The linear complexity of generalized cyclotomic binary and quaternary sequences of period $2p^n$

Vladimir Edemskiy *
Department of Applied Mathematics and Information Science
Yaroslav-the-Wise Novgorod State University
Veliky Novgorod, Russia
vladimir.edemsky@novsu.ru

Nikita Sokolovskii
Department of Applied Mathematics and Information Science
Yaroslav-the-Wise Novgorod State University
Veliky Novgorod, Russia
sokolovskiy.nikita@gmail.com

Abstract

In this paper, we study the linear complexity of new generalized cyclotomic binary sequences of period $2p^n$ recently proposed by Ouyang et al. (Des. Codes Cryptography, 2019). We generalized results presented in this work and discuss the author's conjecture. Further on, we derive the linear complexity of the quaternary sequences over the finite field of order four and the finite ring of order four. These sequences are also constructed from generalized cyclotomic classes modulo $2p^n$.

1 Introduction

The linear complexity of a sequence is defined as the smallest order of linear feedback shift register that can generate the whole sequence. So, the concept of the linear complexity of a sequence is very useful in the study of the security of stream ciphers. The use of cyclotomic classes and generalized cyclotomic classes to design sequences is a well-known method [2]. We can obtain the sequences with high linear complexity this way. Classical cyclotomy was first considered in detail by Gauss. Later, generalized cyclotomies were presented by Whiteman, Ding and Helleseth. There are lots of papers devoted to the study of the linear complexity of Whiteman and Ding-Helleseth-generalized cyclotomic sequences. In particular, binary and quaternary sequences with period $2p^n$ are studied in [15, 5, 4, 6, 7, 13] (see also references here).

*Vladimir Edemskiy and Nikita Sokolovskii are supported by RFBR and NSFC according to the research project No. 19-51-53003.

Recently another construction was presented by Zeng et al. in [12], where the order of the generalized cyclotomic classes depends on the choice of parameters. The linear complexity of new generalized cyclotomic binary sequences with period p^n was studied in [14, 3, 11]. A new family of binary sequences with period $2p^n$ based on the generalized cyclotomic classes from [12] was presented in [8]. Ouyang et al. examined the linear complexity of these sequences for $f = 2^r$, where $p = 1 + ef$ and r is a positive integer. They also offered the conjecture about the linear complexity of these sequences.

In this paper, we first will generalize result from [8] and will prove the conjecture of the authors of this paper. Second, we will study the linear complexity of quaternary sequences over the finite field $\mathbb{F}_4$ and the finite ring $\mathbb{Z}_4$. Generally, these two ways lead to different values for the linear complexity because arithmetics of $\mathbb{F}_4$ and $\mathbb{Z}_4$ differ. These sequences are also derived from generalized cyclotomic classes modulo $2p^n$.

We conclude this section by recalling the notions of new generalized cyclotomic classes from [12, 8], the definitions of sequences and notation of the linear complexity.

1.1 The definition of sequences

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 $\mathbb{Z}_N$.

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 that the odd one from g and $g + p^n$ is also a primitive root modulo $2p^j$ for each integer $j \geq 1$. Hence, we can assume that g is an odd number. Below we recall the definitions of generalized cyclotomic classes introduced in [12] and [8].

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

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

It was shown in [12] and [8] that $\left\{ D_0^{(p^j)}, D_1^{(p^j)}, \ldots, D_{d_j-1}^{(p^j)} \right\}$ and $\left\{ D_0^{(2p^j)}, D_1^{(2p^j)}, \ldots, D_{d_j-1}^{(2p^j)} \right\}$ form a partition of $\mathbb{Z}_{p^j}^*$ and $\mathbb{Z}_{2p^j}^*$ for each integer $j \geq 1$, respectively.

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

$$\begin{aligned} \mathcal{C}_0^{(2p^n)} &= \bigcup_{j=1}^{n} \bigcup_{i=0}^{d_j/2-1} p^{n-j} D_{(i+b) \pmod{d_j}}^{(2p^j)}, \text{ and } \mathcal{C}_1^{(2p^n)} = \bigcup_{j=1}^{n} \bigcup_{i=d_j/2}^{d_j-1} p^{n-j} D_{(i+b) \pmod{d_j}}^{(2p^j)} \\ \mathcal{C}_2^{(2p^n)} &= \bigcup_{j=1}^{n} \bigcup_{i=0}^{d_j/2-1} 2p^{n-j} D_{(i+b) \pmod{d_j}}^{(2p^j)}, \text{ and } \mathcal{C}_3^{(2p^n)} = \bigcup_{j=1}^{n} \bigcup_{i=d_j/2}^{d_j-1} 2p^{n-j} D_{(i+b) \pmod{d_j}}^{(2p^j)}. \end{aligned} \tag{2}$$

It is obvious that

$$\mathbb{Z}_{2p^n} = \bigcup_{j=0}^{3} \mathcal{C}_j^{(2p^n)} \cup \{0, p^n\} \text{ and } |\mathcal{C}_j^{(2p^n)}| = (p^n - 1)/2.$$

Families of balanced binary sequences $s^\infty = (s_0, s_1, s_2, \dots)$ and $\tilde{s}^\infty = (\tilde{s}_0, \tilde{s}_1, \tilde{s}_2, \dots)$ of period $2p^n$ can thus be defined as in [8], i.e.,

$$s_i = \begin{cases} 1, & \text{if } i \pmod{2p^n} \in \mathcal{C}_0^{(2p^n)} \cup \mathcal{C}_2^{(2p^n)} \cup \{0\}, \\ 0, & \text{if } i \pmod{2p^n} \in \mathcal{C}_1^{(2p^n)} \cup \mathcal{C}_3^{(2p^n)} \cup \{p^n\}. \end{cases} \tag{3}$$

and

$$\tilde{s}_i = \begin{cases} 1, & \text{if } i \pmod{2p^n} \in \mathcal{C}_0^{(2p^n)} \cup \mathcal{C}_3^{(2p^n)} \cup \{0\}, \\ 0, & \text{if } i \pmod{2p^n} \in \mathcal{C}_1^{(2p^n)} \cup \mathcal{C}_2^{(2p^n)} \cup \{p^n\}. \end{cases} \tag{4}$$

In the case of $f = 2^r$, the linear complexity of $s^\infty, \tilde{s}^\infty$ was estimated in [8], where a conjecture about the linear complexity of these sequences was also made as follows.

Conjecture.[8] (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 $L(\tilde{s}^\infty) \leq 2p^n - (p-1) - e$.

We will prove this conjecture. Further, we will estimate the linear complexity of quaternary sequences. Let a, b, c and d are pairwise distinct integers between 0 and 3. Then families of balanced quaternary sequences $w^\infty = (s_0, s_1, s_2, \dots)$ of period $2p^n$ can thus be defined as

$$w_i = \begin{cases} a, & \text{if } i \pmod{p^n} \in \mathcal{C}_0^{(2p^n)} \cup \{0\}, \\ b, & \text{if } i \pmod{p^n} \in \mathcal{C}_1^{(2p^n)}, \\ c, & \text{if } i \pmod{p^n} \in \mathcal{C}_2^{(2p^n)} \cup \{p^n\}, \\ d, & \text{if } i \pmod{p^n} \in \mathcal{C}_3^{(2p^n)}. \end{cases} \tag{5}$$

Let $\mathbb{F}_4 = \{0, 1, \mu, \mu+1\}$ be the finite field of 4 elements and let $\varphi(a)$ be the Gray map defined by $\varphi(0) = [0,\ 0]$, $\varphi(1) = [0,\ 1]$, $\varphi(2) = [1,\ 1]$, $\varphi(3) = [1,\ 0]$. We can view $\mathbb{F}_4$ as a vector space over $\mathbb{F}_2$ with basis $\mu,\ 1$ and using Gray map to find $\varphi(a) = \beta$, $\varphi(b) = \gamma$, $\varphi(c) = \zeta$, $\varphi(d) = \eta$. Thus, β, γ, ζ and η are pairwise distinct elements from $\mathbb{F}_4$. Then we define a quaternary sequence u^∞ over $\mathbb{F}_4$ as

$$u_i = \begin{cases} \beta, & \text{if } i \pmod{p^n} \in \mathcal{C}_0^{(2p^n)} \cup \{0\}, \\ \gamma, & \text{if } i \pmod{p^n} \in \mathcal{C}_1^{(2p^n)}, \\ \zeta, & \text{if } i \pmod{p^n} \in \mathcal{C}_2^{(2p^n)} \cup \{p^n\}, \\ \eta, & \text{if } i \pmod{p^n} \in \mathcal{C}_3^{(2p^n)}. \end{cases} \tag{6}$$

In conclusion of the section we recall one method to studying the linear complexity. Let $s^\infty = (s_0, s_1, s_2, \dots)$ be a sequence of period N over the $\mathbb{F}_q$ (the finite field of q elements) and $S(x) = s_0 + s_1 x + \cdots + s_{N-1} x^{N-1}$. It is well known (see, for instance, [2]) that the linear complexity of s^∞ is given by

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

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

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

Thus, if α_n is a primitive root of order p^n of unity in the extension of the field $\mathbb{F}_q$, then in order to find the linear complexity of a sequence, it is sufficient to study the zeros of $S(x)$ in the set $\{\alpha_n^i, i = 0, 1, \ldots, p^n - 1\}$.

2 The linear complexity of binary sequences

In this section we will study the linear complexity of s^∞, $\tilde{s}^\infty$ defined by (3) and (4) for 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 6×10^{17}. Our main result in this section is the following statement.

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 $2p^n$ defined in (3). Then the linear complexity of s^∞ is given by

$$L(s^\infty) = 2p^n - r \cdot \mathrm{ord}_p(2), \quad 0 \le r \le \tfrac{p-1}{\mathrm{ord}_p(2)}.$$

Furthermore, the linear complexity

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

(ii) Let $\tilde{s}^\infty$ be a generalized cyclotomic binary sequence of period $2p^n$ defined in (4). Then for the linear complexity of $\tilde{s}^\infty$ we have

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

Furthermore, the linear complexity

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

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 $\tilde{s}^\infty$ 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 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 [8] 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 when $f = 2^r$ for a positive integer r, the integer v is 1 or also a power of 2, which either equals f or $f/2$ or divides $f/4$. Hence Conjecture from [8] is included in Theorem 1 as a special case for not Wieferich primes.

2.1 Subsidiary lemmas

Let $S(x) = s_0 + s_1x + \cdots + s_{2p^n-1}x^{2p^n-1}$ and $\widetilde{S}(x) = \tilde{s}_0 + \tilde{s}_1x + \cdots + \tilde{s}_{2p^n-1}x^{2p^n-1}$ for the sequences s^∞, $\tilde{s}^\infty$ defined in (3) and (4), respectively. For simplicity, we define polynomials as in [3]. Let

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

Notice that the subscripts i in $D_i^{(p^j)}$, 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 $T_i^{(p^j)}(x)$ were studied in [3]. We have here the following statement.

Lemma 4. *[3] For any $a \in D_k^{(p^j)}$, we see that*

(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* $0 \le l < m$.

(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 u will be an integer 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 $T_i^{(p^m)}(x)$

Lemma 5. *For any $t = 1, 2, \ldots, p^n - 1$, we have*

(i) $\sum_{i \in C_0^{(2p^n)}} \alpha_n^{ti} = T_b^{(p^n)}(\alpha^t)$ *and* $\sum_{i \in C_2^{(2p^n)}} \alpha_n^{ti} = T_{b+u}^{(p^n)}(\alpha^t)$;

(ii) $\sum_{i \in C_1^{(2p^n)}} \alpha_n^{ti} = 1 - T_b^{(p^n)}(\alpha^t)$ *and* $\sum_{i \in C_3^{(2p^n)}} \alpha_n^{ti} = 1 - T_{b+u}^{(p^n)}(\alpha^t)$.

Proof. We will prove only the first statement. The (ii) can be obtained in the same way.

(i) Since $\sum_{i \in p^{n-j} D_{(i+b)}^{(2p^j)}} \alpha^{ti} = \sum_{i \in p^{n-j} D_{(i+b)}^{(p^j)}} \alpha^{ti}$ by (1), from (2) and (7) it follows that

$$\sum_{i \in C_0^{(2p^n)}} \alpha^{ti} = \sum_{j=1}^{n} \sum_{i=0}^{d_j/2-1} \sum_{i \in p^{n-j} D_{(i+b)}^{(2p^j)}} \alpha^{ti} = \sum_{j=1}^{n} \sum_{i=0}^{d_j/2-1} \sum_{i \in D_{(i+b)}^{(p^j)}} \alpha^{tp^{n-j}i} = T_b^{(p^n)}(\alpha^t).$$

We have that $\sum_{i\in 2p^{n-j}D_i^{(2p^j)}}\alpha^{ti}=\sum_{i\in 2D_i^{(p^j)}}\alpha^{tp^{n-j}i}$ and $2D_i^{(p^j)} \pmod{p^j} = D_{i+u}^{(p^j)}$. Hence

$$\sum_{i\in\mathcal{C}_2^{(2p^n)}}\alpha^{ti}=\sum_{j=1}^{n}\sum_{i=0}^{d_j/2-1}\sum_{i\in D_{(i+b+u)}^{(p^j)}}\alpha^{tp^{n-j}i}=T_{b+u}^{(p^n)}(\alpha^t).$$

□

Corollary 6. *With notations as above. 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) $\widetilde{S}(\alpha_n^a)=T_b^{(p^n)}(\alpha_n^a)+T_{b+u}^{(p^n)}(\alpha_n^a)$.

Lemma 7. *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. By Corollary 6 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 $b=0,1,\cdots,d_n-1$. It is clear by Lemma 4 that without loss of generality it is enough to show that $T_0^{(p^m)}(\alpha_m)+T_u^{(p^m)}(\alpha_m)\notin\{0,1\}$ 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

$$1=\left(T_0^{(p^m)}(\alpha_m)+T_u^{(p^m)}(\alpha_m)\right)^2=T_0^{(p^m)}(\alpha_m^2)+T_u^{(p^m)}(\alpha_m^2)=T_u^{(p^m)}(\alpha_m)+T_{2u}^{(p^m)}(\alpha_m),$$

which implies $T_{iu}^{(p^m)}(\alpha_m)+T_{(i+1)u}^{(p^m)}(\alpha_m)=1$ for any integer $i\geq 1$. Hence $T_0^{(p^m)}(\alpha_m)=T_{2iu}^{(p^m)}(\alpha_m)$.

Denote $w=\gcd(2u,d_m)$ where $d_m=p^{m-1}f$. Since p is a non-Wieferich prime, it follows by [3] that w divides f. Since the subscript of $T_i^{(p^m)}(x)$ is taken modulo d_m, it is easily seen that $T_0^{(p^m)}(\alpha_m)=T_{if}^{(p^m)}(\alpha_m)$ for any integer $i\geq 1$. By Lemma 4 (ii) from the last formula we have $T_{d_m/2}^{(p^m)}(\alpha_m)=T_{d_m/2+if}^{(p^m)}(\alpha_m)$. Then we get that

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

Hence, $T_{d_m/2}^{(p^m)}(\alpha_m)=T_{f/2}^{(p^m)}(\alpha_m)$. 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 Lemma 7 and Lemma 4, we only need to study the value of

$$T_b^{(p)}(\alpha_1^a)+T_{b+u}^{(p)}(\alpha_1^a)=T_{b+k}^{(p)}(\alpha_1)+T_{b+u+k}^{(p)}(\alpha_1)$$

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

Lemma 8. *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,*

$$(i)\ \left|\left\{k \in \mathbb{Z}_f \,|\, T_k^{(p)}(\alpha_1) + T_{k+u}^{(p)}(\alpha_1) = 0\right\}\right| = \begin{cases} f, & \text{if } v = f, \\ 0, & \text{if } v|f/2 \text{ or } v = 2, v \neq f. \end{cases}$$

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

Proof. Since $\mathrm{ord}_p(2) = \frac{p-1}{\gcd(p-1,u)}$, it follows that $\gcd(u, f) = \gcd(\frac{(p-1)}{\mathrm{ord}_p(2)}, f) = v$ [3].

(i) For $v = f$ this statement is clear. Suppose $T_k^{(p)}(\alpha_1^a) + T_{k+u}^{(p)}(\alpha_1^a) = 0$ for some integer k. Since $(T_k^{(p)}(\alpha_1))^2 = T_{k+u}^{(p)}(\alpha_1)$, it follows that $T_k^{(p)}(\alpha_1)) \in \{0, 1\}$. By [3] this is not possible for $v|f/2$ or $v = 2, v \neq f$.

(ii) For $v = f/2$ and $v = f$ this statement is clear. Suppose $T_k^{(p)}(\alpha_1) + T_{k+u}^{(p)}(\alpha_1) = 1$ for some integer k. With a similar argument as in the proof of Lemma 7 we get

$$T_0^{(p)}(\alpha_1) = T_{2v}^{(p)}(\alpha_1) = \cdots = T_{2vi}^{(p)}(\alpha_1).$$

So, if $2v$ divides $f/2$, then $T_{f/2}^{(p)}(\alpha_1) = T_{2v \cdot f/4v}^{(p)}(\alpha_1) = T_0^{(p)}(\alpha_1)$, which is a contradiction. □

2.2 Proof of Theorem 1.

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

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

(i) From Lemma 7 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 $i \in p^{n-1}\mathbb{Z}_p^*$, i.e. $i = ap^{n-1},\ a \in \mathbb{Z}_p^*$ we have

$$S(\alpha_n^i) = 1 + T_b^{(p^n)}(\alpha_n^i) + T_{b+u}^{(p^n)}(\alpha_n^i) = 1 + T_b^{(p)}(\alpha_1^a) + T_{b+u}^{(p)}(\alpha_1^a).$$

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

$$1 = T_b^{(p)}(\alpha_1^{2a}) + T_{b+u}^{(p)}(\alpha_1^{2a}) = T_b^{(p)}(\alpha_1^{2^2a}) + T_{b+u}^{(p)}(\alpha_1^{2^2a}) = \dots$$

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

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

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

Further, by (3) we see that

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

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 first statement of this theorem follows from Lemma 8.

(ii) In this case, as earlier we again get

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

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

Here, by (4) we see that

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

and also $\alpha_n^i \widetilde{S}(\alpha_n^i) = T_b^{(p^n)}(\alpha_n^i)$. If $v = f$ then it follows from [3] that

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

Using Lemma 8 completes this proof.

3 The linear complexity of quaternary sequences over the $\mathbb{F}_4$

In this section we will study the linear complexity over the $\mathbb{F}_4$ of u^∞, when p is not also a Wieferich prime. The main result in this section is given as follows.

Theorem 9. *Let p be an odd prime with $2^{p-1} \not\equiv 1 \pmod{p^2}$ and let u^∞ be a generalized cyclotomic quaternary sequence of period $2p^n$ defined in (6). Then we have the following estimate for the linear complexity over $\mathbb{F}_4$ of u^∞*

$$LC(u^\infty) = 2p^n - r \operatorname{ord}_p(2).$$

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

Remark 10. Furthermore,

$$LC(u^\infty) = \begin{cases} 2p^n - p + 1, & \text{if } v = f; \\ 2p^n, & \text{if } v|\frac{f}{2}, \text{ or } v = 2 \text{ and } v \ne f, \end{cases}$$

where $p = ef + 1$ and $v = \gcd(\frac{(p-1)}{\operatorname{ord}_p(2)}, f)$ as early.

Example 11. Let $p = 73, n = 2$. Then $N = 10658$, $\operatorname{ord}_p(2) = 9$ and $v = 8$. Using Berlekamp-Massey algorithm we obtain that $LC(u^\infty) = 10568$ for $f = 2, 4, 8$ but $LC(u^\infty) = 10658$ for $f = 6, 12$ and $LC(u^\infty) = 10622$ for $f = 24$.

3.1 Proof of Theorem 9

Let $U(x) = u_0 + u_1 x + \cdots + u_{2p^n-1}x^{2p^n-1}$ be the generating polynomial of u^∞, defined in (6). From here on we will use denotation α instead α_n.

According to Lemmas 4, 5 and (6) we obtain that

$$U(\alpha^t) = \beta + \zeta + \beta T_b^{(p^n)}(\alpha^t) + \gamma\left(1 - T_b^{(p^n)}(\alpha^t)\right) + \zeta T_{b+u}^{(p^n)}(\alpha^t) + \eta\left(1 - T_{b+u}^{(p^n)}(\alpha^t)\right).$$

Since $\beta + \gamma + \zeta + \eta = 0$, it follows that

$$U(\alpha^t) = (\beta + \gamma)\left(T_b^{(p^n)}(\alpha^t) + T_{b+u}^{(p^n)}(\alpha^t)\right). \tag{8}$$

Thus, by (8) we have $U(\alpha^t) = 0$ iff $T_b^{(p^n)}(\alpha^t)^2 = T_b^{(p^n)}(\alpha^t)$, i.e., $T_b^{(p^n)}(\alpha^t) \in \{0, 1\}$. According to [3], $|\{i : \ T^{(p^n)}(\alpha^i) = 0 \text{ (or 1)}, i = 1, 2, \ldots, p^n - 1\}| = r\,\mathrm{ord}_p(2)$.

Further,

$$U'(x) = \beta \sum_{i \in \mathcal{C}_0^{(2p^n)}} x^{i-1} + \gamma \sum_{i \in \mathcal{C}_1^{(2p^n)}} x^{i-1} + \zeta x^{p^n-1}.$$

Hence,

$$\alpha^t U'(\alpha^t) = \beta T_b^{(p^n)}(\alpha^t) + \gamma\left(1 - T_b^{(p^n)}(\alpha^t)\right) + \zeta = (\beta + \gamma)T_b^{(p^n)}(\alpha^t) + \gamma + \zeta.$$

Thus, if $U(\alpha^t) = 0$ then $U'(\alpha^t) \neq 0$.

To end the proof it is enough to note that $U(1) \neq 0$.

Remark 10 follows from Theorem 5 [3]. According to Theorem 1 these quaternary sequences have high linear complexity over $\mathbb{F}_4$ for $n > 1$.

4 The linear complexity of quaternary sequences over the $\mathbb{Z}_4$

In this section we study the linear complexity of quaternary sequences over the finite ring $\mathbb{Z}_4$. We recall that the linear complexity $LC(w^\infty)$ of $\{w_i\}_{i\geq 0}$ above is the least order L of a linear recurrence relation over $\mathbb{Z}_4$

$$w_{i+L} + c_1 w_{i+L-1} + \ldots + c_{L-1}w_{i+1} + c_L w_i = 0 \quad \text{for } i \geq 0,$$

which is satisfied by $\{w_i\}_{i\geq 0}$ and where $c_1, c_2, \ldots, c_L \in \mathbb{Z}_4$, see [9]. Let $W(x) = s_0 + w_1 x + \ldots + w_{2p^n-1}x^{2p^n-1} \in \mathbb{Z}_4[x]$ be the generating polynomial of $\{w_i\}_{i\geq 0}$. Then

$$\begin{aligned} LC(w^\infty) = \ & \min\{\deg(C(X)) : C(X) \in \mathbb{Z}_4[x], C(0) = 1, \\ & W(x)C(x) \equiv 0 \pmod{x^{2p^n} - 1}\}, \end{aligned} \tag{9}$$

where $C(x) = 1 + c_1 x + \ldots + c_L x^L$ is the connection polynomial of w^∞. We note that $C(0) = 1$.

Our main result in this section is the following statement.

Theorem 12. *Let $p = ef + 1$ be an odd prime with $2^{p-1} \not\equiv 1 \pmod{p^2}$ and let w^∞ be a generalized cyclotomic quaternary sequence of period $2p^n$ defined in (5). Then we have the following estimates for the linear complexity over the $\mathbb{Z}_4$ of w^∞:*

(i) $LC(w^\infty) \geq 2p^n - 2p$ *for* $a + b \not\equiv 0 \pmod 2$.

(ii) $p^n - p + 1 \leq LC(w^\infty) \leq p^n + 1$ *for* $a + b \equiv 0 \pmod 2$.

Let r be the order of 2 modulo p^n. We denote by $GR(4^r, 4)$ the Galois ring of order 4^r of characteristic 4. For the knowledge of Galois ring, please see, for example [10]. The group of units of $GR(4^r, 4)$, denoted by $GR^*(4^r, 4)$, contains a cyclic subgroup of order $2^r - 1$. Since $p^n | (2^r - 1)$ there exist $\alpha \in GR^*(4^r, 4)$ of order p^n. Then we find that $\xi = 3\alpha \in GR^*(4^r, 4)$ is of order $2p^n$. From (9), we will consider the values $W(\xi^v)$ for $v = 0, 1, \ldots, 2p^n - 1$. Due to $W(x) \in \mathbb{Z}_4[x]$, we cannot consider it in the same way as those in finite fields. For example, 1 and 3 are the roots of $2x - 2 \in \mathbb{Z}_4[x]$, but $2x - 2$ is not divisible by $(x - 1)(x - 3)$, i.e., in the ring $\mathbb{Z}_4[X]$ the number of roots of a polynomial can be greater than its degree. But, if $\lambda, \rho \in GR(4^r, 4)$ are roots of some polynomial $P(x) \in \mathbb{Z}_4[x]$ and $\lambda - \rho$ is a unit in $GR(4^r, 4)$, then we have $P(x)$ is divided by $(x - \lambda)(x - \rho)$ [1].

In our case, $\alpha^i - \alpha^j \in GR^*(4^r, 4)$ and $\xi^i - \xi^j \in GR^*(4^r, 4)$ for $i \not\equiv j \pmod{p^n}$. Thus, if $P(\alpha^i) = 0$, $i = 0, 1, 2, \ldots, p^n - 1$ or $P(\xi^i) = 0$, $i = 1, 3, \ldots, 2p^n - 1$ then $P(x)$ is divided by $(x^{p^n} - 1)$ or $(x^{p^n} + 1)$ respectively.

4.1 Proof of Theorem 12

The ring $GR(4^r, 4)$ has a single maximal ideal equal to $2GR(4^r, 4)$ and we have the natural epimorphism from $GR(4^r, 4)$ to $GR(4^r, 4)/2GR(4^r, 4)$. Moreover, $GR(4^r, 4)/2GR(4^r, 4)$ is a Galois field. Denote this field by $\mathbb{F}$. Let $\bar{\chi}$ denote the image of the element $\chi \in GR(4^r, 4)$ under this epimorphism. Then we see that

$$\overline{W(\xi^t)} = \bar{a} \sum_{i \in \mathcal{C}_0^{(2p^n)}} \bar{\xi}^{ti} + \bar{b} \sum_{i \in \mathcal{C}_1^{(2p^n)}} \bar{\xi}^{ti} + \bar{c} \sum_{i \in \mathcal{C}_2^{(2p^n)}} \bar{\xi}^{ti} + \bar{d} \sum_{i \in \mathcal{C}_3^{(2p^n)}} \bar{\xi}^{ti} + \bar{a} + \bar{c}\bar{\xi}^{p^n t}.$$

Since $\bar{\xi}^{p^n} = 1$ in the $\mathbb{F}$, we can derive in the same way as in Section 3 that

$$\overline{W(\xi^t)} = (\bar{a} + \bar{b}) \left(T_b(\bar{\xi}^t) + T_{b+u}(\bar{\xi}^t) \right) \text{ for } t \neq 0, p^n. \tag{10}$$

Lemma 13. *If* $a + b \equiv 0 \pmod 2$ *then* $p^n - p + 1 \leq LC(w^\infty) \leq p^n + 1$.

Proof. At the beginning we note that $W(x)(x + 1)(x^{p^n} - 1)$ is divided by $x^{p^n} - 1$ and $W(x)(x+1)(x^p - 1) = W(x)(x+1)(x^{p^n} + 1) - 2W(x)(x+1)$. Further, by (10) we see that $2W(\xi^t) = 0$ for $t = 1, 3, \ldots, 2p^n - 1$, $t \neq p^n$. Hence $2W(X)(x + 1) \equiv 0 \pmod{x^{p^n} + 1}$. It leads to the result that $LC(w^\infty) \leq p^n + 1$.

Let $W(x)C(x) \equiv 0 \pmod{x^{2p^n} - 1}$. Since $a + b \equiv 0 \pmod 2$, it follows that $W(\pm 1) \in \{1, -1\}$ and $C(x) = (x + 1)C_1(x)$. Then $2C_1(1) = 0$.

We consider two cases.

1. Let $a+b=4$. We can take $a=1$ without loss of generality. In this case,

$$W(\alpha^t)=\sum_{i\in\mathcal{C}_0^{(2p^n)}}\alpha^{ti}+3\sum_{i\in\mathcal{C}_1^{(2p^n)}}\alpha^{ti}+c\sum_{i\in\mathcal{C}_2^{(2p^n)}}\alpha^{ti}+d\sum_{i\in\mathcal{C}_3^{(2p^n)}}\alpha^{ti}+1+c.$$

Since $\mathcal{C}_0\cup\mathcal{C}_1=\{1,3,\ldots,2p^n-3,2p^n-1\}\setminus\{p^n\}$, it follows that

$$\sum_{i\in\mathcal{C}_0^{(2p^n)}}\alpha^{ti}+\sum_{i\in\mathcal{C}_1^{(2p^n)}}\alpha^{ti}+1=\sum_{i=0}^{p^n-1}\alpha^t=(\alpha^{p^nt}-1)/(\alpha^t-1)=0.$$

Thus, $W(\alpha^t)=2\widetilde{W}(\alpha^t)$ for $t=1,2,\ldots,p^n-1$, where

$$\widetilde{W}(\alpha^t)=\sum_{i\in\mathcal{C}_1^{(2p^n)}}\alpha^{ti}+\sum_{i\in\mathcal{C}_2^{(2p^n)}}+1 \text{ or } \widetilde{W}(\alpha^t)=\sum_{i\in\mathcal{C}_1^{(2p^n)}}\alpha^{ti}+\sum_{i\in\mathcal{C}_3^{(2p^n)}}\alpha^{ti}.$$

By Lemma 5, in any case $\overline{\widetilde{W}(\alpha^t)}\neq 0$ if $t\not\equiv 0 \pmod{p^{n-1}}$. Thus, $2C_1(\alpha^t)=0$ and $\deg C_1(x)\geq p^n-p$ and $\deg C(x)\geq p^n-p+1$.

2. Let $a+b=2$. In this case $c+d=4$. So, this case we can consider in the same way as the first case.

Putting everything together, we complete the proof of this statement.

□

Lemma 14. *If $a+b\not\equiv 0 \pmod 2$ then $LC(w^\infty)\geq 2p^n-2p$.*

Proof. Let $W(x)C(x)\equiv 0 \pmod{x^{2p^n}-1}$. According to (10) we obtain that $W(\alpha^t)\in GR^*(4^r,4)$ for $t\not\equiv 0 \pmod{p^{n-1}}$. Hence $C(\alpha^t)=0$ for $t=1,2,\ldots,p^n-1$, $t\not\equiv 0 \pmod{p^{n-1}}$.

Then, $C(x)$ is divided by $(x^{p^n}-1)/(x^p-1)$, i.e., $C(x)=(x^{p^n}-1)/(x^p-1)C_1(x)$. Thus, $W(x)(x^{p^n}-1)C_1(x)\equiv 0 \pmod{x^{2p^n}-1}$ or $W(x)C_1(x)\equiv 0 \pmod{x^{p^n}+1}$. Again, $W(\xi^t)\in GR^*(4^r,4)$ for $t\not\equiv 0 \pmod{p^{n-1}}$ and $C_1(\xi^t)=0$ for $t=1,3,\ldots,2p^n-1$, $t\not\equiv 0 \pmod{p^{n-1}}$. Therefore $C_1(x)$ is divided by $(x^{p^n}-1)/(x^p-1)$ and $\deg C(x)\geq 2p^n-2p$.

□

This lemma completes the proof of Theorem 12.

Acknowledgements

The authors wish to thank the anonymous reviewers for their very valuable comments that helped to improve the presentation and quality of this paper.

References

[1] Z. Chen and V. Edemskiy. Linear complexity of quaternary sequences over Z_4 derived from generalized cyclotomic classes modulo $2p$. *International Journal of Network Security*, 19 (4): 613–622, 2017.

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

[3] V. Edemskiy, C. Li, X. Zeng, T. Helleseth. The linear complexity of generalized cyclotomic binary sequences of period p^n. *Des. Codes Cryptography*, 87 (5): 1183-1197, 2019.

[4] V. Edemskiy, O. Antonova. The linear complexity of generalized cyclotomic sequences with period $2p^n$. *Appl. Algebra Eng. Commun. Comput.*, 25(3): 213-223, 2014.

[5] P. Ke , Y. Zhong, S. Zhang. Linear Complexity of a New Class of Quaternary Generalized Cyclotomic Sequence with Period $2p^m$. *Complexity*, 2020, Article ID 6538970, https://doi.org/10.1155/2020/6538970

[6] P. Ke, S. Zhang. New classes of quaternary cyclotomic sequence of length $2p^m$ with high linear complexity. *Information Processing Letters*, 112 (16): 646-650, 2012.

[7] L. Liu, X. Yang, B. Wei, L. Wu. A new class of quaternary generalized cyclotomic sequences of order $2d$ and length $2p^m$ with high linear complexity. *Int. J. of Wavelets, Multiresolution and Information Processing*, 16(1), Art. ID 1850006, 2018.

[8] Y. Ouyang, X. Xie. Linear complexity of generalized cyclotomic sequences of period $2p^m$. *Des. Codes Cryptography*, 87 (5): 1-12, 2019.

[9] P. Udaya, M. U. Siddiqi. Generalized GMW quadriphase sequences satisfying the Welch bound with equality, *Appl. Algebra Eng. Commun. Comput.*, 10 : 203-225, 2000.

[10] Z. X. Wan. *Finite Fields and Galois Rings*, Singapore. World Scientific Publisher, 2003.

[11] Z. Ye, P. Ke, C. Wu. A further study of the linear complexity of new binary cyclotomic sequence of length p^n. *Appl. Algebra Eng. Commun. Comput.*, 30 (3) 217-231, 2019.

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

[13] X. Zhou, X. Li, J. Xiao, Y. Tang, R. Abbasi, L. Xu. Linear complexity of generalized cyclotomic binary sequences of order 2 d and length $2p^m$. *Int. J. of Wavelets, Multiresolution and Information Processing*, 14 (5), Art. ID 1650040, 2016.

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

[15] J. Zhang, C.-A. Zhao, X. Ma. Linear complexity of generalized cyclotomic binary sequences of length $2p^m$. *Appl. Algebra Eng. Commun. Comput.*, 21 (2):93-108, 2010.