On the linear complexity of binary sequences derived from generalized cyclotomic classes modulo $2^n p^m$

VLADIMIR EDEMSKIY
Novgorod State University
Department of Applied Mathematics and Information Science
41 B. St. Petersburgskaya,
173003 Veliky Novgorod
RUSSIA
Vladimir.Edemsky@novsu.ru

CHENHUANG WU
Putian University
Provincial Key Laboratory of Applied Mathematics
1133 Xueyuan Middle Street,
351100 Putian
P. R. CHINA
ptuwch@163.com

Abstract: The linear complexity of a sequence is an important parameter in its evaluation as a keystream cipher for cryptographic applications. Using of cyclotomic classes to construct sequences is an important method for designing sequences with high linear complexity. In this article, we study the linear complexity of generalized cyclotomic binary sequences of length $2^n p^m$. These sequences were constructed from new generalized cyclotomic classed prepared by X. Zeng at el. We investigate discrete Fourier transform of these sequences and define the sufficient conditions for the existence of sequences with high linear complexity.

Key–Words: Binary sequences, linear complexity, cyclotomy, generalized cyclotomic sequence

1 Introduction

Cyclotomic and generalized cyclotomic classes are widely adopted in communication, coding and cryptography. They play an important role in the design of Hopping sequences, the construction of linear codes and the generation of key streams. In stream cipher, the typical examples are the Legendre sequences derived from cyclotomic classes modulo an odd prime and the Jacobi sequences derived from generalized cyclotomic classes modulo a product of two odd distinct primes. The generalized cyclotomic classes modulo a prime-power or modulo a double of a prime-power are also paid attention in the literature.

We mention here that, for an odd prime p, we find a family of binary sequences considered in [7] were defined from generalized cyclotomic classes modulo $2p^m$ for an integer $m \geq 1$. Later they were extended in [2, 3, 5]. Motivated by these, we will consider the binary sequences via new generalized cyclotomic classes modulo $2^n p^m$, which are defined in another way. In fact, the definition of the new generalized cyclotomic classes was studied in [9, 8] and is related to Fermat-Euler quotients [14]. In this paper we will study the linear complexity of the proposed sequences. The linear complexity of two families of sequences with period $2p^m$ was partly studied in [13] with another definition of sequences.

The linear complexity of a sequence is an important characteristic of its quality. The linear complexity L is the length of the shortest linear feedback shift register that is capable of generating the sequence [6]. Knowledge of just $2L$ consecutive digits of the sequence is sufficient to recover the remainder of the sequence. Thus, it is reasonable to suggest that a sequence of period N is 'good' if its linear complexity $L > N/2$ [1, 6].

We organize the work as follows. In Sect. 2, we propose the sequences via defining the new generalized cyclotomic classes modulo $2^n p^m$. In Sect. 3, we prove a lower bound on the linear complexity of the proposed sequences of period $2^n p^m$ for any $n > 0$. In Sect. 4, we determine the exact values of the linear complexity of the proposed sequences of period $2p^m$, i.e., the case of $n = 1$. Finally we draw a conclusion in Sect. 5.

2 The definition of the new sequences

We denote by $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ the ring of integers modulo N and by $\mathbb{Z}_N^*$ the multiplicative group consisting of all invertible elements in $\mathbb{Z}_N$, where N is a positive integer.

Throughout this paper, let p be an odd prime and $N = 2^n p^m$ for integers $n \geq 1$ and $m \geq 2$. We have the equivalence $\mathbb{Z}_N \cong \mathbb{Z}_{2^n} \times \mathbb{Z}_{p^m}$, which is relative to the isomorphism $\phi(a) = (a \bmod 2^n, a \bmod p^m)$ [4].

Now let $p = ef + 1$ for positive integers e and f

and let g be a primitive root modulo p^2. Then g is a primitive root modulo p^r for all $r \geq 1$, and hence the order of g modulo p^r is $\varphi(p^r) = p^{r-1}(p-1)$, where $\varphi(\cdot)$ is the Euler's totient function. Since

$$\mathbb{Z}_{p^m} = \mathbb{Z}^*_{p^m} \cup p\mathbb{Z}^*_{p^{m-1}} \cup p^2\mathbb{Z}^*_{p^{m-2}} \cup \cdots \cup p^{m-1}\mathbb{Z}^*_p \cup \{0\},$$

we define generalized cyclotomic classes for each $\mathbb{Z}^*_{p^r}$, where $1 \leq r \leq m$, in the following way

$$D_0^{(p^r,f)} \triangleq \langle g^{fp^{r-1}} \rangle = \{g^{kfp^{r-1}} \pmod{p^r} : 0 \leq k < e\}$$

and

$$D_l^{(p^r,f)} \triangleq g^l D_0^{(p^r,f)} = \{g^l \cdot g^{kfp^{r-1}} \pmod{p^r} : 0 \leq k < e\}, \ 1 \leq l < fp^{r-1}.$$

Indeed $D_0^{(p^r,f)}, D_1^{(p^r,f)}, \ldots, D_{fp^{r-1}-1}^{(p^r,f)}$ give a partition of $\mathbb{Z}^*_{p^r}$. We note that the definition is related to Fermat-Euler quotients if $f = 1$, see [10]. If f is even, we define for some integer b

$$\mathcal{B}_0^{(p^r)} = \bigcup_{i=0}^{p^{r-1}f/2-1} D_{i+b}^{(p^r)} \pmod{p^{r-1}f},$$

$$\mathcal{B}_1^{(p^r)} = \bigcup_{i=p^{r-1}f/2}^{p^{r-1}f-1} D_{i+b}^{(p^r)} \pmod{p^{r-1}f}, \quad (1)$$

which have been discussed in [8, 11, 12]. It is clear that $\mathbb{Z}^*_{p^r} = \mathcal{B}_0^{(p^r)} \cup \mathcal{B}_1^{(p^r)}$ and

$$|\mathcal{B}_0^{(p^r)}| = |\mathcal{B}_1^{(p^r)}| = |\mathbb{Z}^*_{p^r}|/2 = p^{r-1}(p-1)/2.$$

Then we select 2^n many subsets $\mathcal{C}_j \subseteq \mathbb{Z}_{p^m}$, $0 \leq j < 2^n$, defined as

$$\mathcal{C}_j = \mathcal{B}_{i_{j,m}}^{(p^m)} \cup p\mathcal{B}_{i_{j,m-1}}^{(p^{m-1})} \cup p^2\mathcal{B}_{i_{j,m-2}}^{(p^{m-2})} \cup \cdots \cup p^{m-1}\mathcal{B}_{i_{j,1}}^{(p)},$$

where $i_{j,1}, i_{j,2}, \ldots, i_{j,m} \in \{0,1\}$. We see that

$$\bigcup_{j=0}^{2^n-1} \{j\} \times \mathcal{C}_j \subseteq \mathbb{Z}_{2^n} \times \mathbb{Z}_{p^m}$$

and hence

$$\bigcup_{j=0}^{2^n-1} \phi^{-1}(\{j\} \times \mathcal{C}_j) \subseteq \mathbb{Z}_{2^n p^m}.$$

Now put

$$\mathcal{C} = \{0, 2p^m, \ldots, (2^n-2)p^m\} \cup \bigcup_{j=0}^{2^n-1} \phi^{-1}(\{j\} \times \mathcal{C}_j) \subseteq \mathbb{Z}_{2^n p^m},$$

which implies $|\mathcal{C}| = 2^{n-1}p^m = N/2$. Then we define a balanced binary sequence (s_u) of period $N = 2^n p^m$ in the following

$$s_u = \begin{cases} 1, & \text{if } u \pmod{N} \in \mathcal{C}, \\ 0, & \text{otherwise.} \end{cases} \quad (2)$$

Below we will consider the linear complexity of (s_u).

Let

$$\mathcal{S}(X) = s_0 + s_1 X + s_2 X^2 + \ldots + s_{N-1} X^{N-1},$$

which is in fact the generating polynomial of (s_u). Then by Eq.(2), we have

$$\mathcal{S}(X) = \sum_{j=0}^{2^{n-1}-1} X^{2jp^m} + \sum_{j=0}^{2^n-1} X^{\phi^{-1}(\{j\} \times \mathcal{C}_j)} = \sum_{j=0}^{2^{n-1}-1} X^{2jp^m} + \sum_{j=0}^{2^n-1} \sum_{r=1}^{m} X^{\phi^{-1}(\{j\} \times p^{m-r}\mathcal{B}_{i_{j,r}}^{(p^r)})}. \quad (3)$$

It is well known (see, for example [1]) that the linear complexity of (s_u), denoted by $L((s_u))$, can be computed by

$$L((s_u)) = N - \deg\big(\gcd(X^N - 1, \mathcal{S}(X))\big). \quad (4)$$

3 A lower bound on the linear complexity of (s_u) of length $2^n p^m$

In the case of $N = 2^n p^m$, we have

$$X^N - 1 = X^{2^n p^m} - 1 = \left(X^{p^m} - 1\right)^{2^n},$$

hence we only to consider the common divisor

$$\gcd(X^{p^m} - 1, \mathcal{S}(X))$$

in the ring $\overline{\mathbb{F}}_2[X]$, where $\overline{\mathbb{F}}_2$ is the split field of $\mathbb{F}_2$, So to compute the linear complexity of (s_u) by (4), it is sufficient to find the zeros of $\mathcal{S}(X)$ in the set $\{\alpha^v, v = 0, 1, \ldots, p^m - 1\}$, where $\alpha \in \overline{\mathbb{F}}_2$ is a p^m-th primitive root of unity.

We introduce the auxiliary polynomials for $r = 1, 2, \ldots, m$

$$T^{(r)}(X) = \sum_{w \in p^{m-r}\mathcal{B}_0^{(p^r)}} X^w.$$

In the sequel we always let $d_r = p^{r-1}f/2$.

Lemma 1 *Let $\mathcal{B}_0^{(p^r)}$ and $\mathcal{B}_1^{(p^r)}$ be defined as in Eq.(1) with $r \geq 1$ and even f. Then in $\mathbb{Z}_{p^m}$ we have*

$$\mathcal{B}_1^{(p^r)} = g^{p^{r-1}f/2}\mathcal{B}_0^{(p^r)} = g^{d_r}\mathcal{B}_0^{(p^r)}.$$

Lemma 2 *Let $\alpha \in \overline{\mathbb{F}}_2$ be a p^m-th primitive root of unity. Let $v \in \mathbb{Z}$ and $l \in \{0,1\}$. Then we have*

$$\sum_{u \in \phi^{-1}(\{j\} \times p^{m-r}\mathcal{B}_l^{(p^r)})} \alpha^{vu} = T^{(r)}(\alpha^{vg^{ld_r}})$$

for all $0 \le j \le 2^n - 1$ and $1 \le r \le m$.

Proof: From

$$\left\{ u \mod p^m \mid u \in \phi^{-1}\left(\{j\} \times p^{m-r}\mathcal{B}_l^{(p^r)}\right)\right\} = p^{m-r}\mathcal{B}_l^{(p^r)}$$

and $\mathcal{B}_l^{(p^r)} = g^{ld_r}\mathcal{B}_0^{(p^r)}$ by Lemma 1, we derive the desired result. □

Lemma 3 *Let $\alpha \in \overline{\mathbb{F}}_2$ be a p^m-th primitive root of unity. Let $v \in \mathbb{Z}$ with $p^h || v$ for some integer $0 \le h \le m-1$[1]. Then we have*

$$T^{(r)}(\alpha^v) + T^{(r)}(\alpha^{vg^{d_r}}) = \begin{cases} 1, & \text{if } h = r-1, \\ 0, & \text{otherwise,} \end{cases}$$

for $1 \le r \le m$.

Proof: Write $v = p^h v_1$ for some v_1 with $\gcd(v_1, p) = 1$. From the definition of $T^{(r)}(X)$ above, we have

$$T^{(r)}(\alpha^v) + T^{(r)}(\alpha^{vg^{d_r}}) = \sum_{w \in p^{m-r}\mathbb{Z}_{p^r}^*} \alpha^{vw} = \sum_{w \in \mathbb{Z}_{p^r}^*} \alpha^{v_1 w p^{m-r+h}}.$$

It is clear that

$$T^{(r)}(\alpha^v) + T^{(r)}(\alpha^{vg^{d_r}}) = |\mathbb{Z}_{p^r}^*| = p^{r-1}(p-1) = 0$$

if $h \ge r$. Now we consider the case $h < r$.

Case (1). If $r = 1$ then $h = 0$, we get that $\sum_{w \in \mathbb{Z}_p^*} \alpha^{v_1 w p^{m-1}} = 1$.

Case (2). If $r > 1$, we see that

$$\begin{aligned} &\sum_{j \in \mathbb{Z}_{p^r}^*} \alpha^{jp^{m-r+h}} \\ &= \sum_{j \in \mathbb{Z}_{p^r}} \alpha^{jp^{m-r+h}} - \sum_{j \in p\mathbb{Z}_{p^r}} \alpha^{jp^{m-r+h}} \\ &= \sum_{j \in \mathbb{Z}_{p^r}} \alpha^{jp^{m-r+h}} - \sum_{j \in \mathbb{Z}_{p^{r-1}}} \alpha^{jp^{m-r+h+1}} \\ &= \begin{cases} \frac{\alpha^{p^{m+h}}-1}{\alpha^{p^{m-r+h}}-1} - \frac{\alpha^{p^{m+h}}-1}{\alpha^{p^{m-r+h+1}}-1} = 0, \\ \quad \text{if } h < r-1, \\ \frac{\alpha^{p^{m+h}}-1}{\alpha^{p^{m-r+h}}-1} + 1 = 1, \\ \quad \text{if } h = r-1. \end{cases} \end{aligned}$$

[1] $p^h || v$ means that $p^h | v$ but $p^{h+1} \nmid v$.

We complete the proof. □

In Sect.2, we use the numbers $i_{j,1}, i_{j,2}, \ldots, i_{j,m} \in \{0,1\}$ to define $\mathcal{C}_j$ for $0 \le j \le 2^n - 1$. Now let

$$R = \left\{ 1 \le r \le m \,\middle|\, \sum_{j=0}^{2^n-1} i_{j,r} \equiv 1 \pmod 2 \right\},$$

$$R^* = \{1, \ldots, m\} \setminus R.$$

We have the following main result.

Theorem 4 *Let (s_u) be the binary sequence of period $2^n p^m$ defined by (2). Then its linear complexity $L((s_u))$ satisfies*

$$L((s_u)) \ge \begin{cases} 2^n p^m - \sum_{r \in R} 2^n p^{m-r}(p-1), & \text{if } n = 1, \\ \sum_{r \in R} 2^n p^{m-r}(p-1), & \text{if } n > 1. \end{cases}$$

Proof: Let $\alpha \in \overline{\mathbb{F}}_2$ be a p^m-th primitive root of unity and $v \in \{0, 1, \ldots, p^m - 1\}$. From the definition of the sequence (s_u) in (2), we have by Eq.(3) and Lemma 2

$$\mathcal{S}(\alpha^v) = 2^{n-1} + \sum_{j=0}^{2^n-1} \sum_{r=1}^{m} T^{(r)}(\alpha^{vg^{d_r \cdot i_{j,r}}}). \quad (5)$$

Due to the fact that $T^{(r)}(\alpha^{vg^{d_r \cdot i_{j_1,r}}}) + T^{(r)}(\alpha^{vg^{d_r \cdot i_{j_2,r}}}) = 0$ if $i_{j_1,r} = i_{j_2,r}$ for a fixed r, we derive from (5)

$$\mathcal{S}(\alpha^v) = 2^{n-1} + \sum_{r \in R} \left(T^{(r)}(\alpha^v) + T^{(r)}(\alpha^{vg^{d_r}}) \right)$$

by the choice of R. Now we check whether $\mathcal{S}(\alpha^v) = 0$ or not.

For $v \in \{1, 2, \ldots, p^m - 1\}$ and $r, r' \in \{1, 2, \ldots, m\}$, if $p^{r-1} || v$ we see that $T^{(r)}(\alpha^v) + T^{(r)}(\alpha^{vg^{d_r}}) = 1$ but $T^{(r')}(\alpha^v) + T^{(r')}(\alpha^{vg^{d_{r'}}}) = 0$ for $r' \ne r$ by Lemma 3. Then we have $\sum_{r \in R} p^{m-r}(p-1)$ many v such that

$$\sum_{r \in R} \left(T^{(r)}(\alpha^v) + T^{(r)}(\alpha^{vg^{d_r}}) \right) = 1$$

but $p^m - 1 - \sum_{r \in R} p^{m-r}(p-1)$ many v such that

$$\sum_{r \in R} \left(T^{(r)}(\alpha^v) + T^{(r)}(\alpha^{vg^{d_r}}) \right) = 0.$$

Hence when $n = 1$, we have $\sum_{r \in R} p^{m-r}(p-1)$ many v such that $\mathcal{S}(\alpha^v) = 0$. And when $n > 1$, we

have $p^m - 1 - \sum_{r\in R} p^{m-r}(p-1)$ many v such that $\mathcal{S}(\alpha^v) = 0$ and here $S(1) = 0$. Considering the multiplicity of the zeros of $\mathcal{S}(X)$, we prove the lower bound on the linear complexity. □

Corollary 5 *Let (s_u) be the binary sequence of period $2^n p^m$ defined by (2). If $R = \varnothing$ and $n = 1$, then $LC((s_u)) = 2p^m$. Also, if $R = \{1, 2, \dots, m\}$ and $n > 1$, then $LC((s_u)) \geq 2^n p^m - 2^n$.*

All sequences satisfying the conditions of Corollary 5 have high linear complexity. Moreover, if $\{i_{j,r}\}$ are such that $m \notin R$ for $n = 1$ then $\sum_{r\in R} p^r(p-1) \leq p^{m-1} - 1$ and

$$LC((s_u)) \geq 2^n p^m - 2^n p^{m-1}.$$

Also, if $m \in R$ for $n > 1$, then $\sum_{r\in R} p^r(p-1) \geq p^{m-1}(p-1)$ and

$$LC((s_u)) \geq 2^n p^{m-1}(p-1).$$

In both cases, we see that $L > N/2$.

For $n > 1$ we can refine the estimate of the linear complexity studying the multiplicity of the zeros α^v of $\mathcal{S}(X)$. For this purpose let us examine the formal derivative $\mathcal{S}'(X)$ of the polynomial $\mathcal{S}(X)$. Since

$$\left(\sum_{i\in\phi^{-1}(\{j\}\times\mathcal{B}_{i_{j,r}}^{(p^r)})} X^i \right)' = 0$$

when j is even, then

$$\mathcal{S}'(\alpha^v) = \alpha^{-v} \sum_{r=1}^{m} \sum_{t=0}^{2^{n-1}-1} \sum_{i\in\phi^{-1}(\{2t+1\}\times p^{m-r}\mathcal{B}_{i_{2t+1,r}}^{(p^r)})} \alpha^{vig^{d_r} i_{2t+1,r}}$$

or by Lemma 2

$$\mathcal{S}'(\alpha^v) = \alpha^{-v} \sum_{r=1}^{m} \sum_{t=0}^{2^{n-1}-1} T^{(r)}(\alpha^{vg^{d_r} i_{2t+1,r}}) \quad (6)$$

It is obvious from (6) that the analysis of $\mathcal{S}'(\alpha^v)$ substantially differs in cases $n = 1$ and $n > 1$.

Let $n > 1$ and let

$$J = \left\{ 1 \leq r \leq m \,\middle|\, \sum_{t=0}^{2^{n-1}-1} i_{2t+1,r} \equiv 1 \pmod 2 \right\},$$

$$J^* = \{1, \dots, m\} \setminus J.$$

Lemma 6 *If $n > 1$ and α^v is a zero of $S(X)$, then α^v is a multiple zero if and only if $v \in \bigcup_{r\in R^*\cap J^*} p^{r-1}\mathbb{Z}_{p^m}^*$.*

Proof: By Theorem 4 we see that if $v \in p^{r-1}\mathbb{Z}_{p^m}^*$ and $\mathcal{S}(\alpha^v) = 0$ then $r \in R^*$. Further, by (6) and the definition of J, we obtain

$$\mathcal{S}'(\alpha^v) = \alpha^{-v} \sum_{r\in J} \left(T^{(r)}(\alpha^v) + T^{(r)}(\alpha^{vg^{d_r}}) \right),$$

similar as in Theorem 4. Then by Lemma 3, it follows that $\mathcal{S}'(\alpha^v) = 0$ for $v \in p^{r-1}\mathbb{Z}_{p^m}^*$ if and only if $r \in J^*$. So, the statement of Lemma 6 follows from the latter note. □

From Theorem 4 and Lemma 6, we get the following bound:

$$LC((s_u)) \geq 2^n p^m - \sum_{r\in R^*\setminus J^*} p^{m-r}(p-1) - 2^n \sum_{r\in R^*\cap J^*} p^{m-r}(p-1) - 2^n.$$

Hence, if $n > 1$, then it is easy to find out for which $\{i_{j,r}\}$ the sequence (s_u) has high linear complexity.

4 Exact values of the linear complexity of (s_u) of length $2p^m$

In this section we determinate the exact values of the linear complexity of (s_u) of length $2p^m$ $(n = 1)$ under a number of conditions for p.

For $n = 1$ we have $R = \{r \mid i_{0,r} + i_{1,r} = 1, r = 1, \dots, m\}$. Further, by (6) we get that

$$S'(\alpha^v) = \alpha^{-v} \sum_{r=0}^{m-1} T^{(r)}(\alpha^{vg^{d_r} i_{1,r}}) \quad (7)$$

Let (w_u) be a binary sequence of length p^m defined by

$$w_u = \begin{cases} 1, & \text{if } i \pmod{p^n} \in \mathcal{C}_1, \\ 0, & \text{otherwise.} \end{cases}$$

Here

$$\mathcal{C}_1 = \mathcal{B}_{i_{1,m}}^{(p^m)} \cup p\mathcal{B}_{i_{1,m-1}}^{(p^{m-1})} \cup p^2\mathcal{B}_{i_{1,m-2}}^{(p^{m-2})} \cup \dots \cup p^{m-1}\mathcal{B}_{i_{1,1}}^{(p)}$$

as earlier. Then

$$\mathcal{S}_w(\alpha^v) = \sum_{r=1}^{m} T^{(r)}(\alpha^{vg^{d_r\cdot i_{1,r}}}). \quad (8)$$

and $\mathcal{S}_w(\alpha^v) = \alpha^v S'(\alpha^v)$ where $\mathcal{S}_w(X) = \sum_{i=0}^{p^m} w_i X^i$. So, in this case the values of $\mathcal{S}'(\alpha^v)$ can be studied in the same way that $\mathcal{S}_w(\alpha^v)$.

The linear complexity of the sequence (w_u) was studied in [12] under the condition that 2 is a primitive root modulo p^m and $2^{p-1} \not\equiv 1 \pmod{p^2}$. Here we consider a slightly more general case. We begin with some simple properties of $T^{(r)}(X)$ and $\mathcal{S}_w(X)$.

Lemma 7 *Let f be even and let $d_r = p^{r-1}f/2$, $r = 1, \dots, m$. Then:*
1) $T^{(r)}(\alpha^{g^{2d_r}}) = T^{(r)}(\alpha)$;
2) $T^{(r)}(\alpha^{g^{d_m}}) = T^{(r)}(\alpha^{g^{d_r}})$.

Proof: The first statement follows immediately from the definitions of the generalized cyclotomic classes, auxiliary polynomials and Lemma 2.

Further, since $g^{d_m - d_r} = g^{p^{r-1}(p^{m-r}-1)f/2}$, it follows that $g^{d_m} \equiv g^{d_r} \pmod{p^r}$ or $p^{m-r}g^{d_m} \equiv p^{m-r}g^{d_r} \pmod{p^m}$. To conclude the proof, it remains to note that $T^{(r)}(X) = \sum_{i \in p^{m-r}\mathcal{B}_0^{(p^r)}} X^i$. □

Lemma 8 *Let $v = 1, 2, \dots, p^m - 1$. Then*

$$\mathcal{S}_w(\alpha^v) + \mathcal{S}_w(\alpha^{vg^{d_m}}) = 1.$$

Proof: By (7) and Lemma 7 we have

$$\mathcal{S}_w(\alpha^{vg^{d_m}}) = \sum_{r=0}^{m-1} T^{(r)}(\alpha^{vg^{d_m}g^{d_r i_{1,r}}}) = \sum_{r=0}^{m-1} T^{(r)}(\alpha^{vg^{d_r}g^{d_r i_{1,r}}}).$$

So,

$$\mathcal{S}_w(\alpha^v) + \mathcal{S}_w(\alpha^{vg^{d_m}}) = \sum_{r=0}^{m-1} \left(T^{(r)}(\alpha^{vg^{d_r i_{1,r}}}) + T^{(r)}(\alpha^{vg^{d_r}g^{d_r i_{1,r}}}) \right).$$

The conclusion of this lemma then follows from Lemma 3. □

Let $\mathrm{ord}_p 2$ be the order of 2 modulo p. The following theorem is a goal of the section.

Theorem 9 *Let (s_u) be the binary sequence of period $N = 2p^m$ defined by (2). If $\gcd(\frac{p-1}{ord_p 2}, f)$ divides $f/2$, then we have*

$$LC((s_u)) = 2p^m - \sum_{r: i_{0,r} + i_{1,r} = 1} p^{m-r}(p-1).$$

Proof: To prove this theorem, it suffices to show $\mathcal{S}_w(\alpha^v) \neq 0, v = 1, 2, \dots, p^m - 1$ since $\mathcal{S}'(\alpha^v) = \mathcal{S}_w(\alpha^v)$.

Suppose there exists $v : \mathcal{S}_w(\alpha^v) = 0$. Denote $\frac{p-1}{\mathrm{ord}_p 2}$ by d. Then we see that $2 \equiv g^{td} \pmod{p}$ for $t : \gcd(t, p-1) = 1$. By the condition $\gcd(d, f)$ divides $f/2$. Hence $\gcd(td, f)$ also divides $f/2$. From this we can establish that there exist integers a, b such that $atd + bf = f/2$. Therefore, we can write $2^a \equiv g^{atd} \equiv g^{f/2 - bf} \pmod{p}$. Then we get that $2^{p^{m-1}a} \equiv g^{p^{m-1}f/2 - bp^{m-1}f} \pmod{p^m}$ or $2^{p^{m-1}a} \equiv g^{d_m - 2bd_m} \pmod{p^m}$. Since by Lemma 7

$$T^{(r)}(\alpha^v)^{2^{p^{m-1}a}} = T^{(r)}(\alpha^{v2^{p^{m-1}a}}) = T^{(r)}(\alpha^{vg^{d_m - 2bd_m}}) = T^{(r)}(\alpha^{vg^{d_m}}),$$

it follows that

$$0 = \mathcal{S}_w(\alpha^v)^{2^{p^{m-1}a}} = \mathcal{S}_w(\alpha^{vg^{d_m}}).$$

We obtain a contradiction with Lemma 8. □

If 2 is a primitive root modulo p^m then $\gcd(\frac{p-1}{\mathrm{ord}_p 2}, f) = 1$ and the condition of Theorem 9 is satisfied.

5 Conclusion

We studied the linear complexity of generalized cyclotomic binary sequences of length $2^n p^m$. These sequences are constructed by new generalized cyclotomic classed prepared by X. Zeng at el. We defined the sufficient conditions for the existence of sequences with high linear complexity. 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.

Acknowledgements: The reported study was funded by RFBR and NSFC according to the research project No. 19-51-53003. Chenhuang Wu was also supported by the National Natural Science Foundation of China under grant No. 61772292, by the Projects of International Cooperation and Exchanges NSFC No. 6181101289 and by the Fujian Provincial Natural Science Foundation of China under grant No. 2018J01425.

References:

[1] T. Cusick, C. Ding, and A. Renvall, *Stream ciphers and number theory*. N.-Holl. Math. Libr. vol.55, 1998.

[2] V. Edemskiy, O. Antonova, The linear complexity of generalized cyclotomic sequences with period $2p^n$. *AAECC*, vol. 25, iss. 3, pp. 213–223, 2014.

[3] V. Edemskiy, O. Antonova, Linear complexity of generalized cyclotomic sequences with period $2^m p^n$. *Applied Discrete Mathematics*, vol. 3, pp. 5–12, 2012 (in Russian).

[4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. Springer, 1982.

[5] P. Ke, J. Zhang, and S. Zhang, On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^m$. *Des. Codes Cryptogr.,* vol.67, no. 3, pp.325–339, 2013

[6] R. Lidl, H. Niederreiter, *Finite Fields.* Addison-Wesley, 1983.

[7] J. W. Zhang, C. A. Zhao, and X. Ma, Linear complexity of generalized cyclotomic binary sequences of length $2p^m$. *AAECC.,* vol. 21, pp. 93–108, 2010.

[8] Z. Xiao, X Zeng, C. Li, and T. Helleseth, New generalized cyclotomic binary sequences of period p^2. *Des. Codes Cryptogr*. DOI 10.1007/s10623-017-0408-7

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

[10] X. Du, Z. Chen, L. Hu., Linear complexity of binary sequences derived from Euler quotients with prime-power modulus. *Inform. Process. Lett.* 112 (2012) 604-609.

[11] V. Edemskiy, C. Li, X. Zeng and T. Helleseth, The linear complexity of generalized cyclotomic binary sequences of period p^n. *Designs, Codes and Cryptography*, 2018, 1-15, DOI: 10.1007/s10623-018-0513-2

[12] 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

[13] Y. Ouyang and X. Xianhong, Linear complexity of generalized cyclotomic sequences of period $2p^m$. Des. Codes Cryptogr. (2019), https://doi.org/10.1007/s10623-019-00638-5

[14] Z. Chen, V. Edemskiy, P. Ke and C. Wu, On k-error linear complexity of pseudorandom binary sequences derived from Euler quotients. *Advances in Mathematics of Communications*. Volume 12, No. 4, 2018, 805-816.