AIMS Mathematics, 7(5): 7997–8011.
DOI: 10.3934/math.2022446
Received: 16 December 2021
Revised: 05 February 2022
Accepted: 10 February 2022
Published: 23 February 2022

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

Research article

On the k-error linear complexity of binary sequences of periods p^n from new cyclotomy

Vladimir Edemskiy[1] **and Chenhuang Wu**[2,3,*]

[1] Department of Applied Mathematics and Information Science, Yaroslav-the-Wise Novgorod State University, Veliky Novgorod, 173003, Russia

[2] Provincial Key Laboratory of Applied Mathematics, Putian University, Putian, Fujian 351100, China

[3] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731, China

* **Correspondence:** Email: ptuwch@163.com.

Abstract: In this paper, we study the k-error linear complexity of binary sequences with periods p^n, which are derived from new generalized cyclotomic classes modulo a power of an odd prime p. We establish a recursive relation and then estimate the k-error linear complexity of the binary sequences with periods p^n, the results extend the case p^2 that has been studied in an earlier work of Wu et al. at 2019. Our results show that the k-error linear complexity of these sequences does not decrease dramatically for $k < (p^n - p^{n-1})/2$.

Keywords: k-error linear complexity; binary sequences; cyclotomy; stream cipher; cryptography
Mathematics Subject Classification: 11B50, 94A55, 94A60

1. Introduction

Pseudo-random sequences are widely used in a lot of fields, in particular for stream ciphers. Cyclotomy is an old topic of elementary number theory connected with difference sets, sequences, coding theory and cryptography. The use of cyclotomic classes is one of the important methods for sequence design [1]. In the past decades, cyclotomic and generalized cyclotomic sequences have been studied from the viewpoint of cryptography [2].

In this work, we will re-visit the families of new cyclotomic binary sequences of periods p^n and $2p^n$ presented in [3, 4] respectively. Such sequences are defined by using the new generalized cyclotomic classes from [5]. Recently, Liu et al. [6] studied the correlation of the sequence defined in [4]. We will

concentrate on the case of p^n defined in [3], and give a brief introduction of the case of $2p^n$ in the final section without proof since it is similar.

We denote by $\mathbb{Z}_N$ the ring of integers modulo N for a positive integer N, and by $\mathbb{Z}_N^*$ the multiplicative group of $\mathbb{Z}_N$. Let p be an odd prime and $p = ef+1$, where e, f are positive integers. Let g be a primitive root modulo p^n.

Let $n \geq 2$ be a positive integer. For $j = 1, 2, \cdots, n$, denote $d_j = p^{j-1}f$ and define

$$\begin{aligned} D_0^{(p^j)} &= \left\{ g^{td_j} \pmod{p^j} : 0 \leq t < e \right\}, \text{ and} \\ D_i^{(p^j)} &= g^i D_0^{(p^j)} = \left\{ g^i x \pmod{p^j} : x \in D_0^{(p^j)} \right\}, \quad 1 \leq i < d_j. \end{aligned} \tag{1.1}$$

By definition we see that $\left\{ D_0^{(p^j)}, D_1^{(p^j)}, \ldots, D_{d_j-1}^{(p^j)} \right\}$ forms a partition of $\mathbb{Z}_{p^j}^*$ for each integer $j \geq 1$. Also for an integer $m \geq 1$,

$$\mathbb{Z}_{p^m} = \bigcup_{j=1}^{m} \bigcup_{i=0}^{d_j-1} p^{m-j} D_i^{(p^j)} \cup \{0\}.$$

Let f be an even integer and b be an integer with $0 \leq b < p^{n-1}f$. Define two families of sets for $m = 1, 2, \ldots, n$

$$\begin{aligned} \mathscr{C}_0^{(p^m)} &= \bigcup_{j=1}^{m} \bigcup_{i=d_j/2}^{d_j-1} p^{m-j} D_{(i+b) \pmod{d_j}}^{(p^j)}, \\ \mathscr{C}_1^{(p^m)} &= \bigcup_{j=1}^{m} \bigcup_{i=0}^{d_j/2-1} p^{m-j} D_{(i+b) \pmod{d_j}}^{(p^j)} \cup \{0\}. \end{aligned} \tag{1.2}$$

It is obvious that $\mathbb{Z}_{p^m} = \mathscr{C}_0^{(p^m)} \cup \mathscr{C}_1^{(p^m)}$ and $|\mathscr{C}_1^{(p^m)}| = (p^m+1)/2$. A family of balanced binary sequences $s^{(m)} = (s_0^{(m)}, s_1^{(m)}, s_2^{(m)}, \ldots)$ of period p^m can thus be defined as

$$s_i^{(m)} = \begin{cases} 0, & \text{if } i \pmod{p^m} \in \mathscr{C}_0^{(p^m)}, \\ 1, & \text{if } i \pmod{p^m} \in \mathscr{C}_1^{(p^m)}. \end{cases} \tag{1.3}$$

The linear complexity of $s^{(m)}$ above was studied in [3] for $m = 2$. Later it was extended to the case $m > 2$ in [7, 8], independently. The linear complexity is an important cryptographic measure of sequences. The linear complexity of a sequence is defined as the length of the shortest linear feedback shift register that can generate the sequence [9].

In [7], we can see that $s^{(m)}$ has high linear complexity. But high linear complexity is not enough for its cryptographic applications, what we need is that the linear complexity doesn't decrease significantly when k or fewer bits of the sequence is changed in one period. This leads to the notion of k-error linear complexity. For integer $k \geq 0$, the *k-error linear complexity* over $\mathbb{F}_2$ (the finite field of order two) of a sequence, denoted by $LC_k^{\mathbb{F}_2}(\cdot)$, is the smallest linear complexity (over $\mathbb{F}_2$) that can be obtained by changing at most k terms of the sequence per period [10].

The k-error linear complexity of $s^{(m)}$ in Eq (1.3) for $m = 2$ has been studied in [11]. So in this work, we will contribute to the k-error linear complexity of $s^{(m)}$ for $m > 2$.

Finally, we remark that the definition of $s^{(m)}$ in Eq (1.3) is in fact related to Fermat-Euler quotients. Some studies of this kind have been carried out in the past decade, see for example [12–19] and references therein.

2. The k-error linear complexity: main results

In this section, we present the main results of this paper.

Theorem 1. *Let $p = ef + 1$ be an odd prime with even f and 2 be a primitive root modulo p^2. Let $s^{(n)}$ be a family of generalized cyclotomic binary sequences of period p^n defined in Eq* (1.3)*. Then we have the following results about the k-error linear complexity of $s^{(n)}$.*

(i) If $p \equiv 1 \pmod 4$, then for $k < (p^n - p^{n-1})/2$ we have

$$LC_k^{\mathbb{F}_2}(s^{(n)}) = p^n - p^{n-1} + LC_k^{\mathbb{F}_2}(s^{(n-1)}).$$

(ii) If $p \equiv 3 \pmod 4$, then for $k < (p^n - p^{n-1})/2$ we have

$$p^n - p^{n-1} + LC_k^{\mathbb{F}_2}(s^{(n-1)}) - 1 \le LC_k^{\mathbb{F}_2}(s^{(n)}) \le p^n - p^{n-1} + LC_k^{\mathbb{F}_2}(s^{(n-1)}) + 1.$$

(iii) For $(p^n - p^{n-t})/2 \le k < (p^n - p^{n-t-1})/2$, where $t = 1, 2, \ldots, n-1$, we have

$$p^{n-t-1}(p-1) \le LC_k^{\mathbb{F}_2}(s^{(n)}) \le p^{n-t}.$$

(iv) For $k = (p^n - 1)/2$, we have $LC_k^{\mathbb{F}_2}(s^{(n)}) = 1$.

(v) For $k > (p^n - 1)/2$, we have $LC_k^{\mathbb{F}_2}(s^{(n)}) = 0$.

By Theorem 1, we see that these sequences have high linear complexity and the linear complexity does not decrease dramatically. Thus, such sequences have good stability. It is easy to see that [11, Theorems 1 and 2] are the special cases of Theorem 1.

3. The proof technique

For $m = 1, 2, \ldots, n$, let $S^{(m)}(X) = \sum_{i \in \mathscr{C}_1^{(p^m)}} X^i$. That is, $S^{(m)}(X)$ is the *generating polynomials* of $s^{(m)}$.

Let $E^{(m)}(X) = e_0 + e_1 X + \cdots + e_{p^m-1} X^{p^m-1}$ be the *error polynomial* of $s^{(m)}$. Here $e_i = 1$ if $s_i^{(m)}$ is changed when we compute the k-error linear complexity of $s^{(m)}$, and otherwise $e_i = 0$ on the same period of $s^{(m)}$. Then, it is well known that the k-error linear complexity of $s^{(m)}$ over $\mathbb{F}_2$ is computed as follows

$$LC_k^{\mathbb{F}_2}(s^{(m)}) = \min_{0 \le wt(E^{(m)}(X)) \le k} \left\{ p^m - \deg\left(\gcd\left(X^{p^m} - 1, S^{(m)}(X) + E^{(m)}(X) \right) \right) \right\}.$$

In this section, we will give a recurrence formula for the generating polynomials of our sequences and prove some auxiliary statements concerning their error polynomials. And the proofs of the main results will be presented in Subsection 3.3.

3.1. The generating polynomial: recurrence formula

Denote $d_i^{(j)}(X) = \sum_{l \in D^{(p^j)}_{(i+b)(\bmod d_j)}} X^l$, where $0 \le b < p^j f$, $j = 1,2,\ldots,m$, $i = 0,1,\ldots,d_j-1$. From Eqs (1.1)–(1.3) we obtain that

$$S^{(m)}(X) = \sum_{j=1}^{m} \sum_{i=0}^{d_j/2-1} d_i^{(j)}(X^{p^{m-j}}) + 1. \tag{3.1}$$

Notice that the subscripts i in $d_i^{(j)}(X)$ are all taken modulo the order d_j. In the rest of this paper the modulo operation will be omitted when no confusion can arise.

The properties of the generalized cyclotomic classes defined in (1.1) are well known, in particular we cite the following statemetns in [7].

Lemma 2. *For $D_i^{(p^j)}$ defined as in Eq* (1.1)*, $j = 2,\ldots,n$ and $i = 1,2,\ldots,d_j-1$, we have*
(i) $D_i^{(p^j)} \pmod{p^{j-1}} = D^{(p^{j-1})}_{i \pmod{d_{j-1}}}$,
(ii) $p^{n-j} D_i^{(p^j)} \pmod{p^{n-1}} = p^{n-j} D^{(p^{j-1})}_{i \pmod{d_{j-1}}}$.

Using Lemma 2 and the definitions of $d_i^{(j)}(X), i = 1,2,\ldots,d_j-1$, we can easily obtain the following statements.

Lemma 3. *For $d_i^{(j)}(X)$ defined as above and $j = 2,\ldots,n$ and $i = 1,2,\ldots,d_j-1$, we have*
(i) $d_i^{(1)}(X^{p^{n-1}}) = e \pmod{X^{p^{n-1}}-1}$,
(ii) $d_i^{(j)}(X^{p^{n-j}}) \pmod{X^{p^{n-1}}-1} = d^{(j-1)}_{i \pmod{d_{j-1}}}(X^{p^{n-j}})$.

By the Lemmas 2 and 3, we can get the following Proposition 1 .

Proposition 1. *Let $s^{(n)}$ be a p^n-periodic binary sequence over $\mathbb{F}_2$ defined in Eq* (1.3)*. For $n \ge 2$ we have*

$$S^{(n)}(X) \pmod{X^{p^{n-1}}-1} = \begin{cases} S^{(n-1)}(X), & \text{if } p \equiv 1 \pmod 4, \\ S^{(n-1)}(X) + \frac{X^{p^{n-1}}-1}{X-1}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. By Eq (3.1) we have

$$S^{(n)}(X) \equiv \sum_{j=1}^{n} \sum_{i=0}^{d_j/2-1} d_i^{(j)}(X^{p^{n-j}}) + 1 \pmod{X^{p^{n-1}}-1}.$$

So, by Lemma 3 we see that

$$S^{(n)}(X) \pmod{X^{p^{n-1}}-1} = \sum_{j=2}^{n} \sum_{i=0}^{d_j/2-1} d_i^{(j-1)}(X^{p^{n-j}}) + ed_1/2 + 1. \tag{3.2}$$

Further, $d_j/2 = (p-1)d_{j-1}/2 + d_{j-1}/2$. Hence

$$\sum_{i=0}^{d_j/2-1} d_i^{(j-1)}(X^{p^{n-j}}) = \frac{p-1}{2} \sum_{i=0}^{d_{j-1}-1} d_i^{(j-1)}(X^{p^{n-j}}) + \sum_{i=0}^{d_{j-1}/2-1} d_i^{(j-1)}(X^{p^{n-j}}). \tag{3.3}$$

For $p \equiv 1 \pmod 4$, we can see that $\frac{p-1}{2} \sum_{i=0}^{d_{j-1}-1} d_i^{(j-1)}(X^{p^{n-j}}) = 0$ in Eq (3.3) over $\mathbb{F}_2$ and again by Eq (3.1) we have

$$S^{(n)}(X) \pmod{X^{p^{n-1}}-1} = \sum_{j=2}^{n} \sum_{i=0}^{d_{j-1}/2-1} d_i^{(j-1)}(X^{p^{n-j}}) + 1 = S^{(n-1)}(X).$$

For $p \equiv 3 \pmod 4$, from Eq (3.3) we see that

$$\sum_{i=0}^{d_j/2-1} d_i^{(j-1)}(X^{p^{n-j}}) = \sum_{i=0}^{d_{j-1}-1} d_i^{(j-1)}(X^{p^{n-j}}) + \sum_{i=0}^{d_{j-1}/2-1} d_i^{(j-1)}(X^{p^{n-j}}).$$

In this case, from Eq (3.2) we have

$$S^{(n)}(X) \pmod{X^{p^{n-1}}-1} = \sum_{j=2}^{n} \sum_{i=0}^{d_{j-1}/2-1} d_i^{(j-1)}(X^{p^{n-j}}) + \sum_{j=2}^{n} \sum_{i=0}^{d_{j-1}-1} d_i^{(j-1)}(X^{p^{n-j}}).$$

By Eq (1.2) and the definition of $d_i^{(j)}(X)$, we have

$$\sum_{j=2}^{n} \sum_{i=0}^{d_{j-1}-1} d_i^{(j-1)}(X^{p^{n-j}}) = \sum_{i=1}^{p^{n-1}-1} X^i,$$

it follows that

$$S^{(n)}(X) \pmod{X^{p^{n-1}}-1} = S^{(n-1)}(X) + \sum_{i=0}^{p^{n-1}-1} X^i = S^{(n-1)}(X) + \frac{X^{p^{n-1}}-1}{X-1}.$$

□

3.2. The error polynomial: weight estimation

Let $\Psi_m^{(t)}(X) = X^{(p^t-1)p^{m-t}} + \cdots + X^{p^{m-t}} + 1$ for $t = 1, 2, \ldots, m$. In this subsection we study the case that $S^{(m)}(X)$ can be divided by $\Psi_m^{(t)}(X)$.

Let $C_0^{(p^m)} = \bigcup_{i=d_m/2}^{d_m-1} D_{i+b}^{(p^m)}$ and $C_1^{(p^m)} = \bigcup_{i=0}^{d_m/2-1} D_{i+b}^{(p^m)}$. According to [12], if $\sum_{i \in C_1^{(p^m)}} X^i + E_m(X)$ is divided by $\Psi_m^{(1)}(X)$, then the least possible weight of $E_m(X)$ is equal to $p^{m-1}(p-1)^2/2$. Using the same way as in [12] we can obtain a more general statement.

We need the following subsidiary lemmas for this.

Lemma 4. *Let $v \in D_l^{(p^{m-t})}$ for $m > t$ and $U_v = \{v, v + p^{m-t}, \ldots, v + (p^t-1)p^{m-t}\}$. Then*

$$|U_v \cap D_i^{(p^m)}| = \begin{cases} 1, & \text{if } i \equiv l \pmod{fp^{m-t-1}}, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. By the condition $v \in D_l^{(p^{m-t})}$, i.e., $v = g^{l+hd_{m-t}} \pmod{p^{m-t}}$ for some $h : 0 \le h < e$.

Supposing $v + ap^{m-t} \in D_i^{(p^m)}$ for $a : 0 \le a \le p^t - 1$, then $v + ap^{m-t} \equiv g^{i+ud_m} \pmod{p^m}$ for some $u : 0 \le u < e$. Hence $g^{l+hd_{m-t}} \equiv g^{i+ud_m} \pmod{p^{m-t}}$ and $l + hd_{m-t} \equiv i + ud_m \pmod{(p-1)p^{m-t-1}}$. Since $p-1 = ef$ and $d_{m-t} = p^{m-t-1}f$, it follows that $i - l \equiv 0 \pmod{fp^{m-t-1}}$. Thus, $|U_v \cap D_i^{(p^m)}| = 0$ for $i \not\equiv l \pmod{fp^{m-t-1}}$.

Further, suppose that $v + ap^{m-t} \in D_i^{(p^m)}$ and $v + bp^{m-t} \in D_i^{(p^m)}$, where $a \ne b$, $a, b = 0, 1, \ldots, p^t - 1$; then $v + ap^{m-t} \equiv g^{i+ud_m} \pmod{p^m}$ and $v + bp^{m-t} \equiv g^{i+zd_m} \pmod{p^m}$ for some $u, z : 0 \le u, z < e$. In this case, $ufp^{m-1} \equiv zfp^{m-1} \pmod{(p-1)p^{m-t-1}}$. This is impossible for $u \ne z : 0 \le u, z < e$.

So, we see that $|U_v \cap D_i^{(p^m)}| \le 1$ for $i \equiv l \pmod{fp^{m-t-1}}$. Since $|U_v| = p^t$ and $|\{i \mid i \equiv l \pmod{fp^{m-t-1}} \text{ and } i = 0, 1, \ldots, p^{m-1}f - 1\}| = p^t$, it follows that $|U_v \cap D_i^{(p^m)}| = 1$ for $i \equiv l \pmod{fp^{m-t-1}}$. □

Corollary 5. *With notations as above for $m > t$.*

$$|U_v \cap \left(D_i^{(p^m)} \cup D_{i+p^{m-t}}^{(p^m)} \cup \cdots \cup D_{i+(p^t-1)p^{m-t}}^{(p^m)}\right)| = \begin{cases} p^t, & \text{if } i \equiv l \pmod{fp^{m-t-1}}, \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 6. *Let $v \in D_l^{(p^{m-t})}$ for $m > t$. Then we have*

(i) $|U_v \cap C_0^{(p^m)}| = (p^t - 1)/2$ and $|U_v \cap C_1^{(p^m)}| = (p^t + 1)/2$ for $l < p^{m-t-1}f/2$: and

(ii) $|U_v \cap C_0^{(p^m)}| = (p^t + 1)/2$ and $|U_v \cap C_1^{(p^m)}| = (p^t - 1)/2$ for $l \ge p^{m-t-1}f/2$.

Proof. If $l < p^{m-t-1}f/2$ then $l + ifp^{m-t-1} < fp^{m-1}/2$ for $i = 0, 1, \ldots, (p^t - 1)/2$ since $l + \frac{p^t-1}{2}fp^{m-t-1} < fp^{m-1}/2$ in this case. Thus, this statement follows from Lemma 4 and Corollary 5. □

The following statement was proved in [12] for $m = t - 1$.

Lemma 7. *Let $E_m(X)$ such that $\sum_{i \in C_1^{(p^m)}} X^i + E_m(X)$ divisible by $\Psi_m^{(t)}(X)$ for $m > t > 0$. Then,* $\min wt(E_m(X)) = p^{m-t-1}(p-1)(p^t-1)/2$.

Proof. By the condition we have

$$\sum_{i \in C_1^{(p^m)}} X^i + E_m(X) = (X^{(p^t-1)p^{m-t}} + \cdots + X^{p^{m-t}} + 1)F(X),$$

where $\deg F(X) < p^{m-t}$ and $F(X) = X^{t_1} + X^{t_2} + \cdots + X^{t_h}$, $0 < t_j < p^{m-t}$, $j = 1, 2, \ldots, h$ and $h < p^{m-t}$. It is clear that we can not consider cases when t_j is congruent to 0 modulo p.

Hence

$$\begin{aligned} E_m(X) &= \sum_{i=1}^{h} \left(X^{t_i} + X^{t_i+p^{m-t}} + \cdots + X^{t_i+(p^t-1)p^{m-t}}\right) + \sum_{i \in C_1^{(p^m)}} X^i \\ &= \sum_{i=1}^{h} \left(X^{t_i} + X^{t_i+p^{m-t}} + \cdots + X^{t_i+(p^t-1)p^{m-t}}\right) \\ &\quad + \sum_{i \in C_1^{(p^{m-t})}} \sum_{l \in U_i \cap C_1^{(p^m)}} X^l + \sum_{i \in C_0^{(p^{m-t})}} \sum_{l \in U_i \cap C_1^{(p^m)}} X^l, \end{aligned}$$

where, as earlier, $U_i = \{i, i+p^{m-t}, \ldots, i+(p^t-1)p^{m-t}\}$. Here we use that $\bigcup_{i\in\mathbb{Z}^*_{p^{m-t}}} U_i = \mathbb{Z}^*_{p^m}$.

Let $I = \{t_1, t_2, \ldots, t_h\}$ and $J = \mathbb{Z}^*_{p^{m-t}} \setminus I$. Using these denotations we obtain

$$\begin{aligned} E_m(X) &= \sum_{i\in I\cap C_1^{(p^{m-t})}} \sum_{l\in U_i\cap C_0^{(p^m)}} X^l + \sum_{i\in J\cap C_1^{(p^{m-t})}} \sum_{l\in U_i\cap C_1^{(p^m)}} X^l \\ &\quad + \sum_{i\in I\cap C_0^{(p^{m-t})}} \sum_{l\in U_i\cap C_0^{(p^m)}} X^l + \sum_{i\in J\cap C_0^{(p^{m-t})}} \sum_{l\in U_i\cap C_1^{(p^m)}} X^l. \end{aligned} \tag{3.4}$$

Denote $z = |I\cap C_1^{(p^{m-t})}|$, then $|J\cap C_1^{(p^{m-t})}| = p^{m-t-1}(p-1)/2 - z$, $|I\cap C_0^{(p^{m-t})}| = h - z$ and $|J\cap C_0^{(p^{m-t})}| = p^{m-t-1}(p-1)/2 - h + z$. Thus, by Lemma 6 and Eq (3.4), we obtain

$$\begin{aligned} wt(E_m(X)) = {} & z(p^t-1)/2 + (p^{m-t-1}(p-1)/2 - z)(p^t+1)/2 + (h-z)(p^t+1)/2 \\ & + (p^{m-t-1}(p-1)/2 - h + z)(p^t-1)/2 \end{aligned}$$

or $wt(E_m(X)) = p^{m-1}(p-1)/2 + h - 2z$.

Supposing $h - 2z < -p^{m-t-1}(p-1)/2$, then $p^{m-t-1}(p-1)/2 - z < z - h \le 0$. This is impossible and $wt(E_m(X)) \ge p^{m-1}(p-1)/2 - p^{m-t-1}(p-1)/2$.

Now we show that there exists $E_m(X)$ with a weight equal to the estimates obtained. We choose $I = C_1^{(p^{m-t})}$ for $m > t$, in this case $h = z = p^{m-t-1}(p-1)/2$ and $wt(E_m(X)) = p^{m-1}(p-1)/2 - p^{m-t-1}(p-1)/2$ for

$$E_m(X) = \sum_{i\in C_1^{(p^{m-t})}} \sum_{l\in U_i\cap C_0^{(p^m)}} X^l + \sum_{i\in C_0^{(p^{m-t})}} \sum_{l\in U_i\cap C_1^{(p^m)}} X^l.$$

Then

$$\sum_{i\in C_1^{(p^m)}} X^i + E_m(X) = \sum_{i\in C_1^{(p^{m-t})}} \sum_{l\in U_i\cap C_0^{(p^m)}} X^l + \sum_{i\in C_1^{(p^{m-t})}} \sum_{l\in U_i\cap C_1^{(p^m)}} X^l$$

and we see that

$$\sum_{i\in C_1^{(p^m)}} X^i + E_m(X) \equiv 0 \pmod{X^{(p^t-1)p^{m-t}} + \cdots + X^{p^{m-t}} + 1}.$$

□

Proposition 2. *Let $S^{(m)}(X) + E^{(m)}(X) \equiv 0 \pmod{\Psi_m^{(t)}(X)}$ for $t = 1, 2, \ldots, m$. Then we have*

$$\min wt(E^{(m)}(X)) = (p^m - p^{m-t})/2.$$

Remark 1. *For $m = 2$ it was first proved in [11].*

Proof. First, we consider the case when $m = t$. In this case we have that sum $S^{(m)}(X) + E^{(m)}(X)$ is divisible by $X^{(p^m-1)} + \cdots + X + 1$. It is clear that $wt(E^{(m)}(X)) \ge (p^m - 1)/2$ and we can choose $E^{(m)}(X) = X^{p^m} - 1 + S^{(m)}(X)$.

Let $m > t$. From Eq (3.1) we get

$$S^{(m)}(X) = \sum_{i=0}^{d_m/2-1} d_i^{(m)}(X) + S^{(m-1)}(X^p) = \sum_{i \in C_1^{(p^m)}} X^i + S^{(m-1)}(X^p). \tag{3.5}$$

So, we will prove this statement by mathematical induction.

Step 1. For $m = 1$, we have only one case $m = 1, t = 1$, i.e., $S^{(1)}(X) + E^{(1)}(X) \equiv 0 \pmod{X^{p-1} + \cdots + X + 1}$. It is clear that $\min wt(E^{(1)}(X)) = (p-1)/2$.

Step 2. Assume this proposition is true for $S^{(m)}(X)$, i.e. there exists $E^{(m)}(X)$ with $wt(E^{(m)}(X)) = (p^m - p^{m-t})/2$ such that $S^{(m)}(X) + E^{(m)}(X)$ is divisible by $\Psi_m^{(t)}(X)$. Then $S^{(m)}(X^p) + E^{(m)}(X^p)$ is divided by $\Psi_m^{(t)}(X^p) = \Psi_{m+1}^{(t)}(X)$ and $\min wt(E^{(m)}(X^p)) = (p^m - p^{m-t})/2$.

By Lemma 7 there exists $E_{m+1}(X)$ such that $\sum_{i \in C_1^{(p^{m+1})}} X^i + E_{m+1}(X)$ is divisible by $\Psi_{m+1}^{(t)}(X)$ and $\min wt(E_{m+1}(X)) = p^{m-t}(p-1)(p^t-1)/2$. Let $E^{(m+1)}(X) = E_{m+1}(X) + E^{(m)}(X^p)$. Then

$$wt(E^{(m+1)}(X)) = p^{m-t}(p-1)(p^t-1)/2 + (p^m - p^{m-t})/2 = (p^{m+1} - p^{(m+1)-t})/2$$

and by Eq (3.5) we see that $S^{(m+1)}(X) + E^{(m+1)}(X)$ is divisible by $\Psi_{m+1}^{(t)}(X)$.

Now we will show that $(p^{m+1} - p^{(m+1)-t})/2$ is the least possible weight of $E^{(m+1)}(X)$.

Suppose $S^{(m+1)}(X) + E^{(m+1)}(X)$ is divisible by $\Psi_{m+1}^{(t)}(X)$ for $m+1 > t$. Then there exists $R(X)$ such that

$$S^{(m+1)}(X) + E^{(m+1)}(X) = \left(X^{(p^t-1)p^{m+1-t}} + \cdots + X^{p^{m+1-t}} + 1\right) R(X) \tag{3.6}$$

and $\deg R(X) < p^{m-t+1}$.

Let $E^{(m+1)}(X) = \sum_{i=0}^{p^{m+1}-1} e_i X^i$ and $R(X) = \sum_{i=0}^{p^{m+1-t}-1} r_i X^i$. Denote $E_0 = \{e_i \mid e_i \neq 0 \text{ and } e_i \equiv 0 \pmod{p}\}$, $E_1 = \{e_i \mid e_i \neq 0 \text{ and } e_i \not\equiv 0 \pmod{p}\}$, $R_0 = \{r_i \mid r_i \neq 0 \text{ and } r_i \equiv 0 \pmod{p}\}$ and $R_1 = \{r_i \mid r_i \neq 0 \text{ and } r_i \not\equiv 0 \pmod{p}\}$. Let us introduce subsidiary polynomials $F_0(X^p) = \sum_{pi \in E_0} X^{pi}, F_1(X) = \sum_{i \in E_1} X^i, R_0(X^p) = \sum_{pi \in R_0} X^{pi}$ and $R_1(X) = \sum_{i \in R_1} X^i$.

Thus, by Eqs (3.5) and (3.6) we get

$$\begin{aligned} &\sum_{i \in C_1^{(p^{m+1})}} X^i + F_1(X) + S^{(m)}(X^p) + F_0(X^p) \\ = \;& \left(X^{(p^t-1)p^{m+1-t}} + \cdots + X^{p^{m+1-t}} + 1\right) R_1(X) \\ &+ \left(X^{(p^t-1)p^{m+1-t}} + \cdots + X^{p^{m+1-t}} + 1\right) R_0(X^p). \end{aligned}$$

Then

$$\sum_{i \in C_1^{(p^{m+1})}} X^i + F_1(X) = \left(X^{(p^t-1)p^{m+1-t}} + \cdots + X^{p^{m+1-t}} + 1\right) R_1(X)$$

and

$$S^{(m)}(X^p) + F_0(X^p) = \left(X^{(p^t-1)p^{m+1-t}} + \cdots + X^{p^{m+1-t}} + 1\right) R_0(X^p).$$

So, by Lemma 7 and induction supposition, we have

$$wt(F_1(X)) \geq p^m(p-1)/2 - p^{m-t}(p-1)/2$$

and

$$wt(F_0(X^p)) \geq (p^m - p^{m-t})/2.$$

Finally, $wt(E^{(m+1)}(X)) \geq wt(F_1(X)) + wt(F_0(X^p)) = (p^{m+1} - p^{(m+1)-t})/2$.

□

3.3. Proofs of main results

Proof of Theorem 1.

Let $\Phi_0(X) = X - 1$, $\Phi_j(X) = 1 + X^{p^{j-1}} + X^{2p^{j-1}} + \ldots + X^{(p-1)p^{j-1}}$, $j = 1, 2, \ldots, n$. Therefore, we can get that

$$X^{p^n} - 1 = \Phi_0(X)\Phi_1(X)\ldots\Phi_n(X).$$

If 2 is the primitive root modulo p^2, then $\Phi_0(X), \Phi_1(X), \ldots, \Phi_n(X)$ are irreducible polynomials over $\mathbb{F}_2$ [20].

(i), (ii) First, we consider $k < (p^n - p^{n-1})/2$. We note by Proposition 2 that in this case, $\Phi_n(X) \nmid (S^{(n)}(X) + E^{(n)}(X))$ for any $E^{(n)}(X)$ with $wt(E^{(n)}(X)) = k < (p^n - p^{n-1})/2$. By Proposition 1, the study of $LC_k^{\mathbb{F}_2}(s^{(n)})$ is reduced to considering $LC_k^{\mathbb{F}_2}(s^{(n-1)})$.

If $S^{(n-1)}(X) + E^{(n)}(X)$ is divided by a polynomial $G(X)$ satisfying $G(X)|(X^{p^{n-1}} - 1)$, then by Proposition 1 we see that $G(X)$ divides $S^{(n)}(X) + E^{(n)}(X)$ for $p \equiv 1 \pmod 4$ and vice versa. This proves (i).

Let $G(X)$ divide $S^{(n)}(X) + E^{(n)}(X)$ for $p \equiv 3 \pmod 4$ and $LC_k^{\mathbb{F}_2}(s^{(n)}) = p^n - \deg G(X)$. By Proposition 1 we have $\gcd(G(X), \Phi_n(X)) = 1$ and $G(X)$ divides

$$S^{(n-1)}(X) + E^{(n)}(X) + (X^{p^{n-1}} - 1)/(X - 1).$$

Let $G_1(X) = G(X)/\gcd(G(X), X - 1)$. Then $S^{(n-1)}(X) + E^{(n)}(X)$ is divided by $G_1(X)$ and

$$\begin{aligned} LC_k^{\mathbb{F}_2}(s^{(n-1)}) &\leq p^{n-1} - \deg G_1(X) \\ &\leq p^{n-1} - \deg G(X) + 1 = p^{n-1} + 1 - \left(p^n - LC_k^{\mathbb{F}_2}(s^{(n)})\right). \end{aligned}$$

So, $LC_k^{\mathbb{F}_2}(s^{(n)}) \geq p^n - p^{n-1} + LC_k^{\mathbb{F}_2}(s^{(n-1)}) - 1$.

Now we will prove in the similar way the right inequality in (ii).

Let $H(X)$ divides $S^{(n-1)}(X) + E^{(n-1)}(X)$ for $p \equiv 3 \pmod 4$ and $LC_k^{\mathbb{F}_2}(s^{(n-1)}) = p^{n-1} - \deg H(X)$. Denote $H_1(X) = H(X)/\gcd(H(X), X - 1)$. Then $H_1(X)$ divides $(X^{p^{n-1}} - 1)/(X - 1)$. Thus, by Proposition 1 $H_1(X)$ divides

$$S^{(n)}(X) + E^{(n-1)}(X) = S^{(n-1)}(X) + E^{(n-1)}(X) + (X^{p^{n-1}} - 1)/(X - 1).$$

Hence

$$\begin{aligned} LC_k^{\mathbb{F}_2}(s^{(n)}) &\leq p^n - \deg H_1(X) \\ &\leq p^n - \deg H(X) + 1 = p^n + 1 - \left(p^{n-1} - LC_k^{\mathbb{F}_2}(s^{(n-1)})\right) \end{aligned}$$

and we see that

$$LC_k^{\mathbb{F}_2}(s^{(n)}) \leq p^n - p^{n-1} + LC_k^{\mathbb{F}_2}(s^{(n-1)}) + 1.$$

(iii) Let $(p^n - p^{n-t})/2 \le k < (p^n - p^{n-t-1})/2$ for $t = 1, 2, \ldots, n-1$.

Then, by Proposition 2 $LC_k^{\mathbb{F}_2}(s^{(n)}) \le p^{n-t}$. Further, again by Proposition 2 we see that $S^{(n)}(X) + E^{(n)}(X)$ is not divisible by

$$X^{(p^{t+1}-1)p^{n-t-1}} + \cdots + X^{p^{n-t-1}} + 1 = (X^{p^n} - 1)/(X^{p^{n-t-1}} - 1).$$

Thus,

$$(X^{(p^t-1)p^{n-t}} + \cdots + X^{p^{n-t}} + 1)\left(X^{p^{n-t}} - 1\right)$$

is the polynomial with the greatest possible degrees that can divide $S^{(n)}(X) + E^{(n)}(X)$ for $k < (p^n - p^{n-t-1})/2$.

Hence

$$LC_k^{\mathbb{F}_2}(s^{(n)}) \ge p^n - (p^{n-t}(p^t - 1) + p^{n-t-1}) = p^{n-t-1}(p-1).$$

The statements (iv) and (v) are clear. □

Thus, we see that these sequences are stable.

We further run a program to confirm our theorems. The experimental data are listed below, and the results are consistent with Theorem 1.

Example 1. *Let $p = 3, b = 0$. Then, by definition we see that*
$s^{(2)} = (1,1,1,1,1,0,0,0,0)$
and
$s^{(3)} = (1,1,1,1,1,1,1,0,1,1,1,0,1,1,0,0,1,0,0,0,1,0,0,0,0,0,0)$ *per period.*

The calculations show that

$$LC_k^{\mathbb{F}_2}(s^{(2)}) = \begin{cases} 9, & \text{if } k = 0, \\ 6, & \text{if } k = 1,2, \\ 2, & \text{if } k = 3, \\ 1, & \text{if } k = 4, \\ 0, & \text{if } k = 5. \end{cases} \quad \text{and } LC_k^{\mathbb{F}_2}(s^{(3)}) = \begin{cases} 26, & \text{if } k = 0, \\ 25, & \text{if } k = 1, \\ 24, & \text{if } k = 2, \\ 21, & \text{if } k = 3, \\ 18, & \text{if } 4 \le k \le 8, \\ 9, & \text{if } k = 9, \\ 6, & \text{if } k = 10,11, \\ 2, & \text{if } k = 12, \\ 1, & \text{if } k = 13, \\ 0, & \text{if } k \ge 14. \end{cases}$$

Hence, in Theorem 1 (ii) all three cases are possible.

4. Conclusions and final remarks

We have re-examined the k-error linear complexity of the generalized cyclotomic binary sequences of periods p^n proposed in [3]. A progress is made in determining the k-error linear complexity of these sequences. We establish a recursive relation and estimate for the k-error linear complexity of these

sequences. From the results, it follows that the k-error linear complexity of this family of sequences does not decrease dramatically for $k < (p^n - p^{n-1})/2$.

Further, using similar techniques, we can also discuss the k-error linear complexity of a new family of binary sequences with period $2p^n$ presented in [4] whose construction was based on the generalized cyclotomic classes from [5]. In the following part, we recall the definition of generalized cyclotomic sequences proposed in [4] and then give the k-error linear complexity of it without a concrete proof.

It is well known [21] that an odd number g or $g + p^n$ is also a primitive root modulo $2p^j$ for each integer $j \geq 1$, where g is a primitive root modulo p^n. Hence, we can assume in this case that g is an odd number.

For $j = 1, 2, \cdots, n$, define

$$\begin{aligned} D_0^{(2p^j)} &= \left\{ g^{t \cdot d_j} \pmod{2p^j} \,|\, 0 \leq t < e \right\}, \text{ and} \\ D_i^{(2p^j)} &= g^i D_0^{(2p^j)} = \left\{ g^i x \pmod{2p^j} : x \in D_0^{(2p^j)} \right\}, \quad 1 \leq i < d_j. \end{aligned} \tag{4.1}$$

It is clear that $\left\{ D_0^{(2p^j)}, D_1^{(2p^j)}, \ldots, D_{d_j-1}^{(2p^j)} \right\}$ forms a partition of $\mathbb{Z}_{2p^j}^*$ for each integer $j \geq 1$ and for an integer $m \geq 1$,

$$\mathbb{Z}_{2p^m} = \bigcup_{j=1}^{m} p^{m-j} \bigcup_{i=0}^{d_j-1} \left(D_i^{(2p^j)} \cup 2D_i^{(2p^j)} \right) \cup \{0\} \cup \{p^m\}.$$

Define four sets

$$\begin{aligned} \mathscr{D}_0^{(2p^m)} &= \bigcup_{j=1}^{m} \bigcup_{i=d_j/2}^{d_j-1} p^{m-j} \left(D_{(i+b) \pmod{d_j}}^{(2p^j)} \cup 2D_{(i+b) \pmod{d_j}}^{(2p^j)} \right) \cup \{p^m\}, \\ \mathscr{D}_1^{(2p^m)} &= \bigcup_{j=1}^{m} \bigcup_{i=0}^{d_j/2-1} p^{m-j} \left(D_{(i+b) \pmod{d_j}}^{(2p^j)} \cup 2D_{(i+b) \pmod{d_j}}^{(2p^j)} \right) \cup \{0\}, \\ \widetilde{\mathscr{D}}_0^{(2p^m)} &= \bigcup_{j=1}^{m} p^{m-j} \left(\bigcup_{i=0}^{d_j/2-1} 2D_{(i+b) \pmod{d_j}}^{(2p^j)} \cup \bigcup_{i=d_j/2}^{d_j-1} D_{(i+b) \pmod{d_j}}^{(2p^j)} \right) \cup \{p^m\}, \\ \widetilde{\mathscr{D}}_1^{(2p^m)} &= \bigcup_{j=1}^{m} p^{m-j} \left(\bigcup_{i=0}^{d_j/2-1} D_{(i+b) \pmod{d_j}}^{(2p^j)} \cup \bigcup_{i=d_j/2}^{d_j-1} 2D_{(i+b) \pmod{d_j}}^{(2p^j)} \right) \cup \{0\}. \end{aligned}$$

It is obvious that

$$\mathbb{Z}_{2p^m} = \mathscr{D}_0^{(2p^m)} \cup \mathscr{D}_1^{(2p^m)} = \widetilde{\mathscr{D}}_0^{(2p^m)} \cup \widetilde{\mathscr{D}}_1^{(2p^m)}$$

and

$$|\mathscr{D}_i^{(2p^m)}| = |\widetilde{\mathscr{D}}_i^{(2p^m)}| = p^m, \;\; i = 0, 1.$$

Families of balanced binary sequences $u^{(m)} = (u_0^{(m)}, u_1^{(m)}, u_2^{(m)}, \ldots)$ and $\tilde{u}^{(m)} = (\tilde{u}_0^{(m)}, \tilde{u}_1^{(m)}, \tilde{u}_2^{(m)}, \ldots)$ of period $2p^m$ can thus be defined as in [4], i.e.,

$$u_i^{(m)} = \begin{cases} 0, & \text{if } i \pmod{2p^m} \in \mathscr{D}_0^{(2p^m)}, \\ 1, & \text{if } i \pmod{2p^m} \in \mathscr{D}_1^{(2p^m)}, \end{cases} \tag{4.2}$$

and

$$\tilde{u}_i^{(m)} = \begin{cases} 0, & \text{if } i \pmod{2p^m} \in \widetilde{\mathscr{D}}_0^{(2p^m)}, \\ 1, & \text{if } i \pmod{2p^m} \in \widetilde{\mathscr{D}}_1^{(2p^m)}. \end{cases} \tag{4.3}$$

Ouyang et al. [4] examined the linear complexity of these sequences for $f = 2^r$, where r is a positive integer (see also [22]). The results in [4] show that $u^{(m)}$ and $\tilde{u}^{(m)}$ have high linear complexity.

In this case, if $H^{(p^m)} = \bigcup_{i=0}^{d_m/2-1}\left(D^{(2p^m)}_{(i+b) \pmod{d_m}} \cup 2D^{(2p^m)}_{(i+b) \pmod{d_m}}\right)$, then

$$\sum_{i\in H^{(p^m)}} X^i \equiv \sum_{i=0}^{d_m/2-1} d_i^{(p^m)}(X) + \sum_{i=0}^{d_m/2-1} d^{(p^m)}_{i+\mathrm{ind}_g^{(p^m)}(2)}(X) \pmod{X^{p^m}-1},$$

where $\mathrm{ind}_g^{(p^m)}(2) \pmod{d_m}$ is the least number ℓ such that $2 \equiv g^\ell \pmod{p^m}$. Thus, the k-error linear complexity of $u^{(m)}$ and $\tilde{u}^{(m)}$ depends on $\mathrm{ind}_g^{(p^m)}(2) \pmod{d_m}$. We need the following denotations.

Let $T_m = \min\left(\mathrm{ind}_g^{(p^m)}(2) \pmod{d_m}, d_m - \mathrm{ind}_g^{(p^m)}(2) \pmod{d_m}\right)$,

$$A_1 = \begin{cases} 2eT_1+1, & \text{if } 1 \le T_1 < f/4, \\ p-1-2eT_1, & \text{if } f/4 \le T_1 \le f/2, \end{cases}$$

and

$$A_m = \begin{cases} 2eT_m, & \text{if } 1 \le T_m \le p^{m-2}(p-1)f/4, \\ p^{m-2}(p-1)^2/2, & \text{if } p^{m-2}(p-1)f/4 \le T_m \le p^{m-2}(p+1)f/4, \\ p^{m-1}(p-1)-2eT_m, & \text{if } p^{m-2}(p+1)f/4 \le T_m < p^{m-1}f/2, \end{cases}$$

for $m > 1$.

Using the method discussed in Theorem 1, it is easy to get the k-error linear complexity of the sequences with period $2p^n$ in [4]. Therefore, omitting the proof, we only present the results of it below.

Theorem 8. *Let $p = ef+1$ be an odd prime with even f. Let 2 be a primitive root modulo p^2. Let $u^{(n)}$ be a family of generalized cyclotomic binary sequences of period $2p^n$ defined in Eq* (4.2)*. Then we have the following results about ther k-error linear complexity of $u^{(n)}$.*

(i) If $p \equiv 1 \pmod 4$, then for $k < \sum_{i=1}^n A_i$ we have

$$LC_k^{\mathbb{F}_2}(u^{(n)}) = 2p^n - 2p^{n-1} + LC_k^{\mathbb{F}_2}(u^{(n-1)}).$$

(ii) If $p \equiv 3 \pmod 4$, then for $k < \sum_{i=1}^n A_i$ we have

$$2p^n - 2p^{n-1} + LC_k^{\mathbb{F}_2}(u^{(n-1)}) - 1 \le LC_k^{\mathbb{F}_2}(u^{(n)}) \le 2p^n - 2p^{n-1} + LC_k^{\mathbb{F}_2}(u^{(n-1)}) + 1.$$

(iii) For $\sum_{i=1}^n A_i \le k < p^{n-1}(p-1)$, we have $p^n - p^{n-1} \le LC_k^{\mathbb{F}_2}(u^{(n)}) \le p^n + p^{n-1}$.

(iv) For $p^n - p^{n-t} \le k < p^n - p^{n-t-1}$, where $t = 1, 2, \ldots, n-1$ we have

$$2p^{n-t-1}(p-1) \le LC_k^{\mathbb{F}_2}(u^{(n)}) \le 2p^{n-t}.$$

(v) For $k = p^n - 1$, we have $LC_k^{\mathbb{F}_2}(u^{(n)}) = 2$.

(vi) For $k \ge p^n$, we have $LC_k^{\mathbb{F}_2}(u^{(n)}) = 0$.

Thus, the k-error linear complexity of $u^{(n)}$ depends on the values of T_i. In this case, we can have a significant drop of the linear complexity when T_i are small.

Example 2. *Let $p=5, n=2, f=4, b=0$ and $g=27$. By Eq* (4.2)*, we see that*

$$u^{(2)} = (1,1,1,1,1,1,1,1,1,0,1,0,1,0,1,0,1,0,0,0,1,0,0,0,1,0,0,1,1,1,0,1,\\ 1,1,0,1,0,1,0,1,0,1,0,0,0,0,0,0,0,0)$$

and $u^{(1)} = (1,1,1,0,1,0,0,1,0,0)$ per period. In this case, $A_1 = A_2 = 2$ and

$$LC_k^{\mathbb{F}_2}(u^{(1)}) = \begin{cases} 10, & \text{if } k=0, \\ 8, & \text{if } k=1, \\ 6, & \text{if } k=2, \\ 4, & \text{if } k=3. \end{cases} \text{ and } LC_k^{\mathbb{F}_2}(u^{(2)}) = \begin{cases} 50, & \text{if } k=0, \\ 48, & \text{if } k=1, \\ 46, & \text{if } k=2, \\ 44, & \text{if } k=3. \end{cases}$$

But $LC_4^{\mathbb{F}_2}(u^{(2)}) = 30$ and $LC_5^{\mathbb{F}_2}(u^{(2)}) = 24$.

Moreover, it can show that if $g = 2 + p^n$ then $LC_k^{\mathbb{F}_2}(s^{(n)}) \leq p^n$ for $k \geq 2n(p-1)/f + 1$. Now, we consider another example.

Example 3. *Let $p=5, n=2, f=4, b=0$ and $g=3$. Here*

$$u^{(2)} = (1,1,1,1,1,1,1,1,0,1,1,1,1,1,1,0,0,1,1,0,1,0,0,0,1,0,1,0,0,1,0,1,1,1,\\ 0,1,0,0,1,1,0,0,0,0,0,1,0,0,0,0,0,0)$$

and $A_1 = 2, A_2 = 6$. Then

$$LC_k^{\mathbb{F}_2}(u^{(1)}) = \begin{cases} 10, & \text{if } k=0, \\ 8, & \text{if } k=1, \\ 6, & \text{if } k=2, \\ 4, & \text{if } k=3, \\ 2, & \text{if } k=4, \\ 0, & \text{if } k=35. \end{cases} \text{ and } LC_k^{\mathbb{F}_2}(u^{(2)}) = \begin{cases} 50, & \text{if } k=0, \\ 48, & \text{if } k=1, \\ 46, & \text{if } k=2, \\ 44, & \text{if } k=3, \\ 42, & \text{if } k=4, \\ 40, & \text{if } k=5. \end{cases}$$

Further, $LC_8^{\mathbb{F}_2}(u^{(2)}) = 30$ and $LC_9^{\mathbb{F}_2}(u^{(2)}) = 24$.

So, such sequences have good stability when values of T_m and $p^{m-2}(p-1)f/4$ are close.

The statements of Theorem 8 are also true for the k-error linear complexity of $\tilde{u}^{(n)}$.

5. Conclusions

In this paper, we derived the k-error linear complexity generalized binary cyclotomic sequences with period p^n. This paper generalizes the results obtained earlier for sequences of length p^2. Our study shows that these sequences have good stability, i.e., their linear complexity does not decrease significantly with changing a few bits of sequence per period. A recursive relation was used to estimate the k-error linear complexity. At the end of the paper, we discussed the generalized cyclotomic sequences with period $2p^n$ and also estimated their k-error linear complexity. In this case, the stability of sequences depends on the choice of their parameters. In will be interesting to study the k-error of new generalized cyclotomic sequences with other periods.

Acknowledgments

V. Edemskiy were supported by Russian Science Foundation according to the research project No. 22-21-00516, https://rscf.ru/en/project/22-21-00516/, C. Wu was partially supported by the Projects of International Cooperation and Exchange NSFC-RFBR No. 61911530130, by the National Natural Science Foundation of China No. 61772292, by the Natural Science Foundation of Fujian Province No. 2020J01905 and by Science and Technology Project of Putian City No. 2021R4001-10.

Conflict of interest

The authors declare no potential conflict of interest in this paper.

References

1. T. W. Cusick, C. Ding, A. R. Renvall, *Stream ciphers and number theory*, Amsterdam: Elsevier, 2004.
2. C. S. Ding, T. Helleseth, New generalized cyclotomy and its applications, *Finite Fields Appl.*, **4** (1998), 140–166. https://doi.org/10.1006/ffta.1998.0207
3. Z. B. Xiao, X. Y. Zeng, C. L. Li, T. Helleseth, New generalized cyclotomic binary sequences of period p^2, *Des. Codes Cryptogr.*, **86** (2018), 1483–1497. https://doi.org/10.1007/s10623-017-0408-7
4. Y. Ouyang, X. H. Xie, Linear complexity of generalized cyclotomic sequences of period $2p^m$, *Des. Codes Cryptogr.*, **87** (2019), 2585–2596. https://doi.org/10.1007/s10623-019-00638-5
5. X. Y. Zeng, H. Cai, X. H. Tang, Y. Yang, Optimal frequency hopping sequences of odd length, *IEEE T. Inform. Theory*, **59** (2013), 3237–3248. https://doi.org/10.1109/TIT.2013.2237754
6. H. N. Liu, X. Liu, On the properties of generalized cyclotomic binary sequences of period $2p^m$, *Des. Codes Cryptogr.*, **89** (2021), 1691–1712. https://doi.org/10.1007/s10623-021-00887-3
7. V. Edemskiy, C. L. Li, X. Y. Zeng, T. Helleseth, The linear complexity of generalized cyclotomic binary sequences of period p^n, *Des. Codes Cryptogr.*, **87** (2019), 1183–1197. https://doi.org/10.1007/s10623-018-0513-2
8. Z. F. Ye, P. H. Ke, C. H. Wu, A further study of the linear complexity of new binary cyclotomic sequence of length p^n, *AAECC*, **30** (2019), 217–231. https://doi.org/10.1007/s00200-018-0368-9
9. S. Golomb, *Shift register sequences*, California: Aegean Park Press, 1967.
10. M. Stamp, C. F. Martin, An algorithm for the k-error linear complexity of binary sequences with period 2^n, *IEEE T. Inform. Theory*, **39** (1993), 1398–1401. https://doi.org/10.1109/18.243455
11. C. H. Wu, C. X. Xu, Z. X. Chen, P. H. Ke, On error linear complexity of new generalized cyclotomic binary sequences of period p^2, *Inform. Process. Lett.*, **144** (2019), 9–15. https://doi.org/10.1016/j.ipl.2018.08.006
12. Z. X. Chen, V. Edemskiy, P. H. Ke, C. H. Wu, On k-error linear complexity of pseudorandom binary sequences derived from Euler quotients, *Adv. Math. Commun.*, **12** (2018), 805–816. https://doi.org/10.3934/amc.2018047

13. Z. X. Chen, Trace representations and linear complexity of binary sequences derived from Fermat quotients, *Sci. China Inf. Sci.*, **57** (2014), 1–10. https://doi.org/10.1007/s11432-014-5092-x

14. Z. X. Chen, X. N. Du, On the linear complexity of binary threshold sequences derived from Fermat quotients, *Des. Codes Cryptogr.*, **67** (2013), 317–323. https://doi.org/10.1007/s10623-012-9608-3

15. Z. X. Chen, A. Ostafe, A. Winterhof, Structure of pseudorandom numbers derived from Fermat quotients, In: *WAIFI 2010: Arithmetic of finite fields*, Berlin, Heidelberg: Springer, 2010, 73–85. https://doi.org/10.1007/978-3-642-13797-6_6

16. Z. X. Chen, Z. H. Niu, C. H. Wu, On the k-error linear complexity of binary sequences derived from polynomial quotients, *Sci. China Inf. Sci.*, **58** (2015), 1–15. https://doi.org/10.1007/s11432-014-5220-7

17. Z. Chen, X. Du, R. Marzouk, Trace representation of pseudorandom binary sequences derived from Euler quotients, *AAECC*, **26** (2015), 555–570. https://doi.org/10.1007/s00200-015-0265-4

18. Z. F. Ye, P. H. Ke, Z. X. Chen, Linear complexity of d-ary sequence derived from Euler quotients over $GF(q)$, *Chinese J. Electron.*, **28** (2019), 529–534. https://doi.org/10.1049/cje.2019.02.004

19. C. Zhao, W. P. Ma, T. J. Yan, Y. H. Sun, Linear complexity of least significant bit of polynomial quotients, *Chinese J. Electron.*, **26** (2017), 573–578. https://doi.org/10.1049/cje.2016.10.008

20. R. Lidl, H. Niederreiter, *Finite fields*, Cambridge: Cambridge University Press, 1997.

21. K. Ireland, M. Rosen, *A classical introduction to modern number theory*, New York: Springer, 1990.

22. V. Edemskiy, N. Sokolovskiy, The estimate of the linear complexity of generalized cyclotomic binary and quaternary sequences with periods p^n and $2p^n$, *Cryptogr. Commun.*, 2021. https://doi.org/10.1007/s12095-021-00534-7

AIMS Press