LETTER

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

Qiuyan WANG[†a)], ***Member and*** **Yang YAN**[††b)], ***Nonmember***

SUMMARY Periodic sequences, used as keys in cryptosystems, plays 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 $\mathbb{F}_q$. The linear complexity (also called linear span) of c over $\mathbb{F}_q$, denoted by $L_q(c)$, is defined to be the smallest positive integer l such that there are constants $a_0 \neq 0, a_1, \ldots, a_l \in \mathbb{F}_q$ satisfying $-a_0c_i = a_1c_{i-1} + a_2c_{i-2} + \cdots + a_lc_{i-l} = 0$ for all $i \geq l$. The Berlekamp-Massey algorithm [1], [10] states that if $L_q(c) > n/2$, then c is considered good with respect to its linear complexity.

For an odd prime n, let $n-1 = ek$ $(e \geq 2)$ and $\mathbb{F}_n$ be the finite field with n elements. Suppose θ is a primitive element of $\mathbb{F}_n^* = \mathbb{F}_n \backslash \{0\}$. Let

$$C_\lambda = C_\lambda^{(e)} = \theta^\lambda C_0, \qquad (0 \leq \lambda \leq e-1),$$

where $C_0 = \langle \theta^e \rangle$ is the subgroup of $\mathbb{F}_n^*$ generated by θ^e and C_λ $(0 \leq \lambda \leq e-1)$ are the cosets of C_0 in $\mathbb{F}_n^*$. 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

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

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 view point 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

$$c^\infty(x) = \sum_{n=0}^{\infty} c_n x^n = \frac{u(x)}{1-x^n},$$
$$u(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]$$

in the power series ring $\mathbb{F}_q[[x]]$.

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

$$c^\infty(x) = \frac{w(x)}{v(x)}, \qquad v(x) = \frac{1-x^n}{h(x)} \qquad w(x) = \frac{u(x)}{h(x)}$$

where $u(x), v(x), h(x) \in \mathbb{F}_q[x]$.

Manuscript received October 3, 2019.
Manuscript revised December 29, 2019.

[†]The author is with School of Computer Science and Technology, Tiangong University, Tianjin, China.
[††]The author is with School of Information Technology Engineering, Tianjin University of Technology and Education, Tianjin, China.
a) E-mail: wangyan198801@163.com
b) E-mail: yanyangucas@126.com

DOI: 10.1587/transfun.2019EAL2137

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 $1 - x^n$ has n distinct zeros ζ_n^i $(0 \le i \le n-1)$ in the algebraic closure Ω_q of $\mathbb{F}_q$. Let

$$m = \#\{i : 0 \le i \le n-1, u(\zeta_n^i) = 0\}.$$

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 $q = p^m$ $(p \ne n)$, let ζ_n be a primitive n-th root of unity in the algebraic closure Ω_q of $\mathbb{F}_q$. The Gauss periods of order e are defined by*

$$\eta_\lambda = \sum_{x \in C_\lambda} \zeta_n^x, \qquad (0 \le \lambda \le e-1).$$

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) $\sum_{\lambda=0}^{e-1} \eta_\lambda = -1$;

(2) For $a = \theta^s$, $\sum_{x \in C_\lambda} \zeta_n^{ax} = \eta_{s+\lambda}$;

(3) For $0 \le \lambda \le e-1$, let

$$g_\lambda = \sum_{x=0}^{n-1} \zeta_n^{x^e \theta^\lambda}.$$

Then

$$g_\lambda = 1 + e\eta_\lambda;$$

(4) For $p \in C_i$,

$$\eta_\lambda^p = \eta_{\lambda+i}.$$

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

$$n = a^2 + b^2, \qquad a, b \in \mathbb{Z},$$

where a is determined by $a \equiv -\left(\frac{2}{n}\right) \pmod 4$, the even integer b is determined up to sign and $\left(\frac{x}{n}\right)$ 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

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

(2) The discriminant of $f(x)$ is

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

Therefore, $f(x)$ has multiple zeros in Ω_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

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

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 $c_S = (c_i)_{i=0}^{\infty}$ with period n is defined by

$$c_i = \begin{cases} 1, & \text{if } (i \bmod n) \in \Sigma_S, \\ 0, & \text{otherwise,} \end{cases} \quad \text{for all } i \ge 0. \tag{3.1}$$

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

$$c(x) = \sum_{\substack{i=1 \\ i \in \Sigma_S}}^{n-1} x^i. \tag{3.2}$$

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

$$L_q(c_S) = n - \deg\ h(x). \tag{3.3}$$

Since the greatest common divisor of $c(x)$ and $1 - x^n$ 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 ζ_n be an n-th primitive root of unity

over the algebraic closure Ω_p of $\mathbb{F}_p$. Then

$$\deg\ h(x) = \#\{i : 0 \le\ i \le\ n-1,\ c(\zeta_n^i) = 0\},$$

where $h(x) = \gcd(x^n - 1, c(x))$. Notice that for $i = 0$, $c(1) = |S| \cdot k$. For $1 \le\ i \le\ n-1$, set $i \in\ C_t = \theta^t C_0$. Direct computation shows

$$\begin{aligned} c(\zeta_n^i) &= \sum_{\substack{x=1 \\ x\in\Sigma_S}}^{n-1} \zeta_n^{ix} \\ &= \sum_{\lambda\in S} \sum_{x\in C_\lambda} \zeta_n^{ix} \\ &= \sum_{\lambda\in S} \eta_{\lambda+t}, \end{aligned}$$

where η_λ is the Gauss period defined in Sect. 2. Let

$$A_t = A_{t,S} = \sum_{\lambda\in S} \eta_{\lambda+t} \in \Omega_p, \qquad (0 \le\ t \le\ n-2). \quad (3.4)$$

$$N = \#\{t : 0 \le t \le e-1, A_t = 0\}. \quad (3.5)$$

As $\eta_\lambda = \eta_{\lambda+e}$, we have $A_t = A_{t+e}$, hence

$$\begin{aligned} \deg\ h(x) &= \delta + \#\{t : 0 \le\ t \le\ n-2, A_t = 0\} \\ &= \delta + k \cdot \#\{t : 0 \le\ t \le\ e-1, A_t = 0\} \\ &= \delta + k \cdot\ N. \end{aligned}$$

where

$$\delta = \begin{cases} 1, & \text{if } |S| \cdot k \equiv 0 \pmod{p}, \\ 0, & \text{otherwise.} \end{cases} \quad (3.6)$$

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

Theorem 3.1 *Let $n - 1 = ek$, $p \ne n$ be an odd prime, and S be a non-empty subset of $\{0, 1, \ldots, e-1\}$. Then for the sequence $c_S = (c_i)_{i=0}^{\infty}$ defined by (3.1), we have*

$$L_p(c_S) = n - \delta - k \cdot\ N,$$

where N and δ 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 Ω_p. For a large **order** e, the following result simplifies the computation of $L_p(c_S)$.

Lemma 3.2 *Let $1 \le\ a \le\ e-1$ and S be a non-empty subset of $\mathbb{Z}_e = \{0, 1, \ldots, e-1\}$. If $S' = a + S = \{a + \lambda \pmod{e} : \lambda \in S\}$, then for any odd prime $p \ne n$, 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

$$\begin{aligned} &N = \#\{t : 0 \le\ t \le\ e-1, A_t = 0\}, \\ &N' = \#\{t : 0 \le\ t \le\ e-1, A_t' = 0\}, \\ &A_t = A_{t,S} = \sum_{\lambda\in S} \eta_{\lambda+t}, \end{aligned}$$

$$A_t' = A_{t,S'} = \sum_{\lambda\in S'} \eta_{\lambda+t} = \sum_{\lambda\in S} \eta_{\lambda+a+t}.$$

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

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 $1 \le |S| \le e-1$ in the sequel. By Lemma 3.2, it is enough to consider $S = \{0\}$ for $e = 2$ and $S = \{0\}, \{0, 1\}, \{0, 1, 2\}$ for $e = 4$.

3.1 Case $e = 2$

In this case, $n - 1 = 2k$, $\mathbb{F}_n^* = \langle\theta\rangle$, furthermore

$$\begin{aligned} C_0 = C_0^{(2)} &= \langle\theta^2\rangle = \left\{a : 1 \le\ a \le\ n-1, \left(\frac{a}{n}\right) = 1\right\}, \\ C_1 = C_1^{(2)} &= \theta C_0 = \left\{a : 1 \le\ a \le\ n-1, \left(\frac{a}{n}\right) = -1\right\}, \end{aligned}$$

where $(\frac{a}{n})$ is the Legendre symbol. From the explanation above, it is enough to consider $S = \{0\}$. In this case, the sequence $c = c_S = (c_i)_{i=0}^{\infty}$ is the Legendre sequence which is defined by

$$c_i = \begin{cases} 1, & \text{if } (i \bmod n) \in\ C_0, \\ 0, & \text{otherwise,} \end{cases} \quad \text{for all } i \ge 0. \quad (3.7)$$

Theorem 3.3 *Let $p \ne\ n$ be an odd prime. Then for the Legendre sequence c defined by* (3.7)*, we have*

$$L_p(c) = \begin{cases} \frac{n-1}{2}, & \text{if } n \equiv 1 \pmod 4 \text{ and } p \mid n-1, \\ \frac{n+1}{2}, & \text{if } n \equiv 3 \pmod 4 \text{ and } p \mid n+1, \\ n-1, & \text{if } n \equiv 3 \pmod 4 \text{ and } p \mid n-1, \\ n, & \text{otherwise.} \end{cases}$$

Proof. For $e = 2$ and $S = \{0\}$,

$$\begin{aligned} A_0 = \eta_0 &= \sum_{x\in C_0} \zeta_n^x, \\ A_1 = \eta_1 &= \sum_{x\in C_1} \zeta_n^x. \end{aligned}$$

By Theorem 3.1 and $k = \frac{n-1}{2}$, we know that

$$L_p(c) = n - \delta - \frac{n-1}{2} \cdot N. \quad (3.8)$$

where $N = \#\{\lambda : \lambda \in \{0, 1\}, \eta_\lambda = 0 \in \mathbb{F}_p\}$. By the definition of δ and $|S| = 1$, we know

$$\delta = \begin{cases} 1, & \text{if } p \mid (n-1), \\ 0, & \text{otherwise.} \end{cases}$$

For $g_\lambda = 1 + 2\eta_\lambda$, it is well known that [2],

$$(x - g_0)(x - g_1) = x^2 - \left(\frac{-1}{n}\right) n \quad (3.9)$$

From (3.9), we have

$$\{g_0, g_1\} = \left\{ \pm \sqrt{\left(\frac{-1}{n}\right) n} \right\}.$$

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

Since $\eta_0 + \eta_1 = -1$, η_0 and η_1 can not be zero at the same time. From (3.8), we get $L_p(c) \in \left\{ \frac{n\pm1}{2}, n, n-1 \right\}$ and

$$\begin{aligned} L_p(c) = \frac{n-1}{2} &\Leftrightarrow \delta = 1 \text{ and } N = 1 \\ &\Leftrightarrow p \mid n-1 \text{ and } 0 = \eta_0\eta_1 = \frac{1}{4}\left(1 - \left(\frac{-1}{n}\right) n\right) \\ &\Leftrightarrow p \mid n-1 \text{ and } p \mid 1 - \left(\frac{-1}{n}\right) n \\ &\Leftrightarrow p \mid n-1 \text{ and } n \equiv 1 \pmod 4. \end{aligned}$$

Similarly,

$$\begin{aligned} L_p(c) = \frac{n+1}{2} &\Leftrightarrow \delta = 0 \text{ and } N = 1 \\ &\Leftrightarrow p \nmid n-1 \text{ and } 0 = \eta_0\eta_1 = \frac{1}{4}\left(1 - \left(\frac{-1}{n}\right) n\right) \\ &\Leftrightarrow p \nmid n-1 \text{ and } p \mid 1 - \left(\frac{-1}{n}\right) n \\ &\Leftrightarrow n \equiv 3 \pmod 4 \text{ and } p \mid n+1. \end{aligned}$$

$$\begin{aligned} L_p(c) = n-1 &\Leftrightarrow \delta = 1 \text{ and } N = 0 \\ &\Leftrightarrow p \mid n-1 \text{ and } p \nmid 1 - \left(\frac{-1}{n}\right) n \\ &\Leftrightarrow n \equiv 3 \pmod 4 \text{ and } p \mid (n-1). \end{aligned}$$

For other cases, $L_p(c_S) = n$. This completes the proof. □

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

$$C_\lambda = C_\lambda^{(4)} = \theta^\lambda \langle \theta^4 \rangle, \qquad (0 \le \lambda \le 3).$$

The prime $n = 1 + 4k$ can be expressed as

$$n = a^2 + b^2,$$

where a is determined by $a \equiv -(\frac{2}{n}) \pmod 4$ and the even integer b is determined up to sign.

By Lemma 2.4, for $g_\lambda = 1 + 4\eta_\lambda$, we know

$$\begin{aligned} \prod_{\lambda=0}^{3}(x - g_\lambda) =& x^4 - 2n\left[1 + 2\left(\frac{2}{n}\right)\right]x^2 - 8\left(\frac{2}{n}\right)anx \\ &+ \left[1 - 4\left(\frac{2}{n}\right)\right]n^2 + 4b^2n, \end{aligned} \tag{3.10}$$

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

$$g_0 = \sqrt{n} + \varepsilon\left[2\left(\frac{2}{n}\right)(n + a\sqrt{n})\right]^{\frac{1}{2}}, \ \varepsilon \in \{\pm 1\}. \tag{3.11}$$

Since $C_0^{(4)} \cup C_2^{(4)} = C_0^{(2)}$ and $C_1^{(4)} \cup C_3^{(4)} = C_1^{(2)}$, by Theorem 1.2.4 in [2] we have

$$\begin{aligned} g_0 + g_2 &= 2 + 4(\eta_0 + \eta_2) \\ &= 2 + 4 \sum_{x \in C_0^{(4)} \cup C_2^{(4)}} \zeta_n^x \\ &= 2 + 4 \sum_{x \in C_0^{(2)}} \zeta_n^x \\ &= 2\sqrt{n}. \end{aligned}$$

From (3.11) we get

$$g_2 = \sqrt{n} - \varepsilon\left[2\left(\frac{2}{n}\right)\left(n + a\sqrt{n}\right)\right]^{\frac{1}{2}}, \ \varepsilon \in \{\pm 1\}. \tag{3.12}$$

Similarly,

$$g_1 + g_3 = 2 + 4(\eta_1 + \eta_3) = 2 + 4 \sum_{x \in C_1^{(2)}} \zeta_n^x = -2\sqrt{n}.$$

Then by (3.10) and the Viete's formula [15], we have

$$\begin{aligned} -2n\left[1 + 2\left(\frac{2}{n}\right)\right] &= (g_0 + g_2)(g_1 + g_3) + g_0g_2 + g_1g_3 \\ &= -4n + n - 2\left(\frac{2}{n}\right)(n + a\sqrt{n}) + g_1g_3. \end{aligned}$$

Therefore, $g_1g_3 = n - 2\left(\frac{2}{n}\right)(n - a\sqrt{n})$ and

$$z^2 - (g_1 + g_3)z + g_1g_3 = z^2 + 2\sqrt{n}z + n - 2\left(\frac{2}{n}\right)(n - a\sqrt{n}).$$

We get

$$\{g_1, g_3\} = \left\{ -\sqrt{n} \pm \left[2\left(\frac{2}{n}\right)(n - a\sqrt{n})\right]^{\frac{1}{2}} \right\}. \tag{3.13}$$

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*

$$\{\eta_0, \eta_2\} = \left\{ \frac{1}{4}\left(-1 + \sqrt{n} \pm \left[2\left(\frac{2}{n}\right)\left(n + a\sqrt{n}\right)\right]^{\frac{1}{2}} \right) \right\},$$

$$\{\eta_1, \eta_3\} = \left\{ \frac{1}{4}\left(-1 - \sqrt{n} \pm \left[2\left(\frac{2}{n}\right)\left(n - a\sqrt{n}\right)\right]^{\frac{1}{2}} \right) \right\}.$$

As we mentioned before, it is enough to consider the sequence c_S for $S = \{0\},\{0,1\}$ and $\{0,1,2\}$, where $c_S = (c_i)_{i=0}^{\infty}$ is defined by

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

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

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

where

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

$$N = \#\left\{ t : 0 \leq t \leq 3, \sum_{\lambda \in S} \eta_{\lambda+t} = 0 \in \mathbb{F}_p \right\}. \tag{3.17}$$

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 δ is defined by (3.16).

Proof. By Theorem 3.1, $L_p(c_S) = n - \delta - \frac{n-1}{4} \cdot N$, where δ 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 $\eta_\lambda^p = \eta_{\lambda+1}$ or $\eta_{\lambda+3}$, 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. □

Theorem 3.6 *If $p \in C_2$, then then the linear complexity of c_S with period n is given by*
(1) for $S = \{0\}$,

$$L_p(c_S) = \begin{cases} \frac{n-1}{2}, & \text{if } n \equiv 1 \pmod p \text{ and } a \equiv -1 \pmod p, \\ n-1, & \text{if } n \equiv 1 \pmod p \text{ and } a \not\equiv -1 \pmod p, \\ n, & \text{otherwise.} \end{cases}$$

(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 δ is defined by (3.16).

Proof. If $p \in C_2$, then $\eta_\lambda^p = \eta_{\lambda+2}$ for $0 \leq \lambda \leq 3$.
(1) For $S = \{0\}$, by the value of η_λ given in Lemma 3.4, we know that

$$\begin{aligned} \eta_0 = 0 &\Leftrightarrow \eta_2 = 0 \\ &\Leftrightarrow -1 + \sqrt{n} \pm \left[2\left(\frac{2}{n}\right)\left(n + a\sqrt{n}\right) \right]^{\frac{1}{2}} = 0 \in \mathbb{F}_p \\ &\Leftrightarrow \sqrt{n} = 1 \text{ and } a + \sqrt{n} = 0 \text{ in } \mathbb{F}_p \\ &\Leftrightarrow \sqrt{n} \equiv 1 \text{ and } a \equiv -1 \pmod p. \end{aligned}$$

By a similar computation,

$$\begin{aligned} \eta_1 = 0 &\Leftrightarrow \eta_3 = 0 \\ &\Leftrightarrow \sqrt{n} \equiv -1 \text{ and } a \equiv -1 \pmod p. \end{aligned}$$

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 $(\eta_\lambda + \eta_{\lambda+1})^p = \eta_{\lambda+2} + \eta_{\lambda+3}$ and $\eta_\lambda + \eta_{\lambda+1} + \eta_{\lambda+2} + \eta_{\lambda+3} = -1$,
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 $S = \{0,1,2\}$,

$$\begin{aligned} N &= \#\{\lambda : 0 \leq \lambda \leq 3, \eta_\lambda + \eta_{\lambda+1} + \eta_{\lambda+2} = 0\} \\ &= \#\{\lambda : 0 \leq \lambda \leq 3, \eta_\lambda = -1\}. \end{aligned}$$

But

$$\begin{aligned} \eta_0 = -1 &\Leftrightarrow \eta_2 = -1 \\ &\Leftrightarrow \frac{1}{4}\left(-1 + \sqrt{n} \pm \left[2\left(\frac{2}{n}\right)\left(n + a\sqrt{n}\right) \right]^{\frac{1}{2}} \right) = -1 \in \mathbb{F}_p \\ &\Leftrightarrow \sqrt{n} + a = 0 \text{ and } -1 + \sqrt{n} = -4 \\ &\Leftrightarrow \sqrt{n} \equiv -3 \text{ and } a \equiv 3 \pmod p. \end{aligned}$$

By a similar computation,

$$\begin{aligned} \eta_1 = -1 &\Leftrightarrow \eta_3 = -1 \\ &\Leftrightarrow \frac{1}{4}\left(-1 - \sqrt{n} \pm \left[2\left(\frac{2}{n}\right)(n - a\sqrt{n}) \right]^{\frac{1}{2}} \right) = -1 \in \mathbb{F}_p \\ &\Leftrightarrow \sqrt{n} \equiv a \equiv 3 \pmod p. \end{aligned}$$

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). □

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

$$L_p(c_S) = \begin{cases} n - \delta, & if\ A_0 \not\equiv 0 \pmod p, \\ \frac{3n+1}{4} - \delta, & if\ A_0 \equiv 0, A_1 \not\equiv 0 \pmod p, \\ \frac{n+1}{2} - \delta, & if\ A_0 \equiv A_1 \equiv 0, A_2 \not\equiv 0 \pmod p, \\ \frac{n+3}{4} - \delta, & if\ A_0 \equiv A_1 \equiv A_2 \equiv 0 \pmod p. \end{cases}$$

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

$$L_p(c_S) = \begin{cases} \frac{n+1}{2} - \delta, & if\ n \equiv \left(\frac{2}{p}\right) \pmod p\ and\ p \mid b, \\ \frac{3n+1}{4} - \delta, & if\ 1 - \left(\frac{2}{n}\right)n \equiv \pm b\sqrt{n} \pmod p \\ & and\ p \nmid b, \\ n - \delta, & otherwise. \end{cases}$$

(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

$$L_p(c_S) = \begin{cases} n - \delta, & if\ B_0 \not\equiv 0 \pmod p, \\ \frac{3n+1}{4} - \delta, & if\ B_0 \equiv 0, B_1 \not\equiv 0 \pmod p, \\ \frac{n+1}{2} - \delta, & if\ B_0 \equiv B_1 \equiv 0, B_2 \not\equiv 0 \pmod p, \\ \frac{n+3}{4} - \delta, & if\ B_0 \equiv B_1 \equiv B_2 \equiv 0 \pmod p. \end{cases}$$

where δ is defined by (3.16).

Proof. (1) For $S = \{0\}$, we have

$$L_p(c_S) = n - \delta - \frac{n-1}{4} \cdot N,$$

where

$$\delta = \begin{cases} 1, & \text{if } n - 1 \equiv 0 \pmod p, \\ 0, & \text{otherwise.} \end{cases}$$

and

$$N = \#\{\lambda : 0 \le \lambda \le 3, \eta_\lambda = 0\}$$
$$= \#\{\lambda : 0 \le \lambda \le 3, g_\lambda = 1 + 4\eta_\lambda = 1\},$$

According to Lemma 2.4,

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

Then

$$\prod_{\lambda=0}^{3}(x - (g_\lambda - 1)) = f(x+1) = x^4 + 4x^3 + 2A_2x^2 + 4A_1x + A_0.$$

Therefore,

$$N = 0 \iff A_0 \not\equiv 0 \pmod p;$$
$$N = 1 \iff A_0 \equiv 0, A_1 \not\equiv 0 \pmod p;$$
$$N = 2 \iff A_0 \equiv A_1 \equiv 0, A_2 \not\equiv 0 \pmod p;$$
$$N = 3 \iff A_0 \equiv A_1 \equiv A_2 \equiv 0 \pmod p.$$

The final result follows from $L_p(c_S) = n - \delta - \frac{n-1}{4} \cdot N$.
(2) For $S = \{0, 1\}$, then

$$N = \#\{\lambda : 0 \le \lambda \le 3, \eta_\lambda + \eta_{\lambda+1} = 0\}.$$

As $\eta_0 + \eta_1 + \eta_2 + \eta_3 = -1$, we have
either $\eta_0+\eta_1$ or $\eta_2+\eta_3$ is zero $\iff$ $(\eta_0+\eta_1)(\eta_2+\eta_3) = 0$

$$\begin{aligned} \iff \quad 0 \quad = \quad & [-1 + \sqrt{n} + \varepsilon\left(2\left(\tfrac{2}{n}\right)(n + a\sqrt{n})\right)^{\frac{1}{2}} \\ & -1 - \sqrt{n} + \mu(2\left(\tfrac{2}{n}\right)(n - a\sqrt{n}))^{\frac{1}{2}}]\cdot \\ & [-1 + \sqrt{n} - \varepsilon(2\left(\tfrac{2}{n}\right)(n + a\sqrt{n}))^{\frac{1}{2}} \\ & -1 - \sqrt{n} - \mu(2\left(\tfrac{2}{n}\right)(n - a\sqrt{n}))^{\frac{1}{2}}] \\ & (\varepsilon, \mu \in \{\pm 1\}) \\ = \quad & [-2 + \varepsilon(2\left(\tfrac{2}{n}\right)(n + a\sqrt{n}))^{\frac{1}{2}} + \mu(2\left(\tfrac{2}{n}\right) \\ & (n - a\sqrt{n}))^{\frac{1}{2}}]\cdot \\ & [-2 - \varepsilon(2\left(\tfrac{2}{n}\right)(n + a\sqrt{n}))^{\frac{1}{2}} - \mu(2\left(\tfrac{2}{n}\right) \\ & (n - a\sqrt{n}))^{\frac{1}{2}}] \\ = \quad & 4 - 2\left(\tfrac{2}{n}\right)(n + a\sqrt{n}) - 2\left(\tfrac{2}{n}\right)(n - a\sqrt{n}) \\ & -2\varepsilon\mu\left(4(n^2 - a^2n)\right)^{\frac{1}{2}} \\ = \quad & 4 - 4\left(\tfrac{2}{n}\right)n - 4\varepsilon\mu b\sqrt{n} \\ \iff \quad & \left(\tfrac{2}{n}\right)n - 1 \equiv -\varepsilon\mu b\sqrt{n} \pmod p. \end{aligned}$$

Similarly,

either $\eta_1 + \eta_2$ or $\eta_0 + \eta_3$ is zero $\Leftrightarrow (\eta_1 + \eta_2)(\eta_0 + \eta_3) = 0$

$$\Leftrightarrow \left(\frac{2}{n}\right)n - 1 \equiv \varepsilon\mu\, b\sqrt{n} \pmod p.$$

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

$$N = \#\left\{\lambda : 0 \le \lambda \le 3, \eta_\lambda + \eta_{\lambda+1} + \eta_{\lambda+2} = 0 \in \mathbb{F}_p\right\}$$
$$= \#\{\lambda : 0 \le \lambda \le 3, \eta_\lambda = -1\}$$
$$= \#\{\lambda : 0 \le \lambda \le 3, g_\lambda = 1 + 4\eta_\lambda = -3\}.$$

Table 1 The linear complexity of some segments of Legendre sequences.

period p	the starting point k	segment length N	$L_2(c^{'})$
$p = 89$	17	35	19
$p = 89$	45	20	10
$p = 89$	31	47	23
$p = 97$	3	50	25
$p = 97$	27	65	33
$p = 97$	15	45	21

Direct computation shows that

$$\prod_{\lambda=0}^{3}(x-(g_\lambda+3)) = f(x-3) = x^4-12x^3+2B_2x^2+4B_1x+B_0.$$

If $N = 4$, then $L_p(c_S) = 0$ or 1 which is impossible since c_S is not a constant sequence. Therefore,

$$\begin{aligned}
&N = 0 \iff B_0 \not\equiv 0 \pmod{p};\\
&N = 1 \iff B_0 \equiv 0, B_1 \not\equiv 0 \pmod{p};\\
&N = 2 \iff B_0 \equiv B_1 \equiv 0, B_2 \not\equiv 0 \pmod{p};\\
&N = 3 \iff B_0 \equiv B_1 \equiv B_2 \equiv 0 \pmod{p},\ p \neq 3.
\end{aligned}$$

Then the final result follows from $L_p(c_s) = n - \delta - \frac{n-1}{4} \cdot N$. This finishes the proof. □

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 uniformly compute $L_p(c)$. 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 η_t $(0 \le t \le e-1)$. 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.*

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. 18JCQNJC70300, the Science & Technology Development Fund of Tianjin Education Commission for Higher Education under grant No. 2018KJ215, 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, NFSC No. 61872359, 61972456 and 61802281.

References

[1] E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.
[2] B.C. Berndt, R.J. Evans, and K.S. Williams, Gauss and Jacobi Sums, Wiley, New York, 1998.
[3] T.W. Cusick, C. Ding, and A. Renvall, Stream Ciphers and Number Theorey, North Holland, Amsterdam, 1998.
[4] C. Ding, "Cyclotomic codes from cyclotomic sequences of order four," Finite Fields and Their Applications, vol.23, pp.8–34, 2013.
[5] C. Ding, T. Helleseth, and W. Shan, "On the linear complexity of Legendre sequences," IEEE Trans. Inf. Theory, vol.44, no.3, pp.1276–1278, 1998.
[6] C. Ding and T. Helleseth, "On cyclotomic generator of order r," Inform. Process. Lett., vol.66, no.1, pp.21–25, 1998.
[7] V.A. Edemskii, "On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes," Discrete Math. Appl., vol.20, no.1, pp.75–84, 2010.
[8] T. Helleseth, "On the crosscorrelation of m-sequences and related sequences with ideal autocorrelation," Sequences and their Applications (Bergen, 2001), pp.34–45, Discrete Math. Theor. Comput. Sci. (Lond.), Springer, London, 2002.
[9] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, New York, 1997.
[10] J.L. Massey, "Shift register synthesis and BCH decoding," IEEE Trans. Inf. Theory, vol.15, no.1, pp.122–127, 1969.
[11] W. Meidl and A. Winterhof, "On the autocorrelation of cyclotomic generators," International Conference on Finite Fields and Applications, Springer, Berlin, Heidelberg, 2003.
[12] R.E.A.C. Paley, "On orthogonal matrices," J. Math. Phys., vol.12, no.1-4, pp.311–320, 1933.
[13] O. Perron, "Bemerkungen über die Verteilung der quadratischen Reste," Math. Z., vol.56, pp.122–130, 1952.
[14] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, Berlin, 1986.
[15] E.B. Vinberg, A Course in Algebra, American Mathematical Society Providence, Rhode Island, 2003.
[16] Q. Wang, D. Lin, and X. Guang, "On the linear complexity of Legendre sequences over $\mathbb{F}_q$," IEICE Trans. Fundamentals, vol.E97-A, no.7, pp.1627–1630, July 2014.