A note on a conjecture of new binary cyclotomic sequences of length $p^n$

Zhifan Ye$^{a,b}$, Pinhui Ke$^{b,*}$, Chenhuang Wu$^c$

$^a$Department of Mathematics and Physics, Fujian Jiangxia University, Fuzhou, Fujian, 350108, P. R. China
$^b$Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou, Fujian, 350117, P. R. China
$^c$School of Mathematics, Putian University, Putian, Fujian, 351100, P. R. China

Abstract

Recently, a conjecture on the linear complexity of a new class of generalized cyclotomic binary sequences of period $p^n$ were proposed by Z. Xiao et al. (Des. Codes Cryptogr. DOI 10.1007/s10623-017-0408-7). Later, for the case $f$ being the form $2^r$ with $r \geq 1$, Vladimir Edemskiy proved the conjecture (arXiv:1712.03947). In this paper, we first introduce a generic construction of $p^n$-periodic binary sequence based on the generalized cyclotomy, which admits a flexible support set and includes Xiao’s construction as a special case. Then, under the assumption of $2$ being a primitive root modulo $p^2$, the linear complexity of the new proposed sequence over GF(2) is determined by using the Euler quotient. As a byproduct, in the case of $2$ being a primitive root modulo $p^2$, the conjecture given by Z. Xiao et al. is proved to be correct for a general $f$.

Keywords: Linear complexity, generalized cyclotomy, binary sequence.

1. Introduction

Sequences with good pseudo-random properties are widely used in simulation, ranging systems, code-division multiple-access systems, and cryptographic applications such as stream ciphers [1, 2]. Linear complexity is one of the most important properties of a sequence for its applications in cryptography. The linear complexity $L((s_i))$ of an $N$-periodic sequence $(s_i)$ over a finite field $\mathbb{F}_q$ is the smallest positive integer $L$ for which there exist constants $c_0, c_1, \ldots, c_{L-1} \in \mathbb{F}_q$ such that $s_{i+L} = c_{L-1}s_{i+L-1} + \cdots + c_1s_{i+1} + c_0s_i$, for all $i \geq 0$ [2]. By the Berlekamp-Massey algorithm, for a sequence with period $N$, if its linear com-

*Corresponding author

Email addresses: yzffjnu@163.com (Zhifan Ye), keph@fjnu.edu.cn (Pinhui Ke), wuchenhuang2008@126.com (Chenhuang Wu)
plexity is large than $\frac{N}{2}$, then it is considered good with respect to the linear complexity $\frac{N}{2}$.

Blahut’s theorem is a common method to compute the linear complexity of a sequence. Let $(s_i)$ be an $N$-periodic sequence, then the generating polynomial of the sequence $(s_i)$ is defined as

$$S(x) = s_0 + s_1 x + \cdots + s_{N-1} x^{N-1}.$$  

Let $\alpha$ be a primitive $N$-th root of unity in an extension field of $\mathbb{F}_q$. Then by Blahut’s theorem, the linear complexity of sequence $(s_i)$ is defined as

$$L((s_i)) = N - |\{t | S(\alpha^t) = 0, t = 0, 1, \ldots, N - 1\}|.$$  

Thus, one could determine the linear complexity of a sequence $S$ by counting the number of roots of $S(x)$ in the set $\{\alpha^t | t = 0, 1, \ldots, N - 1\}$.

For an odd prime $p$, let $p = ef + 1$ and $g$ be a primitive root modulo $p^2$. It is well known that $g$ is also a primitive root modulo $p^j$ for each integer $j \geq 1$.

For an integer $j \geq 1$, define

$$D_n^{(p^r)} = \{g^{n+kfp^j} \mod p^j : 0 \leq k < e - 1\},$$

where $n = 0, 1, \ldots, p^{j-1}f - 1$. Then we get generalized cyclotomic classes of order $p^{j-1}f$ with respect to $p^j$. It was shown that $\{D_0^{(p^r)}, D_1^{(p^r)}, \ldots, D_{p^{j-1}f-1}^{(p^r)}\}$ forms a partition of $\mathbb{Z}_{p^j}$ in [4].

Recently, when $f = 2^r$ with $r \geq 1$, a new family of binary sequences $(s_i)$ of length $p^2$ were introduced by Xiao, Zeng, Li and Helleseth [5] via the aforementioned cyclotomic classes for the cases of $j = 1$ and 2, where

$$s_i = \begin{cases} 
1, & \text{if } i \in \bigcup_{j=0}^{2^r-1} pD_j^{(p^r)} \bigcup_{j=0}^{2^r-1} D_j^{(p^2)} \bigcup \{0\}; \\
0, & \text{otherwise.}
\end{cases}$$

In [5], Xiao et al. determined the linear complexity of the sequences and showed that the sequences have large linear complexity if $p$ is a non-Wieferich prime.

As it was remarked at the end of [5], it is natural to generalize above construction of new generalized cyclotomic sequences of period $p^2$ to the case of period $p^r$ for an odd prime $p$ and an integer $r \geq 3$ as follows. For $0 \leq i \leq p^r - 1$, let $b$ be an integer with $0 \leq b \leq p^{r-1}f - 1$, define

$$s_i = \begin{cases} 
1, & \text{if } i \in C_1; \\
0, & \text{otherwise,}
\end{cases}$$

where

$$C_1 = \bigcup_{j=1}^{r} \bigcup_{i=0}^{p^{r-1}j-1} p^{r-j}D^{(p^r)}_{i+b} (\text{mod } p^{r-1}f) \bigcup \{0\}.$$
For above sequence, the authors failed to determine the linear complexity by
the similar method in [5] and left a conjecture as follows.

**Conjecture** Let $p$ be a non-Wieferich odd prime and let $(s)$ be a general-
ized cyclotomic binary sequence of period $p^r$ defined by (1). Then its linear
complexity is given by

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

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

In [6], Vladimir Edemskiy proved the conjecture for the case $f$ being the
form $2^r$ with $r \leq 1$. In this paper, we will further study this problem. Different
from the method in [6], we will introduce a generic construction of generalized
cyclotomic binary sequence of period $p^r$, in which the generalized cyclotomic
classes could be chosen arbitrary as its support set. Thus, our generic con-
struction includes the sequence (1) as a special case. Then for the case 2 being
a primitive root modulo $p^2$, we will give an efficient method to determine the
linear complexity over GF(2) of the generalized cyclotomic binary sequence de-
erived from the generic construction by using Euler quotient. As a byproduct,
for the case 2 being a primitive root modulo $p^2$, the conjecture given by Z. Xiao
et al. is proved completely.

The remainder of this paper is organized as follows. In Section 2, we will
first introduce a generic construction of generalized cyclotomic binary sequence
of period $p^r$, which includes the construction in [8] as a special case. Then, we
will present our main theorem. The proof of the main result will be given in
Section 3. Firstly, we recall the definition of Euler quotients and its cyclotomic
characterization. We also establish the relationship between the generalized
cyclotomic classes derived from Euler quotients and the generalized cyclotomic
classes defined in [4]. Then some useful lemmas will be given. Lastly, by using
the Euler quotient, the main theorem will be proved and some example will be
illustrated.

2. A generic construction and main theorem

2.1. A generic construction

Let $p$ be an odd prime with $p = ef + 1$ and $r \geq 1$ be an integer. Denote $Y_t$
a subset of $\mathbb{Z}_{p^t-1} \times \mathbb{Z}_f$, i.e. $Y_t \subseteq \{(l, m) : l \in \mathbb{Z}_{p^t-1}, m \in \mathbb{Z}_f\}$, for $t = 1, \ldots, r$.
Define $X_t = \{l + mp^{t-1} : (l, m) \in Y_t\}$, and

$$C_1 = \bigcup_{i \in X_1} p^{r-1}D_1^{(p)} \bigcup_{i \in X_2} p^{r-2}D_1^{(p^2)} \bigcup_{i \in X_r} D_1^{(p^r)} \bigcup \{0\}.$$ 

Then a $p^r$-periodic sequence can be defined as follows

$$s_i = \begin{cases} 
1, & \text{if } i \in C_1; \\
0, & \text{otherwise.}
\end{cases}$$

(2)
Remark 1. Choosing \( Y_t = \mathbb{Z}_{p^{t-1}} \times \mathbb{Z}_p \) for \( t = 1, \ldots, r \), the sequence in \((2)\) is just the sequence defined in \((3)\). Thus the sequence defined in \((2)\) is a special case of the sequence in our generic construction. In the sequel, we denote \( D_{l+mp^{r-1}}^{(p^r)} \) by \( D_{(l,m)}^{(p^r)} \) for convenience.

2.2. Main theorem

For the sequence \((1)\), if \( f \) has the form of a power of 2, its linear complexity over \( \mathbb{GF}(2) \) was determined under the assumption of \( 2^{p-1} \not\equiv 1 \) mod \( p^2 \) in \([5, 6]\). However, for the linear complexity of the sequence in \((2)\), the situation will be very different, since in our generic construction, the support sets can be chosen arbitrary and \( f \) can be any positive divisor of \( p - 1 \), without the limitation of being a power of 2. For our purpose, we concentrate on the case of 2 being a primitive root modulo \( p \).

Following is the main result of this paper, based on which an efficient algorithm of computing the linear complexity of the sequence in \((2)\) could be easily deduced.

Theorem 1. (Main theorem) Let the sequence \( s \) defined as \((1)\), then the linear complexity of \( S \) over \( \mathbb{GF}(2) \), with 2 being a primitive root modulo \( p^2 \), can be represented as

\[
L((s)) = \delta + (p - 1) \sum_{i=0}^{r-1} \delta_i p^i,
\]

where

\[
\delta = \begin{cases} 
1, & \text{if } 2 | \sum_{j=1}^{r} |X_j|; \\
0, & \text{otherwise.}
\end{cases}
\]

and \( \delta_i \in \{0, 1\}, i = 0, \ldots, r - 1 \), which can be determined by the Lemma 6.

Remark 2. As we have remarked in Remark 1, the sequence \((1)\) can be constructed by choosing \( Y_t = \mathbb{Z}_{p^{t-1}} \times \mathbb{Z}_p \) for \( t = 1, \ldots, r \). In this case, \( \delta_i, i = 0, \ldots, r - 1 \) equal to 1 by Lemma 6. By definition,

\[
|X_j| = \frac{fp^j - 1}{2}, \quad \text{and} \quad \sum_{j=1}^{r} |X_j| = \frac{p^r - 1}{2}.
\]

Thus,

\[
L((s)) = \delta + (p - 1) \sum_{i=0}^{r-1} \delta_i p^i = \delta(p^r - 1) + p^r - 1 = p^r - \delta(p^r + 1).
\]

Hence, under the assumption of 2 being a primitive root modulo \( p^2 \), the conjecture is proved.
3. Proof of the Main Theorem and an Efficient Algorithm

In this section, we will prove the main theorem. To this end, we will recall the definition of Euler quotient and give some auxiliary lemmas firstly, based on which the main theorem can be easily proved. Two examples will also be given to illustrate the efficiency of our method.

3.1. Euler quotient and its cyclotomic characterization

For an odd prime $p$, an integer $r \geq 1$ and $u$ with $\gcd(u, p) = 1$, the Euler quotient $Q_{p^r}(u)$ modulo $p^r$ is defined as the unique integer with

$$Q_{p^r}(u) \equiv \frac{u^{\phi(p^r)} - 1}{p^r} \mod p^r, \quad 0 \leq Q_{p^r}(u) \leq p^r - 1,$$

where $\phi(\cdot)$ is the Euler function and it is also defined that $Q_{p^r}(kp) = 0$, $k \in \mathbb{Z}$.

The following properties are useful for the calculation of Euler quotient,

$$Q_{p^r}(u + kp^r) \equiv Q_{p^r}(u) - kp^r - 1 \mod p^r;$$
$$Q_{p^r}(uv) \equiv Q_{p^r}(u) + Q_{p^r}(v) \mod p^r;$$

for $\gcd(u, p) = 1$ and $\gcd(v, p) = 1$. A partition of $\mathbb{Z}_{p^r+1}^*$ is then induced by Euler quotient. In detail, let

$$\widetilde{D}_{l}(p^r + 1) = \{u : 0 \leq u \leq p^r + 1 - 1, \gcd(u, p) = 1, Q_{p^r}(u) = l\},$$

where $0 \leq l \leq p^r - 1$. Then, $\mathbb{Z}_{p^r+1}^* = \bigcup_{l=0}^{p^r-1} \widetilde{D}_{l}(p^r + 1)$. In [8], it is shown that $\widetilde{D}_{l}(p^r + 1)$ can also be represented as

$$\widetilde{D}_{l}(p^r + 1) = \{g^{1+kp^r} \mod p^{r+1} : 0 \leq k < p - 1\},$$

where $g$ is a primitive element modulo $p^{r+1}$ with $Q_{r}(g) = 1$. Meanwhile, $\widetilde{D}_{l}(p^{r+1})$ are also called generalized cyclotomic classes of order $p^r$ with respect to $p^{r+1}$.

Remark 3. Comparing with the generalized cyclotomic classes defined in [4, 5]

$$D_{n}(p^r) = \{g^{n+kfp^r-1} \mod p^r : 0 \leq k < e - 1\},$$

where $n = 0, 1, \ldots, p^{r-1}f - 1$, it is easy to see that

$$\widetilde{D}_{l}(p^r) = \bigcup_{m=0}^{f-1} D_{l+mp^r-1}^{(p^r)}.$$
Remark 4. Euler quotient has been used to construct sequence with high linear complexity. In [7], Chen et al. proposed a class of $p^2$-periodic binary sequences derived from the Euler quotients and investigated the $k$-error linear complexity, under the assumption of 2 being a primitive root modulo $p^2$ in [8]. Inspired by this construction, we proposed a general construction of binary sequences based on Euler quotient (and specially, Fermat quotient) with flexible support sets in [9, 10]. Then, Du et al. defined a class of $d$-ary sequence using the Euler quotient, which can be regarded as a generalization of the binary case, and then analyze the linear complexity of the proposed sequence [11]. For more details, please refer to above mentioned references and the references therein.

3.2. Auxiliary lemmas

Lemma 1.

(1) For any $n \geq 1$ and $0 \leq l \leq p^n - 1$, if $u \mod p^{n+1} \in D_{(l,m)}^{(p^{n+1})}$ for some $0 \leq l' \leq p^n - 1$, $0 \leq l' \leq f - 1$, we have

$$uD_{(l,m)}^{(p^{n+1})} = \{uv \mod p^{n+1} : v \in D_{(l,m)}^{(p^{n+1})} \} = D_{((l+l')p^n,(m+m'+\lfloor \frac{l'}{p^n}\rfloor))}^{(p^{n+1})}.$$

(2) For any $1 \leq n \leq n'$, $0 \leq l \leq p^n - 1$ and $0 \leq m \leq f - 1$, we have

$$D_{(l,m)}^{(p^{n+1})} \mod p^{n+1} = D_{(l,m)}^{(p^{n})} \mod p^n.$$

Specially,

$$D_{(l,m)}^{(p^{n})} \mod p = D_{(0,(l+m)_f)}^{(p)}.$$

Proof: Since

$$D_{(l,m)}^{(p^{n+1})} = \{g^{l+(kf+m)p^n} \mod p^{n+1} : 0 \leq k < e - 1\},$$

we have

$$uD_{(l,m)}^{(p^{n+1})} \mod p^n = \{g^{l+l'+(kf+m+m')p^n} \mod p^{n+1} : 0 \leq k < e - 1\}.$$

By the limitation of $l$ and $m$, we get the property (1). Similarly,

$$D_{(l,m)}^{(p^{n+1})} \mod p^{n+1} = \{g^{l+(kf+m)p^{n-1}} \mod p^{n+1} : 0 \leq k < e - 1\},$$

the result then follows. □

3.2. Auxiliary lemmas

Lemma 2. For any $0 \leq l, l' \leq p^n - 1$, if $a, a' \in D_{(l)}^{(p^n)}$ we have

$$D_{l}^{(p^n)}(\theta_n^a) = D_{l}^{(p^n)}(\theta_n^{a'}).$$
Proof: Assume \( u \in p^{r-n}D_{(l,m)}^{(n)} \), such that \( S(\theta^u_r) = 0 \), then we have \( S(\theta^u_r) = 0 \) for all \( u \in p^{r-n}D_{(l,m)}^{(n)} \) by Lemma 2. Since 2 is a primitive root modulo \( p \), we know 2 is a primitive root modulo \( p^n \) for any positive integer \( n \). Hence, \( 2^nD_{(l,m)}^{(n)} \) will run through \( \mathbb{Z}_p^n \) when \( a \) run through \( (p-1)p^{n-1} \). Since \( S(\theta^u_r)^{2^n} = S(\theta^{2^n u}_r) \) in \( GF(2) \), the result then follows. \( \square \)

**Lemma 4.** For any given integer \( v \) belong to \( D_{(l,m)}^{(p^{n+1})} \) and \( T_{(v,n)} = \{ v, v + p^n, v + 2p^n, \ldots, v + (p-1)p^n \} \), then we have
\[
T_{(v,n)} \cap D_{(l+ip^{n-1},(m-i)_f)}^{(p^{n+1})} = 1, \text{ for } i = 0, 1, \ldots, p-1.
\]
Furthermore, \( v \) could be selected with random from \( D_{(l+ip^{n-1},(m-i)_f)}^{(p^{n+1})} \), for \( i = 0, 1, \ldots, p-1 \).

Proof: From the property of Euler Quotient, we find \( Q_{p^n} (v + kp^n) \) run through \( l + ip^{n-1} \) for \( i = 0, 1, \ldots, p-1 \) when \( k \) run through \( i = 0, 1, \ldots, p-1 \). Therefore, we have
\[
T_{(v,n)} \cap D_{(l+ip^{n-1})}^{(p^{n+1})} = 1, \text{ for } i = 0, 1, \ldots, p-1.
\]
In addition, let \( T_{(v,n)} \cap D_{(l+ip^{n-1},(m-i)_f)}^{(p^{n+1})} \) exist in \( D_{(l+ip^{n-1},(m-i)_f)}^{(p^{n+1})} \), since
\[
v \equiv v + p^n \equiv \cdots \equiv v + (p-1)p^n \mod p,
\]
we have
\[
D_{(l+ip^{n-1},(m-i)_f)}^{(p^{n+1})} = D_{(0,(l+m_0)_f)}^{(p)} \mod p.
\]
Therefore,
\[
l + ip^{n-1} + m_i \equiv l + m_0 \mod f,
\]
that is,
\[
m_i + i \equiv m_0 \mod f.
\]
The result then follows. \( \square \)

**Lemma 5.** Let the symbol be the same as before, there exist \( Y \subseteq \mathbb{Z}_p^n \) such that
\[
\bigcup_{v \in Y} T_{(v,n)} = \bigcup_{(i,j) \in X_{n+1}} D_{(i,j)}^{(p^{n+1})},
\]
if and only if
\[
X_{n+1} = \bigcup_{(l,m) \in X} \{ (i,j) : (i,j) = (l + kp^{n-1}, (m-k)_f), k = 0, 1, \ldots, p-1 \},
\]
where \( X \) is a subset of \( \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_f \).
Proof: By Lemma 4, if $v \in D_{(l,m)}^{(p^n+1)}$ we have

$$T_{(v,n)} \subseteq \bigcup_{i=0}^{p-1} D_{(l+ip^n-1,(m-i)f)}^{(p^n+1)}.$$ 

Hence,

$$\bigcup_{v \in D_{(l,m)}^{(p^n+1)}} T_{(v,n)} \subseteq \bigcup_{i=0}^{p-1} D_{(l+ip^n-1,(m-i)f)}^{(p^n+1)}.$$ 

Note that $T_{(v,n)} \cap T_{(v',n)} = \emptyset$ for any $v \neq v' \in D_{(l,m)}^{(p^n+1)}$ and the size of two sets on both sides of above equation is equal to $ep$, so

$$\bigcup_{v \in D_{(l,m)}^{(p^n+1)}} T_{(v,n)} = \bigcup_{i=0}^{p-1} D_{(l+ip^n-1,(m-i)f)}^{(p^n+1)}.$$ 

Since at least one element of $T_{(v,n)}$ belongs to $\mathbb{Z}_{p^n}^*$, we can choose the $v$ from $\mathbb{Z}_{p^n}^*$ to construct $T_{(v,n)}$. Therefore, there exist $Y \subseteq \mathbb{Z}_{p^n}^*$ such that

$$\bigcup_{v \in Y} T_{(v,n)} = \bigcup_{i=0}^{p-1} D_{(l+ip^n-1,(m-i)f)}^{(p^n+1)}.$$ 

Based on $T_{(v,n)} \cap T_{(v',n)} = \emptyset$ for any $v \neq v' \in \mathbb{Z}_{p^n}^*$ and $D_{(i,j)}^{(p^n+1)} \cap D_{(i',j')}^{(p^n+1)}$ for any $(i, j) \neq (i', j') \in \mathbb{Z}_{p^n}^* \times \mathbb{Z}_f$, the set $X_{n+1}$ should be the union of some set $\bigcup_{i=0}^{p-1} D_{(l+ip^n-1,(m-i)f)}^{(p^n+1)}$. The result then follows. \hfill \Box

3.3. An important lemma

To determine the exact values of $\delta_i$, $i = 0, \ldots, r-1$ in the main theorem, we need the following lemma. In the sequel, we will consider the representation of $C_1$ modulo $p^n$ for different $n$. Hence, some elements will be repeated. Since we consider the sequence over GF(2), the occurrence number should modulo 2. For example, \{1, 3, 5\} mod 4 = \{3\} and \{1, 3, 5\} mod 2 = \{1\}. Due to $T_{(v,n)} = T_{(v+kp^n,n)} \mod p^{n+1}$ for any integer $k$, we denote $T_{(v,n)}$ only for $v \in \mathbb{Z}_{p^n}$ here and hereafter.

Lemma 6. Let symbols be the same as before. If 2 is a primitive root modulo $p$, then for any $n$, $0 \leq n \leq r-1$,

$$S(\theta^u) = 0, \text{ for all } u \in p^{r-n-1}\mathbb{Z}_{p^{n+1}},$$

if and only if

$$1 + \sum_{j>n} e|X_{r-j}| \equiv 1 \mod 2,$$
we have $p D^{(r-n)}_{(l,m)} \pmod{p^{n+1}} = T_{(0,n)} \setminus \{0\}$, and

$$X_{r-j} \pmod{f p^{n-j}} \bigcup_{w \in W} \{w + k f p^{n-j-1} : k = 0, 1, \ldots, p - 1\},$$

where $W$ is a subset of $\mathbb{Z}_{f p^{n-j-1}},$ for $j < n$.

Proof: Assume that $S(\theta^u_r) = 0$, for all $u \in p^{r-n_0-1} \mathbb{Z}_{p^{n_0+1}}^*$, for a fixed integer $n_0$, where $0 \leq n_0 \leq r - 1$. Since all $(\phi(p^{n_0+1})$ many) elements $\theta^u_r$ for $u \in p^{r-n_0} \mathbb{Z}_{p^{n_0+1}}^*$ are all roots of $\Phi_{p^{n_0}}(x) = 1 + x p^{n_0} + x^2 p^{n_0} + \ldots + x^{(n-1)} p^{n_0} \in F_2[x]$, we have $\Phi_{p^{n_0}}(x) \mid S(x)$ in an extension field of $\mathbb{F}_2$. Then there exists a polynomial $\Psi(x)$ over $\mathbb{F}_2$ such that

$$S(x) \equiv \Phi_{p^{n_0}}(x) \Psi(x) \pmod{x^{p^{n_0+1}} - 1}. \quad (3)$$

Note that

$$x^{p^{n_0}} \Phi_{p^{n_0}}(x) \equiv \Phi_{p^{n_0}}(x) \pmod{x^{p^{n_0+1}} - 1}.$$ We can restrict $\deg(\Psi(x)) < p^{n_0}$. Note that the exponents of $\Phi_{p^{n_0}}(x) \Psi(x)$ can be form as $\bigcup_{v \in U} T_{(v,n_0)}$ for some $U \subset \mathbb{Z}_{p^{n_0}}$. Therefore, the equation (2) holds if and only if there exist $U \subset \mathbb{Z}_{p^{n_0}}$, such that

$$C_1 \pmod{p^{n_0+1}} = \bigcup_{v \in U} T_{(v,n_0)}. \quad (4)$$

Then we need to consider the case of $j \leq n_0$. Note that the elements in $p^{r}D^{(r-j)}_{(l,m)} \pmod{p^{n_0+1}}$ only appear in the $T_{(v,n_0)}$ if $v \in p^{j} \mathbb{Z}_{p^{n_0-j}}$. By Lemma, we have $D^{(r-j)}_{(l,m)} \pmod{p^{n_0+1-j}} = D^{(p^{n_0+1-j})}_{((l,p^{n_0-j} : l / p^{n_0-j}))}$ for $j \leq n_0$. Therefore, we have

$$X_{r-j} \pmod{f p^{n_0-j}} = \bigcup_{(l,m) \in X} \{l + k p^{n_0-j} + (m-k) f p^{n_0-j} : k = 0, 1, \ldots, p - 1\}, \quad (5)$$

where $X$ is a subset of $\mathbb{Z}_{p^{n_0-j-1}} \times \mathbb{Z}_f$ based on Lemma 6. Note that the difference of adjacent element in the right set from above equation is $p^{n_0-j} - p^{n_0-j-1} \pmod{p^{n_0-j} f}$. Therefore, the difference will run through $k f p^{n_0-j-1} \pmod{p^{n_0-j} f}$ for $k = 0, 1, \ldots, p - 1$. Hence, we get

$$X_{r-j} \pmod{f p^{n_0-j}} = \bigcup_{w \in W} \{w + k f p^{n_0-j} : k = 0, 1, \ldots, p - 1\},$$

where $W$ is a subset of $\mathbb{Z}_{f p^{n_0-j-1}}$. In particular, the aforementioned condition is impossible to achieved when $j = n_0$. The closest case is

$$\bigcup_{(l,m) \in Y_{r-n_0}} p^{n_0} D^{(r-n_0)}_{(l,m)} \pmod{p^{n_0+1}} = T_{(0,n_0)} \setminus \{0\}.$$
If \( j > n_0 \), \( p^j D \left( \frac{p^r - 1}{(r,m)} \right) \mod p^{n_0 + 1} \) equals to \( \{0\} \) or \( \emptyset \). Hence,

\[
1 + \sum_{j > n_0} c_j X_{r-j} \equiv 1 \mod 2
\]

can make the case of \( j = n_0 \) to meet the equation \( \square \).

Thus, we complete the proof. \( \square \)

**Remark 5.** For \( i = 0, \ldots, r - 1 \), \( \delta_i = 1 \) is equivalent to \( S(\theta_r^u) = 0 \), for all \( u \in p^{r-i-1} \mathbb{Z}_{p^r+1} \). So by Lemma 6, for \( i = 0, \ldots, r - 1 \), \( \delta_i = 1 \) if and only if three conditions in Lemma 6 are satisfied simultaneously.

### 3.4. Proof of the main theorem

Now we are already to give a proof of the main theorem.

**Proof of the main theorem.** Based on Lemma 3, the linear complexity of the sequence \( S \) defined as (1) should be form as the representation in our main theorem. With repeated use of Lemma 6, we can get the exact value of \( \delta_i \). That is, if the condition of Lemma 6 is achieved, then \( \delta_i = 0 \). Otherwise \( \delta_i = 1 \). The value of \( \delta \) depends on \( S(1) \), i.e. the weight of the sequence. The result then follows. \( \square \)

**Remark 6.** If the condition in Lemma 6 is not satisfied for \( n = r \), then the linear complexity of the sequence defined in (1) is at least \((p-1)p^r\), which is larger than half of its period.

### 3.5. Examples

**Example 1.** Let \( p = 11 \), \( r = 2 \), \( e = 2 \), \( f = 5 \),

\[
X_1 = \{0, 1, 2, 3, 4\}, \quad X_2 = \{0, 1, \ldots, 24\}.
\]

Then

\[
X_2 \mod f = \{0, 1, 2, 3, 4\}
\]

Then condition in Lemma 6 is achieved when modula \( p \). Hence,

\[
L = 1 + (p - 1)p^2 = 111,
\]

and the balanced sequence \( (s_i) \) defined in (1) is

\[
[1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0,
0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0,
0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0,
1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0,
1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0].
\]

The linear complexity of this sequence is 111.
Example 2. Let \( p = 5, \ r = 3, \ e = 2, \ f = 2, \)

\[ X_1 = \{0, 1\}, \ X_2 = \{0, 2, 4, 6, 8\}, \ X_3 = \{0, 10, 20, 30, 40\}. \]

Then condition in Lemma 6 is achieved when modulo \( p^3 \). Hence,

\[ L = 1 + (p - 1)(1 + p) = 25, \]

and the sequence \((s_i)\) defined in (1) is

\[ [1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0]. \]

The linear complexity of this sequence is 25.

4. Conclusion

In this paper, we present a generic construction of binary sequences with period \( p^r \), which can be regarded as a generalization of the construction introduced by Xiao et al. By using the Euler quotient, we determined the linear complexity of the proposed sequence over GF(2) under the assumption of 2 being a primitive root of \( p^2 \). As a byproduct, we showed that a conjecture proposed by Xiao et al. holds for the case 2 being a primitive root of \( p^2 \). For the general case \( 2^{p-1} \neq 1 \mod p^2 \), Vladimir Edemskiy proved the conjecture when \( f \) is a power of 2. Hence, for the conjecture, it will be interesting to determine linear complexity of the sequence in the case of \( 2^{p-1} \neq 1 \mod p^2 \) but 2 not being a primitive root of \( p^2 \). That is, the order of 2 modulo \( p^2 \) has the form of \( pt \) with \( t \) being a proper factor of \( p - 1 \).

Acknowledgements

This work was supported by National Natural Science Foundation of China (No. 61772292, 61772476), Natural Science Foundation of Fujian Province (No.2015J01237), Fujian Normal University Innovative Research Team (No. IRTL1207).

References

[1] V. Tomasevic, S. Bojanic, O. Niteo-Taladriz. “Fiding an internal state of RC4 stream cipher,” Information Sciences. vol.177, pp. 1715-1727, 2007.

[2] G. Golomb, G. Gong. Signal designs with good correlations: For wireless communications, cryptography and radar applications, Cambridge, U.K.: Cambridge University Press, 2005.
[3] J. L. Massey. “Shift register synthesis and BCH decoding,” IEEE Trans. Inf. Theory, vol. 15, no. 1, pp. 122-127, 1969.

[4] X. Y. Zeng, H. Cai, X. H. Tang, Y. Yang. “Optimal frequency hopping sequences of odd length,” IEEE Trans. Inf. Theory, vol. 59, no. 5, pp. 3237-3248, 2013.

[5] Z. B. Xiao, X. Y. Zeng, C. L. Li, T. Helleseth. New generalized cyclotomic binary sequences of period p^2. Designs, Codes and Cryptography, https://doi.org/10.1007/s10623-017-0408-7., (2017)

[6] Vladimir Edemskiy. “The linear complexity of new binary cyclotomic sequences of period p^n”, ArXiv:1712.03947.

[7] Z. X. Chen, Z. H. Niu and C. H. Wu. “On the k-error linear complexity of binary sequences derived from polynomial quotients,” Science China-Inform. Sci. 58.9 (2015): 92107-092107.

[8] Z. X. Chen, X. N. Du and R. Marzouk. “Trace representation of pseudorandom binary sequences derived from Euler quotients,” Appl. Algebra Eng. Commun. Comput. vol.26, no.6, pp. 555-570, 2015.

[9] Z. F. Ye, P. H. Ke, S. Y. Zhang, Z. L. Chang. “Some Notes on Pseudorandom Binary Sequences Derived from Fermat-Euler quotients,” IEICE Trans. on Fundamentals, vol.98, no.10, pp. 2199-2202., 2015.

[10] Z. F. Ye, P. H. Ke, Z. X. Chen. ”Further results on pseudorandom binary sequences derived from Fermat-Euler quotients,” Information, Communications and Signal Processing (ICICS), 2015 10th International Conference on (pp. 1-4). IEEE.

[11] X. N. Du, Z. X. Chen and L. Hu. “Linear complexity of binary sequences derived from Euler quotients with prime-power modulus,” Inform. Process. Lett. vol. 112, pp.604-609, 2012.