Hindawi
Complexity
Volume 2019, Article ID 8635209, 7 pages
https://doi.org/10.1155/2019/8635209

Research Article

On the k-Error Linear Complexity of Binary Sequences Derived from the Discrete Logarithm in Finite Fields

Zhixiong Chen[1] **and Qiuyan Wang**[1,2]

[1] *Provincial Key Laboratory of Applied Mathematics, Putian University, Putian, Fujian 351100, China*
[2] *School of Computer Science and Technology, Tianjin Polytechnic University, Tianjin 300387, China*

Correspondence should be addressed to Qiuyan Wang; wangyan198801@163.com

Received 27 February 2019; Accepted 13 June 2019; Published 4 July 2019

Academic Editor: Carlos F. Aguilar-Ibáñez

Let $\mathbb{F}_q$ be the finite field with $q = p^r$ elements, where p is an odd prime. For the ordered elements $\xi_0, \xi_1, \ldots, \xi_{q-1} \in \mathbb{F}_q$, the binary sequence $\sigma = (\sigma_0, \sigma_1, \ldots, \sigma_{q-1})$ with period q is defined over the finite field $\mathbb{F}_2 = \{0, 1\}$ as follows: $\sigma_n = \{0$, if $n = 0$, $(1 - \chi(\xi_n))/2$, if $1 \le n < q\}$, $\sigma_{n+q} = \sigma_n$, where χ is the quadratic character of $\mathbb{F}_q$. Obviously, σ is the Legendre sequence if $r = 1$. In this paper, our first contribution is to prove a lower bound on the linear complexity of σ for $r \ge 2$, which improves some results of Meidl and Winterhof. Our second contribution is to study the distribution of the k-error linear complexity of σ for $r = 2$. Unfortunately, the method presented in this paper seems not suitable for the case $r > 2$ and we leave it open.

1. Introduction

Pseudorandom sequences play an important role in cryptography; for example, they are used as keys in private-key cryptosystems [1, 2]. One of the most remarkable cryptosystems is the one-time pad (also referred to as Vernam cipher), where the plaintext message is added bit by bit (or in general character by character) to a nonrepeating random sequence of the same length [1, 2]. The security of the one-time pad entirely relies on the key sequence with special cryptographic properties, such as the balance, small correlation, and high linear complexity [3]. There are many ways to design suitable sequences. Legendre sequence introduced below is a classic sequence defined using (multiplicative) character of finite fields.

Let p be an odd prime; the *Legendre sequence* $\ell = (\ell_0, \ell_1, \ldots, \ell_{p-1})$ of period p is defined as

$$\ell_n = \begin{cases} 0, & \text{if } n \equiv 0 \bmod p, \\ \dfrac{1 - (n/p)}{2}, & \text{otherwise}, \end{cases} \tag{1}$$

where $(\cdot/p)$ is the Legendre symbol. Legendre sequence has a number of good properties; the reader is referred to [4–8] for details.

It is natural to extend the Legendre symbol construction to the extension field $\mathbb{F}_q$ of $\mathbb{F}_p$, where $q = p^r$. We define below an ordered set for $\mathbb{F}_q$.

For a fix basis $\{\gamma_1 = 1, \gamma_2, \ldots, \gamma_r\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$, we define for $0 \le n < q$

$$\xi_n = n_1\gamma_1 + n_2\gamma_2 + \cdots + n_r\gamma_r, \tag{2}$$

if

$$n = n_1 + n_2 p + \cdots + n_r p^{r-1}, \quad 0 \le n_i < p, \ i = 1, \ldots, r. \tag{3}$$

Then $\mathbb{F}_q = \{\xi_0 = 0, \xi_1 = 1, \ldots, \xi_{q-1}\}$.

Given a primitive element $\alpha \in \mathbb{F}_q$ and any $\beta \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, the *discrete logarithm* of β with respect to α is the integer k, $0 \le k < q - 1$, satisfying the following.

$$\beta = \alpha^k \tag{4}$$

We write $k = \operatorname{ind}_\alpha(\beta)$. The computation of discrete logarithms is of considerable importance in cryptography. The

security of many public-key cryptosystems depends on the intractability of the discrete logarithm problem [9].

Then the (d-ary) discrete logarithm sequence $\sigma = (\sigma_0, \sigma_1, \ldots, \sigma_{q-1})$ of period q is derived for an integer $d > 1$:

$$\sigma_n = \begin{cases} 0, & \text{if } n = 0, \\ \operatorname{ind}_{\alpha,d}(\xi_n), & \text{if } 1 \le n < q, \end{cases} \qquad \sigma_{n+q} = \sigma_n, \tag{5}$$

where $\xi_n \in \mathbb{F}_q^*$ and $\operatorname{ind}_{\alpha,d}(\xi_n) \in \{0, 1, \ldots, d-1\}$ denotes $\operatorname{ind}_\alpha(\xi_n) \bmod d$. The autocorrelation of σ was analyzed in [10] and its linear complexity was studied in [11, 12].

In cryptographic applications, attention has been focused on the binary sequences over the finite field $\mathbb{F}_2$, since arithmetic is much easier to implement, with respect to both software and hardware. Therefore in this work we consider the case of $d = 2$. Then the binary sequence σ given by (5) can be defined equivalently as

$$\sigma_n = \begin{cases} 0, & \text{if } n = 0, \\ \dfrac{(1 - \chi(\xi_n))}{2}, & \text{if } 1 \le n < q, \end{cases} \qquad \sigma_{n+q} = \sigma_n, \tag{6}$$

where χ is the quadratic character of $\mathbb{F}_q$ and $\xi_n \in \mathbb{F}_q$ for $1 \le n < q$. Indeed, the *multiplicative characters* of the finite filed $\mathbb{F}_q$ [13] are given by

$$\psi_j(\alpha^i) = e^{2\pi\sqrt{-1}ij/(p-1)}, \quad i = 0, 1, \ldots, q-2, \tag{7}$$

for a primitive element of $\alpha \in \mathbb{F}_q^*$ and the quadratic character $\chi = \psi_{(q-1)/2}$ satisfies

$$\chi(\beta) = \begin{cases} 1, & \text{if } \beta \text{ is the square of an element of } \mathbb{F}_q^*, \\ -1, & \text{otherwise.} \end{cases} \tag{8}$$

It is easy to see that σ is balanced ($(q+1)/2$ many 0's and $(q-1)/2$ many 1's) with least period q. The measures of pseudorandomness of the binary sequence σ were studied in [14] and some related problems were considered in [15–17]. It is noted that when $r = 1$, the σ is just the Legendre sequence ℓ introduced above. Its linear complexity has been determined in [6], and its k-error linear complexity over $\mathbb{F}_p$ has been calculated by Aly and Winterhof [18]. Therefore, it is natural to investigate the linear complexity of the binary sequence σ in (6) and its k-error linear complexity for $r \ge 2$.

We organize our contributions as follows. The coming section contains the notions of the linear complexity and k-error linear complexity of periodic sequences. In Section 3, we give a lower bound on the linear complexity of σ in (6) for $r \ge 2$. In Section 4, we present k-error linear complexity of σ for $r = 2$. It should be noted that the results are different from [18, 19], in which the binary sequence σ is treated over $\mathbb{F}_p$. Finally in Section 5, we draw some conclusions and present some open problems.

2. Preliminaries

In this section, we recall the notions of linear complexity and k-error linear complexity of periodic sequences over the finite field $\mathbb{F}_2$.

Let $s = (s_0, s_1, \ldots, s_{N-1})$ be a binary sequence over $\mathbb{F}_2$ of period N. The *linear complexity* of s, denoted by $L(s)$, is the smallest positive integer l satisfying the following linear recurrence relation

$$s_{i+l} = c_{l-1}s_{i+l-1} + \ldots + c_1 s_{i+1} + c_0 s_i \quad \text{for } i \ge 0, \tag{9}$$

where $c_0, c_1, \ldots, c_{l-1} \in \mathbb{F}_2$. From the viewpoint of engineers, the linear complexity (also called linear span) of a sequence s is the shortest length of a linear feedback shift register (LFSR) that produces s. Hence the linear complexity provides information on predictability and thus unsuitability for cryptography and plays an important role in the analysis of stream ciphers.

Let $c(x) = 1 + c_{l-1}x + c_{l-2}x^2 + \cdots + c_0 x^l$, which is called a *characteristic polynomial* of s. A characteristic polynomial with the smallest degree is called a *minimal polynomial* of s [1]. Let $s(x) = s_0 + s_1 x + \cdots + s_{N-1}x^{N-1} \in \mathbb{F}_2[x]$, which is called the *generating polynomial* of s. Then the following lemma gives a way to determine the linear complexity and minimal polynomial of periodic sequences.

Lemma 1 (see [13]). *Let s be a binary sequence over $\mathbb{F}_2$ of period N. Then the minimal polynomial $m(x)$ of s is*

$$m(x) = \frac{x^N - 1}{\gcd(x^N - 1, s(x))}, \tag{10}$$

and the linear complexity $L(s)$ of s is given by

$$N - \deg\left(\gcd\left(x^N - 1, s(x)\right)\right), \tag{11}$$

where $s(x)$ is the generating polynomial of s.

Not only should periodic sequences used as key-streams have a large linear complexity, but also altering a few bits should not cause a significant decrease of the linear complexity. Hence we have the following notion.

Definition 2 (see [20]). Let s be a binary sequence over $\mathbb{F}_2$ of period N. For $k \ge 1$, the k-error linear complexity $L_k(s)$ of s is the smallest linear complexity of a sequence s' obtained from s by altering at most k elements among s_i $(0 \le i \le N-1)$ and continuing these changes periodically with the period N.

The concept of k-error linear complexity (the sphere complexity, a similar notion of k-error linear complexity, was defined even earlier, please see [1] for details) is very useful in the study of the security of stream ciphers for cryptographic applications. A necessary condition for a key-stream generator is that sequences produced by it should possess high linear complexity and k-linear complexity. An efficient algorithm for determining the k-error linear complexity of binary sequences of period 2^n was designed by Stamp and Martin in [20], and it was generalized to p^n-periodic sequences over the finite field $\mathbb{F}_{p^m}$, where p is an odd prime [21].

3. A Lower Bound on Linear Complexity

In this section, we prove a lower bound on the linear complexity of the binary sequence σ defined by (6) for $r \geq 2$. A bound also has been given in [11, 12], but the result in Theorem 4 improves that in [11, 12] greatly.

Let $\mathrm{ord}_m(2)$ denote the *order* of 2 modulo m; i.e., $\mathrm{ord}_m(2)$ is the smallest positive integer d such that $2^d \equiv 1 \pmod{m}$.

Lemma 3. *Let $\lambda = \mathrm{ord}_p(2)$ with $1 < \lambda < p$. For $r \geq 2$, if $2^{p-1} \not\equiv 1 \pmod{p^2}$, we have*

$$\mathrm{ord}_{p^r}(2) = \lambda p^{r-1}. \tag{12}$$

Proof. Suppose $\mu = \mathrm{ord}_{p^r}(2)$. By $2^\lambda \equiv 1 \pmod{p}$, we have $2^\lambda = 1 + ap$ for some integer a. It is easy to verify that

$$\begin{aligned} 2^{\lambda p^{r-1}} &= (1+ap)^{p^{r-1}} = 1 + ap^r + \ldots, \\ 2^{\lambda p^{r-1}} &\equiv 1 \pmod{p^r}. \end{aligned} \tag{13}$$

This implies that μ is a divisor of λp^{r-1}. Since $2^{p-1} \not\equiv 1 \pmod{p^2}$, we see that $a \not\equiv 0 \pmod{p}$.

The assumption $2^{p-1} \not\equiv 1 \pmod{p^2}$ implies that $\mu \geq p$. Then we write $\mu = \lambda p^w$ for some positive integer w and $w \leq r-1$. Supposing $w < r-1$, we have

$$2^{\lambda p^w} = (1+ap)^{p^w} = 1 + ap^{w+1} + \ldots, \tag{14}$$

which contradicts the fact that $2^\mu = 2^{\lambda p^w}$ and $2^{\lambda p^w} \equiv 1 \pmod{p^r}$. Hence $w = r-1$ and $\mu = \lambda p^{r-1}$. This completes the proof of this lemma. □

Theorem 4. *Let symbols be the same as before. If $2^{p-1} \not\equiv 1 \bmod p^2$, then the linear complexity of σ in (6) with period $q = p^r$ $(r \geq 2)$ satisfies*

$$L(\sigma) \geq \lambda p^{r-1}, \tag{15}$$

where λ is the order of 2 modulo p and $1 < \lambda < p$.

Proof. By the definition of σ, we know that the least period of σ is $q = p^r$. Let

$$\begin{aligned} \Phi^{(r)}(x) &= 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \ldots + x^{(p-1)p^{r-1}} \\ &\in \mathbb{F}_2[x]. \end{aligned} \tag{16}$$

Then $x^{p^r} - 1 = (x^{p^{r-1}} - 1) \cdot \Phi^{(r)}(x)$ and $\Phi^{(r)}(x)$ has exactly $p^r - p^{r-1}$ roots, which are p^r-th primitive elements in the algebraic closure of $\mathbb{F}_2$. By Lemma 3, the polynomial $\Phi^{(r)}(x)$ can be written as the product of $(p-1)/\lambda$ irreducible polynomials of degree λp^{r-1}, i.e.,

$$\Phi^{(r)}(x) = \varphi_1^{(r)}(x)\, \varphi_2^{(r)}(x) \cdots \varphi_{(p-1)/\lambda}^{(r)}(x). \tag{17}$$

In the sequel, we will show that there exists i_0 $(1 \leq i_0 \leq (p-1)/\lambda)$ such that $\varphi_{i_0}^{(r)}(x) \nmid s(x)$, where $s(x)$ is the generating polynomial of σ.

Suppose $\Phi^{(r)}(x) \mid s(x)$; then $s(x) = H(x) \cdot \Phi^{(r)}(x)$ for some polynomial $H(x) = h_0 + h_1 x + \ldots + h_{p^{r-1}-1} x^{p^{r-1}-1} \in \mathbb{F}_2[x]$ of degree $< p^{r-1}$. By the product of two polynomials, we obtain

$$\sigma_i = \sigma_{i+p^{r-1}} = \ldots = \sigma_{i+(p-1)p^{r-1}} = \begin{cases} 0, & \text{if } h_i = 0, \\ 1, & \text{if } h_i = 1, \end{cases} \tag{18}$$

for $0 \leq i < p^{r-1}$, which implies $\sigma_n = \sigma_{n+p^{r-1}}$ for any integer n and hence the period of σ equals p^{r-1}. This contradicts the fact that σ is a p^r-periodic sequence. Hence there exists at least one $\varphi_{i_0}^{(r)}(x)$ such that $\varphi_{i_0}^{(r)}(x) \nmid s(x)$ and then $\Phi^{(r)}(x) \nmid s(x)$. By Lemma 1, we have

$$L(\sigma) \geq \deg\left(\varphi_{i_0}^{(r)}(x)\right) = \lambda p^{r-1}. \tag{19}$$

□

The bound is much better than that of [11, Thms. 1 and 2] and [12]. Some examples are listed in Table 1. The bound is tight for certain q; see, for example, $q = 25$ in the table. It should emphasized that Theorem 4 is indeed a general result for any p^r-periodic binary sequences over $\mathbb{F}_2$.

Prop. 2 in [22] indicates that the linear complexity of p^r-periodic sequences over $\mathbb{F}_{p^m}$ is at least $p^{r-1} + 1$. Theorem 4 is a similar statement to that in [22] for binary sequences. We remark that Theorem 4 covers almost all primes. It is shown that primes satisfying $2^{p-1} \equiv 1 \pmod{p^2}$ are very rare. Up to 6×10^{17}, there are only two such primes (a prime p satisfying $2^{p-1} \equiv 1 \bmod p^2$ is called a Wieferich prime), 1093 and 3511 [23].

4. k-Error Linear Complexity

In this section we let $q = p^2$. The proof of Theorem 4 helps us to give a lower bound on the k-error linear complexity of σ in (6). We choose $\{1, \gamma\}$ as a basis of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$. Then for $n = n_1 + n_2 p$ with $0 \leq n_1,\ n_2 < p$, we write $\xi_n = n_1 + n_2\gamma \in \mathbb{F}_{p^2}$.

We first prove some lemmas.

Lemma 5. *For $0 \leq i < p$, let $T_i = \{i + j\gamma :\ 0 \leq j < p\} \subseteq \mathbb{F}_{p^2}$. Then we have*

$$i \cdot T_1 = \{i(1 + j\gamma) :\ 0 \leq j < p\} = T_i. \tag{20}$$

Proof. For each $1 \leq i < p$, when j runs through the set $\{0, 1, \ldots, p-1\}$, so does $[ij]$, where $[ij]$ denotes $ij \bmod p$. Then, for $0 \leq j_1,\ j_2 < p$, we have

$$\begin{aligned} i(1 + j\gamma) &= i + [ij]\gamma \in T_i, \\ i(1 + j_1\gamma) &\neq i(1 + j_2\gamma), \end{aligned} \tag{21}$$

if $j_1 \neq j_2$. The proof is finished. □

Lemma 6. *For the binary sequence σ in (6), let $\mathbf{v_i} = (\sigma_i, \sigma_{i+p}, \ldots, \sigma_{i+(p-1)p}) \in \mathbb{F}_2^p$ and $wt(\mathbf{v_i})$ denotes the weight of the vector $\mathbf{v_i}$. Then we have the following:*

Table 1: Comparison of bounds on $L(\sigma)$.

$q = p^r$	exact value of $L(\sigma)$	our bound	Meidl and Winterhof's bound
$q = 5^2$	20	20	1 (by [11, Thm. 2])
$q = 5^3$	124	100	6 (by [11, Thm. 1])
$q = 5^4$	620	500	2 (by [12, Coro. 1])
$q = 5^5$	3124	2500	10 (by [11, Thm. 1])
$q = 5^6$	15620	12500	3 (by [12, Coro. 1])
$q = 7^3$	340	147	9 (by [11, Thm. 1])
$q = 7^4$	2394	1029	2 (by [12, Coro. 1])

(1) *for* $1 \le i < p$, $wt(\mathbf{v_0}) = p - 1$ *and* $wt(\mathbf{v_i}) = (p-1)/2$ *if* $\chi(\gamma) = -1$;

(2) *for* $1 \le i < p$, $wt(\mathbf{v_0}) = 0$ *and* $wt(\mathbf{v_i}) = (p+1)/2$ *if* $\chi(\gamma) = 1$.

Proof. Firstly, we show $\chi(i) = 1$ for any $i \in \{1, 2, \ldots, p-1\} \subseteq \mathbb{F}_{p^2}$. Since χ is the quadratic character of $\mathbb{F}_{p^2}$, χ can be written as $\chi = \eta^{(p^2-1)/2}$, where η is a character of order $p^2 - 1$ of $\mathbb{F}_{p^2}$. From $i^{(p^2-1)/2} = (i^{p-1})^{(p+1)/2} = 1 + ap$ for some integer a, we have

$$\chi(i) = \eta\left(i^{(p^2-1)/2}\right) = \eta(1) = 1. \tag{22}$$

Consequently, for $1 \le j < p$, we obtain $\chi(\xi_{jp}) = \chi(j\gamma) = \chi(j)\chi(\gamma) = \chi(\gamma)$. Then we derive

$$wt(\mathbf{v_0}) = \begin{cases} p-1, & \text{if } \chi(\gamma) = -1, \\ 0, & \text{otherwise.} \end{cases} \tag{23}$$

Secondly, by (6), we see that $\chi(\xi_n) = (-1)^{\sigma_n}$ for any $0 \ne \xi_n \in \mathbb{F}_{p^2}$. Hence by Lemma 5, $wt(\mathbf{v_i}) = wt(\mathbf{v_j})$ for $1 \le i \ne j < p$. Since there are $(p^2-1)/2$ many $\xi_n \in \mathbb{F}_{p^2}$ such that $\chi(\xi_n) = 1$, we have

$$\sum_{0 \le i < p} wt(\mathbf{v_i}) = \frac{(p^2-1)}{2}. \tag{24}$$

Hence, for $1 \le i < p$

$$wt(\mathbf{v_i}) = \begin{cases} \dfrac{p-1}{2}, & \text{if } \chi(\gamma) = -1, \\ \dfrac{p+1}{2}, & \text{otherwise.} \end{cases} \tag{25}$$

□

For the binary sequence σ defined in (6) with $q = p^2$, let

$$V_i(x) = \sum_{j=0}^{p-1} \sigma_{i+jp} x^{i+jp}, \quad 0 \le i < p. \tag{26}$$

Then the generating polynomial of σ is $s(x) = \sum_{i=0}^{p-1} V_i(x)$.

Theorem 7. *Let symbols be the same as before. If* $2^{p-1} \not\equiv 1 \pmod{p^2}$, *then the k-error linear complexity of* σ *in (6) with period* p^2 *satisfies*

$$L_k(\sigma) \ge \lambda p, \tag{27}$$

where λ $(1 < \lambda < p)$ *is the order of 2 modulo p and*

$$0 \le k < \begin{cases} \dfrac{(p-1)^2}{2}, & \text{if } \chi(\gamma) = 1, \\ 1 + \dfrac{(p-1)^2}{2}, & \text{if } \chi(\gamma) = -1. \end{cases} \tag{28}$$

Proof. By Lemma 3, $\Phi^{(2)}(x) = 1 + x^p + x^{2p} + \ldots + x^{(p-1)p} \in \mathbb{F}_2[x]$ is the product of $(p-1)/\lambda$ many irreducible polynomials of degree λp; i.e.,

$$\Phi^{(2)}(x) = \varphi_1^{(2)}(x)\varphi_2^{(2)}(x)\cdots\varphi_{(p-1)/\lambda}^{(2)}(x). \tag{29}$$

Let $s_k(x)$ be a polynomial of degree smaller than p^2 over $\mathbb{F}_2$, and $s_k(x)$ has k many different terms from $s(x)$, the generating polynomial of σ. Then we have

$$s_k(x) = s(x) + e(x) \in \mathbb{F}_2[x], \tag{30}$$

where $e(x)$ is a polynomial of degree smaller than p^2 and has exactly k many monomials. In the sequel, we will find an $e(x)$ with the smallest k such that $\Phi^{(2)}(x) \mid s_k(x)$.

Suppose

$$s_k(x) = s(x) + e(x) = h(x)\Phi^{(2)}(x), \tag{31}$$

where $h(x) = h_0 + h_1 x + \ldots + h_{p-1}x^{p-1} \in \mathbb{F}_2[x]$ and the $\deg(h(x))$ is smaller than p. Then

$$e(x) = \sum_{0 \le i < p} \left(h_i X^i \Phi^{(2)}(x) - V_i(x)\right). \tag{32}$$

Clearly, $e(x)$ contains a summation $V_i(x)$ if $h_i = 0$ and $x^i\Phi^{(2)}(x) - V_i(x)$ otherwise.

If $\chi(\gamma) = 1$, by Lemma 6 we have $V_0(x) = 0$ and each $V_i(x)$ $(1 \le i < p)$ has $(p+1)/2$ many terms. It can be easily verified that $e(x)$ in (32) is the polynomial with the smallest $k = (p-1)^2/2$ terms such that $\Phi^{(2)}(x) \mid s_k(x)$. The argument implies that if $k < (p-1)^2/2$, there is no $e(x)$ with k terms such that $\Phi^{(2)}(x) \mid s_k(x)$. Among $\varphi_1^{(2)}(x), \ldots, \varphi_{(p-1)/\lambda}^{(2)}(x)$, there exists at

least one $\varphi_i^{(2)}(x)$ such that $\varphi_i^{(2)}(x) \nmid s_k(x)$, where $k < (p-1)^2/2$. By Lemma 1, we have $L_k(\sigma) \geq \lambda p$.

If $\chi(\gamma) = -1$, let

$$\begin{aligned} e(x) &= \Phi^{(2)}(x) - V_0(x) + \sum_{1\leq i<p} V_i(x) \\ &= 1 + \sum_{1\leq i<p} V_i(x). \end{aligned} \tag{33}$$

By Lemma 6, $e(x)$ is the polynomial with the smallest $k = 1 + (p-1)^2/2$ terms such that $\Phi^{(2)}(x) \mid s_k(x)$. Using the same method above, we have $L_k(\sigma) \geq \lambda p$ if $k < 1 + (p-1)^2/2$.

This completes the proof of this theorem. □

Next we consider the case that 2 is primitive modulo p^2 and the following lemma is required.

Lemma 8. *For $0 \leq i < p$, let $V_i(x) = \sum_{0\leq j<p} \sigma_{i+jp} x^{i+jp} \in \mathbb{F}_2[x]$. Then we have*

$$\begin{aligned} V_0(x) &\equiv 0 \mod (x^p - 1) \\ \text{and } V_i(x) &\equiv w x^i \mod (x^p - 1), \end{aligned} \tag{34}$$

where

$$w = \begin{cases} \dfrac{p+1}{2}, & \text{if } \chi(\gamma) = 1, \\ \dfrac{p-1}{2}, & \text{if } \chi(\gamma) = -1. \end{cases} \tag{35}$$

Proof. The proof can be derived directly from Lemma 6. □

Theorem 9. *Let symbols be the same as before. If $\chi(\gamma) = 1$ and 2 is primitive modulo p^2, then the k-error linear complexity of σ in (6) with period p^2 satisfies the following:*

(1) *When $p \equiv 5 \pmod 8$, we have*

$$L_k(\sigma) = \begin{cases} p^2 - 1, & \text{if } k = 0, \\ p^2 - p + 1, & \text{if } 1 \leq k < p-1, \\ p^2 - p, & \text{if } p-1 \leq k < \dfrac{(p-1)^2}{2}, \\ p - 1, & \text{if } k = \dfrac{(p-1)^2}{2}, \\ 0, & \text{if } k \geq \dfrac{(p^2-1)}{2}. \end{cases} \tag{36}$$

(2) *When $p \equiv 3 \pmod 8$, we have*

$$L_k(\sigma) = \begin{cases} p^2 - p, & \text{if } 0 \leq k < \dfrac{(p-1)^2}{2}, \\ p - 1, & \text{if } k = \dfrac{(p-1)^2}{2}, \\ 0, & \text{if } k \geq \dfrac{(p^2-1)}{2}. \end{cases} \tag{37}$$

Proof. Since 2 is primitive modulo p^2, the two polynomials $\Phi^{(2)}(x) = 1 + x^p + \ldots + x^{(p-1)p}$ and $1 + x + \ldots + x^{p-1}$ are irreducible over $\mathbb{F}_2$.

For any $e(x)$ with $k < (p-1)^2/2$ many terms, from the proof of Theorem 7 we have $\Phi^{(2)}(x) \nmid s(x)$ and $\Phi^{(2)}(x) \nmid s_k(x)$ for $s_k(x) = s(x) + e(x)$, where $s(x)$ is the generating polynomial of σ. This means that $L_k(\sigma) \geq p^2 - p$ for $k < (p-1)^2/2$.

Now we consider $s(x)$ modulo $(x^p - 1)$. By Lemma 8, we have

$$\begin{aligned} s(x) &\equiv \frac{p+1}{2}\left(x + x^2 + \ldots + x^{p-1}\right) \mod (x^p - 1) \\ &\equiv \begin{cases} x + x^2 + \ldots + x^{p-1}, & \text{if } p \equiv 5 \pmod 8, \\ 0, & \text{if } p \equiv 3 \pmod 8. \end{cases} \end{aligned} \tag{38}$$

For the case $p \equiv 5 \bmod 8$, from (38) we obtain the following:

(1) $s(1) = 0$ and $\gcd(s(x), (x^{p^2} - 1)/(x-1)) = 1$, then we have $L_0(\sigma) = p^2 - 1$.

(2) $s(x) + 1 \equiv 1 + x + \ldots + x^{p-1} \bmod (x^p - 1)$, which indicates that $L_1(\sigma) = p^2 - p + 1$.

(3) $s(x) + x + \ldots + x^{p-1} \equiv 0 \bmod (x^p - 1)$, which indicates that $L_{p-1}(\sigma) = p^2 - p$.

Putting everything together, the first statement of Theorem 9 is proved. For the case $p \equiv 3 \bmod 8$, it can be easily verified that $L_0(\sigma) = p^2 - p$ and the second statement of this theorem can be similarly proved. □

Theorem 10. *Let symbols be the same as before. If $\chi(\gamma) = -1$ and 2 is primitive modulo p^2, then the k-error linear complexity of σ in (6) with period p^2 satisfies the following:*

(1) *When $p \equiv 5 \pmod 8$, we have*

$$L_k(\sigma) = \begin{cases} p^2 - p, & \text{if } 0 \leq k < 1 + \dfrac{(p-1)^2}{2}, \\ p, & \text{if } k = 1 + \dfrac{(p-1)^2}{2}, \\ 0, & \text{if } k \geq \dfrac{(p^2-1)}{2}. \end{cases} \tag{39}$$

(2) *When $p \equiv 3 \pmod 8$, we have*

$$\begin{aligned} &L_k(\sigma) \\ &= \begin{cases} p^2 - 1, & \text{if } k = 0, \\ p^2 - p + 1, & \text{if } 1 \leq k < p-1, \\ p^2 - p, & \text{if } p-1 \leq k < 1 + \dfrac{(p-1)^2}{2}, \\ p, & \text{if } k = 1 + \dfrac{(p-1)^2}{2}, \\ 0, & \text{if } k \geq \dfrac{(p^2-1)}{2}. \end{cases} \end{aligned} \tag{40}$$

Proof. The proof of Theorem 10 is similar to that of Theorem 9 and we omit it. □

Theorems 9 and 10 indicate that σ defined in (6) has good stability, or, in other words, the linear complexity is not significantly decreased by changing only a few (but not many) terms.

5. Final Remarks

In this work, we have studied an extension of the Legendre sequence, which has been widely considered in the literature. More exactly, we have investigated the linear complexity and k-error linear complexity of a binary p^r-periodic sequence derived from the discrete logarithm in finite fields. We only give a lower bound on the linear complexity for $r \geq 2$ and the distribution of the k-error linear complexity for $r = 2$. Therefore, it is interesting to consider the k-error linear complexity for $r > 2$; we describe an open problem as follows.

Open Problem. Determine the k-error linear complexity of σ defined in (6) for the case when $r > 2$.

By Lemma 6, we find that $\sigma_1 = \sigma_2 = \cdots = \sigma_{p-1}$ and $\sigma_p = \sigma_{2p} = \cdots = \sigma_{(p-1)p}$. This sacrifices the pseudorandomness of the sequence. Therefore, we can modify the construction of σ (with period p^2) as follows:

$$(-1)^{\sigma_n} = \begin{cases} 1, & \text{if } n = 0, \\ \left(\dfrac{j}{p}\right), & \text{if } n = jp \text{ and } 1 \leq j < p, \\ \left(\dfrac{i}{p}\right)\chi(\xi_n), & \text{if } n = i + jp \text{ and } 1 \leq i < p,\ 0 \leq j < p. \end{cases} \tag{41}$$

The method given in this work can be used to consider the linear complexity and k-error linear complexity.

Finally it should be remarked that there is another way to order the elements in $\mathbb{F}_q$. Let α be a primitive element of $\mathbb{F}_q$ and $\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$ is an ordered set. The sequence $\rho = (\rho_0, \rho_1, \ldots)$ is defined as

$$\rho_n = \begin{cases} 0, & \text{if } n = \dfrac{(q-1)}{2}, \\ \dfrac{(1 - \chi(\alpha^n - 1))}{2}, & \text{otherwise.} \end{cases} \tag{42}$$

The sequence ρ is referred to as a *generalized Sidelnikov sequence*, and the k-error linear complexity of ρ was determined over $\mathbb{F}_p$ for $r = 1$) [18]. It is interesting to consider the k-error linear complexity over $\mathbb{F}_2$ of ρ.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors wish to thank Prof. Arne Winterhof for helpful suggestions and some corrections of the proof. Z. Chen was partially supported by the National Natural Science Foundation of China under grant No. 61772292, the Projects of International Cooperation and Exchanges NSFC-RFBR No. 61911530130, the Provincial Natural Science Foundation of Fujian under grant No. 2018J01425, and the Program for Innovative Research Team in Science and Technology in Fujian Province University under grant No. 2018-49. Q. Wang was also supported by the National Science Foundation of China under grant No. 61602342, Science Foundation of Tianjin under grant No. 18JCQNJC70300, the Science & Technology Development Fund of Tianjin Education Commission for Higher Education under grant No. 2018KJ215 and No. 16JCYBJC41500, the Key Laboratory of Applied Mathematics of Fujian Province University (Putian University) under grant No. SX201804, and the China Scholarship Council (No. 201809345010).

References

[1] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers*, vol. 561 of *Lecture Notes in Computer Science*, Springer, Berlin, Germany, 1991.

[2] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, Berlin, Germany, 1986.

[3] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*, Gulf Professional Publishing, 2004.

[4] A. J. Bromfield and F. C. Piper, "Linear recursion properties of unrelated binary sequences," *Discrete Applied Mathematics*, vol. 27, no. 3, pp. 187–193, 1990.

[5] I. B. DamgÅrd, "On the randomness of Legendre and Jacobi sequences," in *Advances in Cryptology*, S. Goldwasser, Ed., vol. 403 of *Lecture Notes in Comput. Sci.*, pp. 163–172, Springer, Berlin, Germany, 1990.

[6] D. Cunsheng, T. Hesseseth, and S. Weijuan, "On the linear complexity of Legendre sequences," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1276–1278, 1998.

[7] D. Cunsheng, "Pattern distributions of Legendre sequences," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1693–1698, 1998.

[8] J. Kim and H. Song, "Trace representation of Legendre sequences," *Designs, Codes and Cryptography*, vol. 24, pp. 343–348, 2001.

[9] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, New York, NY, USA, 1997.

[10] W. Meidl and A. Winterhof, "On the autocorrelation of cyclotomic generator," in *Lecture Notes in Computer Science*, pp. 1–11, Springer, Berlin, Germany, 2003.

[11] W. Meidl and A. Winterhof, "Lower bounds on the linear complexity of the discrete logarithm in finite fields," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 2807–2811, 2001.

[12] A. Winterhof, "A note on the linear complexity profile of the discrete logarithm in finite fields," in *Coding, Cryptography and Combinatorics*, K. Feng, H. Niederreiter, and C. Xing, Eds., vol. 23 of *Progr. Comput. Sci. Appl. Logic*, pp. 359–367, Birkhäuser, Basel, Switzerland, 2004.

[13] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, Mass, USA, 1983.

[14] A. Sárközy and A. Winterhof, "Measures of pseudorandomness for binary sequences constructed using finite fields," *Discrete Mathematics*, vol. 309, no. 6, pp. 1327–1333, 2009.

[15] K. Gyarmati, C. Mauduit, and A. Sárközy, "On finite pseudorandom binary lattices," *Discrete Applied Mathematics*, vol. 216, pp. 589–597, 2017.

[16] K. Gyarmati, A. Sárközy, and C. L. Stewart, "On Legendre symbol lattices," *Uniform Distribution Theory*, vol. 4, no. 1, pp. 81–95, 2009.

[17] K. Gyarmati, A. Sárközy, and C. L. Stewart, "On Legendre symbol lattices," *II. Uniform Distribution Theory*, vol. 8, no. 1, pp. 47–65, 2013.

[18] H. Aly and A. Winterhof, "On the k-error linear complexity over of Legendre and Sidelnikov sequences," *Designs, Codes and Cryptography*, vol. 40, no. 3, pp. 369–374, 2006.

[19] H. Aly, W. Meidl, and A. Winterhof, "On the k-error linear complexity of cyclotomic sequences," *Journal of Mathematical Cryptology*, vol. 1, no. 3, pp. 283–296, 2007.

[20] M. Stamp and C. F. Martin, "An algorithm for the k-error linear complexity of binary sequences with period 2n," *Institute of Electrical and Electronics Engineers Transactions on Information &Theory*, vol. 39, no. 4, pp. 1398–1401, 1993.

[21] T. Kaida, S. Uehara, and K. Imamura, "A new algorithm for the k-error linear complexity of sequences over GF(pm) with period pn," in *Sequences and Their Applications*, C. Ding, T. Helleseth, and H. Niederreiter, Eds., pp. 284–296, Springer, London, UK, 1999.

[22] S. R. Blackburn, T. Etzion, and K. G. Paterson, "Permutation polynomials, de bruijn sequences, and linear complexity," *Journal of Combinatorial Theory, Series A*, vol. 76, no. 1, pp. 55–82, 1996.

[23] A. Akbary and S. Siavashi, "The largest known Wieferich numbers," *Integers. Electronic Journal of Combinatorial Number Theory*, vol. 18-A3, pp. 1–6, 2018.