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

VLADIMIR EDEMSKIY
Novgorod State University
Department of Applied Mathematics and Informatics
ul. B. St. Petersburgskaya, 41 173003, Veliky Novgorod
RUSSIA
Vladimir.Edemskiy@novsu.ru

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.

Key–Words: Binary sequences, linear complexity, cyclotomy

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.

We will study the linear complexity of new sequence family from [6] 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 6×10^{17} [1, 3].

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

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

So, if $N = 2p^n$ then we see that

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

Thus, if α_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 $\{\alpha_n^i, i = 0, 1, \dots, p^n - 1\}$ 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 $j \ge 1$. Hence, we can assume that g is an odd number. Further, the order of g modulo $2p^j$ is equal to $\varphi(2p^j) = p^{j-1}(p-1)$, where $\varphi(\cdot)$ 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

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

The cosets $D_i^{(p^j)}$, $i = 0, 1, \cdots, d_j - 1$, are called *generalized cyclotomic classes* of order d_j with respect to p^j. It was shown in [8] that $\left\{ D_0^{(p^j)}, D_1^{(p^j)}, \ldots, D_{d_j-1}^{(p^j)} \right\}$ forms a partition of $\mathbb{Z}_{p^j}^*$ for each integer $j \ge 1$ and for an integer $m \ge 1$. Also $\left\{ D_0^{(2p^j)}, D_1^{(2p^j)}, \ldots, D_{d_j-1}^{(2p^j)} \right\}$ forms a partition of $\mathbb{Z}_{2p^j}^*$ for each integer $j \ge 1$ and for an integer $m \ge 1$.

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

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

It is obvious that $\mathbb{Z}_{2p^n} = \mathcal{C}_0^{(2p^n)} \cup \mathcal{C}_1^{(2p^n)} = \widetilde{\mathcal{C}}_0^{(2p^n)} \cup \widetilde{\mathcal{C}}_1^{(2p^n)}$ and $|\mathcal{C}_i^{(2p^n)}| = |\widetilde{\mathcal{C}}_i^{(2p^n)}| = p^n$, $i = 0, 1$. 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.,

$$s_i = \begin{cases} 0, & \text{if } i \pmod{p^n} \in \mathcal{C}_0^{(2p^n)}, \\ 1, & \text{if } i \pmod{p^n} \in \mathcal{C}_1^{(2p^n)}. \end{cases} \quad (3)$$

and

$$\tilde{s}_i = \begin{cases} 0, & \text{if } i \pmod{p^n} \in \widetilde{\mathcal{C}}_0^{(2p^n)}, \\ 1, & \text{if } i \pmod{p^n} \in \widetilde{\mathcal{C}}_1^{(2p^n)}. \end{cases} \quad (4)$$

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

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

2.3 Main Result

This subsection will study the linear complexity of s^∞, $\tilde{s}^\infty$ in (3) and (4) for some even integers f. 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 $\mathrm{ord}_p(2)$ denote the order of 2 modulo p and $v = \gcd\left(\frac{p-1}{\mathrm{ord}_p(2)}, f\right)$.*
(i) Let s^∞ be a generalized cyclotomic binary sequence of period p^n defined in (3). Then the linear complexity of s^∞ is given by

$$L(s^\infty) = 2p^n - r \cdot \mathrm{ord}_p(2),$$

where $0 \le r \le \frac{p-1}{\mathrm{ord}_p(2)}$.

Furthermore, the linear complexity

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

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

$$2p^n - 2r\cdot \mathrm{ord}_p(2) \le L(\widetilde{s}^{\infty}) \le 2p^n - r\cdot \mathrm{ord}_p(2),$$

where $0\le r\le \frac{p-1}{\mathrm{ord}_p(2)}$. Furthermore, the linear complexity

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

Corollary 2 *Let $f=2^r$. Then:*
(i) The linear complexity of s^{∞} 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 $\widetilde{s}^{\infty}$ 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 3 *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 $2^e\equiv 1 \pmod p$ in Conjecture from [6] is equivalent to $v = \gcd\left(\frac{p-1}{\mathrm{ord}_p(2)}, f\right) = f$ 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 $S(x)=s_0+s_1x+\cdots+s_{2p^n-1}x^{2p^n-1}$ and $\widetilde{S}(x)=\widetilde{s}_0+\widetilde{s}_1x+\cdots+\widetilde{s}_{2p^n-1}x^{2p^n-1}$ for the generalized cyclotomic sequences s^{∞}, $\widetilde{s}^{\infty}$ defined in (3) and (4), respectivly. Then,

$$S(x)=\sum_{t\in\mathcal{C}_1^{(p^n)}} x^t \text{ and } \widetilde{S}(x)=\sum_{t\in\widetilde{\mathcal{C}}_1^{(p^n)}} x^t \qquad (5)$$

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

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

and

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

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.

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 $\alpha_j=\alpha_n^{p^{n-j}}$, $j=1,2\ldots,n-1$.

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

Lemma 4 *[4] 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) $T_i^{(p^m)}(\alpha_m^a) + T_{i+d_m/2}^{(p^m)}(\alpha_m^a) = 1$.
(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 $m>1$.

Throughout this paper an integer u will be such that $2\equiv g^u \pmod{p^n}$. Now we will show that the studying of linear complexity of above sequences is equivalent to the investigation of properties of $T_i^{(p^m)}(x)$

Proposition 5 *Let α_n be a p^n-th primitive root of unity and let $2\equiv g^u \pmod{p^n}$. Given any element $a\in\mathbb{Z}_{p^n}$, we have*
(i) $S(\alpha_n^a)=1+T_b^{(p^n)}(\alpha_n^a)+T_{b+u}^{(p^n)}(\alpha_n^a)$; and
(ii) $S(\alpha_n^a)=T_b^{(p^n)}(\alpha_n^a)+T_{b+u}^{(p^n)}(\alpha_n^a)$.

Proof: (i) Since $\sum_{t\in p^{n-j}D_{(i+b)}^{(2p^j)}}\alpha^{at} = \sum_{t\in p^{n-j}D_{(i+b)}^{(p^j)}}\alpha^{at}$ by (1), it follows from our definitions and Lemma 4 that

$$S(\alpha_n^a)=1+T_b^{(p^n)}(\alpha_n^a)+T_{b+u}^{(p^n)}(\alpha_n^a).$$

(ii) Similarly we have

$$\widetilde{S}(\alpha_n^a)=T_b^{(p^n)}(\alpha_n^a)+T_{b+u}^{(p^n)}(\alpha_n^a).$$

□

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

Proposition 6 *Let p be a non-Wieferich prime. Then $S(\alpha_n^i) \neq 0$ and $\widetilde{S}(\alpha_n^a) \neq 0$ for $i \in \mathbb{Z}_{p^n} \setminus p^{n-1}\mathbb{Z}_p$.*

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

2. Let $T_0^{(p^m)}(\alpha_m) + T_u^{(p^m)}(\alpha_m) = 1$.

It then follows from Lemma 4 (i) that $T_{iu}^{(p^m)}(\alpha_m) + T_{(i+1)u}^{(p^m)}(\alpha_m) = 1$ 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 $T_i^{(p^m)}(x)$ is taken modulo d_m, it is easily seen that

$$T_0^{(p^m)}(\alpha_m) = T_{iw}^{(p^m)}(\alpha_m), \quad \text{for any integer } i \geq 1. \tag{8}$$

By Lemma 4 (ii) from the last formula we have $T_{d_m/2}^{(p^m)}(\alpha_m) = T_{d_m/2+iw}^{(p^m)}(\alpha_m)$ or $T_{d_m}^{(p^m)}(\alpha_m) = T_{d_m/2+jf}^{(p^m)}(\alpha_m)$. Then we get that $T_{d_m/2}^{(p^m)}(\alpha_m) = T_{f/2}^{(p^m)}(\alpha_m)$. Thus, by Lemma 4 (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 4 (iv). □

By Proposition 6, we only need to study the value of $T_b^{(p^n)}(\alpha_n^i) + T_{b+u}^{(p^n)}(\alpha_n^i)$ for integers i in the set $p^{n-1}\mathbb{Z}_p$. Suppose $i = p^{n-1}a, \quad a \in D_i^{(p)}$. Then, it follows from Proposition 5 and Lemma 4 that

$$S(\alpha_n^i) = 1 + H_k^{(p)}(\alpha_1) + H_{k+u}^{(p)}(\alpha_1),$$

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 $\mathrm{ord}_p(2)$.

Proposition 7 *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) $\left|\left\{k \in \mathbb{Z}_f \mid H_k^{(p)}(\alpha_1) + H_{k+u}^{(p)}(\alpha_1) = 0\right\}\right| = \begin{cases} f, & \text{if } v = f, \\ 0, & \text{if } v \mid f/2 \text{ or } v = 2, v \neq f. \end{cases}$

(ii) $\left|\left\{k \in \mathbb{Z}_f \mid H_k^{(p)}(\alpha_1) + H_{k+u}^{(p)}(\alpha_1) = 1\right\}\right| = \begin{cases} f, & \text{if } v = f/2, \\ 0, & \text{if } v = 1, \text{ or } v = f \text{ or } 2v \mid f/2. \end{cases}$

Proof: Since $\mathrm{ord}_p(2) = \frac{p-1}{\gcd(p-1, u)}$, it follows that $\gcd(u, f) = \gcd(\frac{(p-1)}{\mathrm{ord}_p(2)}, f) = v$ [4].

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

Let $v \mid f/2$ 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 $H_k^{(p)}(\alpha_1)) \in \{0,1\}$. By [4] this is not possible for $v \mid f/2$ 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 $H_k^{(p)}(\alpha_1) + H_{k+u}^{(p)}(\alpha_1) = 1$ 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 $\gcd(u, f) = \gcd(\frac{(p-1)}{\mathrm{ord}_p(2)}, f) = v$, by a similar argument as in the proof of Proposition 6 we get

$$H_0^{(p)}(\alpha_1) = H_{2v}^{(p)}(\alpha_1) = \cdots = H_{2vi}^{(p)}(\alpha_1).$$

So, if $2v$ divides $f/2$, then $H_{f/2}^{(p)}(\alpha_1) = H_{2v \cdot f/4v}^{(p)}(\alpha_1) = H_0^{(p)}(\alpha_1)$, 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 $E_i^{(p)}(\alpha_1) + E_{i+f/2}^{(p)}(\alpha_1) + 1 = 0, \quad i = 0, 1, \ldots, f-1$. In [4] it was shown that this is impossible. □

Proof of Theorem 1. Recall that the linear complexity of s^∞ is given by

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

(i) From Proposition 6 we know $S(\alpha_n^i) \neq 0$ 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

$$S(\alpha_n^i) = 1 + H_b^{(p)}(\alpha_1^a) + H_{b+u}^{(p)}(\alpha_1^a)$$

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

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

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

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

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

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

Further, by (5) we see that

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

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

Then the statement of this theorem follows from Proposition 6.

(ii) In this case

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

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

Then as earlier we again get

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

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

Here, by (5) we see that

$$x\widetilde{S}'(x) = \sum_{j=1}^{n} \sum_{i=0}^{d_j/2-1} \sum_{t \in D_{i+b \pmod{d_j}}^{(2p^j)}} x^{p^{n-j}t}.$$

and also $\alpha_n^i \widetilde{S}(\alpha_n^i) = T_b^{(p^n)}(\alpha_n^i)$. If $v = f$ then it follows from [4] that

$$|\{i: \ T_b^{(p^n)}(\alpha_n^i) = 0, i = 1, 2, \ldots, p^n - 1\}| = (p-1)/2.$$

Then the statement of this theorem follows from Proposition 6.

$\square$

Acknowledgements: The reported study was funded by RFBR and NSFC according to the research project No 19-55-53003.

References:

[1] A. Akbary and S. Siavashi, The largest known Wieferich numbers, *Integers* 18-A3, 2018, pp. 1–6.

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

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

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

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

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

[7] Z. Ye, P. Ke and C. Wu, 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] X. Zeng, H. Cai, X. Tang and Y. Yang, Optimal frequency hopping sequences of odd length. *IEEE Transactions on Information Theory*, 59(5), 2013, pp. 3237–3248 (2013).

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