n \) be an odd prime and \( n - 1 = ek \). Let \( q = p^m \) for an odd prime \( p \) and satisfy \( \gcd(n, q) = 1 \). For a non-empty subset \( S \) of \( \{0, 1, \ldots, e-1\} \), the binary cyclotomic sequence \( c_S = (c_i)_{i=0}^{\phi(n)} \) with period \( n \) is defined by

\[
c_i = \begin{cases} 1, & \text{if } (i \mod n) \in \Sigma_S, \quad \text{for all } i \geq 0. \\ 0, & \text{otherwise}, 
\end{cases}
\]

(3.1)

Let \( c(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_q[x] \). It is not difficult to see that

\[
c(x) = \sum_{i=1}^{n-1} c_i x^i.
\]

(3.2)

Let \( h(x) = \gcd(x^n - 1, c(x)) \). Then

\[
L_q(c_S) = n - \deg h(x).
\]

(3.3)

Since the greatest common divisor of \( c(x) \) and \( 1 - x^a \) over \( \mathbb{F}_q \) is equal to that of these two polynomials over \( \mathbb{F}_p \), we then get the following fact. For a binary periodic sequence \( c \), we have \( L_q(c) = L_p(c) \).

Due to the above fact, we will focus on the prime field \( \mathbb{F}_p \) in the following. Let \( \zeta_n \) be an \( n \)-th primitive root of unity.
over the algebraic closure $\Omega_p$ of $\mathbb{F}_p$. Then
\[
\deg h(x) = \#\{i : 0 \leq i \leq n - 1, \, c(\zeta^i) = 0\},
\]
where $h(x) = \gcd(x^{|S|} - 1, \, c(x))$. Notice that for $i = 0, \, c(1) = |S| \cdot k$. For $1 \leq i \leq n - 1$, set $i \in C_i = \theta C_0$. Direct computation shows
\[
c(\zeta^i) = \sum_{n=0}^{n-1} \frac{\zeta^i}{n} = \sum_{n \in S} \frac{\zeta^i}{n} = \sum_{n \in S} \eta_{k+i},
\]
where $\eta_k$ is the Gauss period defined in Sect. 2. Let
\[
A_t = A_{t,S} = \sum_{n \in S} \eta_{k+i} \in \Omega_p, \quad (0 \leq t \leq n - 2).
\]
(3.4)
\[
N = \#\{t : 0 \leq t \leq e - 1, A_t = 0\}.
\]
As $\eta_k = \eta_{k+c}$, we have $A_t = A_{t+c}$, hence
\[
\deg h(x) = \delta + \#\{t : 0 \leq t \leq n - 2, A_t = 0\}
= \delta + k \cdot \#\{t : 0 \leq t \leq e - 1, A_t = 0\}
= \delta + k \cdot N.
\]
where
\[
\delta = \begin{cases} 1, & \text{if } |S| \cdot k \equiv 0 \pmod{p}, \\ 0, & \text{otherwise}. \end{cases}
\]
(3.6)

By (3.3), we get a key result for the whole paper.

**Theorem 3.1** Let $n - 1 = ek$, $p \neq n$ be an odd prime, and $S$ be a non-empty subset of $\{0, 1, \ldots, e - 1\}$. Then for the sequence $c_S = c_i_{i=0}^n$ defined by (3.1), we have
\[
L_p(c_S) = n - \delta - k \cdot N,
\]
where $N$ and $\delta$ are defined by (3.5) and (3.6) respectively.

By Theorem 3.1, the complexity $L_p(c_S)$ is reduced to determining how many $A_t$ are zero in $\Omega_p$. For a large order $e$, the following result simplifies the computation of $L_p(c_S)$.

**Lemma 3.2** Let $1 \leq a \leq e - 1$ and $S$ be a non-empty subset of $\{0, 1, \ldots, e - 1\}$. If $S' = a + S = \{a + \lambda \pmod{e} : \lambda \in S\}$, then for any odd prime $p \neq n$, we have
\[
L_p(c_S) = L_p(c_{S'}).
\]

**Proof.** By Theorem 3.1, $L_p(c_S) = n - \delta - kN$ and $L_p(c_{S'}) = n - \delta - kN'$, where
\[
N = \#\{t : 0 \leq t \leq e - 1, A_t = 0\},
N' = \#\{t : 0 \leq t \leq e - 1, A'_{t} = 0\},
A_t = A_{t,S} = \sum_{n \in S} \eta_{k+i},
\]
\[
A'_t = A_{t,S'} = \sum_{\lambda \in S} \eta_{k+i} = \sum_{\lambda \in S} \eta_{k+i}.\]

Therefore $N = N'$ and $L_p(c_S) = L_p(c_{S'})$. \qed

For the case $S = \{0, 1, \ldots, e - 1\}$, the period has only one 0 with the rest 1’s and this is a trivial case. Hence, we assume $1 \leq |S| \leq e - 1$ in the sequel. By Lemma 3.2, it is enough to consider $S = \{0\}$ for $e = 2$ and $S = \{0, 1\}, \{0, 1, 2\}$ for $e = 4$.

3.1 Case $e = 2$

In this case, $n - 1 = 2k$, $\mathbb{F}_n^0 = \langle \theta \rangle$, furthermore
\[
C_0 = c^{(2)}_0 = \langle \theta \rangle = \left\{a : 1 \leq a \leq n - 1, \left(\frac{a}{n}\right) = 1\right\},
C_1 = c^{(2)}_1 = \theta C_0 = \left\{a : 1 \leq a \leq n - 1, \left(\frac{a}{n}\right) = -1\right\},
\]
where $(\frac{a}{n})$ is the Legendre symbol. From the explanation above, it is enough to consider $S = \{0\}$ in this case, the sequence $c = c_S = c_i_{i=0}^n$ is the Legend sequence which is defined by
\[
c_i = \begin{cases} 1, & \text{if } (i \mod n) \in C_0, \\ 0, & \text{otherwise}, \end{cases}
\]
(3.7)

**Theorem 3.3** Let $p \neq n$ be an odd prime. Then for the Legend sequence $c$ defined by (3.7), we have
\[
L_p(c) = \begin{cases} \frac{n-1}{2}, & \text{if } n \equiv 1 \pmod{4} \text{ and } p | n - 1, \\ \frac{n-1}{2}, & \text{if } n \equiv 3 \pmod{4} \text{ and } p | n + 1, \\ n - 1, & \text{if } n \equiv 3 \pmod{4} \text{ and } p | n - 1, \\ n, & \text{otherwise}. \end{cases}
\]

**Proof.** For $e = 2$ and $S = \{0\}$,
\[
A_0 = \eta_0 = \sum_{x \in C_0} \zeta^x,
A_1 = \eta_1 = \sum_{x \in C_1} \zeta^{x}.
\]
By Theorem 3.1 and $k = \frac{n-1}{2}$, we know that
\[
L_p(c) = n - \delta - \frac{n - 1}{2} \cdot N.
\]
(3.8)

where $N = \#\{\lambda : \lambda \in [0, 1], \eta_1 = 0 \in \mathbb{F}_p\}$. By the definition of $\delta$ and $|S| = 1$, we know
\[
\delta = \begin{cases} 1, & \text{if } p | (n - 1), \\ 0, & \text{otherwise}. \end{cases}
\]

For $g_1 = 1 + 2\eta_1$, it is well known that [2],
\[
(x - g_0)(x - g_1) = x^2 - \left(-\frac{1}{n}\right)n
\]
(3.9)
From (3.9), we have
\[
\{g_0, g_1\} = \left\{ \pm \sqrt{-\frac{1}{n}} \right\}.
\]

Therefore, \(\{\eta_0, \eta_1\} = \left\{ \frac{1}{2} \left( -1 \pm \sqrt{\frac{-1}{n}} \right) \right\} \).

Since \(\eta_0 + \eta_1 = -1\), \(\eta_0\) and \(\eta_1\) cannot be zero at the same time. From (3.8), we get \(L_p(c) \in \left\{ \frac{m+1}{2}, n, n-1 \right\}\) and
\[
L_p(c) = \frac{n-1}{2} \Leftrightarrow \delta = 1 \text{ and } N = 1
\]
\[
\Leftrightarrow p \mid n-1 \text{ and } 0 = \eta_0 \eta_1 = \frac{1}{4} \left( 1 - \left( -\frac{1}{n} \right) n \right)
\]
\[
\Leftrightarrow p \mid n-1 \text{ and } p \mid 1 - \left( -\frac{1}{n} \right) n
\]
\[
\Leftrightarrow p \mid n-1 \text{ and } n \equiv 1 \pmod{4}.
\]

Similarly,
\[
L_p(c) = \frac{n+1}{2} \Leftrightarrow \delta = 0 \text{ and } N = 1
\]
\[
\Leftrightarrow p \nmid n-1 \text{ and } 0 = \eta_0 \eta_1 = \frac{1}{4} \left( 1 - \left( -\frac{1}{n} \right) n \right)
\]
\[
\Leftrightarrow p \nmid n-1 \text{ and } p \mid 1 - \left( -\frac{1}{n} \right) n
\]
\[
\Leftrightarrow n \equiv 3 \pmod{4} \text{ and } p \mid n+1.
\]

For other cases, \(L_p(c_S) = n\). This completes the proof. \(\square\)

3.2 Case \(e = 4\)

In this case, \(n = 4k + 1\) is an odd prime. Let \(p\) be an odd prime and \(p \neq n, \mathbb{F}_n^* = \langle \theta \rangle\) and
\[
C_\lambda = C_\lambda^{(4)} = \theta^\lambda \langle \theta^4 \rangle, \quad (0 \leq \lambda \leq 3).
\]
The prime \(n = 1 + 4k\) can be expressed as
\[
n = a^2 + b^2,
\]
where \(a\) is determined by \(a \equiv -\left( \frac{2}{n} \right) \pmod{4}\) and the even integer \(b\) is determined up to sign.

By Lemma 2.4, for \(g_1 = 1 + 4\eta_\lambda\), we know
\[
\prod_{j=0}^{3} (x - g_\lambda) = x^4 - 2n \left[ 1 + 2 \left( \frac{2}{n} \right) \right] x^2 - 8 \left( \frac{2}{n} \right) an x
\]
\[
+ \left[ 1 - 4 \left( \frac{2}{n} \right) \right] n^2 + 4b^2 n,
\]
where
\[
\left( \frac{2}{n} \right) = \begin{cases} 1, & \text{if } n \equiv 1 \pmod{8}, \\ -1, & \text{if } n \equiv 5 \pmod{8}, \end{cases}
\]
and
\[
g_0 = \sqrt{n} + e \left[ 2 \left( \frac{2}{n} \right) (n + a \sqrt{n}) \right] \text{, } e \in \{ \pm 1 \}. \tag{3.11}
\]

Since \(C_0^{(4)} \cup C_2^{(4)} = C_2^{(2)}\) and \(C_1^{(4)} \cup C_3^{(4)} = C_1^{(2)}\), by Theorem 1.2.4 in [2] we have
\[
g_0 + g_2 = 2 + 4(\eta_0 + \eta_2)
\]
\[
= 2 + 4 \sum_{x \in C_0^{(2)} \cup C_2^{(4)}} \zeta_{4n}^x
\]
\[
= 2 + 4 \sum_{x \in C_0^{(2)}} \zeta_4^x
\]
\[
= 2 \sqrt{n}.
\]

From (3.11) we get
\[
g_2 = \sqrt{n} - e \left[ 2 \left( \frac{2}{n} \right) (n + a \sqrt{n}) \right] \text{, } e \in \{ \pm 1 \}. \tag{3.12}
\]

Similarly,
\[
g_1 + g_3 = 2 + 4(\eta_1 + \eta_3)
\]
\[
= 2 + 4 \sum_{x \in C_1^{(2)}} \zeta_4^x = -2 \sqrt{n}.
\]

Then by (3.10) and the Vite’s formula [15], we have
\[
-2n \left[ 1 + 2 \left( \frac{2}{n} \right) \right] = (g_0 + g_2)(g_1 + g_3) + g_0 g_2 + g_1 g_3
\]
\[
= -4n + n - 2 \left( \frac{2}{n} \right) (n + a \sqrt{n}) + g_1 g_3.
\]

Therefore, \(g_1 g_3 = n - 2 \left( \frac{2}{n} \right) (n - a \sqrt{n})\) and
\[
z^2 - (g_1 + g_3)z + g_1 g_3 = z^2 + 2 \sqrt{n} z + n - 2 \left( \frac{2}{n} \right) (n - a \sqrt{n}).
\]

We get
\[
\{g_1, g_3\} = \left\{ -\sqrt{n} \pm \left[ 2 \left( \frac{2}{n} \right) (n - a \sqrt{n}) \right] \right\}. \tag{3.13}
\]

From (3.11), (3.12), (3.13) and \(g_\lambda = 1 + 4\eta_\lambda\), we get the following result.

**Lemma 3.4** Let symbols be the same as before. Then we have
\[
\{\eta_0, \eta_2\} = \left\{ \frac{1}{4} \left( 1 - \sqrt{n} \pm \left[ 2 \left( \frac{2}{n} \right) (n + a \sqrt{n}) \right] \right) \right\},
\]
\[
\{\eta_1, \eta_3\} = \left\{ \frac{1}{4} \left( 1 - \sqrt{n} \pm \left[ 2 \left( \frac{2}{n} \right) (n - a \sqrt{n}) \right] \right) \right\}.
\]
As we mentioned before, it is enough to consider the sequence \( c_S \) for \( S = \{0\}, \{0, 1\} \) and \( \{0, 1, 2\} \), where \( c_S = (c_i)_{i=0}^{n-1} \) is defined by

\[
c_i = \begin{cases} 
1, & \text{if } (i \mod n) \in \Sigma_S, \\
0, & \text{otherwise},
\end{cases} \text{ for all } i \geq 0. \tag{3.14}
\]

By Theorem 3.1, we know that for any odd prime \( p \neq n \),

\[
L_p(c_S) = n - \delta - \frac{n-1}{4} \cdot N, \tag{3.15}
\]

where

\[
\delta = \begin{cases} 
1, & \text{if } (n-1) \cdot |S| \equiv 0 \pmod{p}, \\
0, & \text{otherwise},
\end{cases} \tag{3.16}
\]

\[
N = \# \{ t : 0 \leq t \leq 3, \sum_{\lambda \in \Sigma} \eta_{t+\lambda} = 0 \in \mathbb{F}_p \}. \tag{3.17}
\]

With the conditions and notations introduced at the beginning of this case, we have the following results.

**Theorem 3.5** If the odd prime \( p \in C_1 \cup C_3 \), then for \( S = \{0\}, \{0, 1\}, \{0, 1, 2\}, \)

\[
L_p(c_S) = n - \delta,
\]

where \( \delta \) is defined by (3.16).

**Proof.** By Theorem 3.1, \( L_p(c_S) = n - \delta - \frac{n-1}{4} \cdot N \), where \( \delta \) and \( N \) are defined by (3.16) and (3.17) respectively.

If \( p \in C_1 \cup C_3 \), we need to show that \( N = 0 \) for \( S = \{0\}, \{0, 1\} \) and \( \{0, 1, 2\} \). For \( S = \{0\}, N = \# \{ \lambda : 0 \leq \lambda \leq 3, \eta_\lambda = 0 \in \mathbb{F}_p \} \). From \( \eta_0 = \eta_1 + \eta_2 + \eta_3 = -1 \) and \( \eta_0^p = \eta_{t+1} \) or \( \eta_{t+3} \), we know that \( N = 0 \).

Similarly, we can show that for \( S = \{0, 1\} \),

\[
N = \# \{ \lambda : 0 \leq \lambda \leq 3, \eta_\lambda + \eta_{\lambda+1} = 0 \} = 0,
\]

and for \( S = \{0, 1, 2\} \),

\[
N = \# \{ \lambda : 0 \leq \lambda \leq 3, \eta_\lambda + \eta_{\lambda+1} + \eta_{\lambda+2} = 0 \} = 0.
\]

This finishes the proof of Theorem 3.5. \( \square \)

**Theorem 3.6** If \( p \in C_2 \), then then the linear complexity of \( c_S \) with period \( n \) is given by

(1) for \( S = \{0\} \),

\[
L_p(c_S) = \begin{cases} 
\frac{n+1}{2}, & \text{if } n \equiv 1 \pmod{p} \text{ and } a \equiv -1 \pmod{p}, \\
n-1, & \text{if } n \equiv 1 \pmod{p} \text{ and } a \equiv -1 \pmod{p}, \ \\
n, & \text{otherwise}.
\end{cases}
\]

(2) for \( S = \{0, 1\} \),

\[
L_p(c_S) = n - \delta;
\]

(3) for \( S = \{0, 1, 2\} \),

\[
L_p(c_S) = \begin{cases} 
\frac{n+1}{2}, & \text{if } p \neq 3 \text{ and } (n, a) \equiv (9, 3) \pmod{p}, \ \\
n-\delta, & \text{otherwise};
\end{cases}
\]

where \( \delta \) is defined by (3.16).

**Proof.** If \( p \in C_2 \), then \( \eta_0^p = \eta_{t+2} \) for \( 0 \leq \lambda \leq 3 \).

(1) For \( S = \{0\} \), by the value of \( \eta_1 \) given in Lemma 3.4, we know that

\[
\eta_0 = 0 \iff \eta_2 = 0
\]

\[
\iff -1 + \sqrt{n} \pm \left[ \left( \frac{2}{n} \right) \left( n + a \sqrt{n} \right) \right]^2 = 0 \in \mathbb{F}_p
\]

\[
\iff \sqrt{n} = 1 \text{ and } a + \sqrt{n} = 0 \text{ in } \mathbb{F}_p
\]

\[
\iff \sqrt{n} \equiv 1 \text{ and } a \equiv -1 \pmod{p}.
\]

By a similar computation,

\[
\eta_1 = 0 \iff \eta_3 = 0
\]

\[
\iff \sqrt{n} \equiv -1 \text{ and } a \equiv -1 \pmod{p}.
\]

Therefore, \( N = 2 \) if \( n \equiv 1 \) and \( a \equiv -1 \pmod{p} \), \( N = 0 \) otherwise. Then the result follows from (3.15).

(2) For \( S = \{0, 1\} \),

\[
N = \# \{ \lambda : 0 \leq \lambda \leq 3, \eta_\lambda + \eta_{\lambda+1} = 0 \}.
\]

From \( (\eta_1 + \eta_{t+1})^p = \eta_{t+2} + \eta_{t+3} \) and \( \eta_1 + \eta_{t+1} + \eta_{t+2} + \eta_{t+3} = -1 \), we know that

\[
N = \# \{ \lambda : 0 \leq \lambda \leq 3, \eta_\lambda + \eta_{\lambda+1} = 0 \} = 0.
\]

Therefore, \( L_p(c_S) = n - \delta \).

(3) For \( S = \{0, 1, 2\} \),

\[
N = \# \{ \lambda : 0 \leq \lambda \leq 3, \eta_\lambda + \eta_{\lambda+1} + \eta_{\lambda+2} = 0 \}
\]

\[
= \# \{ \lambda : 0 \leq \lambda \leq 3, \eta_\lambda = -1 \}.
\]

But

\[
\eta_0 = -1 \iff \eta_2 = -1
\]

\[
\iff \frac{1}{4} \left( -1 + \sqrt{n} \pm \left[ 2 \left( \frac{2}{n} \right) \left( n + a \sqrt{n} \right) \right]^2 = -1 \in \mathbb{F}_p
\]

\[
\iff a + 3 \equiv -3 \pmod{p}\]

By a similar computation,

\[
\eta_1 = -1 \iff \eta_3 = -1
\]

\[
\iff \frac{1}{4} \left( -1 - \sqrt{n} \pm \left[ 2 \left( \frac{2}{n} \right) \left( n - a \sqrt{n} \right) \right]^2 = -1 \in \mathbb{F}_p
\]

\[
\iff \sqrt{n} \equiv a \equiv 3 \pmod{p}.
\]

Therefore, \( N = 2 \) and \( \delta = 0 \) if \( p \neq 3 \), \( n \equiv 9 \) and \( a \equiv 3 \pmod{p} \), \( N = 0 \) otherwise. The result follows from (3.15). \( \square \)

**Theorem 3.7** Assume that \( p \in C_0 \), then the linear complexity of \( c_S \) with period \( n \) satisfies:
(1) For \( S = \{0\} \), let
\[
A_0 = 1 - 2n \left[ 1 + 2 \left( \frac{2}{n} \right) + 4 \left( \frac{2}{n} \right) a - 2b^2 \right] + n^2 \left[ 1 - 4 \left( \frac{2}{n} \right) \right],
\]
\[
A_1 = 1 - n \left[ 1 + 2 \left( \frac{2}{n} \right) (1 + a) \right],
\]
\[
A_2 = 3 - n \left[ 1 + 2 \left( \frac{2}{n} \right) \right].
\]
Then
\[
L_p(c_S) = \begin{cases} 
n - \delta, & \text{if } A_0 \not\equiv 0 \pmod{p}, 
\frac{3n+1}{4} - \delta, & \text{if } A_0 \equiv 0, A_1 \not\equiv 0 \pmod{p}, 
\frac{n+3}{4} - \delta, & \text{if } A_0 \equiv A_1 \equiv 0, A_2 \not\equiv 0 \pmod{p}, 
n - \delta, & \text{if } A_0 \equiv A_1 \equiv A_2 \equiv 0 \pmod{p}. 
\end{cases}
\]

(2) For \( S = \{0, 1\} \),
\[
B_0 = 81 - 2n \left[ 9 + 18 \left( \frac{2}{n} \right) - 2 \left( \frac{2}{n} \right) a - 2b^2 \right] + n^2 \left[ 1 - 4 \left( \frac{2}{n} \right) \right],
\]
\[
B_1 = -27 + n \left[ 3 + 6 \left( \frac{2}{n} \right) - 2 \left( \frac{2}{n} \right) a \right],
\]
\[
B_2 = 27 - n \left[ 1 + 2 \left( \frac{2}{n} \right) \right].
\]
Then
\[
L_p(c_S) = \begin{cases} 
n - \delta, & \text{if } B_0 \not\equiv 0 \pmod{p}, 
\frac{3n+1}{4} - \delta, & \text{if } B_0 \equiv 0, B_1 \not\equiv 0 \pmod{p}, 
\frac{n+3}{4} - \delta, & \text{if } B_0 \equiv B_1 \equiv 0, B_2 \not\equiv 0 \pmod{p}, 
n - \delta, & \text{if } B_0 \equiv B_1 \equiv B_2 \equiv 0 \pmod{p}. 
\end{cases}
\]

(3) For \( S = \{0, 1, 2\} \), let
\[
B_0 = 81 - 2n \left[ 9 + 18 \left( \frac{2}{n} \right) - 12 \left( \frac{2}{n} \right) a - 2b^2 \right] + n^2 \left[ 1 - 4 \left( \frac{2}{n} \right) \right],
\]
\[
B_1 = -27 + n \left[ 3 + 6 \left( \frac{2}{n} \right) - 2 \left( \frac{2}{n} \right) a \right],
\]
\[
B_2 = 27 - n \left[ 1 + 2 \left( \frac{2}{n} \right) \right].
\]
Then
\[
L_p(c_S) = \begin{cases} 
n - \delta, & \text{if } B_0 \not\equiv 0 \pmod{p}, 
\frac{3n+1}{4} - \delta, & \text{if } B_0 \equiv 0, B_1 \not\equiv 0 \pmod{p}, 
\frac{n+3}{4} - \delta, & \text{if } B_0 \equiv B_1 \equiv 0, B_2 \not\equiv 0 \pmod{p}, 
n - \delta, & \text{if } B_0 \equiv B_1 \equiv B_2 \equiv 0 \pmod{p}. 
\end{cases}
\]

where \( \delta \) is defined by (3.16).

Proof. (1) For \( S = \{0\} \), we have
\[
L_p(c_S) = n - \delta - \frac{n-1}{4}. \quad N,
\]
where
\[
\delta = \begin{cases} 
1, & \text{if } n - 1 \equiv 0 \pmod{p}, 
0, & \text{otherwise.}
\end{cases}
\]
and
\[
N = \# \{ \lambda : 0 \leq \lambda \leq 3, \eta_\lambda = 0 \} 
= \# \{ \lambda : 0 \leq \lambda \leq 3, g_\lambda = 1 + 4\eta_\lambda = 1 \}.
\]
According to Lemma 2.4,
\[
f(x) = \prod_{i=0}^{3} (x - g_i) = x^4 - 2n \left[ 1 + 2 \left( \frac{2}{n} \right) \right] x^2 - 8 \left( \frac{2}{n} \right) anx
\]
\[
+ \left[ 1 - 4 \left( \frac{2}{n} \right) \right] n^2 + 4b^2 n.
\]
Then
\[
\prod_{i=0}^{3} (x - (g_{i+1} - 1)) = f(x+1) = x^4 + 4x^3 + 2A_2x^2 + 4A_1x + A_0.
\]
Therefore,
\[
\begin{align*}
N = 0 & \iff A_0 \not\equiv 0 \pmod{p}; \\
N = 1 & \iff A_0 \equiv 0, A_1 \not\equiv 0 \pmod{p}; \\
N = 2 & \iff A_0 \equiv A_1 \equiv 0, A_2 \not\equiv 0 \pmod{p}; \\
N = 3 & \iff A_0 \equiv A_1 \equiv A_2 \equiv 0 \pmod{p}.
\end{align*}
\]
The final result follows from \( L_p(c_S) = n - \delta - \frac{n-1}{4} \cdot N \).

(2) For \( S = \{0, 1\} \), then
\[
N = \# \{ \lambda : 0 \leq \lambda \leq 3, \eta_\lambda + \eta_{\lambda+1} = 0 \}.
\]
As \( \eta_0 + \eta_1 + \eta_2 + \eta_3 = -1 \), we have
\[
either \eta_0 + \eta_1 or \eta_2 + \eta_3 is zero \iff (\eta_0 + \eta_1)(\eta_2 + \eta_3) = 0
\]
\[
\iff 0 = \begin{cases} 
[ -1 + \sqrt{n} + \epsilon (2 \left( \frac{2}{n} \right)) (n + a \sqrt{n})^\frac{1}{2} \\
-1 - \sqrt{n} + \mu(2 \left( \frac{2}{n} \right)) (n - a \sqrt{n})^\frac{1}{2} \\
-1 + \sqrt{n} - \epsilon(2 \left( \frac{2}{n} \right)) (n + a \sqrt{n})^\frac{1}{2} \\
-1 - \sqrt{n} - \mu(2 \left( \frac{2}{n} \right)) (n - a \sqrt{n})^\frac{1}{2} \\
\end{cases} \\
\iff 0 = \begin{cases} 
[ -2 + \epsilon(2 \left( \frac{2}{n} \right)) (n + a \sqrt{n})^\frac{1}{2} + \mu(2 \left( \frac{2}{n} \right)) (n - a \sqrt{n})^\frac{1}{2} \\
[ -2 - \epsilon(2 \left( \frac{2}{n} \right)) (n + a \sqrt{n})^\frac{1}{2} - \mu(2 \left( \frac{2}{n} \right)) (n - a \sqrt{n})^\frac{1}{2} \\
\end{cases} \\
\iff 0 = 4 - 2 \left( \frac{2}{n} \right) (n + a \sqrt{n}) - 2 \left( \frac{2}{n} \right) (n - a \sqrt{n}) \\
\iff 0 = 4 - 4 \left( \frac{2}{n} \right) n - 4 \epsilon\mu b \sqrt{n} \\
\iff \begin{cases} 
\epsilon(2 \left( \frac{2}{n} \right)) n - 1 \equiv -\epsilon\mu b \sqrt{n} \pmod{p}.
\end{cases}
\]

Similarly,
\[
\epsilon(2 \left( \frac{2}{n} \right)) n - 1 \equiv -\epsilon\mu b \sqrt{n} \pmod{p}.
\]

Therefore when \( p \mid b \), we have \( N = 2 \) if \( n \equiv (\frac{2}{n}) \pmod{p} \) and \( N = 0 \) otherwise.

When \( p \not\mid b \), we have \( N = 1 \) if \( 1 - \left( \frac{2}{n} \right) n \equiv b \sqrt{n} \) or \(-b \sqrt{n} \pmod{p} \) and \( N = 0 \) otherwise. Then the result follows from \( L_p(c_S) = n - \delta - \frac{n-1}{4} \cdot N \).

(3) For \( S = \{0, 1, 2\} \), we have
\[
N = \# \{ \lambda : 0 \leq \lambda \leq 3, \eta_\lambda + \eta_{\lambda+1} + \eta_{\lambda+2} = 0 \in \mathbb{F}_p \} 
= \# \{ \lambda : 0 \leq \lambda \leq 3, \eta_\lambda = -1 \} 
= \# \{ \lambda : 0 \leq \lambda \leq 3, g_\lambda = 1 + 4\eta_\lambda = -3 \}.
Direct computation shows that
\[
\prod_{\lambda=0}^{3} (x - (g_{\lambda} + 3)) = f(x-3) = x^{3} - 12x^{3} + 2B_{3}x^{2} + 4B_{1}x + B_{0}.
\]
If \( N = 4 \), then \( L_{p}(c_{S}) = 0 \) or 1 which is impossible since \( c_{S} \) is not a constant sequence. Therefore,
\[
\begin{align*}
N = 0 & \iff B_{0} \neq 0 \pmod{p}; \\
N = 1 & \iff B_{0} \equiv 0, B_{1} \neq 0 \pmod{p}; \\
N = 2 & \iff B_{0} \equiv B_{1} \equiv 0, B_{2} \neq 0 \pmod{p}; \\
N = 3 & \iff B_{0} \equiv B_{1} \equiv B_{2} \equiv 0 \pmod{p}, \ p \neq 3.
\end{align*}
\]
Then the final result follows from \( L_{p}(c_{i}) = n - \delta - \frac{n-1}{4} \cdot N \).

Remark 1. For \( e = 2 \) and \( e = 4 \), the linear complexity of the cyclotomic sequences have been determined in [16] and [4], respectively. But in this paper we use Gauss periods to compute \( L_{p}(c_{i}) \). By (3.4) and Theorem 1, we can deduce that the linear complexity \( L_{p}(c_{S}) \) of \( c_{S} \) can be computed by determining the values of \( \eta_{t} \), \( (0 \leq t \leq e - 1) \). It can be seen that the results of this paper are based on Theorem 3.1, which gives a formula on \( L_{p}(c_{S}) \) and the Gauss periods of order \( e. \) Hence, if the values of Gauss periods of order \( e \) are known, then \( L_{p}(c_{S}) \) can be computed. By the results in Theorem 4.1.2 and Theorem 4.1.4 of [2], the Gauss periods of order \( 6 \) can be determined. Therefore, the method presented in this paper works for the case \( e = 6 \). Here we omit it, since the computation is too complicated.

Remark 2. As pointed out by one of the anonymous reviewers, we consider the linear complexity of some segments of Legendre sequences. In brief, for the Legendre sequence \( c = (c_{0}, c_{1}, \ldots, c_{p-1}) \) we compute the linear complexity \( L_{2}(c') \) of \( c' \) by the help of NIST SP 800-22, where \( c' = (c_{k}, c_{k+1}, \ldots, c_{k+N-1}) \), \( k \) denotes the starting point of \( c' \) and \( N \) denotes the segment length of \( c' \). The results are listed in Table 1. From Table 1, we know Legendre sequences are complex enough in the view of linear complexity.

<table>
<thead>
<tr>
<th>period ( p )</th>
<th>the starting point ( k )</th>
<th>segment length ( N )</th>
<th>( L_{2}(c') )</th>
</tr>
</thead>
<tbody>
<tr>
<td>89</td>
<td>17</td>
<td>35</td>
<td>19</td>
</tr>
<tr>
<td>89</td>
<td>45</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>89</td>
<td>31</td>
<td>47</td>
<td>23</td>
</tr>
<tr>
<td>97</td>
<td>3</td>
<td>50</td>
<td>25</td>
</tr>
<tr>
<td>97</td>
<td>27</td>
<td>65</td>
<td>33</td>
</tr>
<tr>
<td>97</td>
<td>15</td>
<td>45</td>
<td>21</td>
</tr>
</tbody>
</table>

4. Concluding Remarks

From the results we know that once we fix an odd prime \( n \), the linear complexity of \( n \)-periodic cyclotomic sequences over \( \mathbb{F}_{p} \) is exactly \( n \) for all but a finite number of \( p \), which means that the sequences reach high complexity in many cases and can resist the attack of the Berlekamp-Massey algorithm [1], [10].

Acknowledgments

This work was supported by the National Science Foundation of China under grant No. 61602342, Natural Science Foundation of Tianjin under grant No. 18JQNCJC70300, the Science & Technology Development Fund of Tianjin Education Commission for Higher Education under grant No. 2018JKJ215, KYQD1817, the Key Laboratory of Applied Mathematics of Fujian Province University (Putian University) under grant No. SX201904 and No. SX201804, the China Scholarship Council (No. 201809345010 and No. 201907760008), the Science and Technology Development Fund of Tianjin Education Commission for Higher Education, No. 2017KJ237, NSFT No. 16JCYBJC41500 and No. 16JCYBJC42300, No. 16JCYBJC42300, NSFC No. 61872359, 61972456 and 61802281.

References