Note about the linear complexity of new generalized cyclotomic binary sequences of period $2p^n$

Vladimir Edemskiy

March 12, 2019

Abstract

This paper examines the linear complexity of new generalized cyclotomic binary sequences of period $2p^n$ recently proposed by Yi Ouang et al. (arXiv:1808.08019v1 [cs.IT] 24 Aug 2018). We generalize results obtained by them and discuss author’s conjecture of this paper.

Keywords: binary sequences, linear complexity, cyclotomy

Mathematics Subject Classification (2010): 94A55, 94A60, 11B50.

1 Introduction

The cyclotomic classes and the generalized cyclotomic classes are often used for design sequences with high linear complexity, which is an important characteristic of sequence for the cryptography applications [2]. Recently, new generalized cyclotomic classes were presented in [8]. The linear complexity of new generalized cyclotomic binary sequences with period $p^n$ was studied in [9, 4, 7]. A new family of binary sequences with period $2p^n$ based on the generalized cyclotomic classes from [8] was presented in [6]. Yi Ouang et al. examined the linear complexity of these sequences for $f = 2^r$, where $p = 1 + ef$ and $r$ is a positive integer. They offered new studying method of the linear complexity of these sequences. Their method based on ideas from [4].

In this paper we show that for study of the linear complexity of new sequence family from [6] we can use only old the method from [4]. Furthermore, it will be enough for obtaining more generalized results than in [6] and for the proof and
the correction of the conjecture of the authors of this paper. Here we keep the notation and the structure of [4], i.e., in Sect. 2 we introduce some basics and recall the definition of a generalized cyclotomic sequence and the conjecture from [6]. 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 \( \mathbb{Z}_N \).

First of all we will recall some basics of the linear complexity of a periodic sequence and introduce the generalized cyclotomic sequences proposed in [6].

2.1 Linear Complexity

Let \( s^\infty = (s_0,s_1,s_2,\ldots) \) be a binary sequence of period \( N \) and \( S(x) = s_0 + s_1x + \cdots + s_{N-1}x^{N-1} \). It is well known (see, for instance, [2] Page 171) that the linear complexity of \( s^\infty \) is given by

\[
L(s^\infty) = N - \deg \left( \gcd \left( x^N - 1, S(x) \right) \right).
\]

So, if \( N = 2p^n \) then we see that

\[
L(s^\infty) = 2p^n - \deg \left( \gcd \left( (x^{2^p}) - 1, S(x) \right) \right).
\]

Thus, if \( \alpha_n \) is a primitive root of order \( p^n \) of unity in the extension of the field \( \mathbb{F}_2 \) (the finite field of two elements) then in order to find the linear complexity of a sequence it is sufficient to find the zeros of \( S(x) \) in the set \( \{ \alpha_n^i, i = 0, 1, \ldots, p^n - 1 \} \) and determine their multiplicity.

2.2 New Generalized Cyclotomic Sequences Length \( 2p^n \)

Let \( p \) be an odd prime and \( p = ef + 1 \), where \( e, f \) are positive integers. Let \( g \) be a primitive root modulo \( p^n \). It is well known [5] that an odd number from \( g \) or \( g + p^n \) is also a primitive root modulo \( 2p^j \) for each integer \( j \geq 1 \). Hence, we can assume that \( g \) is an odd number. Further, the order of \( g \) modulo \( 2p^j \) is equal to
\( \phi(2p^j) = p^{j-1}(p - 1) \), where \( \phi(\cdot) \) is the Euler’s totient function. Below we recall the definitions of generalized cyclotomic classes introduced in [8] and [6].

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

\[
D_{0}^{(p^j)} = \left\{ g^i \cdot d_j \pmod{p^j} \mid 0 \leq t < e \right\}, \quad \text{and} \\
D_{i}^{(p^j)} = g^i \cdot D_{0}^{(p^j)} = \left\{ g^i x \pmod{p^j} : x \in D_{0}^{(p^j)} \right\}, \quad 1 \leq i < d_j,
\]

(1)

The cosets \( D_j^{(p^j)}, i = 0, 1, \cdots, d_j - 1 \), are called \textit{generalized cyclotomic classes} of order \( d_j \) with respect to \( p^j \). It was shown in [8] that \( \left\{ D_0^{(p^j)}, D_1^{(p^j)}, \cdots, D_{d_j-1}^{(p^j)} \right\} \) forms a partition of \( \mathbb{Z}^*_{p^j} \) for each integer \( j \geq 1 \) and for an integer \( m \geq 1 \),

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

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

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

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

\[
\mathcal{C}_0^{(2p^j)} = \bigcup_{j=1}^{n} \bigcup_{i=d_j/2}^{d_j-1} p^{n-j} \left( D_{(i+b)}^{(2p^j)} \pmod{d_j} \cup 2D_{(i+b)}^{(2p^j)} \pmod{d_j} \right) \cup \{p^n\}, \quad \text{and}
\]

\[
\mathcal{C}_1^{(2p^j)} = \bigcup_{j=1}^{n} \bigcup_{i=0}^{d_j/2-1} p^{n-j} \left( D_{(i+b)}^{(2p^j)} \pmod{d_j} \cup 2D_{(i+b)}^{(2p^j)} \pmod{d_j} \right) \cup \{0\},
\]

\[
\mathcal{C}_0^{(2p^j)} = \bigcup_{j=1}^{n} p^{n-j} \left( \bigcup_{i=0}^{d_j/2-1} 2D_{(i+b)}^{(2p^j)} \pmod{d_j} \cup \bigcup_{i=d_j/2}^{d_j-1} D_{(i+b)}^{(2p^j)} \pmod{d_j} \right) \cup \{p^n\}, \quad \text{and}
\]

\[
\mathcal{C}_1^{(2p^j)} = \bigcup_{j=1}^{n} p^{n-j} \left( \bigcup_{i=0}^{d_j/2-1} D_{(i+b)}^{(2p^j)} \pmod{d_j} \cup \bigcup_{i=d_j/2}^{d_j-1} 2D_{(i+b)}^{(2p^j)} \pmod{d_j} \right) \cup \{0\}.
\]
Theorem 1. The main result in this paper is given as follows.

It is obvious that \( \mathbb{Z}_{2p^n} = \mathcal{G}_0(2p^n) \cup \mathcal{G}_1(2p^n) = \mathcal{G}_0(2p^n) \cup \mathcal{G}_1(2p^n) \) and \( |\mathcal{G}_0(2p^n)| = |\mathcal{G}_1(2p^n)| = p^n, \ i = 0, 1 \). Families of balanced binary sequences \( s^\infty = (s_0, s_1, s_2, \ldots) \) and \( \tilde{s}^\infty = (\tilde{s}_0, \tilde{s}_1, \tilde{s}_2, \ldots) \) of period \( p^n \) can thus be defined as in [6], i.e.,

\[
\tilde{s}_i = \begin{cases} 
0, & \text{if } i \pmod{p^n} \in \mathcal{G}_0(2p^n), \\
1, & \text{if } i \pmod{p^n} \in \mathcal{G}_1(2p^n).
\end{cases}
\]

and

\[
\tilde{s}_i = \begin{cases} 
0, & \text{if } i \pmod{p^n} \in \mathcal{G}_0(2p^n), \\
1, & \text{if } i \pmod{p^n} \in \mathcal{G}_1(2p^n).
\end{cases}
\]

In the case of \( f = 2^r \), the linear complexity of \( s^\infty \), \( \tilde{s}^\infty \) was estimated in [6], where a conjecture about the linear complexity of these sequences was also made as follows.

**Conjecture.** (1) If \( 2^r \equiv -1 \pmod{p} \) but \( 2^r \not\equiv -1 \pmod{p^2} \), then the linear complexity \( L(s^\infty) = 2p^n - (p - 1) \).

(2) If \( 2^r \equiv 1 \pmod{p} \) but \( 2^r \not\equiv 1 \pmod{p^2} \), then the linear complexity \( L(s^\infty) = 2p^n - (p - 1) - e \).

### 2.3 Main Result

This subsection will study the linear complexity of \( s^\infty \), \( \tilde{s}^\infty \) in (3) and (4) for some even integers \( f \) and when \( p \) is not a Wieferich prime, i.e. \( 2^{p-1} \not\equiv 1 \pmod{p^2} \). It was shown that there are only two such primes, 1093 and 3511, up to \( 6 \times 10^{17} \) [1][3]. The main result in this paper is given as follows.

**Theorem 1.** Let \( p = ef + 1 \) be an odd prime with \( 2^{p-1} \not\equiv 1 \pmod{p^2} \) and \( f \) is an even positive integer. Let \( \text{ord}_p(2) \) denote the order of 2 modulo \( p \) and \( v = \gcd\left(p-1, \frac{p}{\text{ord}_p(2)}, f\right) \).

(i) Let \( s^\infty \) be a generalized cyclotomic binary sequence of period \( p^n \) defined in (3). Then the linear complexity of \( s^\infty \) is given by

\[
L(s^\infty) = 2p^n - r \cdot \text{ord}_p(2), \quad 0 \leq r \leq \frac{p-1}{\text{ord}_p(2)}.
\]
Furthermore, the linear complexity

$$L(s^\infty) = \begin{cases} 2p^n - p + 1, & \text{if } v = f/2; \\ 2p^n, & \text{if } v = 1 \text{ or } 2v|f, \text{ or } f = v. \end{cases}$$

(ii) Let $\tilde{s}^\infty$ be a generalized cyclotomic binary sequence of period $p^n$ defined in (4). Then for the linear complexity of $\tilde{s}^\infty$ we have

$$2p^n - 2r \cdot \text{ord}_p(2) \leq L(\tilde{s}^\infty) \leq 2p^n - r \cdot \text{ord}_p(2), \quad 0 \leq r \leq \frac{p-1}{\text{ord}_p(2)}.$$}

Furthermore, the linear complexity

$$L(\tilde{s}^\infty) = \begin{cases} 2p^n - 3(p - 1)/2, & \text{if } v = f; \\ 2p^n, & \text{if } v|f, \text{ or } v = 2, v \neq f. \end{cases}$$

**Corollary 2.** Let $f = 2^r$. Then:

(i) The linear complexity of $s^\infty$ is given by

$$L(s^\infty) = \begin{cases} 2p^n - p + 1, & \text{if } v = f/2; \\ 2p^n, & \text{otherwise}. \end{cases}$$

(ii) The linear complexity of $\tilde{s}^\infty$ is given by

$$L(\tilde{s}^\infty) = \begin{cases} 2p^n - 3(p - 1)/2, & \text{if } v = f; \\ 2p^n, & \text{otherwise}. \end{cases}$$

**Remark 1.** Suppose $2 \equiv g^u \pmod{p}$ for some integer $u$. It is easily seen that $\gcd\left(\frac{p-1}{\text{ord}_p(2)}, f\right) = \gcd(u, f)$. Thus the condition $2^e \equiv 1 \pmod{p}$ in Conjecture from [6] is equivalent to $v = \gcd\left(\frac{p-1}{\text{ord}_p(2)}, f\right) = f$ and the condition $2^e \equiv -1 \pmod{p}$ is equivalent to $v = f/2$. 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 $f/2$ or divides $f/4$. Hence Conjecture from [6] is included in Theorem 1 as a special case. Here we make the correction of Conjecture (ii).

If 2 is a primitive roots modulo $p$ then $v = 1$.

For the proof of Theorem 1 we will use the same definitions and same method that as [4].
Let $S(x) = s_0 + s_1 x + \cdots + s_{2^p - 1} x^{2^p - 1}$ and $\tilde{S}(x) = \tilde{s}_0 + \tilde{s}_1 x + \cdots + \tilde{s}_{2^p - 1} x^{2^p - 1}$ for the generalized cyclotomic sequences $s^\infty$, $\tilde{s}^\infty$ defined in (3) and (4), respectively. Then,

$$\begin{align*}
S(x) &= \sum_{t \in \mathcal{D}_1^{(p^d)}} x^t = 1 + \sum_{j=1}^n \sum_{i=0}^{d_j/2-1} \left( \sum_{t \in \mathcal{D}_{i+b}^{(2p^j)}} x^{p^n t} + \sum_{t \in 2\mathcal{D}_{i+b}^{(2p^j)} \mod d_j} x^{p^{n-1} t} \right), \\
\tilde{S}(x) &= \sum_{t \in \mathcal{D}_1^{(p^d)}} x^t = 1 + \sum_{j=1}^n \sum_{i=0}^{d_j/2-1} \sum_{t \in \mathcal{D}_{i+b}^{(2p^j)} \mod d_j} x^{p^n t} + \sum_{j=1}^n \sum_{i=d_j/2}^{d_j} \sum_{t \in 2\mathcal{D}_{i+b}^{(2p^j)} \mod d_j} x^{p^{n-1} t}.
\end{align*}$$

For simplicity of presentation, we define polynomials as in [4]

$$E_i^{(p^j)}(x) = \sum_{t \in \mathcal{D}_i^{(p^j)}} x^t, \quad 1 \leq j \leq n, \ 0 \leq i < d_j, \quad (6)$$

and

$$H_k^{(p^j)}(x) = \sum_{i=0}^{d_j/2-1} E_{i+k}^{(p^j)}(x) \pmod{d_j}, \quad 0 < k < d_j, \quad T_k^{(p^m)}(x) = \sum_{j=1}^m H_k^{(p^j)}(x^{p^{m-j}}), \quad m = 1, 2, \cdots, n. \quad (7)$$

Notice that the subscripts $i$ in $\mathcal{D}_i^{(p^j)}$, $H_i^{(p^j)}(x)$ 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.

Let $\overline{\mathbb{F}}_2$ be an algebraic closure of $\mathbb{F}_2$ and $\alpha_n \in \overline{\mathbb{F}}_2$ be a primitive $p^n$-th root of unity. Denote $\alpha_j = \alpha_n^{p^{m-j}}$, $j = 1, 2, \ldots, n-1$.

The properties of considered polynomials were studied in [4]. We have here the following statement.

**Lemma 3.** [4] For any $a \in \mathcal{D}_k^{(p^j)}$, we have

(i) $T_i^{(p^m)}(\alpha_m^{p^j}) = T_{i+k}^{(p^m)}(\alpha_{m-1}) + (p^l - 1)/2 \pmod{2}$ for $0 \leq l < m$; and

(ii) $T_i^{(p^m)}(\alpha_m) + T_{i+d_m/2}^{(p^m)}(\alpha_m^a) = 1$.

(iii) Let $p$ be a non-Wieferich prime. Then $T_i^{(p^m)}(\alpha_m) \notin \{0, 1\}$ for $m > 1$.

(iv) Let $p$ be a non-Wieferich prime. Then $T_i^{(p^m)}(\alpha_m) + T_{i+f/2}^{(p^m)}(\alpha_m) \neq 1$ for $m > 1$. 

6
Proposition 2. Let \( p \) be a non-Wieferich prime. Then \( S \in \mathcal{T}_p \) see that in this case it is enough proof, 

\[
\text{Proof. This is sufficient to prove that } T_b^{(p^m)}(\alpha_m) + T_{b+u}^{(p^m)}(\alpha_m) = \text{(i) Since definitions and Lemma 3 that}
\]

\[
\sum_{t \in \mathbb{Z}/p^n} \alpha^a = \sum_{j=1}^{n} \sum_{i=0}^{d_i/2-1} \sum_{t \in \mathbb{Z}/p^n} \alpha^a + \sum_{t \in \mathbb{Z}/p^n} \alpha^a + 1 = 1 + T_b^{(p^m)}(\alpha_m^a) + T_{b+u}^{(p^m)}(\alpha_m^a).
\]

(ii) Similarly we have

\[
\tilde{S}(\alpha_m^a) = 1 + T_b^{(p^m)}(\alpha_m^a) + T_{b+u}^{(p^m)}(\alpha_m^a) = T_b^{(p^m)}(\alpha_m^a) + T_{b+u}^{(p^m)}(\alpha_m^a).
\]

We now examine the value of \( T_b^{(p^m)}(\alpha_m^i) + T_{b+u}^{(p^m)}(\alpha_m^i) \) for some integers \( i \in \mathbb{Z}/p^n \).

Proposition 2. Let \( p \) be a non-Wieferich prime. Then \( S(\alpha_m^i) \neq 0 \) and \( \tilde{S}(\alpha_m^i) \neq 0 \) for \( i \in \mathbb{Z}/p^n \setminus p^{n-1}\mathbb{Z}/p \).

\text{Proof. This is sufficient to prove that } T_b^{(p^m)}(\alpha_m^i) + T_{b+u}^{(p^m)}(\alpha_m^i) \neq \{0, 1\} \text{ for } i \in \mathbb{Z}/p^n \setminus p^{n-1}\mathbb{Z}/p \text{ and } b = 0, 1, \cdots, d_n - 1. \] As it was shown in [4] that without loss of generality it is enough proof, \( T_0^{(p^m)}(\alpha_m) + T_u^{(p^m)}(\alpha_m) \neq \{0, 1\} \text{ for } m > 1. \)

We consider two cases.

1. Let \( T_0^{(p^m)}(\alpha_m) + T_u^{(p^m)}(\alpha_m) = 0. \) Since \( (T_0^{(p^m)}(\alpha_m))^2 = T_u^{(p^m)}(\alpha_m) = 0, \) we see that in this case \( T_0^{(p^m)}(\alpha_m) \in \{0, 1\}. \) We obtain a contradiction with Lemma [3] (iii).

2. Let \( T_0^{(p^m)}(\alpha_m) + T_u^{(p^m)}(\alpha_m) = 1. \)
It then follows from Lemma 3(i) that
\[ 1 = \left( T_0^{(p^m)}(\alpha_m) + T_u^{(p^m)}(\alpha_m) \right)^2 = T_0^{(p^m)}(\alpha_m^2) + T_u^{(p^m)}(\alpha_m^2) = T_u^{(p^m)}(\alpha_m) + T_{2u}^{(p^m)}(\alpha_m), \]
which implies \( T_{iiu}^{(p^m)}(\alpha_m) + T_{(i+1)u}^{(p^m)}(\alpha_m) = 1 \) for any integer \( i \geq 1 \). Hence \( T_0^{(p^m)}(\alpha_m) = T_{2iu}^{(p^m)}(\alpha_m) \).

Denote \( w = \gcd(2u, d_m) \). Since \( p \) is a non-Wieferich prime, it follows by [4] that \( w \) divides \( f \). Since the subscript of \( T_j^{(p^m)}(x) \) is taken modulo \( d_m \), it is easily seen that
\[ T_0^{(p^m)}(\alpha_m) = T_{iv}^{(p^m)}(\alpha_m), \text{ for any integer } i \geq 1. \] (8)

By Lemma 3(ii) from the last formula we have \( T_{dm/2}^{(p^m)}(\alpha_m) = T_{dm/2+iv}^{(p^m)}(\alpha_m) \) or \( T_{dm}^{(p^m)}(\alpha_m) = T_{dm/2+ff}^{(p^m)}(\alpha_m) \). Then we get that
\[ T_{dm/2+(p^m-1)/2}^{(p^m)}(\alpha_m) = T_{dm/2+(p^m-1)/2}^{(p^m)}(\alpha_m) = T_{f/2}^{(p^m)}(\alpha_m) = T_{f+2}^{(p^m)}(\alpha_m). \]

Hence, \( T_{dm/2}^{(p^m)}(\alpha_m) = T_{f/2}^{(p^m)}(\alpha_m) \). Thus, by Lemma 3(ii) we obtain that \( T_0^{(p^m)}(\alpha_m) + 1 = T_{f/2}^{(p^m)}(\alpha_m) \). But the latest equality is not possible for \( m > 1 \) by Lemma 3(iv).

By Proposition 2, we only need to study the value of \( T_b^{(p^m)}(\alpha_n^i) + T_{b+u}^{(p^m)}(\alpha_n^i) \) for integers \( i \) in the set \( p^n-1 \mathbb{Z}_p \). Suppose \( i = p^{n-1}a, \ a \in D_i^{(p)} \). Then, it follows from Proposition 1 and Lemma 3 that
\[ S(\alpha_n^i) = 1 + T_b^{(p^m)}(\alpha_n^i) + T_{b+u}^{(p^m)}(\alpha_n^i) = 1 + T_b^{(p)}(\alpha_n^i) + T_{b+u}^{(p)}(\alpha_n^i) = 1 + H_k^{(p)}(\alpha_1) + H_{k+u}^{(p)}(\alpha_1), \]
where \( k \equiv b+i \pmod{f} \). The following proposition examines the value of \( H_k^{(p)}(\alpha_1) + H_{k+u}^{(p)}(\alpha_1) \) according to the relation between \( f \) and \( \text{ord}_p(2) \).

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

(i) \[ \left\{ k \in \mathbb{Z}_f \mid H_k^{(p)}(\alpha_1) + H_{k+u}^{(p)}(\alpha_1) = 0 \right\} = \begin{cases} f, & \text{if } v = f, \\ 0, & \text{if } v \mid f/2 \text{ or } v = 2, v \neq f. \end{cases} \]

(ii) \[ \left\{ k \in \mathbb{Z}_f \mid H_k^{(p)}(\alpha_1) + H_{k+u}^{(p)}(\alpha_1) = 1 \right\} = \begin{cases} f, & \text{if } v = f/2, \\ 0, & \text{if } v = 1, \text{ or } v = f \text{ or } 2v \mid f/2. \end{cases} \]
Proof. Since ord\(p(2) = \frac{p-1}{\gcd(p-1, a)}\), it follows that gcd\((u, f) = \gcd(\frac{p-1}{\text{ord}_p(2)}, f) = v\) [4].

(i) For \(v = f\) this statement is clear.

Let \(v|f/2\) or \(v = 2, v \neq f\). We shall prove this case by contradiction. Suppose \(H_k(p)(\alpha_1) + H_{k+u}(p)(\alpha_1) = 0\) for some integer \(k\). Since \((H_k(p)(\alpha_1))^2 = H_{k+u}(p)(\alpha_1)\), it follows that \(H_k(p)(\alpha_1)\) is in \(\{0, 1\}\). By [4] this is not possible for \(v|f/2\) or \(v = 2, v \neq f\).

(ii) For \(v = f/2\) this statement is clear. If \(v = f\) then \(2 \in D_0^{(p)}\) and we have \(H_k(p)(\alpha_1) + H_{k}(p)(\alpha_1) = 1\). This is impossible.

Suppose \(H_k(p)(\alpha_1) + H_{k+u}(p)(\alpha_1) = 0\) for some integer \(k\). Without loss of generality, we assume \(k = 0\) and \(H_0(p)(\alpha_1) = H_u(p)(\alpha_1) + 1\).

In the case when \(v \neq f\). Since gcd\((u, f) = \gcd(\frac{p-1}{\text{ord}_p(2)}, f) = v\), by a similar argument as in the proof of Proposition[2] we get

\[
H_0(p)(\alpha_1) = H_{2v}(p)(\alpha_1) = \cdots = H_{2vf}(p)(\alpha_1).
\]

So, if \(2v\) divides \(f/2\), then \(H_{f/2}(p)(\alpha_1) = H_{2v+f/4v}(p)(\alpha_1) = H_0(p)(\alpha_1)\), which is a contradiction.

Let \(v = 1\). Then we get \(H_i(p)(\alpha_1) + H_{i+1}(p)(\alpha_1) + 1 = 0, i = 0, 1, \ldots, f - 1\) and then \(E_i(p)(\alpha_1) + E_{i+f/2}(p)(\alpha_1) + 1 = 0, i = 0, 1, \ldots, f - 1\). In [4] it was shown that this is impossible.

\[\square\]

**Proof of Theorem**[1] Recall that the linear complexity of \(s^\infty\) is given by

\[
L(s^\infty) = N - \deg\left(\gcd\left((x^n - 1)^2, S(x)\right)\right).
\]

(i) From Proposition[2] we know \(S(\alpha^i_j) \neq 0\) for \(i \in \mathbb{Z}_{p^n} \setminus p^{n-1}\mathbb{Z}_p\). For the remaining set \(p^{n-1}\mathbb{Z}_p\), if \(i = 0\), then \(S(1) = 1\); if \(i \in p^{n-1}\mathbb{Z}_p^*\), we have

\[
S(\alpha^i_n) = 1 + T_b(p)(\alpha^i_n) + T_{b+u}(p)(\alpha^i_n) = 1 + T_b(p)(\alpha^1_n) + T_{b+u}(p)(\alpha^1_n) = 1 + H_b(p)(\alpha^1_n) + H_{b+u}(p)(\alpha^1_n)
\]

for some integer \(a \in \mathbb{Z}_p^*\).

Suppose \(H_k(p)(\alpha^a_1) + H_{k+u}(p)(\alpha^a_1) = 1\) for some integer \(k\). Then

\[
1 = (H_k(p)(\alpha_1))^2 + H_{k+u}(p)(\alpha^2_1) = H_{k+u}(\alpha_1) + H_{k+2u}(\alpha_1),
\]

9
and so on (here \( u \not\equiv 0 \pmod{f} \)). So, we have

\[
| \{ i : \ S(\alpha_i^j) = 0, i = 1, 2, \ldots, p^n - 1 \} | = r \text{ord}_p(2).
\]

where \( r \) is an integer with \( 0 \leq r \leq \frac{p-1}{\text{ord}_p(2)} \).

Further, by (5) we see that

\[
xS'(x) = \sum_{j=1}^{n} \sum_{i=0}^{d_j/2-1} \sum_{t \in D_i+b \pmod{d_j}} x^{p^{n-1}t}.
\]

Hence, \( \alpha_n^i S(\alpha_n^i) = T_{b_{i+1}}^{(p^n)}(\alpha_n^i) \). So, if \( \alpha_n^i \) is a root of \( S(x) \) and \( S'(x) \) then \( 1 + T_{b_{i+1}}^{(p^n)}(\alpha_n^i) + (T_{b_{i+1}}^{(p^n)}(\alpha_n^i))^2 = 0 \) and \( T_{b_{i+1}}^{(p^n)}(\alpha_n^i) = 0 \). It is not possible and any root of \( S(x) \) is simple.

Then the statement of this theorem follows from Proposition 2.

(ii) In this case

\[
S(\alpha_n^i) = H_b^{(p)}(\alpha_1^a) + H_{b^u}(\alpha_1^a)
\]

for some integer \( a \in \mathbb{Z}_p^* \).

Then as earlier we again get

\[
| \{ i : \ S(\alpha_n^i) = 0, i = 1, 2, \ldots, p^n - 1 \} | = r \text{ord}_p(2).
\]

where \( r \) is an integer such that \( 0 \leq r \leq \frac{p-1}{\text{ord}_p(2)} \).

Here, by (5) we see that

\[
x\tilde{S}'(x) = \sum_{j=1}^{n} \sum_{i=0}^{d_j/2-1} \sum_{t \in D_i+b \pmod{d_j}} x^{p^{n-1}t}.
\]

and also \( \alpha_n^i \tilde{S}(\alpha_n^i) = T_{b_{i+1}}^{(p^n)}(\alpha_n^i) \). If \( v = f \) then it follows from [4] that

\[
| \{ i : \ T_{b_{i+1}}^{(p^n)}(\alpha_n^i) = 0, i = 1, 2, \ldots, p^n - 1 \} | = (p-1)/2.
\]

Then the statement of this theorem follows from Proposition 2.

\( \square \)
2.4 Additional remark

Let $p$ be a Wieferich prime. Wieferich primes are very rare \[3], hence we could ignore these numbers but nonetheless we show that the old method also works in this case. In this subsection we consider only the case when $f = 2^r$, where $r$ is a positive integer. Denote $D = \{k : \ 2^{p-1} \equiv 1 \ (\text{mod} \ p^k)\}$ and $wn = \max k$.

Suppose $2 \equiv \ g^u \ (\text{mod} \ p^{nw})$. Then $u \equiv 0 \ (\text{mod} \ p^{nw-1})$. Thus, $u = p^{nw-1}z$ where $\gcd(z, p) = 1$. It is easy to check that $2 \equiv g^{p^{j-1}z} \ (\text{mod} \ p^j)$ for $j \leq nw$.

Let $v = \gcd(z, f)$. First, we study the value of $T_k^{(p^j)}(\alpha_j^i)$ for integers $i$ in the set $\mathbb{Z}_{p^j}$. Let $T_k^{(p^j)}(\alpha_j^i) \in \{0, 1\}$ and $v \neq f$. Without loss of generality, we assume $T_k^{(p^j)}(\alpha_j^i) = 0$. As earlier we obtain that

$$0 = T_k^{(p^j)}(\alpha_j^i) = T_{k+lv p^{j-1}}^{(p^j)}(\alpha_j^i) \text{ for } l = 0, 1, 2, \ldots.$$ 

Since $vp^{j-1}$ divides $d/2 = p^{j-1}f/2$ for $f = 2^r$, we have a contradiction. So, $T_k^{(p^j)}(\alpha_j^i) \in \{0, 1\}$ for $i \in \mathbb{Z}_{p^j}$ only when $v = f$.

We consider a few cases.

(i) Suppose $v = f$. Then $2 \in D_0^{(p^j)}$ for $j \leq nw$. In this case $T_k^{(p^j)}(\alpha_j^i) = (T_k^{(p^j)}(\alpha_j^i))^2$ and $T_k^{(p^j)}(\alpha_j^i) \in \{0, 1\}$ for any $k$ and $i \in \mathbb{Z}_{p^j}$. Thus, $S(\alpha_j^i) = 1$ for $i \in \mathbb{Z}_{p^j}$. Further, $S(\alpha_j^i) = 0$ for $i \in \mathbb{Z}_{p^j}$, $i \neq 0$ and $|\{i : S(\alpha_j^i) = 0, i = 1, \ldots, p^j-1\}| = (p^j-1)/2$.

(ii) Suppose $v = f/2$. In this case $(T_k^{(p^j)}(\alpha_j^i))^2 = T_{k+d_j/2}^{(p^j)}(\alpha_j^i)$. Thus, by Lemma\[3] $S(\alpha_j^i) = 1$ for $i \in \mathbb{Z}_{p^j}$. Further, $S(\alpha_j^i) = 0$ and $S'(\alpha_j^i) \neq 0$ for $i \in \mathbb{Z}_{p^j}$, $i \neq 0$.

(iii) $v \neq f/2, f$. Here $(T_k^{(p^j)}(\alpha_j^i))^2 = T_{k+lp p^{i-1}}^{(p^j)}(\alpha_j^i)$. So, if $T_k^{(p^j)}(\alpha_j^i) + T_{k+u}^{(p^j)}(\alpha_j^i) = 0$ then $T_k^{(p^j)}(\alpha_j^i) = T_{k+lp p^{i-1}}^{(p^j)}(\alpha_j^i)$ for $l \geq 0$. Also, if $T_k^{(p^j)}(\alpha_j^i) + T_{k+u}^{(p^j)}(\alpha_j^i) = 1$ then $T_k^{(p^j)}(\alpha_j^i) = T_{k+2lp p^{i-1}}^{(p^j)}(\alpha_j^i)$ for $l \geq 0$.

Since $f = 2^r$ and $v \neq f/2, f$, it follows that $2v p^{j-1}$ divides $p^{j-1}f/2$. We obtain a contradiction with Lemma\[3].

If $j \geq wn$ then $[\mathbb{F}_2(\alpha_{j+1}) : \mathbb{F}_2(\alpha_j)] = p$, where $\alpha_j = \alpha_n p^{r-j}$ and $\alpha_n$ is a primitive $p^r$-th root of unity. In this case we can use the method from \[4] as earlier.

Let $m = \min(n, wn)$. So, for $f = 2^r$ we can obtain that the linear complexity of $s^\infty$ is given by
\[
L(s^\infty) = \begin{cases} 
2p^n - (p^m - 1), & \text{if } v = f/2; \\
2p^n, & \text{otherwise},
\end{cases}
\]

and the linear complexity of \(\tilde{s}^\infty\) for \(n \geq wn\) is given by

\[
L(\tilde{s}^\infty) = \begin{cases} 
2p^n - 3(p^m - 1)/2, & \text{if } v = f; \\
2p^n, & \text{otherwise}.
\end{cases}
\]

References

[1] Akbary, A., Siavashi S.: The largest known Wieferich numbers, Integers **18-A3** 1-6 (2018).

[2] Cusick, T., Ding, C., Renvall, A.: Stream Ciphers and Number Theory. North-Holland mathematical library. Elsevier (2004).

[3] Dorais, F.G., Klyve, D.: A Wieferich prime search up to \(6.7 \times 10^{15}\). Journal of Integer Sequences **14**(11.9.2), 1–14 (2011).

[4] Edemskiy, V., Li, C., Zeng, X., Helleseth, T.: The linear complexity of generalized cyclotomic binary sequences of period \(p^n\). Designs, Codes and Cryptography. PP., 1-15. DOI: 10.1007/s10623-018-0513-2

[5] Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory. Graduate Texts in Mathematics. Springer (1990).

[6] Ouyang, Y., Xie, X.: Linear complexity of generalized cyclotomic sequences of period \(2p^m\). arXiv:1808.08019v1 [cs.IT] 24 Aug 2018

[7] Ye, Z., Ke, P., Wu, C.: A further study of the linear complexity of new binary cyclotomic sequence of length \(p^n\). AAECC (2018). https://doi.org/10.1007/s00200-018-0368-9

[8] Zeng, X., Cai, H., Tang, X., Yang, Y.: Optimal frequency hopping sequences of odd length. IEEE Transactions on Information Theory **59**(5), 3237–3248 (2013).

[9] Xiao, Z., Zeng, X., Li, C., Helleseth, T.: New generalized cyclotomic binary sequences of period \(p^2\). Des. Codes Cryptography **86**(7) (2018) 1483-1497.