Designs, Codes and Cryptography (2019) 87:1183–1197
https://doi.org/10.1007/s10623-018-0513-2

The linear complexity of generalized cyclotomic binary sequences of period p^n

Vladimir Edemskiy[1] · Chunlei Li[2] · Xiangyong Zeng[3] · Tor Helleseth[2]

Received: 3 January 2018 / Revised: 16 June 2018 / Accepted: 21 June 2018 / Published online: 30 June 2018

Abstract
This paper examines the linear complexity of a family of generalized cyclotomic binary sequences of period p^n recently proposed by Xiao et al. (Des Codes Cryptogr, 2017, https://doi.org/10.1007/s10623-017-0408-7), where a conjecture about the linear complexity in the special case that $f = 2^r$ for a positive integer r was made. We prove the conjecture and also extend the result to more general even integers f.

Keywords Binary sequence · Linear complexity · Cyclotomy · Generalized cyclotomic sequence

Mathematics Subject Classification 94A55 · 94A60

1 Introduction

Pseudo-random sequences used for stream ciphers are required to have the property of unpredictability. Linear complexity is one of the main components that indicate this feature. The linear complexity of a sequence is defined as the length of the shortest linear feedback shift register that can generate the sequence [11]. Due to the Berlekamp–Massey algorithm, it is

Communicated by C. Ding.

✉ Xiangyong Zeng
xzeng@hubu.edu.cn

Vladimir Edemskiy
Vladimir.Edemsky@novsu.ru

Chunlei Li
chunlei.li@uib.no

Tor Helleseth
tor.helleseth@uib.no

[1] Novgorod State University, Veliky Novgorod, Russia

[2] University of Bergen, Bergen, Norway

[3] Hubei University, Wuhan, China

reasonable to suggest that the linear complexity of a "good" sequence should be at least a half of the period.

Cyclotomy is an old topic of elementary number theory and is related to difference sets, sequences, coding theory and cryptography [4]. In the past decades generalized cyclotomy has been extensively studied [4,5,10,19,25]. Whiteman [19] introduced a generalized cyclotomy with respect to pq, which was extended with respect to odd integers in [5]. Whiteman's generalized cyclotomy is not consistent with classical cyclotomy. A new generalized cyclotomy that includes classical cyclotomy as a special case was later introduced by Ding and Helleseth [4]. A unified approach that determines both of the Whiteman and Ding-Helleseth generalized cyclotomy was proposed by Fan and Ge [10]. Recently another construction was presented in [25], where the order of the generalized cyclotomic classes depends on the choice of parameters.

Classical and generalized cyclotomies have been used in the construction of cyclic codes [3,15] and sequences [2,4,7] with desirable properties. In recent years there has been some research on generalized cyclotomic binary and non-binary sequences of period p^n [1,7,8,16, 20,23] (see also references therein). Based on the generalized cyclotomic classes in [25], Xiao et al. presented a new family of cyclotomic binary sequences of period p^n and determined the linear complexity of the sequences in the case that $n = 2$ and $f = 2^r$ for a positive integer r [22]. As the exponent n increases, the experimental result indicates that the linear complexity of this family of sequences is very close to p^n. Based on this observation, the authors of [22] made a conjecture about the linear complexity for any positive integer n and even integer $f = 2^r$. In this paper, we revisit the conjecture and prove it based on a detailed investigation of some polynomials over certain extension fields of $\mathbb{F}_2$. With the help of this new technique, we also extend the conjectured result from the special case $f = 2^r$ to more general even integers f.

The remainder of this paper is organized as follows. In Sect. 2 we introduce some basics and recall the generalized cyclotomic sequences and the conjecture in [22]. Section 3 is dedicated to the study of the linear complexity of this family of cyclotomic sequences. Section 4 concludes the work in this paper.

2 Preliminaries

Throughout this paper, we will 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 $\mathbb{Z}_N$, namely, $\mathbb{Z}_N^* = \{x \in \mathbb{Z}_N \mid \gcd(x, N) = 1\}$.

In the following we will recall some basics of the linear complexity of a periodic sequence and introduce the generalized cyclotomic sequences proposed in [22].

2.1 Linear complexity

Let $s^\infty = (s_0, s_1, s_2, \ldots)$ be a binary sequence of period N and $S(x) = s_0 + s_1 x + \cdots + s_{N-1}x^{N-1}$. It is well known (see, for instance, [2, p. 171]) that the minimal polynomial of s^∞ is given by

$$(x^N - 1)\big/ \gcd\left(x^N - 1, S(x)\right)$$

and the linear complexity of s^∞ is given by

$$L = N - \deg\Big(\gcd\left(x^N - 1, S(x)\right)\Big).$$

This formula allows one to determine the linear complexity of s^∞ by examining the roots of $S(x)$ in an extension of $\mathbb{F}_2$ (the finite field of two elements). More specifically, the linear complexity of s^∞ can be given by

$$L = N - \left|\left\{i \in \mathbb{Z}_N \mid S(\beta^i) = 0\right\}\right|, \tag{1}$$

where β is a primitive Nth root of unity in an extension field of $\mathbb{F}_2$.

2.2 New generalized cyclotomic sequences

Let p be an odd prime and $p = ef + 1$, where e, f are positive integers. Let g be a primitive root modulo p^2. It is well known [12] that g is also a primitive root modulo p^j for each integer $j \geq 1$, namely, the order of g modulo p^j is equal to $\varphi(p^j) = p^{j-1}(p-1)$, where $\varphi(\cdot)$ is the Euler's totient function. Below we recall the generalized cyclotomic classes introduced in [25] and the cyclotomic sequences proposed in [22].

Let n be a positive integer. For $j = 1, 2, \ldots, n$, denote $d_j = \varphi(p^j)/e = p^{j-1}f$ and define

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

The cosets $D_i^{(p^j)}, i = 0, 1, \ldots, d_j - 1$, are called *generalized cyclotomic classes* of order d_j with respect to p^j. It was shown in [25] 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 $j \geq 1$ and for an integer $m \geq 1$,

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

Based on the above generalized cyclotomic classes, a family of almost balanced binary sequences was proposed in [22], where f is chosen to be 2^r for a positive integer r. Indeed, the construction of the sequence in [22] can be naturally extended to any even integer f as follows.

Let f be a positive even integer and b an integer with $0 \leq b < p^{n-1}f$. Define two sets

$$\begin{aligned} \mathscr{C}_0^{(p^n)} &= \bigcup_{j=1}^{n} \bigcup_{i=d_j/2}^{d_j-1} p^{n-j} D_{(i+b) \pmod{d_j}}^{(p^j)}, \text{ and} \\ \mathscr{C}_1^{(p^n)} &= \bigcup_{j=1}^{n} \bigcup_{i=0}^{d_j/2-1} p^{n-j} D_{(i+b) \pmod{d_j}}^{(p^j)} \cup \{0\}. \end{aligned} \tag{3}$$

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

$$s_i = \begin{cases} 0, & \text{if } i \pmod{p^n} \in \mathscr{C}_0^{(p^n)}, \\ 1, & \text{if } i \pmod{p^n} \in \mathscr{C}_1^{(p^n)}. \end{cases} \tag{4}$$

In the case of $f = 2^r$, the linear complexity of s^∞ for $n = 2$ was determined in [22], where a conjecture about the linear complexity of s^∞ for any integer $n \geq 3$ was also made as follows.

Conjecture 1 *[22] Let s^{∞} be a generalized cyclotomic binary sequence of period p^n defined by (4). If $2^{(p-1)} \not\equiv 1 \pmod{p^2}$ and $f = 2^r$, where r is a positive integer, then the linear complexity of s^{∞} is given by*

$$L = \begin{cases} p^n - \frac{p-1}{2} - \delta\left(\frac{p^n+1}{2}\right), & \textit{if } 2 \in D_0^{(p)}, \\ p^n - \delta\left(\frac{p^n+1}{2}\right), & \textit{if } 2 \notin D_0^{(p)}, \end{cases}$$

where $\delta(t) = 1$ if t is even and $\delta(t) = 0$ if t is odd.

In the next section we will revisit Conjecture 1 and develop a new technique to prove it. It turns out that the new technique also works for other even integers f and leads to more general result.

3 Linear complexity of generalized cyclotomic sequences

In this section, we will first give some subsidiary lemmas, and then investigate the linear complexity of s^{∞} defined in (4). The main result will be presented in Sect. 3.2.

3.1 Subsidiary lemmas

An odd prime p satisfying $2^{p-1} \equiv 1 \pmod{p^2}$ is known as a Wieferich prime. It is shown in [6] that there are only two Wieferich primes 1093 and 3511 up to 6.7×10^{15}. In this paper we will only focus on non-Wieferich primes.

For a non-Wieferich prime p with $2^{p-1} \not\equiv 1 \pmod{p^2}$, some properties related to 2 $(\bmod\ p^j)$ for integers $j \geq 1$ are discussed below.

Lemma 1 *Let p be a non-Wieferich prime and let $2 \equiv g^u \pmod{p^2}$ for some integer u. Then* $\gcd(u, p) = 1$.

Proof Suppose $\gcd(u, p) \neq 1$, namely, $p|u$. Then $2^{p-1} \equiv g^{u(p-1)} \equiv 1 \pmod{p^2}$. This contradicts the condition that p is a non-Wieferich prime. □

Lemma 2 *Let p be a non-Wieferich prime and $\tau = \mathrm{ord}_p(2)$ be the order of 2 modulo p. Then the order of 2 modulo p^j for an integer $j \geq 1$ is τp^{j-1}.*

Proof The statement for $j = 1$ is trivial and we only need to consider the case that $j \geq 2$. Since p is a non-Wieferich prime and τ is the order of 2 modulo p, there exists an integer t such that $2^{\tau} = 1 + pt$ with $\gcd(p, t) = 1$.

Let σ be the order of 2 modulo p^j, namely, σ is the least positive integer satisfying $2^{\sigma} \equiv 1 \pmod{p^j}$. By the properties of binomial coefficients,

$$2^{\tau p^{j-1}} = (1 + pt)^{p^{j-1}} \equiv 1 \pmod{p^j}.$$

This implies $\sigma \mid \tau p^{j-1}$. On the other hand, it is clear that τ divides σ. Denote $\sigma = \tau d p^l$, where $\gcd(p, d) = 1$ and $l \geq 0$. Again by the properties of binomial coefficients we have

$$2^{\sigma} = 2^{\tau d p^l} = (1 + pt)^{d p^l} \equiv 1 + d t p^{l+1} \pmod{p^{l+2}}.$$

Since $\gcd(dt, p) = 1$, it follows that $2^{\sigma} \pmod{p^j} = 1$ if and only if $l + 1 \geq j$. Hence τp^{j-1} divides $\sigma = \tau d p^l$. From the above analysis the desired conclusion follows. □

Let $\overline{\mathbb{F}}_2$ be the algebraic closure of $\mathbb{F}_2$ and $\alpha_n \in \overline{\mathbb{F}}_2$ be a primitive p^nth root of unity. Denote $\alpha_j = \alpha_n^{p^{n-j}}$, $j = 1, 2 \ldots, n-1$. Then α_j is a primitive p^jth root of unity in an extension field of $\mathbb{F}_2$. As usual, we denote by $\mathbb{F}_2(\alpha_j)$ a simple extension of $\mathbb{F}_2$ obtained by adjoining an algebraic element α_j [18]. The dimension of the vector space $\mathbb{F}_2(\alpha_j)$ over $\mathbb{F}_2$ is called the degree of $\mathbb{F}_2(\alpha_j)$ over $\mathbb{F}_2$, in symbols $[\mathbb{F}_2(\alpha_j) : \mathbb{F}_2]$.

Lemma 3 *For a non-Wieferich prime p, we have*

$$[\mathbb{F}_2(\alpha_{j+1}) : \mathbb{F}_2(\alpha_j)] = p, \quad j = 1, 2, \ldots, n-1,$$

where $\alpha_j = \alpha_n^{p^{n-j}}$ and α_n is a primitive p^nth root of unity.

Proof It is well known [18] that if $\mathbb{F}$ is a finite extension of $\mathbb{F}_2$, then $|\mathbb{F}| = 2^{[\mathbb{F}:\mathbb{F}_2]}$ and the order of any nonzero element $\mathbb{F}$ divides $|\mathbb{F}| - 1$. Let τ be the order of 2 modulo p. It follows from Lemma 2 that $2^{\tau p^{j-1}} \equiv 1 \pmod{p^j}$ and $2^{\tau p^{j-1}} \not\equiv 1 \pmod{p^{j+1}}$ for any integer $j \geq 1$, which implies $\alpha_j \in \mathbb{F}_{2^{\tau p^{j-1}}}$ and $\alpha_{j+1} \notin \mathbb{F}_{2^{\tau p^{j-1}}}$. That is to say, $[\mathbb{F}_2(\alpha_j) : \mathbb{F}_2] = \tau p^{j-1}$ for $j = 1, 2, \ldots, n$. The desired result immediately follows. □

The following lemma discusses some of the basic properties of the generalized cyclotomic classes defined in (2). Despite the simplicity, the proof is included here for completeness.

Lemma 4 *For $D_i^{(p^j)}$ defined as in (2), we have*

(i) $a D_i^{(p^j)} = D_{i+k \pmod{d_j}}^{(p^j)}$ *for $a \in D_k^{(p^j)}$; and*

(ii) $D_i^{(p^j)} \pmod{p^l} = D_{i \pmod{d_l}}^{(p^l)}$ *for $1 \leq l \leq j$.*

Proof (i) By the definition in (2), any element a in $D_k^{(p^j)}$ can be written as $a = g^{k+t_0 d_j}$ for some integer t_0 with $0 \leq t_0 < e$. Thus,

$$a D_i^{(p^j)} = \left\{ g^{k+t_0 d_j} \cdot g^{i+t d_j} \mid 0 \leq t < e \right\} = \left\{ g^{i+k \,(\mathrm{mod}\, d_j)} \cdot g^{t' d_j} \mid 0 \leq t' < e \right\} = D_{i+k \,(\mathrm{mod}\, d_j)}^{(p^j)}.$$

(ii) For any positive integer l with $l \leq j$, since g is also a primitive root modulo p^l, one has

$$g^{d_j} \,(\mathrm{mod}\, p^l) = g^{(p^{l-1}(p^{j-l}-1)+p^{l-1})f} \,\mathrm{mod} p^l) = g^{d_l} \,(\mathrm{mod}\, p^l),$$

whence

$$g^{i+d_j t} \,(\mathrm{mod}\, p^l) = g^{i \,(\mathrm{mod}\, d_l)+t_i d_l+t d_j} \,(\mathrm{mod}\, p^l) = g^{i \,(\mathrm{mod}\, d_l)+t' d_l} \,(\mathrm{mod}\, p^l).$$

The desired result thus follows.

□

The above auxiliary lemmas will be heavily used in our investigation of the linear complexity of s^∞ in the next subsection.

3.2 Main result

This subsection will investigate the linear complexity of s^∞ defined in (4) for some even integers f. The main result in this paper is given as follows.

Theorem 5 *Let $p = ef + 1$ be an odd prime with $2^{p-1} \not\equiv 1 \pmod{p^2}$ and f being an even positive integer. Let s^∞ be the generalized cyclotomic binary sequence of period p^n defined in (4). Let $\mathrm{ord}_p(2)$ denote the order of 2 modulo p and $v = \gcd\left(\frac{p-1}{\mathrm{ord}_p(2)}, f\right)$. Then the linear complexity of s^∞ is given by*

$$L = p^n - r \cdot \mathrm{ord}_p(2) - \delta\left(\tfrac{p^n+1}{2}\right), \quad 0 \le r \le \tfrac{p-1}{2\mathrm{ord}_p(2)},$$

where $\delta(t) = 1$ if t is even and $\delta(t) = 0$ if t is odd. Furthermore,

(i) *for $p \equiv \pm 3 \pmod 8$, the linear complexity $L = p^n - \delta\left(\frac{p^n+1}{2}\right)$; and*
(ii) *for $p \equiv \pm 1 \pmod 8$, the linear complexity*

$$L = \begin{cases} p^n - \frac{p-1}{2} - \delta\left(\frac{p^n+1}{2}\right), & \text{if } v = f; \\ p^n - \delta\left(\frac{p^n+1}{2}\right), & \text{if } v | \frac{f}{2}, \text{ or } v = 2 \text{ and } v \neq f. \end{cases}$$

Remark 1 Suppose $2 \equiv g^u \pmod p$ for some integer u. It is easily seen that $\gcd\left(\frac{p-1}{\mathrm{ord}_p(2)}, f\right) = \gcd(u, f)$. Thus the condition $2 \in D_0^{(p)}$ in Conjecture 1 is equivalent to $v = \gcd\left(\frac{p-1}{\mathrm{ord}_p(2)}, f\right) = f$. In the case that $f = 2^r$ for a positive integer r, the integer v is also a power of 2, which either equals f or divides $f/2$. Hence Conjecture 1 is included in Theorem 5 as a special case.

Remark 2 A recent paper [24] studied the linear complexity of a family of generalized cyclotomic sequences and also proved Conjecture 1. The authors of [24] pointed out that their work is significantly different from the early version [9] of this paper with respect to the sequences in consideration and the technique used in the computation of linear complexity. When the sequences in the two papers are the same, the explicit result obtained in [24] is a special case of Theorem 5.

Remark 3 Given an odd prime p with $p \equiv \pm 1 \pmod 8$, one can flexibly choose a number of even integers f satisfying the conditions in Theorem 5 (ii) according to the parity of $\frac{p-1}{\mathrm{ord}_p(2)}$ as follows.

(i) If $\mathrm{ord}_p(2)$ is even, then any integer f with $\nu_2(f) > \nu_2(\frac{p-1}{\mathrm{ord}_p(2)})$ will satisfy the condition $v \mid \frac{f}{2}$, where $\nu_2(t)$ denotes the exponent of the largest power of 2 dividing an integer t. In particular, when 2 is a primitive root modulo p, any even integer f satisfies the condition.
(ii) If $\mathrm{ord}_p(2)$ is odd, then any even integer $f = 2f_1$ with $\gcd(\frac{p-1}{\mathrm{ord}_p(2)}, f_1) = 1$ will satisfy the condition $v = 2$.

On the other hand, when an even integer f is not covered by Theorem 5 (ii), the experimental result indicates that the linear complexity of s^∞ varies for different choices of f (see, e.g., Example 2).

Before we start with the proof of Theorem 5, we need to introduce some polynomials derived from the sequence s^∞ and investigate their properties.

Let $S(x) = s_0 + s_1 x + \cdots + s_{p^n-1} x^{p^n-1}$ for the generalized cyclotomic sequences s^∞ defined in (4) . Then,

$$S(x) = \sum_{i=0}^{p^n-1} s_i x^i = \sum_{t \in \mathscr{C}_1^{(p^n)}} x^t = 1 + \sum_{j=1}^{n} \sum_{i=0}^{d_j/2-1} \sum_{t \in D_{i+b \pmod{d_j}}^{(p^j)}} x^{p^{n-j}t}. \tag{5}$$

For simplicity of presentation, we define polynomials

$$E_i^{(p^j)}(x) = \sum_{t \in D_i^{(p^j)}} x^t, \quad 1 \le j \le n,\ 0 \le i < d_j, \tag{6}$$

and

$$H_k^{(p^j)}(x) = \sum_{i=0}^{d_j/2-1} E_{i+k \pmod{d_j}}^{(p^j)}(x), \quad 0 \le k < d_j,$$

$$T_k^{(p^m)}(x) = \sum_{j=1}^{m} H_k^{(p^j)}(x^{p^{m-j}}), \quad m = 1, 2, \ldots, n. \tag{7}$$

Notice that the subscripts i in $D_i^{(p^j)}$, $H_i^{(p^j)}(x)$ and $T_i^{(p^j)}(x)$ 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.

It can be easily seen from (5)–(7) that $S(x) = 1 + T_b^{(p^n)}(x)$. By (1) the linear complexity of s^∞ in (4) can thus be given by

$$L = N - \left|\left\{i \in \mathbb{Z}_{p^n} \mid T_b^{(p^n)}(\alpha_n^i) = 1\right\}\right|, \tag{8}$$

where α_n is a p^nth primitive root of unity. In the following we shall investigate the value of $T_b^{(p^n)}(\alpha_n^i)$ as i runs through $\mathbb{Z}_{p^n}$.

From the definitions in (6) and (7), the polynomial $T_b^{(p^n)}(x)$ heavily depends on the polynomials $E_i^{(p^j)}(x)$ and $H_i^{(p^j)}(x)$ for $1 \le j \le n$ and $0 \le i < d_j$. Some basic properties of these polynomials are given in the following lemma.

Lemma 6 *Let $\alpha_j = \alpha_n^{p^{n-j}}$, $1 \le j \le n$, be a p^jth primitive root of unity. Given any element $a \in D_k^{(p^j)}$, we have*

(i) $E_i^{(p^j)}(\alpha_j^{p^l a}) = E_{i+k}^{(p^{j-l})}(\alpha_{j-l})$ *and* $H_i^{(p^j)}(\alpha_j^{p^l a}) = H_{i+k}^{(p^{j-l})}(\alpha_{j-l})$ *for* $0 \le l < j$*; and*

(ii) $E_i^{(p^j)}(\alpha_j^{p^l a}) = e \pmod 2$ *and* $H_i^{(p^j)}(\alpha_j^{p^l a}) = p^{j-1}(p-1)/2 \pmod 2$ *for* $l \ge j$.

Proof (i) In this case, it follows from Lemma 4 (i) that

$$E_i^{(p^j)}\left(\alpha_j^{p^l a}\right) = \sum_{t \in D_i^{(p^j)}} \left(\alpha_j^{p^l a}\right)^t = \sum_{t \in D_{i+k}^{(p^j)}} \left(\alpha_j^{p^l}\right)^t = \sum_{t \in D_{i+k}^{(p^j)}} \alpha_{j-l}^t.$$

Since α_{j-l} is a p^{j-l}th primitive root of unity, one has $\alpha_{j-l}^t = \alpha_{j-l}^{t \pmod{p^{j-l}}}$ for $t \in D_{i+k}^{(p^j)}$. Lemma 4 (ii) implies $D_{i+k}^{(p^j)} \pmod{p^{j-l}} = D_{i+k}^{(p^{j-l})}$, whence

$$E_i^{(p^j)}\left(\alpha_j^{p^l a}\right) = \sum_{t \in D_{i+k}^{(p^j)}} \alpha_{j-l}^t = \sum_{t \in D_{i+k}^{(p^{j-l})}} \alpha_{j-l}^t = E_{i+k}^{(p^{j-l})}(\alpha_{j-l}).$$

Furthermore, by the definition of $H_i^{(p^j)}(x)$ we have

$$H_i^{(p^j)}\left(\alpha_j^{p^l a}\right) = \sum_{i'=0}^{d_j/2-1} E_{i'+i}^{(p^j)}\left(\alpha_j^{p^l a}\right) = \sum_{i'=0}^{d_j/2-1} E_{i'+i+k}^{(p^{j-l})}(\alpha_{j-l}).$$

We observe that

$$\sum_{i'=d_{j-l}/2}^{d_j/2-1} E_{i'+i+k}^{(p^{j-l})}(\alpha_{j-l}) = \frac{p^l-1}{2}\sum_{i'=0}^{d_{j-l}-1} E_{i'}^{(p^{j-l})}(\alpha_{j-l}) = \frac{p^l-1}{2}\sum_{t\in\mathbb{Z}_{p^{j-l}}^*} \alpha_{j-l}^t = 0.$$

This implies

$$H_i^{(p^j)}\left(\alpha_j^{p^l a}\right) = \sum_{i'=0}^{d_{j-l}/2-1} E_{i'+i+k}^{(p^{j-l})}(\alpha_{j-l}) = H_{i+k}^{(p^{j-l})}(\alpha_{j-l}).$$

(ii) In this case we have $\alpha_j^{p^l} = 1$. Then

$$E_i^{(p^j)}\left(\alpha_j^{p^l a}\right) = E_i^{(p^j)}(1) = |D_i^{(p^j)}| \pmod 2 = e \pmod 2,$$

and $H_i^{(p^j)}(\alpha_j^{p^l a}) = ed_j/2 \pmod 2 = p^{j-1}(p-1)/2 \pmod 2$.

□

The following proposition characterizes some properties of $T_i^{(p^m)}(x)$ for $1 \le m \le n$.

Proposition 1 *For any $a \in D_k^{(p^j)}$, we have*

(i) $T_i^{(p^m)}(\alpha_m^{p^l a}) = T_{i+k}^{(p^{m-l})}(\alpha_{m-l}) + (p^l-1)/2 \pmod 2$ *for* $0 \le l < m$; *and*
(ii) $T_i^{(p^m)}(\alpha_m^a) + T_{i+d_m/2}^{(p^m)}(\alpha_m^a) = 1$.

Proof (i) From the definition in (6), Lemma 4 (ii) and Lemma 6, it follows that

$$\begin{aligned}
T_i^{(p^m)}\left(\alpha_m^{p^l a}\right) &= \sum_{j=1}^{m} H_i^{(p^j)}\left(\alpha_m^{p^{m-j+l}a}\right)\\
&= \sum_{j=l+1}^{m} H_i^{(p^j)}\left(\alpha_{j-l}^a\right) + \sum_{j=1}^{l} H_i^{(p^j)}(1)\\
&= \sum_{j=l+1}^{m} H_{i+k}^{(p^{j-l})}\left(\alpha_{j-l}\right) + (p^l-1)/2 \pmod 2\\
&= \sum_{j=1}^{m-l} H_{i+k}^{(p^j)}\left(\alpha_j\right) + (p^l-1)/2 \pmod 2. \qquad (9)
\end{aligned}$$

Similarly we have

$$T_{i+k}^{(p^{m-l})}(\alpha_{m-l}) = \sum_{j=1}^{m-l} H_{i+k}^{(p^j)}\left(\alpha_{m-l}^{p^{m-l-j}}\right) = \sum_{j=1}^{m-l} H_{i+k}^{(p^j)}\left(\alpha_j\right).$$

The desired result thus follows.

(ii) By $\gcd(a, p) = 1$ we know that α_m^a is also a primitive p^mth root of unity. Thus α_m^a is a root of the polynomial $f(x) = (x^{p^m} - 1)/(x-1) = x^{p^m-1} + x^{p^m-2} + \cdots + x + 1$. By the definitions in (2), (6) and (7), it can be readily shown that

$$T_i^{(p^m)}(x) + T_{i+d_m/2}^{(p^m)}(x) = x^{p^m-1} + x^{p^m-2} + \cdots + x = f(x) + 1,$$

which immediately yields the desired result.

□

We now examine the value of $T_b^{(p^n)}(\alpha_n^i)$ for some integers $i \in \mathbb{Z}_{p^n}$.

Proposition 2 *Let p be a non-Wieferich prime. Then* $T_b^{(p^n)}(\alpha_n^i) \notin \{0, 1\}$ *for* $i \in \mathbb{Z}_{p^n} \setminus p^{n-1}\mathbb{Z}_p$ *and* $b = 0, 1, \ldots, d_n - 1$.

Proof We will show $T_b^{(p^n)}(\alpha_n^i) \notin \{0, 1\}$ by contradiction. Suppose there exists an integer $i_0 \in \mathbb{Z}_{p^n} \setminus p^{n-1}\mathbb{Z}_p$ such that $T_b^{(p^n)}(\alpha_n^{i_0}) \in \{0, 1\}$. The integer i_0 can be written as $i_0 = p^{n-m}a$, where $1 < m \leq n$ and $a \in \mathbb{Z}_{p^m}^*$. Assume $a \in D_k^{(p^m)}$. By Proposition 1 (i) we have

$$T_b^{(p^n)}(\alpha_n^{i_0}) = T_b^{(p^n)}(\alpha_n^{p^{n-m}a}) = T_{b+k}^{(p^m)}(\alpha_m) + (p^{n-m} - 1)/2 \pmod 2,$$

whence $T_{b+k}^{(p^m)}(\alpha_m) \in \{0, 1\}$. Without loss of generality, we can assume $b+k \equiv 0 \pmod{d_m}$ and $T_0^{(p^m)}(\alpha_m) = 0$.

Suppose $2 \equiv g^u \pmod{p^m}$ for some integer u. Letting $u_1 \equiv u \pmod{d_m}$, we have $2 \in D_{u_1}^{(p^m)}$. It then follows from Proposition 1 (i) that

$$T_0^{(p^m)}(\alpha_m) = \left(T_0^{(p^m)}(\alpha_m)\right)^2 = T_0^{(p^m)}(\alpha_m^2) = T_{u_1}^{(p^m)}(\alpha_m),$$

which implies $T_0^{(p^m)}(\alpha_m) = T_{iu_1}^{(p^m)}(\alpha_m) = 0$ for any integer $i \geq 1$.

Denote $v = \gcd(u_1, d_m)$. Since the subscript of $T_i^{(p^m)}(x)$ is taken modulo d_m, it is easily seen that

$$0 = T_0^{(p^m)}(\alpha_m) = T_{iv}^{(p^m)}(\alpha_m), \quad i = 1, \ldots, d_m/v - 1. \tag{10}$$

By Proposition 1 (ii) we have $T_0^{(p^m)}(\alpha_m) + T_{d_m/2}^{(p^m)}(\alpha_m) = 1$, whence $T_{d_m/2}^{(p^m)}(\alpha_m) = 1$. Thus v does not divide $d_m/2$. Since $v = \gcd(u_1, d_m) = \gcd(u, d_m)$ and $\gcd(u, p) = 1$ (by Lemma 1), it follows that v divides f but does not divide $f/2$. A similar argument as in (10) gives

$$1 = T_{d_m/2}^{(p^m)}(\alpha_m) = T_{d_m/2+if}^{(p^m)}(\alpha_m) \quad i = 1, \ldots, d_m/v - 1,$$

which implies $T_{f/2}^{(p^m)}(\alpha_m) = T_{d_m/2+f(p^{m-1}+1)/2}^{(p^m)}(\alpha_m) = 1$. Hence we have

$$T_0^{(p^m)}(\alpha_m) + T_{f/2}^{(p^m)}(\alpha_m) = 1.$$

Denote $\xi = H_0^{(p^m)}(\alpha_m) + H_{f/2}^{(p^m)}(\alpha_m)$. Since

$$T_0^{(p^m)}(\alpha_m) + T_{f/2}^{(p^m)}(\alpha_m) = \sum_{j=1}^{m} \left(H_0^{(p^j)}\left(\alpha_m^{p^{m-j}}\right) + H_{f/2}^{(p^j)}\left(\alpha_m^{p^{m-j}}\right)\right),$$

it follows that

$$\xi = 1 + \sum_{j=1}^{m-1} \left(H_0^{(p^j)}\left(\alpha_{m-1}^{p^{m-1-j}}\right) + H_{f/2}^{(p^j)}\left(\alpha_{m-1}^{p^{m-1-j}}\right)\right) \in \mathbb{F}_2(\alpha_{m-1}).$$

On the other hand, by eliminating the overlapping terms in $H_0^{(p^m)}(\alpha_m)$ and $H_{f/2}^{(p^m)}(\alpha_m)$ we obtain

$$\xi = E_0^{(p^m)}(\alpha_m) + \cdots + E_{f/2-1}^{(p^m)}(\alpha_m) + E_{d_m/2}^{(p^m)}(\alpha_m) + \cdots + E_{f/2+d_m/2-1}^{(p^m)}(\alpha_m) = \sum_{t\in\mathscr{D}} \alpha_m^t, \tag{11}$$

where $\mathscr{D} = D_0^{(p^m)} \cup \cdots \cup D_{f/2-1}^{(p^m)} \cup D_{d_m/2}^{(p^m)} \cup \cdots \cup D_{f/2+d_m/2-1}^{(p^m)}$. Observe that

$$\begin{aligned}\mathscr{D} \pmod p &= D_0^{(p)} \cup \cdots \cup D_{f/2-1}^{(p)} \cup D_{d_m/2 \pmod f}^{(p)} \cup \cdots \cup D_{f/2+d_m/2-1 \pmod f}^{(p)} \\ &= D_0^{(p)} \cup \cdots \cup D_{f/2-1}^{(p)} \cup D_{f/2}^{(p)} \cup \cdots \cup D_{f-1}^{(p)} \\ &= \mathbb{Z}_p^*.\end{aligned}$$

Thus, by letting $t \pmod p = \bar{t}$ for any $t \in \mathscr{D}$ we have

$$\xi = \sum_{t\in\mathscr{D}} \alpha_m^t = \sum_{t\in\mathscr{D}} \alpha_m^{(t-\bar{t})+\bar{t}} = \sum_{t\in\mathscr{D}} \alpha_{m-1}^{(t-\bar{t})/p} \alpha_m^{\bar{t}} = \sum_{i=1}^{p-1} c_i \alpha_m^i, \quad c_i \in \mathbb{F}_2(\alpha_{m-1}).$$

It means that α_m is a root of the polynomial $f(x) = \sum_{i=1}^{p-1} c_i x^i + \xi$ over $\mathbb{F}_2(\alpha_{m-1})$. This implies $[\mathbb{F}_2(\alpha_m) : \mathbb{F}_2(\alpha_{m-1})] < p$, which is in contradiction with Lemma 3. □

Remark 4 Proposition 2 greatly excludes the integers $i \in \mathbb{Z}_{p^n}$ that potentially lead to $T_b^{(p^n)}(\alpha_n^i) = 1$, which is critical for the proof of the main theorem. The technique used in the proof of Proposition 2 is generic and works for any integer $n \geq 2$. In the case of $n = 2$, it can be used to prove the statement in Lemma 6 [22], where the documented proof works only for $f = 2$.

By Proposition 2, we only need to study the value of $T_b^{(p^n)}(\alpha_n^i)$ for integers i in the set $p^{n-1}\mathbb{Z}_p$. For any $a \in \mathbb{Z}_p^*$, it follows from Proposition 1 and Lemma 6 that

$$T_b^{(p^n)}(\alpha_n^{p^{n-1}a}) = T_b^{(p)}(\alpha_1^a) = H_b^{(p)}(\alpha_1^a) = H_k^{(p)}(\alpha_1),$$

where $a \in D_i^{(p)}$ for some integer i and $k \equiv b + i \pmod f$. The following proposition examines the value of $H_k^{(p)}(\alpha_1)$ according to the relation between f and $\mathrm{ord}_p(2)$.

Proposition 3 *Let $p = ef + 1$ be an odd prime with f being an even positive integer and $v = \gcd(\frac{p-1}{\mathrm{ord}_p(2)}, f)$. Then,*

(i) $\left|\left\{k \in \mathbb{Z}_f \mid H_k^{(p)}(\alpha_1) = 0\right\}\right| = \left|\left\{k \in \mathbb{Z}_f \mid H_k^{(p)}(\alpha_1) = 1\right\}\right| = f/2$ *if* $v = f$*; and*

(ii) $\left|\left\{k \in \mathbb{Z}_f \mid H_k^{(p)}(\alpha_1) = 0\right\}\right| = \left|\left\{k \in \mathbb{Z}_f \mid H_k^{(p)}(\alpha_1) = 1\right\}\right| = 0$ *if* $v \mid \frac{f}{2}$*, or* $v = 2$ *and* $f \neq v$.

Proof From the definition of $H_k^{(p)}(x)$ we have

$$H_k^{(p)}(\alpha_1) + H_{k+f/2}^{(p)}(\alpha_1) = \alpha_1^{p-1} + \alpha_1^{p-2} + \cdots + \alpha_1 = 1 \tag{12}$$

for $k = 0, 1, \ldots, f-1$. Thus $\left|\left\{k \in \mathbb{Z}_f \mid H_k^{(p)}(\alpha_1) = 0\right\}\right| = \left|\left\{k \in \mathbb{Z}_f \mid H_k^{(p)}(\alpha_1) = 1\right\}\right|$.

Assume $2 \equiv g^u \pmod{p}$ for some integer u in $\mathbb{Z}_p^*$. Since $\mathrm{ord}_p(2) = \frac{p-1}{\gcd(p-1,u)}$, it follows that $\gcd(p-1, u) = \frac{p-1}{\mathrm{ord}_p(2)}$. Thus we can write u as $u = \frac{(p-1)t}{\mathrm{ord}_p(2)}$ with t co-prime to f. Denote $u_1 \equiv u \pmod{f}$. It follows that $2 \in D_{u_1}^{(p)}$ and $\gcd(u_1, f) = \gcd(u, f) = \gcd(\frac{(p-1)t}{\mathrm{ord}_p(2)}, f) = \gcd(\frac{(p-1)}{\mathrm{ord}_p(2)}, f) = v$.

(i) In this case we have $u_1 \equiv 0 \pmod{f}$. Then $2 \in D_0^{(p)}$ and

$$\left(H_k^{(p)}(\alpha_1)\right)^2 = H_k^{(p)}(\alpha_1^2) = H_k^{(p)}(\alpha_1)$$

for any $k \in \mathbb{Z}_f$, which implies $H_k^{(p)}(\alpha_1) \in \mathbb{F}_2$. The desired result immediately follows from (12).

(ii) We shall prove this case by contradiction. Suppose $H_k^{(p)}(\alpha_1) \in \mathbb{F}_2$ for some integer k. Without loss of generality, we assume $k = 0$ and $H_0^{(p)}(\alpha_1) = 0$.

In the case that $v \neq f$, we have $u_1 < f$. Since $2 \in D_{u_1}^{(p)}$ and $v = \gcd(u_1, f)$, by a similar argument as in the proof of Proposition 2 we get

$$0 = H_0^{(p)}(\alpha_1) = H_v^{(p)}(\alpha_1) = \cdots = H_{(f/v-1)v}^{(p)}(\alpha_1),$$

and

$$1 = H_{f/2}^{(p)}(\alpha_1) = H_{f/2+v}^{(p)}(\alpha_1) = \cdots = H_{f/2+(f/v-1)v}^{(p)}(\alpha_1).$$

If v divides $f/2$, then $H_{f/2}^{(p)}(\alpha_1) = H_{f/2+v\cdot f/2v}^{(p)}(\alpha_1) = H_0^{(p)}(\alpha_1)$, which is a contradiction.

Let $v = 2$, $v \neq f$ and v does not divide $f/2$, it is clear that $f/2$ is odd. Then we get

$$0 = H_0^{(p)}(\alpha_1) = H_2^{(p)}(\alpha_1) = \cdots = H_{(f-2)}^{(p)}(\alpha_1),$$

and

$$1 = H_1^{(p)}(\alpha_1) = H_3^{(p)}(\alpha_1) = \cdots = H_{f-1}^{(p)}(\alpha_1).$$

So, we see that $H_i^{(p)}(\alpha_1) + H_{i+1}^{(p)}(\alpha_1) + 1 = 0, i = 0, 1, \ldots, f-1$ and then

$$E_i^{(p)}(\alpha_1) + E_{i+f/2}^{(p)}(\alpha_1) + 1 = 0, \quad i = 0, 1, \ldots, f-1. \tag{13}$$

By the definition we can easily choose an integer j such that $(p-1) \notin \left(D_j^{(p)} \cup D_{j+f/2}^{(p)}\right)$.

We define $f(x) = E_j^{(p)}(x) + E_{j+f/2}^{(p)}(x) + 1$. Given any $a \in \mathbb{Z}_p^*$, assuming $a \in D_k^{(p)}$ for an integer k, we obtain from Lemma 6 and (13) that $f(\alpha_1^a) = E_{j+k}^{(p)}(\alpha_1) + E_{j+f/2+k}^{(p)}(\alpha_1) + 1 = 0$. That is to say, $f(\alpha_1^a) = 0$ for any $a \in \mathbb{Z}_p^*$. This is a contradiction since the polynomial $f(x)$ has degree less than $p-1$. □

With the preceding preparations, we are now in a position to prove the main theorem.

Proof of Theorem 5 Recall that the linear complexity of s^∞ is given by

$$L = p^n - \left|\left\{i \in \mathbb{Z}_{p^n} \mid T_b^{(p^n)}(\alpha_n^i) = 1\right\}\right|.$$

From Proposition 2 we know $\left|\left\{i \in \mathbb{Z}_{p^n} \setminus p^{n-1}\mathbb{Z}_p \mid T_b^{(p^n)}(\alpha_n^i) = 1\right\}\right| = 0$. For the remaining set $p^{n-1}\mathbb{Z}_p$, if $i = 0$, then $T_b^{(p^n)}(\alpha_n^i) = \frac{p^n-1}{2} \pmod 2$; if $i \in p^{n-1}\mathbb{Z}_p^*$, we have

$$T_b^{(p^n)}(\alpha_n^i) = T_b^{(p)}(\alpha_1^a) = H_b^{(p)}(\alpha_1^a)$$

for some integer $a \in \mathbb{Z}_p^*$. It is easily seen that $\left|\left\{a \in \mathbb{Z}_p^* \mid H_b^{(p)}(\alpha_1^a) = 1\right\}\right| = e\left|\left\{k \in \mathbb{Z}_f \mid H_k^{(p)}(\alpha_1) = 1\right\}\right|$ for any integer b with $0 \le b < d_n$. Hence the linear complexity

$$L = p^n - \delta\left(\tfrac{p^n+1}{2}\right) - e\left|\left\{k \in \mathbb{Z}_f \mid H_k^{(p)}(\alpha_1) = 1\right\}\right|. \tag{14}$$

Suppose $H_k^{(p)}(\alpha_1) = 1$ for some integer k. Then

$$1 = (H_k^{(p)}(\alpha_1))^2 = H_k^{(p)}(\alpha_1^2) = H_{k+u_1}^{(p)}(\alpha_1^2),$$

where $2 \in D_{u_1}^{(p)}$ for some integer u_1. From the fact that $H_k^{(p)}(\alpha_1) + H_{k+f/2}^{(p)}(\alpha_1^a) = 1$ for any $k \in \mathbb{Z}_f$, we have

$$L = p^n - \delta(\tfrac{p^n+1}{2}) - r\,\mathrm{ord}_p(2),$$

where r is an integer with $0 \le r \le \frac{p-1}{2\,\mathrm{ord}_p(2)}$.

(i) For $p \equiv \pm 3 \pmod 8$, it is well known [12] that 2 is a quadratic non-residue of primes since the Legendre symbol $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Assume $2 = g^u \pmod p$ for some odd integer u. It follows that $\gcd\left(\frac{p-1}{\mathrm{ord}_p(2)}, f\right) = \gcd(u, f)$ is odd, which always divides $f/2$. From Proposition 3 (ii) the desired result follows.

(ii) For $p \equiv \pm 1 \pmod 8$, we immediately obtain the desired result from Proposition 3. □

At the end of this section, we give some examples demonstrating the main result in this paper.

Example 1 Choose an odd prime $p = 13$. The possible even divisors f of $p-1$ are 2, 4, 6, 12 and in this case 2 is a primitive root. To avoid confusion we take a primitive root $g = 6$.

(i) For $n = 1$ and $f = 2, 4, 6, 12$, we take $b = 1$ and then obtain the following four sequences:

1010011110010, 1010111000101, 1001011110100, 1010001011101.

Our experimental result shows that all these sequences have linear complexity 13, which matches the statement of Theorem 5 (i).

(ii) For $n = 2$ and $f = 2, 4, 6, 12$, we randomly take $b = 7$ and then obtain the following four sequences:

1000110111000001000101001111010001110010111101001010001101010001010010
1110010111111100111111101001110100101000101011000101001011110100111000
10111100101000100000111011000,
1000100110000110100101011000100010110111111000101100010011010101100111
1110101101101110001001001010000001100101010011011100101110000001001011
10111001010110100111100110111,
1000110010000001110100011100010111110011010001101011000101010010110111
1011011111001000010011111011011110110100101010001101011000101100111110
10001110001011100000010011000,
1000110110110111100111111000111011000011101011101000100011111101111101
0110001000100110011011101110010100000100000011101110100010100011110010
00111000000110000100100100111.

Our experimental result shows that all these sequences have linear complexity 169, which matches the statement of Theorem 5 (i).

(iii) For $3 \leq n \leq 6$ and $f = 2, 4, 6, 12$, we also compute the linear complexities of the sequences s^{∞} with a Magma program. Our experimental results are all consistent with the statement of Theorem 5 (i).

Example 2 Choose an odd prime $p = 31$. We have $\text{ord}_p(2) = 5$ and a primitive root $g = 3$. For all possible even integers f that divide $p - 1$, the relation between $v = \left(\frac{p-1}{\text{ord}_p(2)}, f\right)$ and f is given as follows.

f	2	6	10	30
v	2	6	2	6
relation	$v = f$	$v = f$	$v = 2$	–

Here the dash indicates that the relation is not included in Theorem 5 (ii).

(i) For $n = 1$ and $f = 2, 6, 10, 30$, we take $b = 3$ and then obtain the following four sequences s_1, s_2, s_3, s_4, respectively.

s_1 : 100100100000111010100011110110111 s_2 : 100000010001011100010111011111111
s_3 : 101000100011000001111001110111101 s_4 : 100000001010010011011010111111111

Our experimental result shows that the linear complexities of s_1, s_2, s_3, s_4 are 15, 15, 30, 25, respectively. The linear complexities of s_1, s_2, s_3 match the statement of Theorem 5 (ii), and the linear complexity of s_4 matches the general statement of Theorem 5.

(ii) For $n = 2$ and $f = 2, 6, 10, 30$, we take $b = 0$ and obtain four sequences s_1, s_2, s_3, s_4, respectively. Our experimental result shows that the linear complexities of s_1, s_2, s_3, s_4 are 946, 946, 961, 956, respectively. These results are consistent with the statement of Theorem 5.

(iii) For $n = 3, 4$ and $f = 2, 6, 10, 30$, we also compute the linear complexity of the sequences s^∞ with a magma program. Our experimental results show that the linear complexities of s^∞ corresponding to $f = 2, 6, 10$ match the statement of Theorem 5 (ii), and the linear complexities of s^∞ corresponding to $f = 30$ match the the general statement of Theorem 5.

Remark 5 Low autocorrelation is one of the desirable properties of pseudo-random sequences in cryptography and digital communication. Unfortunately some cyclotomic binary sequences with high linear complexity do not have satisfactory autocorrelation properties [13,14,17]. For the sequences s^∞ studied in this paper, because the generalized cyclotomic classes in (2) have varying orders for $1 \le j \le n$, it is challenging to obtain theoretical result on the autocorrelation values of s^∞. We checked all the sequences in Examples 1 and 2 by a computer program. Unfortunately, these sequences s^∞ have many autocorrelation values with a large maximum out-of-phase autocorrelation. This makes a theoretical study of autocorrelation properties of this family of sequences intractable and less interesting.

Very recently Wu et al. [21] studied the error linear complexity of the cyclotomic binary sequences of period p^2 in [22] for the case $f = 2$, and showed that the sequences are stable in terms of kth error linear complexity. The error linear complexity of the cyclotomic sequences of period p^n is beyond the focus of this paper and interested readers are invited to work on this topic.

4 Conclusion

This paper re-examined the linear complexity of a family of generalized cyclotomic binary sequences of period p^n. The major contribution of this paper is that it proved the conjecture by Xiao et al. about the linear complexity of this family of sequences with a new technique, and it applied the new technique to extend the conjectured result to more general cases.

Acknowledgements The authors are very grateful to the anonymous reviewers and the Editor for their comments that improved the presentation of this paper. V. Edemskiy was supported by the Russian Ministry of Education, project No. 8.7367.2017/8.9. C. Li and T. Helleseth were supported by the Research Council of Norway under Grant 247742/O70. C. Li was also partly supported by the research project (No. 720025) from UH-nett Vest in Norway. X. Zeng was supported by National Natural Science Foundation of China under Grant 61472120 and National Natural Science Foundation of Hubei Province of China under Grant 2017CFB143.

References

1. Çeşmelioğlu A., Meidl W.: A general approach to construction and determination of the linear complexity of sequences based on cosets. In: Carlet C., Pott A. (eds.) Sequences and Their Applications—SETA 2010, pp. 125–138. Springer, Berlin (2010).
2. Cusick T., Ding C., Renvall A.: Stream Ciphers and Number Theory. North-Holland Mathematical Library. Elsevier, North-Holland (2004).
3. Ding C.: Cyclotomic constructions of cyclic codes with length being the product of two primes. IEEE Trans. Inf. Theory **58**(4), 2231–2236 (2012).
4. Ding C., Helleseth T.: New generalized cyclotomy and its applications. Finite Fields Appl. **4**(2), 140–166 (1998).
5. Ding C., Helleseth T.: Generalized cyclotomic codes of length $p_1^{e_1} \ldots p_t^{e_t}$. IEEE Trans. Inf. Theory **45**(2), 467–474 (1999).
6. Dorais F.G., Klyve D.: A Wieferich prime search up to 6.7×10^{15}. J. Integer Seq. **14**(11.9.2), 1–14 (2011).
7. Du X., Chen Z.: A generalization of the Hall's sextic residue sequences. Inf. Sci. **222**, 784–794 (2013).

8. Edemskiy V.: About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1}. Des. Codes Cryptogr. **61**(3), 251–260 (2011).
9. Edemskiy V.: The linear complexity of new binary cyclotomic sequences of period p^n. CoRR (2017). arXiv:1712.03947
10. Fan C., Ge G.: A unified approach to Whiteman's and Ding-Helleseth's generalized cyclotomy over residue class rings. IEEE Trans. Inf. Theory **60**(2), 1326–1336 (2014).
11. Golomb S.W.: Shift Register Sequences. Holden-Day, San Francisco (1967).
12. Ireland K., Rosen M.: A Classical Introduction to Modern Number Theory. Graduate Texts in Mathematics. Springer, New York (1990).
13. Jin S.Y., Kim Y.J., Song H.Y.: Autocorrelation of new generalized cyclotomic sequences of period p^n. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **93**(11), 2345–2348 (2010).
14. Ke P., Zhang J., Zhang S.: On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^m$. Des. Codes Cryptogr. **67**(3), 325–339 (2013).
15. Kewat P.K., Kumari P.: Cyclic codes from the second class two-prime Whiteman's generalized cyclotomic sequence with order 6. Cryptogr. Commun. **9**(4), 475–499 (2017).
16. Kim Y.J., Song H.Y.: Linear complexity of prime n-square sequences. In: 2008 IEEE International Symposium on Information Theory, pp. 2405–2408 (2008).
17. Li S., Chen Z., Fu X., Xiao G.: Autocorrelation values of new generalized cyclotomic sequences of order two and length pq. J. Comput. Sci. Technol. **22**(6), 830–834 (2007).
18. Lidl R., Niederreiter H.: Finite Fields. Encyclopedia of Mathematics and Its Applications, vol. 20. Addison-Wesley, Reading (1983).
19. Whiteman A.L.: A family of difference sets. Illinois J. Math. **6**(1), 107–121 (1962).
20. Wu C., Chen Z., Du X.: The linear complexity of q-ary generalized cyclotomic sequences of period p^m. J. Wuhan Univ. **59**(2), 129–136 (2013).
21. Wu C., Xu C., Chen Z., Ke P.: On error linear complexity of new generalized cyclotomic binary sequences of period p^2. CoRR (2017). arXiv:1711.06063
22. Xiao Z., Zeng X., Li C., Helleseth T.: New generalized cyclotomic binary sequences of period p^2. Des. Codes Cryptogr. (2017). https://doi.org/10.1007/s10623-017-0408-7.
23. Yan T., Li S., Xiao G.: On the linear complexity of generalized cyclotomic sequences with the period p^m. Appl. Math. Lett. **21**(2), 187–193 (2008).
24. Ye Z., Ke P., Wu C.: A note on a conjecture of new binary cyclotomic sequences of length p^n. CoRR (2017). arXiv:1712.08886
25. Zeng X., Cai H., Tang X., Yang Y.: Optimal frequency hopping sequences of odd length. IEEE Trans. Inf. Theory **59**(5), 3237–3248 (2013).