# The linear complexity of new $q$-ary generalized cyclotomic sequences of period $p^n$

*Vladimir* Edemskiy[1,*] and *Nikita* Sokolovskiy[1]

[1]Novgorod State University, Veliky Novgorod, Russia

**Abstract.** In this paper, we study the linear complexity of new $q$-ary generalized cyclotomic sequences of length $p^n$ over the finite field of order $q$. We show that these sequences have the high linear complexity when $n \geq 2$. These sequences are constructed by new generalized cyclotomic classed prepared by X. Zeng at el.

## 1 Introduction

Linear complexity ($L$) is a very important merit factor for measuring unpredictability of pseudo-random sequences, which are often used as key stream sequences in stream ciphers. It is defined as the length of the shortest linear feedback shift register that can generate the sequence [7]. According to the Berlekamp-Massey algorithm [11], the whole sequences can be deduced from the knowledge of just $2L$ consecutive digits of the sequence. Thus, it is reasonable to suggest that a "good" sequence should satisfy $L > N/2$ (where $N$ denotes the period of the sequence) from the viewpoint of cryptography [11].

Cyclotomy is an old topic of elementary number theory and is related to difference sets, sequences, coding theory and cryptography. Using classical cyclotomic classes and generalized cyclotomic classes to construct sequences, which are called classical cyclotomic sequences and generalized cyclotomic sequences, respectively, is an important method for sequence design [2]. There are a lot of papers devoted to studying the linear complexity of cyclotomic sequences and generalized cyclotomic sequences. In particular, in recent years there has been some research on generalized cyclotomic binary and non-binary sequences of period $p^n$ [1, 3–5, 10, 13, 15] (see also references therein).

Based on the generalized cyclotomic classes in [17], Xiao et al. presented a new family of cyclotomic binary sequences of period $p^n$. The linear complexity of these sequences was studied in [6, 14, 16]. In this paper, we generalize the construction from [6] and study the linear complexity of new $q$-ary generalized cyclotomic sequences of period $p^n$ over a finite field of $q$ elements.

## 2 Preliminaries

First of all, we will recall some basics of the linear complexity of a periodic sequence, the definition of new generalized cyclotomic classes from [17] and consider the generalization of binary cyclotomic sequences proposed in [14].

### 2.1 Linear Complexity

Let $s^\infty = (s_0, s_1, s_2, \dots)$ be a sequence of period $N$ 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 $s^\infty$ is given by

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

Thus, we can examine the roots of $S(x)$ in an extension of $\mathbb{F}_q$ (the finite field of $q$ elements) to determine the linear complexity of $s^\infty$ by the above formula. More specifically, by Blahut's theorem the linear complexity of $s^\infty$ can be given by

$$L = N - \Big|\big\{i \in \mathbb{Z}_N \,|\, S(\beta^i) = 0\big\}\Big|, \tag{1}$$

where $\beta$ is a primitive $N$-th root of unity in an extension field of $\mathbb{F}_q$ and $\mathbb{Z}_N$ is the ring of integers modulo $N$ for a positive integer $N$. Hence, we will study the discrete Fourier transform of the sequence.

### 2.2 New $q$-ary Generalized Cyclotomic Sequences

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 order of $g$ modulo $p^j$ is equal to $\varphi(p^j) = p^{j-1}(p-1)$, where $\varphi(\cdot)$ is the Euler's totient function [9]. Below we recall the definition of the new generalized cyclotomic classes introduced in [17].

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

$$D_0^{(p^j)} = \Big\{g^{t\cdot d_j} \ (\mathrm{mod}\, p^j) \,|\, 0 \leq t < e\Big\}, \text{ and}$$
$$D_i^{(p^j)} = g^i D_0^{(p^j)} = \Big\{g^i x \ (\mathrm{mod}\, p^j) : x \in D_0^{(p^j)}\Big\}, \quad 1 \leq i < d_j. \tag{2}$$

*e-mail: Vladimir.Edemsky@novsu.ru. The reported study was funded by RFBR and NSFC according to the research project No 19-55-53003.

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 [17] that $\left\{D_0^{(p^j)}, D_1^{(p^j)}, \ldots, D_{d_j-1}^{(p^j)}\right\}$ forms a partition of the multiplicative group $\mathbb{Z}_{p^j}^*$ for each integer $j \geq 1$ and for an integer $m \geq 1$,

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

The linear complexity of family of almost balanced binary sequences based on the above generalized cyclotomic classes was studied in [6, 14], when $f$ is an even integer. We can generalize this construction and consider $q$-ary sequences, where $q > 2$ is a prime.

Let $q$ be an odd prime and $q|f$ and let $b$ be an integer with $0 \leq b < p^{n-1}f$. Denote $d_j/q = p^{j-1}f/q$ by $h_j$ and define $q$ sets $H_0^{(p^j)} = \bigcup_{i=0}^{h_j-1} D^{(p^j)}_{(i+b) \pmod{d_j}}$, $H_1^{(p^j)} = \bigcup_{i=h_j}^{2h_j-1} D^{(p^j)}_{(i+b) \pmod{d_j}}$, $\ldots, H_{q-1}^{(p^j)} = \bigcup_{i=(q-1)h_j}^{qh_j-1} D^{(p^j)}_{(i+b) \pmod{d_j}}$ and

$$\mathscr{C}_k^{(p^n)} = \bigcup_{j=1}^{n} p^{n-j} H_k^{(p^j)}, \ k = 0,1,\ldots,q-1.$$

It is clear that $\mathbb{Z}_{p^n} = \mathscr{C}_0^{(p^n)} \cup \mathscr{C}_1^{(p^n)} \cup \cdots \cup \mathscr{C}_{q-1}^{(p^n)} \cup \{0\}$ and $|\mathscr{C}_j^{(p^n)}| = (p^n-1)/q$. A family of almost balanced $q$-ary sequences $s^\infty = (s_0, s_1, s_2, \ldots)$ of period $p^n$ can thus be defined as

$$s_i = \begin{cases} 0, & \text{if } i \pmod{p^n} \in \mathscr{C}_0^{(p^n)} \cup \{0\}, \\ k, & \text{if } i \pmod{p^n} \in \mathscr{C}_k^{(p^n)}. \end{cases} \tag{3}$$

In this paper we will study the linear complexity of these sequences over $\mathbb{F}_q$. In the particular case when $n = 1$, $q = f$ the linear complexity of this sequence was studied in [8].

## 3 Linear complexity of sequences

First of all, we investigate the linear complexity of $s^\infty$ defined in (3) for $p$ such that $q^{p-1} \not\equiv 1 \pmod{p^2}$. By [12] such $p$ is not frequent. If $2^{p-1} \not\equiv 1 \pmod{p^2}$ then $p$ is called Wieferich prime.

### 3.1 Main Result

This subsection will investigate the linear complexity of $s^\infty$ defined in (3) for some integers $f$ such that $q|f$. The main result of this paper is given as follows.

**Theorem 1** *Let $p = ef+1$ be an odd prime with $q^{p-1} \not\equiv 1 \pmod{p^2}$ and $q$ divides $f$. Let $s^\infty$ be a generalized cyclotomic $q$-ary sequence of period $p^n$ defined in* (3)*. Let $\mathrm{ord}_p(q)$ denote the order of $q$ modulo $p$ and $v = \gcd\left(\frac{p-1}{\mathrm{ord}_p(q)}, f\right)$. Then the linear complexity of $s^\infty$ over $GF(q)$ is given by*

$$L = p^n - r \cdot \mathrm{ord}_p(q) - 1, \quad 0 \leq r \leq \frac{p-1}{q\mathrm{ord}_p(q)}.$$

*Furthermore,*

$$L = \begin{cases} p^n - \frac{p-1}{q} - 1, & \text{if } v = f; \\ p^n - 1, & \text{if } v | \frac{f}{2}, \text{ or } v = 2 \text{ and } v \neq f. \end{cases}$$

Below we make some preparations for the proof of the main theorem.

### 3.2 Subsidiary lemmas

Let $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$ and $\alpha_n \in \overline{\mathbb{F}}_q$ be a primitive $p^n$-th root of unity. Denote $\alpha_j = \alpha_n^{p^{n-j}}$, $j = 1,2\ldots,n-1$. Then $\alpha_j$ is a primitive $p^j$-th root of unity in an extension of the field $\mathbb{F}_q$. As usual, we denote by $\mathbb{F}_q(\alpha_j)$ a simple extension of $\mathbb{F}_q$ obtained by adjoining an algebraic element $\alpha_j$ [11]. The dimension of the vector space $\mathbb{F}_q(\alpha_j)$ over $\mathbb{F}_q$ is called the degree of $\mathbb{F}_q(\alpha_j)$ over $\mathbb{F}_q$, in symbols $[\mathbb{F}_q(\alpha_j) : \mathbb{F}_q]$.

The following statement we can prove similar to Lemmas 1-3 from [6]

**Lemma 2** *Let $p$ be a prime such that $q^{p-1} \not\equiv 1 \pmod{p^2}$.*

1. *If $q \equiv g^u \pmod{p^2}$ for some integer $u$ then $\gcd(u,p) = 1$.*
2. *Let $\tau = \mathrm{ord}_p(q)$ be the order of $q$ modulo $p$. Then the order of $q$ modulo $p^j$ for an integer $j \geq 1$ is $\tau p^{j-1}$.*
3. *$[\mathbb{F}_q(\alpha_{j+1}) : \mathbb{F}_q(\alpha_j)] = p, \quad j = 1,2,\cdots,n-1$, where $\alpha_j = \alpha_n^{p^{n-j}}$ and $\alpha_n$ is a primitive $p^n$-th root of unity.*

The following properties of the generalized cyclotomic classes discussed in [6].

**Lemma 3** *[6] For $D_i^{(p^j)}$ defined as in* (2)*, we have*
*(i) $aD_i^{(p^j)} = D^{(p^j)}_{i+k \pmod{d_j}}$ for $a \in D_k^{(p^j)}$; and*
*(ii) $D_i^{(p^j)} \pmod{p^l} = D^{(p^l)}_{i \pmod{d_l}}$ for $1 \leq l \leq j$.*

The above auxiliary lemmas will be heavily used in our investigation of the linear complexity of $s^\infty$ in the next subsection.

### 3.3 Polynomial Sequences Properties

Before we start with the proof of Theorem 1, we need to introduce some polynomials derived from the sequence $s^\infty$ and investigate their properties.

Let $S(x) = s_0 + s_1 x + \cdots + s_{p^n-1}x^{p^n-1}$ for the generalized cyclotomic sequences $s^\infty$ defined in (3) . Then,

$$\begin{aligned} S(x) &= \sum_{i=0}^{p^n-1} s_i x^i = \sum_{l=0}^{q-1} l \sum_{t \in \mathscr{C}_l^{(p^n)}} x^t \\ &= \sum_{l=0}^{q-1} l \sum_{j=1}^{n} \sum_{i=lh_j}^{(l+1)h_j-1} \sum_{t \in D^{(p^j)}_{i+b \pmod{d_j}}} x^{p^{n-j}t}. \end{aligned} \tag{4}$$

For convenience of presentation, we define polynomials

$$E_i^{(p^j)}(x) = \sum_{t \in D_i^{(p^j)}} x^t, \quad 1 \le j \le n, 0 \le i < d_j, \tag{5}$$

and

$$\begin{aligned} G_k^{(p^j)}(x) &= \sum_{l=0}^{q-1} l \sum_{i=lh_j}^{lh_j+h_j-1} E_{i+k \pmod{d_j}}^{(p^j)}(x), \quad 0 \le k < d_j, \\ F_k^{(p^m)}(x) &= \sum_{j=1}^{m} G_k^{(p^j)}(x^{p^{m-j}}), \quad m = 1, 2, \cdots, n. \end{aligned} \tag{6}$$

Notice that the subscripts $i$ in $D_i^{(p^j)}$, $G_i^{(p^j)}(x)$ and $F_i^{(p^j)}(x)$ 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.

Since $\alpha_m$ is a $p^m$-th primitive root of unity, it follows that $1 + \alpha_m + \alpha_m^2 + \cdots + \alpha_m^p + \cdots + \alpha_m^{p^m-1} = 0$. Hence

$$\sum_{j=1}^{m} \sum_{i=0}^{d_j-1} E_i^{(p^j)}(\alpha_m^{p^{m-j}}) = -1 \tag{7}$$

It can be easily seen from (4) - (6) that $S(x) = F_b^{(p^n)}(x)$. By (1) the linear complexity of $s^\infty$ in (3) can thus be given by

$$L = N - \left| \left\{ i \in \mathbb{Z}_{p^n} \mid F_b^{(p^n)}(\alpha_n^i) = 0 \right\} \right|. \tag{8}$$

In the following we shall study the value of $F_b^{(p^n)}(\alpha_n^i)$ when $i$ belongs to $\mathbb{Z}_{p^n}$.

From the definitions in (5) and (6), the polynomial $F_b^{(p^n)}(x)$ depends on the polynomials $E_i^{(p^j)}(x)$ and $G_i^{(p^j)}(x)$ for $1 \le j \le n$ and $0 \le i < d_j$. Some basic properties of these polynomials are given in the following lemma.

**Lemma 4** *Let $\alpha_j = \alpha_n^{p^{n-j}}$, $1 \le j \le n$, be a $p^j$-th primitive root of unity. Given any element $a \in D_k^{(p^j)}$, we have*
*(i) $E_i^{(p^j)}(\alpha_j^{p^l a}) = E_{i+k}^{(p^{j-l})}(\alpha_{j-l})$ and $G_i^{(p^j)}(\alpha_j^{p^l a}) = G_{i+k}^{(p^{j-l})}(\alpha_{j-l})$ for $0 \le l < j$; and*
*(ii) $E_i^{(p^j)}(\alpha_j^{p^l a}) = e \pmod q$ and $G_i^{(p^j)}(\alpha_j^{p^l a}) = 0$ for $l \ge j$.*

The proof of this lemma is similar to the proof of Lemma 6 from [6].

The following proposition characterizes some properties of $F_i^{(p^m)}(x)$ for $1 \le m \le n$.

**Proposition 1** *For any $a \in D_k^{(p^j)}$, we have*
*(i) $F_i^{(p^m)}(\alpha_m^{p^l a}) = F_{i+k}^{(p^{m-l})}(\alpha_{m-l})$ for $0 \le l < m$; and*
*(ii) $F_{i+h_m}^{(p^m)}(\alpha_m^a) = F_i^{(p^m)}(\alpha_m^a) + 1$, where $h_m = p^{m-1} f/q$.*

Proof. (i) From the definition in (6), Lemma 3 and Lemma 4, it follows that

$$\begin{aligned} F_i^{(p^m)}(\alpha_m^{p^l a}) &= \sum_{j=1}^{m} G_i^{(p^j)}\left(\alpha_m^{p^{m-j+l}a}\right) = \sum_{j=l+1}^{m} G_i^{(p^j)}\left(\alpha_{j-l}^a\right) \\ &+ \sum_{j=1}^{l} G_i^{(p^j)}(1) = \sum_{j=l+1}^{m} G_{i+k}^{(p^{j-l})}\left(\alpha_{j-l}\right) = \sum_{j=1}^{m-l} G_{i+k}^{(p^j)}\left(\alpha_j\right). \end{aligned}$$

Similarly we have

$$F_{i+k}^{(p^{m-l})}(\alpha_{m-l}) = \sum_{j=1}^{m-l} G_{i+k}^{(p^j)}\left(\alpha_{m-l}^{p^{m-l-j}}\right) = \sum_{j=1}^{m-l} G_{i+k}^{(p^j)}\left(\alpha_j\right).$$

The desired result thus follows.

(ii) By definition we see that

$$F_i^{(p^m)}(\alpha_m^a) = \sum_{j=1}^{m} \sum_{l=0}^{q-1} l \sum_{k=lh_j}^{lh_j+h_j-1} E_{i+k}^{(p^j)}(\alpha_m^{ap^{m-j}}).$$

Further,

$$\begin{aligned} l \sum_{k=lh_j}^{lh_j+h_j-1} E_{i+k+h_j}^{(p^j)}(\alpha_m^{ap^{m-j}}) + \sum_{k=lh_j}^{lh_j+h_j-1} E_{i+k+h_j}^{(p^j)}(\alpha_m^{ap^{m-j}}) \\ = (l+1) \sum_{t=(l+1)h_j}^{(l+1)h_j+h_j-1} E_{i+t}^{(p^j)}(\alpha_m^{ap^{m-j}}), \end{aligned}$$

We see that $h_m \equiv h_j \pmod{d_j}$. Hence

$$F_{i+h_m}^{(p^m)}(\alpha_m^a) + \sum_{j=1}^{m} \sum_{l=0}^{q-1} \sum_{k=lh_j}^{lh_j+h_j-1} E_{i+k+h_j}^{(p^j)}(\alpha_m^{ap^{m-j}}) = F_i^{(p^m)}(\alpha_m^a).$$

By (7) we have

$$\sum_{j=1}^{m} \sum_{l=0}^{q-1} \sum_{k=lh_j}^{lh_j+h_j-1} E_{i+k+h_j}^{(p^j)}(\alpha_m^{ap^{m-j}}) = \sum_{j=1}^{m} \sum_{i=0}^{d_j-1} E_i^{(p^j)}(\alpha_j^{p^{m-j}}) = -1$$

then we obtain that $F_{i+h_m}^{(p^m)}(\alpha_m^a) - 1 = F_i^{(p^m)}(\alpha_m^a)$.

**Corollary 5** *$F_{i+kh_m}^{(p^m)}(\alpha_m^a) = F_i^{(p^m)}(\alpha_m^a) + k$ for $k = 1, 2, q-1$.*

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

**Proposition 2** *Let $q : \quad q^{p-1} \not\equiv 1 \pmod{p^2}$. Then $F_b^{(p^n)}(\alpha_n^i) \ne 0$ for $i : \quad i \not\equiv 0 \pmod{p^{n-1}}$.*

Proof. We will show $F_b^{(p^n)}(\alpha_n^i) \ne 0$ by contradiction. Suppose there exists an integer $i_0 \in \mathbb{Z}_{p^n} \setminus p^{n-1}\mathbb{Z}_p$ such that $F_b^{(p^n)}(\alpha_n^{i_0}) \in \{0, 1\}$. Without loss of generality, we can assume $F_0^{(p^m)}(\alpha_m) = 0$ for $m > 1$.

Suppose $q \equiv g^u \pmod{p^m}$ for some integer $u$. By Lemma 2 $u \not\equiv 0 \pmod{p}$. Letting $u_1 \equiv u \pmod{d_m}$, we have $q \in D_{u_1}^{(p^m)}$ and $u_1 \ne 0$. It then follows from Proposition 1 (i) and from properties of $\mathbb{F}_q$ that

$$F_0^{(p^m)}(\alpha_m) = \left(F_0^{(p^m)}(\alpha_m)\right)^q = F_0^{(p^m)}(\alpha_m^q) = F_{u_1}^{(p^m)}(\alpha_m),$$

which implies $F_0^{(p^m)}(\alpha_m) = F_{iu_1}^{(p^m)}(\alpha_m) = 0$ for any integer $i \ge 1$.

Denote $v = \gcd(u_1, d_m)$. Since the subscript of $F_i^{(p^m)}(x)$ is taken modulo $d_m$, it is easily seen that

$$0 = F_0^{(p^m)}(\alpha_m) = F_{iv}^{(p^m)}(\alpha_m), \quad i = 1, \cdots, d_m/v - 1. \tag{9}$$

By Proposition 1 (ii) we have $F^{(p^m)}_{d_m/q}(\alpha_m) = F^{(p^m)}_0(\alpha_m) + 1$, whence $F^{(p^m)}_{d_m/q}(\alpha_m) = 1$. Thus $v$ does not divide $d_m/q$. Since $v = \gcd(u_1, d_m) = \gcd(u, d_m)$ and $\gcd(u,p) = 1$ (by Lemma 2), it follows that $v$ divides $f$ but does not divide $f/q$. A similar argument as in (9) gives

$$1 = F^{(p^m)}_{d_m/q}(\alpha_m) = F^{(p^m)}_{d_m/q+if}(\alpha_m) \quad i = 1, \cdots, d_m/v - 1,$$

which implies $F^{(p^m)}_{f/q}(\alpha_m) = F^{(p^m)}_{d_m/q+f(p^{m-1}+1)/q}(\alpha_m) = 1$. Hence we have

$$F^{(p^m)}_0(\alpha_m) - F^{(p^m)}_{f/q}(\alpha_m) = -1.$$

Denote $\xi = G^{(p^m)}_0(\alpha_m) - G^{(p^m)}_{f/q}(\alpha_m)$. Since

$$F^{(p^m)}_0(\alpha_m) - F^{(p^m)}_{f/q}(\alpha_m) = \sum_{j=1}^{m} \left( G^{(p^j)}_0(\alpha_m^{p^{m-j}}) - G^{(p^j)}_{f/q}(\alpha_m^{p^{m-j}}) \right),$$

it follows that

$$\xi = -1 - \sum_{j=1}^{m-1} \left( G^{(p^j)}_0(\alpha_{m-1}^{p^{m-1-j}}) - G^{(p^j)}_{f/q}(\alpha_{m-1}^{p^{m-1-j}}) \right) \in \mathbb{F}_q(\alpha_{m-1}).$$

On the other hand, by eliminating the overlapping terms in $G^{(p^m)}_0(\alpha_m)$ and $G^{(p^m)}_{f/q}(\alpha_m)$ we obtain

$$\begin{aligned}
&\xi = G^{(p^m)}_0(\alpha_m) - G^{(p^m)}_{f/q}(\alpha_m) \\
&= \sum_{l=0}^{q-1} l \sum_{i=lh_m}^{lh_m+h_m-1} E^{(p^j)}_i(\alpha_m) - \sum_{l=0}^{q-1} l \sum_{i=lh_m}^{lh_m+h_m-1} E^{(p^j)}_{i+f/q}(\alpha_m) \\
&= \sum_{l=0}^{q-1} \left( E^{(p^j)}_{lh_m}(\alpha_m) + E^{(p^j)}_{lh_m+1}(\alpha_m) + \cdots + E^{(p^j)}_{lh_m+f/q-1}(\alpha_m) \right) \\
&= \sum_{t \in \mathscr{D}} \alpha_m^t,
\end{aligned}$$

where $\mathscr{D} = D^{(p^m)}_0 \cup \cdots \cup D^{(p^m)}_{f/q-1} \cup D^{(p^m)}_{d_m/q} \cup \cdots \cup D^{(p^m)}_{d_m/q+f/q-1} \cup \cdots \cup D^{(p^m)}_{(q-1)d_m/q} \cup \cdots \cup D^{(p^m)}_{(q-1)d_m/q+f/q-1}$. We recall that $h_m = d_m/q$. Observe that $ld_m/q \equiv lf/q \pmod f$ for $l = 0, 1 \ldots, q-1$ and $m > 1$ we see that $D^{(p^m)}_{ld_m/q+t} \pmod p = D^{(p)}_{lf/q+t \pmod f}$. Hence

$$\mathscr{D} \pmod p = D^{(p)}_0 \cup \cdots \cup \cdots \cup D^{(p)}_{f-1} = \mathbb{Z}_p^*.$$

Thus, by letting $t \pmod p = \bar{t}$ for any $t \in \mathscr{D}$ we have

$$\xi = \sum_{t \in \mathscr{D}} \alpha_m^t = \sum_{t \in \mathscr{D}} \alpha_m^{(t-\bar{t})+\bar{t}} = \sum_{t \in \mathscr{D}} \alpha_{m-1}^{(t-\bar{t})/p} \alpha_m^{\bar{t}} = \sum_{i=1}^{p-1} c_i \alpha_m^i,$$

and $c_i \in \mathbb{F}_q(\alpha_{m-1})$.

It means that $\alpha_m$ is a root of the polynomial $f(x) = \sum_{i=1}^{p-1} c_i x^i + \xi$ over $\mathbb{F}_q(\alpha_{m-1})$. This implies $[\mathbb{F}_q(\alpha_m) : \mathbb{F}_q(\alpha_{m-1})] < p$, which is in contradiction with Lemma 2.

By Proposition 2, we only need to study the values of $F^{(p^n)}_b(\alpha_n^i)$ for integers $i$ in the set $p^{n-1}\mathbb{Z}_p$. For any $a \in \mathbb{Z}_p^*$, it follows from Proposition 1 and Lemma 4 that

$$F^{(p^n)}_b(\alpha_n^{p^{n-1}a}) = F^{(p)}_b(\alpha_1^a) = G^{(p)}_b(\alpha_1^a) = G^{(p)}_k(\alpha_1),$$

where $a \in D^{(p)}_i$ for some integer $i$ and $k \equiv b + i \pmod f$. The following proposition examines the value of $G^{(p)}_k(\alpha_1)$ according to the relation between $f$ and $\mathrm{ord}_p(q)$.

**Proposition 3** *Let $p = ef + 1$ be an odd prime, $q$ divides $f$ and $v = \gcd(\frac{p-1}{\mathrm{ord}_p(q)}, f)$. Then,*

*(i)* $\left| \left\{ k \in \mathbb{Z}_f \,|\, G^{(p)}_k(\alpha_1) = 0 \right\} \right| \leq f/q$ *and* $\left| \left\{ k \in \mathbb{Z}_f \,|\, H^{(p)}_k(\alpha_1) = 0 \right\} \right| = f/q$ *if $v = f$;*

*(ii)* $\left| \left\{ k \in \mathbb{Z}_f \,|\, G^{(p)}_k(\alpha_1) = 0 \right\} \right| = 0$ *if $v \mid \frac{f}{q}$, or $v = 2$ and $f \neq v$.*

Proof. (i) Since $G^{(p)}_k(x) = F^{(p)}_k(x)$, it follows by Proposition 1 that $G^{(p)}_{k+lf/q}(\alpha_1) = G^{(p)}_k(\alpha_1) + l$ for $l = 1, \ldots, q-1$ Thus, if $G^{(p)}_k(\alpha_1) = 0$ then $G^{(p)}_{k+lf/q}(\alpha_1) \neq 0$ for $l = 1, \ldots, q-1$ and we obtain the first part of statement of (i).

Further, suppose $v = f$; then $q \in D^{(p)}_0$ and $G^{(p)}_k(\alpha_1) \in \mathbb{F}_q$ for any $k$. In this case we see that only one from numbers $G^{(p)}_{k+lf/q}(\alpha_1)$, $l = 0, 1, \ldots, q-1$ is equal to zero.

(ii) Assume $q \equiv g^u \pmod p$ for some integer $u$ in $\mathbb{Z}_p^*$. Then $q \in D^{(p)}_{u_1}$ and $\gcd(u_1, f) = \gcd(u, f) = \gcd(\frac{(p-1)t}{\mathrm{ord}_p(q)}, f) = \gcd(\frac{(p-1)}{\mathrm{ord}_p(q)}, f) = v$.

We shall prove this case by contradiction. Suppose $G^{(p)}_k(\alpha_1) = 0$ for some integer $k$. Without loss of generality, we assume $k = 0$ and $G^{(p)}_0(\alpha_1) = 0$.

In the case when $v \neq f$, we have $u_1 < f$. Since $\in D^{(p)}_{u_1}$ and $v = \gcd(u_1, f)$, by a similar argument as in the proof of Proposition 2 we get

$$0 = G^{(p)}_0(\alpha_1) = G^{(p)}_v(\alpha_1) = \cdots = G^{(p)}_{(f/v-1)v}(\alpha_1),$$

and

$$1 = G^{(p)}_{f/q}(\alpha_1) = G^{(p)}_{f/q+v}(\alpha_1) = \cdots = G^{(p)}_{f/q+(f/v-1)v}(\alpha_1).$$

If $v$ divides $f/q$, then $G^{(p)}_{f/q}(\alpha_1) = G^{(p)}_{f/q+v\cdot f/qv}(\alpha_1) = G^{(p)}_0(\alpha_1)$, which is a contradiction.

Let $v = 2, v \neq f$ and $v$ does not divide $f/q$, it is clear that $f/q$ is odd. In this case we get as above that

$$0 = G^{(p)}_0(\alpha_1) = G^{(p)}_2(\alpha_1) = \cdots = G^{(p)}_{f-2}(\alpha_1),$$

and

$$1 = G^{(p)}_1(\alpha_1) = G^{(p)}_3(\alpha_1) = \cdots = G^{(p)}_{f-1}(\alpha_1).$$

So, we see that $G^{(p)}_i(\alpha_1) - G^{(p)}_{i+1}(\alpha_1) + 1 = 0, i = 0, 1, \ldots, f-1$ and then for $i = 0, 1, \ldots, f-1$ we have

$$E^{(p)}_i(\alpha) + E^{(p)}_{i+f/q}(\alpha) + \cdots + E^{(p)}_{i+(q-1)f/q}(\alpha) + 1 = 0. \quad (10)$$

For $v \neq f$ we can easily choose an integer $j$ such that

$$(p-1) \notin \left( D^{(p)}_j \cup D^{(p)}_{j+f/q} \cup \cdots \cup D^{(p)}_{j+(q-1)f/q} \right).$$

We define $f(x) = E^{(p)}_j(x) + E^{(p)}_{j+f/q}(x) + \cdots + E^{(p)}_{j+(q-1)f/q}(x) + 1$. Given any $a \in \mathbb{Z}_p^*$, assuming

$a \in D_k^{(p)}$ for an integer $k$, we obtain from Lemma 4 and (10) that $f(\alpha_1^a) = E_{j+k}^{(p)}(\alpha) + E_{j+k+f/q}^{(p)}(\alpha) + \cdots + E_{j+k+(q-1)f/q}^{(p)}(\alpha) + 1 = 0$. That is to say, $f(\alpha_1^a) = 0$ for any $a \in \mathbb{Z}_p^*$. This is a contradiction since the polynomial $f(x)$ has degree less than $p-1$.

### 3.4 Proof of Theorem

Recall that the linear complexity of $s^\infty$ is given by

$$L = p^n - \left|\left\{i \in \mathbb{Z}_{p^n} \,|\, F_b^{(p^n)}(\alpha_n^i) = 0\right\}\right|.$$

It is easy to see that $F_b^{(p^n)}(1) = 0$. Proposition 2 we know $\left|\left\{i \in \mathbb{Z}_{p^n} \setminus p^{n-1}\mathbb{Z}_p \,|\, F_b^{(p^n)}(\alpha_n^i) = 0\right\}\right| = 0$. For the remaining set $p^{n-1}\mathbb{Z}_p$, if $i = 0$, then $F_b^{(p^n)}(\alpha_n^i) = 0$; if $i \in p^{n-1}\mathbb{Z}_p^*$, we have

$$F_b^{(p^n)}(\alpha_n^i) = F_b^{(p)}(\alpha_1^a) = G_b^{(p)}(\alpha_1^a)$$

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

Suppose $G_k^{(p)}(\alpha_1) = 0$ for some integer $k$. Then as in Proposition 2 we obtain

$$0 = G_k^{(p)}(\alpha_1) = G_{k+v}^{(p)}(\alpha_1) = G_{k+iv}^{(p)}(\alpha_1),$$

for $i = 0, 1, \mathrm{ord}_p(q) - 1$ and $G_{k+iv+lf/q}^{(p)}(\alpha_1) \neq 0$ for $l = 1, 2, \ldots, q-1$. So, we have

$$L = p^n - 1 - r\,\mathrm{ord}_p(q),$$

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

Furthermore, if $v = f$ or $v|f/2$ and $v \neq f$ then by Proposition 3 we see that $r = \frac{p-1}{\mathrm{ord}_p(q)}$ in the first case and $r = 0$ in the second case. This concludes the proof of Theorem 1.

**Remark 6** *If $v \neq f$ then $r$ can have different values. For example, let $q = 3$, $f = 24$ and $p = 193$. We obtain by Berlekamp-Massey algorithm that here $L = 160$. Further, in this case $\mathrm{ord}_p(q) = 16$ and $r = 2 < \frac{p-1}{\mathrm{ord}_p(q)}$. Also for $p = 577$.*

*Let $q = 5, f = 15$ and $p = 641$. Here $L = 576$, $\mathrm{ord}_p(q) = 64$ and $r = 1$.*

### 3.5 Additional remark

Let $D = \{k : \ q^{p-1} \equiv 1 \pmod{p^k}\}$ and $wn = \max_{k \in D} k$. In this case we can obtain for $n \geq wn$ that the linear complexity of $s^\infty$ over $\mathbb{F}_q$ is given by

$$L = p^n - r \cdot \mathrm{ord}_p(q) - 1, \quad 0 \leq r \leq \tfrac{p^{wn}-1}{q\mathrm{ord}_p(q)}.$$

Furthermore,

$$L = \begin{cases} p^n - \frac{p^{nw}-1}{q} - 1, & \text{if } v = f; \\ p^n - 1, & \text{if } v|\frac{f}{q}. \end{cases}$$

Here $v = \gcd\left(\frac{p-1}{\mathrm{ord}_p(q)}, f\right)$ as earlier.

## 4 Conclusion

We studied the linear complexity of new $q$-ary generalized cyclotomic sequences of length $p^n$ over the finite field of order $q$. We showed that these sequences have high linear complexity when $n \geq 2$. These sequences are constructed by new generalized cyclotomic classed prepared by X. Zeng at el. We generalized the results about new binary cyclotomic sequences obtained by Z. Xiao, X. Zeng at el. earlier.

## References

[1] A. Çeşmelioğlu, W. Meidl, A general approach to construction and determination of the linear complexity of sequences based on cosets. In: C. Carlet, A. Pott (eds.) Sequences and Their Applications – SETA 2010, 125–138. Springer Berlin Heidelberg, Berlin, Heidelberg (2010).

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

[3] C. Ding, T. Helleseth, New generalized cyclotomy and its applications. Finite Fields and Their Applications **4**(2), 140–166 (1998).

[4] X. Du, Z. Chen, A generalization of the Hall's sextic residue sequences. Information Sciences **222**, 784–794 (2013).

[5] V. Edemskiy, About computation of the linear complexity of generalized cyclotomic sequences with period $p^{n+1}$. Designs, Codes and Cryptography **61**(3), 251–260 (2011).

[6] 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

[7] S. W. Golomb, Shift Register Sequences, Holden-Day, San Francisco (1967).

[8] D.H. Green, M.D. Smith and N. Martzoukos. Linear complexity of polyphase power residue sequences. IEE Proc. Commun., **149**, ( 4), 195-201 (2002)

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

[10] Y.J. Kim, H.Y Song, Linear complexity of prime $n$-square sequences. In: 2008 IEEE International Symposium on Information Theory, 2405–2408 (2008).

[11] R. Lidl, H. Niederreiter, *Finite Fields.* Encyclopedia of Mathematics and Its Applications, vol. 20. (Addison-Wesley, 1983).

[12] Peter L. Montgomery, New Solutions of $a^{p-1} \equiv 1 \pmod{p^2}$. Mathematics of Computation, **61**, (203), Special Issue Dedicated to Derrick Henry Lehmer, 361-363 ( 1993)

[13] C. Wu, Z. Chen, X. Du, The linear complexity of $q$-ary generalized cyclotomic sequences of period $p^m$. Journal of Wuhan University **59**(2), 129–136 (2013).

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

[15] T. Yan, S. Li, G. Xiao, On the linear complexity of generalized cyclotomic sequences with the period $p^m$. Applied Mathematics Letters **21**(2), 187–193 (2008).

[16] Z. Ye, P. Ke, C. Wu, A further study of the linear complexity of new binary cyclotomic sequence of length $p^n$. AAECC, **30** (3), 217-23, (2019)

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