Hindawi
Complexity
Volume 2020, Article ID 6538970, 7 pages
https://doi.org/10.1155/2020/6538970

Research Article

Linear Complexity of a New Class of Quaternary Generalized Cyclotomic Sequence with Period $2p^m$

Pinhui Ke, Yan Zhong, and Shengyuan Zhang

Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou, Fujian 350117, China

Correspondence should be addressed to Pinhui Ke; keph@fjnu.edu.cn

Received 19 August 2019; Accepted 10 February 2020; Published 10 March 2020

Academic Editor: Chittaranjan Hens

Sequences with high linear complexity property are of importance in applications. In this paper, based on the theory of generalized cyclotomy, new classes of quaternary generalized cyclotomic sequences with order 4 and period $2p^m$ are constructed. In addition, we determine their linear complexities over finite field $\mathbb{F}_4$ and over $\mathbb{Z}_4$, respectively.

1. Introduction

Pseudorandom sequence has a wide range of applications in the spread spectrum communication, radar navigation, code division multiple access, stream cipher, and so on [1]. The linear complexity $L(\{s(u)\})$ of a sequence $\{s(u)\}$ is defined as the smallest order of linear feedback shift register (LFSR) that can generate the whole sequence. According to Berlekamp–Massey algorithm [2], if the linear complexity of the sequence is l, then $2l$ consecutive terms of the sequence can be used to restore the whole sequence. Hence, a "high" linear complexity $L(\{s(u)\})$ should be no less than one half of the length (or minimum period) of the sequence [3]. For cryptographic applications, sequences with high linear complexity are required.

Sequences with high linear complexity can be constructed based on cyclotomic classes. Generally, sequences based on classical cyclotomic classes and generalized cyclotomic classes are called classical cyclotomic sequences and generalized cyclotomic sequences, respectively. There are lots of works on linear complexity of binary cyclotomic sequences, see [4–7], for instance. Recently, Xiao et al. presented a new class of cyclotomic binary sequences of period p^2 and determined the linear complexity of the sequences in the case of $f = 2^r$ for a positive integer r and showed that the sequences have large linear complexity if p is a non-Wieferich prime [8]. Moreover, Edemskiy et al. examined the linear complexity of sequences and extended the result to more general even integers f [9]. At the same time, the results were also generalized by Ye and Ke in [10] by considering a new construction with a flexible support set, which includes the original construction as a special case. Very recently, in [11], Ouyang and Xie extended the construction to the case of $2p^m$ and showed that the constructed sequences have high linear complexity when $m \geq 2$.

Compared with the binary case, less attention has been paid to quaternary sequences with high linear complexity. In [12], Kim et al. constructed a class of generalized cyclotomic sequences with period $2p$ over $\mathbb{Z}_4$ and analyzed the autocorrelation properties of these sequences. In [13], Chen and Edemskiy determined the linear complexity of these sequences over $\mathbb{Z}_4$. In [14], Du and Chen defined a family of quaternary sequences over $\mathbb{F}_4$ of period $2p$ using generalized cyclotomic classes over the residue class ring modulo $2p$. They determined the linear complexities of the sequences and then showed that the sequences have large linear complexity. The autocorrelation values of the sequences were further studied in [15]. In [16], Ke et al. generalized the construction of [14] to the case of $2p^m$. They proved that the constructed sequences are balanced and also possess high linear complexity. Recently, in [17], Liu et al. further extended the sequence construction of [16, 18]. A class of quaternary generalized cyclotomic sequences with order $2d$ period $2p^m$ over $\mathbb{F}_4$ are constructed, and their linear

complexities are studied. In addition, in [19], Edemskiy and Ivanov constructed another kind of new quaternary generalized cyclotomic sequences with period $2p$ based on the Chinese Remainder Theorem and studied their autocorrelation properties and linear complexities over $\mathbb{F}_4$ as well as $\mathbb{Z}_4$.

Although the sequence they constructed are both quaternary sequences, it can be seen by comparison that [16, 17, 19] have their advantages and disadvantages. On the one hand, by definition in [16, 17], the elements in a fixed support set of the sequence are all even or odd, while the sequence proposed by Edemskiy and Ivanov in [19] takes value more random. On the other hand, in [19], the sequence has period $2p$, while in [17], the sequence has a more general period $2p^m$. In this paper, combining the advantages of the above two constructions, we will define a new class of quaternary generalized cyclotomic sequences of order 4 with period $2p^m$ over $\mathbb{F}_4$ as well as $\mathbb{Z}_4$. Furthermore, we determine the linear complexities of the new defined sequences over $\mathbb{F}_4$ and $\mathbb{Z}_4$, respectively.

This paper is organized as follows. In Section 2, we introduce some necessary preliminary concepts and present a general construction of quaternary generalized cyclotomic sequences with period $2p^m$ over $\mathbb{Z}_4$. In addition, based on a mapping from $\mathbb{Z}_4$ to $\mathbb{F}_4$, quaternary sequences over $\mathbb{F}_4$ can be derived directly from the quaternary sequences over $\mathbb{Z}_4$. In Section 3, we compute the linear complexity of sequences we constructed over $\mathbb{F}_4$. In Section 4, we compute the linear complexity of sequences that we constructed over $\mathbb{Z}_4$. In Section 5, we conclude this paper.

2. Perliminaries

Let p be an odd prime with $p \equiv 1 \pmod 4$. Let g be a primitive root of $\mathbb{Z}_{p^2}^*$, where $\mathbb{Z}_n^*$ denotes the set of all invertible elements of $\mathbb{Z}_n$. It is well known that g is also a primitive root of $\mathbb{Z}_{p^m}^*$ $(m \geq 1)$.

For $j = 1, 2, \ldots, m$ and $l = 0, 1, 2, 3$, we define

$$\begin{aligned} D_0^{(p^j)} &= \langle g^4 \rangle \pmod{p^j}, \\ D_l^{(p^j)} &= g^l \langle g^4 \rangle \pmod{p^j}, \\ D_0^{(2p^j)} &= \langle g^4 \rangle \pmod{2p^j}, \\ D_l^{(2p^j)} &= g^l \langle g^4 \rangle \pmod{2p^j}, \end{aligned} \tag{1}$$

where $D_l^{(p^j)}$ are called generalized cyclotomic classes of order 4 with respect to p^j and $D_l^{(2p^j)}$ are called generalized cyclotomic classes of order 4 with respect to $2p^j$.

It is easy to verify that

$$\begin{aligned} \mathbb{Z}_{2p^m} &= \bigcup_{j=1}^{m} p^{m-j}\left(\mathbb{Z}_{2p^j}^* \cup 2\mathbb{Z}_{p^j}^*\right) \cup p^m \mathbb{Z}_2^* \cup \{0\} \\ &= \bigcup_{j=1}^{m}\Big(p^{m-j}D_0^{(2p^j)} \cup \cdots \cup p^{m-j}D_3^{(2p^j)} \cup 2p^{m-j}D_0^{(p^j)} \cup \cdots \\ &\quad \cup 2p^{m-j}D_3^{(p^j)}\Big) \cup \{0, p^m\}. \end{aligned} \tag{2}$$

For simplicity, we denote

$$\begin{aligned} H_l^{(p^j)} &= p^{m-j} D_l^{(p^j)}, \\ H_l^{(2p^j)} &= p^{m-j} D_l^{(2p^j)}, \\ & \qquad l = 0, 1, 2, 3. \end{aligned} \tag{3}$$

Definition 1. Let $2 \in D_k^{(p)}, 0 \leq k \leq 3$. Then, we define the sequences $\{s_1(u)\}_{u \geq 0}$ and $\{s_2(u)\}_{u \geq 0}$ over $\mathbb{Z}_4$ of length $2p^m$ by

$$s_1(u) = \begin{cases} 0, & \text{if } u \in \bigcup_{j=1}^{m}\left(2H_{0-k \bmod 4}^{(p^j)} \cup H_1^{(2p^j)}\right) \cup \{0\}; \\ 1, & \text{if } u \in \bigcup_{j=1}^{m}\left(2H_{1-k \bmod 4}^{(p^j)} \cup H_2^{(2p^j)}\right); \\ 2, & \text{if } u \in \bigcup_{j=1}^{m}\left(2H_{2-k \bmod 4}^{(p^j)} \cup H_3^{(2p^j)}\right) \cup \{p^m\}; \\ 3, & \text{if } u \in \bigcup_{j=1}^{m}\left(2H_{3-k \bmod 4}^{(p^j)} \cup H_0^{(2p^j)}\right), \end{cases} \tag{4}$$

$$s_2(u) = \begin{cases} 0, & \text{if } u \in \bigcup_{j=1}^{m}\left(2H_{0-k \bmod 4}^{(p^j)} \cup H_2^{(2p^j)}\right) \cup \{0\}; \\ 1, & \text{if } u \in \bigcup_{j=1}^{m}\left(2H_{2-k \bmod 4}^{(p^j)} \cup H_0^{(2p^j)}\right); \\ 2, & \text{if } u \in \bigcup_{j=1}^{m}\left(2H_{1-k \bmod 4}^{(p^j)} \cup H_3^{(2p^j)}\right) \cup \{p^m\}; \\ 3, & \text{if } u \in \bigcup_{j=1}^{m}\left(2H_{3-k \bmod 4}^{(p^j)} \cup H_1^{(2p^j)}\right), \end{cases} \tag{5}$$

respectively.

The well-known Gray-mapping $\phi\colon \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ is defined as

$$\begin{aligned} \phi(0) &= (0, 0), \\ \phi(1) &= (0, 1), \\ \phi(2) &= (1, 1), \\ \phi(3) &= (1, 0). \end{aligned} \tag{6}$$

Let $\mathbb{F}_4 = \mu\mathbb{F}_2 + \mathbb{F}_2$ be a finite field of order 4, where μ satisfies the relation $\mu^2 + \mu + 1 = 0$. Let σ be a map from $\mathbb{F}_2 \times \mathbb{F}_2$ to $\mathbb{F}_4$ which is defined as follows:

$$\begin{aligned} \sigma\colon \mathbb{F}_2 \times \mathbb{F}_2 &\longrightarrow \mathbb{F}_4, \\ (a, b) &\longmapsto a\mu + b, \end{aligned} \tag{7}$$

where $a, b \in \mathbb{F}_2$.

Then, we have $\sigma \circ \phi\colon \mathbb{Z}_4 \longrightarrow \mathbb{F}_4$, i.e.,

$$\begin{aligned} \sigma \circ \phi(0) &= 0, \\ \sigma \circ \phi(1) &= 1, \\ \sigma \circ \phi(2) &= \mu + 1, \\ \sigma \circ \phi(3) &= \mu. \end{aligned} \tag{8}$$

By this way, the sequences over $\mathbb{Z}_4$ defined in (4) and (5) can be modified to be sequences over $\mathbb{F}_4$ as follows, i.e.,

$$b_1(u)=\begin{cases}0, & \text{if } u\in\bigcup_{j=1}^{m}\left(2H_{0-k\ \bmod 4}^{(p^j)}\cup H_1^{(2p^j)}\right)\cup\{0\};\\ 1, & \text{if } u\in\bigcup_{j=1}^{m}\left(2H_{1-k\ \bmod 4}^{(p^j)}\cup H_2^{(2p^j)}\right);\\ \mu+1, & \text{if } u\in\bigcup_{j=1}^{m}\left(2H_{2-k\ \bmod 4}^{(p^j)}\cup H_3^{(2p^j)}\right)\cup\{p^m\};\\ \mu, & \text{if } u\in\bigcup_{j=1}^{m}\left(2H_{3-k\ \bmod 4}^{(p^j)}\cup H_0^{(2p^j)}\right).\end{cases} \tag{9}$$

Similarly,

$$b_2(u)=\begin{cases}0, & \text{if } u\in\bigcup_{j=1}^{m}\left(2H_{0-k\ \bmod 4}^{(p^j)}\cup H_2^{(2p^j)}\right)\cup\{0\};\\ 1, & \text{if } u\in\bigcup_{j=1}^{m}\left(2H_{2-k\ \bmod 4}^{(p^j)}\cup H_0^{(2p^j)}\right);\\ \mu+1, & \text{if } u\in\bigcup_{j=1}^{m}\left(2H_{1-k\ \bmod 4}^{(p^j)}\cup H_3^{(2p^j)}\right)\cup\{p^m\};\\ \mu, & \text{if } u\in\bigcup_{j=1}^{m}\left(2H_{3-k\ \bmod 4}^{(p^j)}\cup H_1^{(2p^j)}\right).\end{cases} \tag{10}$$

Remark 1. Obviously, the support sets of sequences defined in this paper are more random than those in [16, 17], where the support sets all consist of even or odd numbers. In addition, the quaternary sequences constructed in [19] can be considered as a special case of the sequences defined above by taking $m=1$. In other words, in the case of length $2p$, the constructions in [19] and this paper, although they were expressed in different forms, are the same in essence. In detail, the difference between these two constructions is that, in [19], the sequences were constructed by using the Chinese Remainder Theorem, while the sequences in this paper are defined directly. Therefore, this paper can be regarded as a generalization of [19].

3. Linear Complexity of the Sequence over $\mathbb{F}_4$

In this section, we discuss the linear complexity over $\mathbb{F}_4$. Hence, we focus on the quaternary sequences in (9) and (10). Let $s^\infty=(s_0,\cdots,s_i,\cdots)$ be a sequence over $\mathbb{F}_4$, and its linear complexity $L(s^\infty)$ is the smallest positive integer L for which there exist constants $c_1,c_2,\cdots,c_L$ such that

$$s_j+c_1s_{j-1}+c_2s_{j-2}+\cdots+c_Ls_{j-L}=0,\quad j\geq L. \tag{11}$$

Let $s^\infty=\{s_u\}_{u=0}^{N}$ be a periodic sequence of period N over $\mathbb{F}_4$. And $S(x)=\sum_{u=0}^{N-1}s_ux^u$ is called the generating polynomial of the sequence. Then, the minimal polynomial of $\{s_u\}_{u=0}^{N}$ is given by

$$\frac{m(x)=(x^N-1)}{\gcd(x^N-1,S(x))}, \tag{12}$$

and the linear complexity of $\{s_u\}_{u=0}^{N}$ is given by

$$L(\{s_N\})=N-\deg\left(\gcd\left(x^N-1,S(x)\right)\right). \tag{13}$$

Let d be the order of 4 modulo p^m, that is, d is the smallest integer such that $4^d\equiv 1(\bmod p^m)$. Let ξ be a primitive element of $\mathbb{F}_{4^d}$; then, the order of $\alpha=\xi^{4^d-1/p^m}$ is p^m, and $\theta=\alpha^{p^{m-1}}$ has order p.

According to the definition of the linear complexity of the sequence, we should compute the number of common roots of the generating polynomial $S(x)$ and polynomials x^N-1. Notice that $\gcd(x^N-1,S(x))=\gcd(x^{2p^m}-1,S(x))=\gcd((x^{p^m}-1)^2,S(x))$, so we may check that if $\alpha^v\,(0\leq v\leq p^m-1)$ is a root of $S(x)$. Furthermore, if it is a root of $S(x)$, we need to verify if it is a multiple root of $S(x)$ [20].

To this end, we need some auxiliary polynomials:

$$\begin{aligned}T_4(x)&=\sum_{u\in D_0^{(p)}}x^u,\\ T_2(x)&=\sum_{u\in D_0^{(p)}\cup D_2^{(p)}}x^u,\\ R_l^{(j)}(x)&=\sum_{u\in H_l^{(2p^j)}}x^u,\\ S_l^{(j)}(x)&=\sum_{u\in 2H_l^{(p^j)}}x^u,\end{aligned} \tag{14}$$

where $l=0,1,2,3$ and $j=1,2,\cdots,m$.

Lemma 1 (see [18]). *For $l=0,1,2,3$, $1\leq j\leq m$, we have*

$$\sum_{u\in H_l^{(2p^j)}}\alpha^u=\sum_{u\in H_l^{(p^j)}}\alpha^u. \tag{15}$$

Lemma 2 (see [16]). *For $l=0,1,2,3$, $1\leq j\leq m$, we have*

(i) $D_l^{(p^j)}=\left\{x+py\colon x\in D_l^{(p)},y\in\mathbb{Z}_{p^{j-1}}\right\}$,

(ii) $D_l^{(2p^j)}=\left\{x+py+\delta_{x,y}\colon x\in D_l^{(p)},y\in\mathbb{Z}_{p^{j-1}}\right\}$,

where

$$\delta_{x,y}=\begin{cases}0, & \text{if } x+py \text{ is odd},\\ p^j, & \text{otherwise}.\end{cases} \tag{16}$$

Lemma 3. *Let $v=tp^i,0\leq i\leq m-1$, $1\leq j\leq m, gcd(t,p)=1$, and $2\in D_k^{(p)}$. For $0\leq k,l\leq 3$, we have*

$$\begin{aligned}R_l^{(j)}(\alpha^v)&=\begin{cases}\dfrac{p^{j-1}(p-1)}{4}, & if\ j\leq i;\\ \sum_{u\in D_l^{(p)}}\theta^{tu}, & if\ j=i+1;\\ 0, & if\ j>i+1,\end{cases}\\ S_l^{(j)}(\alpha^v)&=\begin{cases}\dfrac{p^{j-1}(p-1)}{4}, & if\ j\leq i;\\ \sum_{u\in D_{l+k(\bmod 4)}^{(p)}}\theta^{tu}, & if\ j=i+1;\\ 0, & if\ j>i+1.\end{cases}\end{aligned} \tag{17}$$

Proof. Since the proof is similar, only the case of $R_l^{(j)}(\alpha^v)$ is considered here. By Lemma 1, we have

$$R_l^{(j)}(\alpha^v) = \sum_{u\in H_l^{(2p^j)}} \alpha^{vu} = \sum_{u\in H_l^{(2p^j)}} \alpha^{tp^i u} = \sum_{u\in tp^{m+i-j}D_l^{(2p^j)}} \alpha^u = \sum_{u\in tp^{m+i-j}D_l^{(p^j)}} \alpha^u. \tag{18}$$

(1) If $j \le i$, note that $\alpha^u = 1$ for any $u \in tp^{m+i-j}D_l^{(p^j)}$. Obviously, $|D_l^{(p^j)}| = \varphi(p^j)/4$. Hence,

$$R_l^{(j)}(\alpha^v) = \sum_{u\in tp^{m+i-j}D_l^{(p^j)}} \alpha^u = \frac{\varphi(p^j)}{4} = \frac{p^{j-1}(p-1)}{4}. \tag{19}$$

(2) If $j = i+1$, then

$$R_l^{(j)}(\alpha^v) = \sum_{u\in tp^{m-1}D_l^{(p^j)}} \alpha^u = \sum_{u\in D_l^{(p^j)}} \theta^{tu} = \sum_{u\in D_l^{(p)}} \theta^{tu}, \tag{20}$$

where $\theta = \alpha^{p^{m-1}}$.

(3) If $j > i+1$, suppose that $\alpha^{tp^{m+i-j}} = \eta$, $\eta^{p^j} = 1$, and $\eta^p \ne 1$; then, $\sum_{t\in\mathbb{Z}_{p^{j-1}}} \eta^{tp} = 0$. So,

$$R_l^{(j)}(\alpha^v) = \sum_{u\in tp^{m+i-j}D_l^{(p^j)}} \alpha^u = \sum_{t_1\in D_l^{(p)}} \eta^{t_1} \sum_{t_2\in\mathbb{Z}_{p^{j-1}}} \eta^{t_2} = 0. \tag{21}$$

The proof is thus completed. □

Lemma 4 (see [4]). *For $1 \le t \le p-1$, let θ be a primitive pth root of unity in the extension of the field $\mathbb{F}_2$, and define $T_2(x) = \sum_{u\in D_0^{(p)}\cup D_2^{(p)}} x^u$. Then, we have*

$$T_2(\theta^t) = \begin{cases} T_2(\theta), & if\ t \in D_0^{(p)} \cup D_2^{(p)}; \\ T_2(\theta)+1, & if\ t \in D_1^{(p)} \cup D_3^{(p)}. \end{cases} \tag{22}$$

Lemma 5 (see [4]). *With the above notation, then $T_2(\theta) \in \mathbb{F}_2$ if $2 \in D_0^{(p)} \cup D_2^{(p)}$; otherwise, $T_2(\theta) \in \mathbb{F}_4/\mathbb{F}_2$.*

Lemma 6 (see [21]). *With notations defined as above, if $2 \in D_k^{(p)}$, then $T_4^2(\theta) = T_4(\theta^{g^k})$.*

Theorem 1. *Let $p \equiv 1 (mod\ 4)$ be an odd prime. Let $\{b_1(u)\}_{u\ge0}$ be a generalized cyclotomic quaternary sequence of period $2p^m$ defined in (9). Then, the linear complexity of $\{b_1(u)\}_{u\ge0}$ over $\mathbb{F}_4$ is given by*

$$L(\{b_1(u)\}) = \begin{cases} 2p^m, & if\ p \equiv 1 \pmod 8; \\ \dfrac{3p^m+1}{2}, & if\ p \equiv 5 \pmod 8. \end{cases} \tag{23}$$

Proof. By the definition of the sequence $\{b_1(u)\}_{u\ge0}$, the generating polynomial $S(x)$ of $\{b_1(u)\}_{u\ge0}$ is given by

$$\begin{aligned} S(x) = (\mu+1)x^{p^m} &+ \sum_{j=1}^{m}\left(S_{1-k(\mathrm{mod}4)}^{(j)}(x) + R_2^{(j)}(x)\right) \\ &+ (\mu+1)\sum_{j=1}^{m}\left(S_{2-k\ (\mathrm{mod}4)}^{(j)}(x) + R_3^{(j)}(x)\right) \\ &+ \mu\sum_{j=1}^{m}\left(S_{3-k\ (\mathrm{mod}4)}^{(j)}(x) + R_0^{(j)}(x)\right). \end{aligned} \tag{24}$$

It is easily seen that if $v = 0$, then $S(1) = \mu+1 \ne 0$. Hence, 1 is not root of $S(x)$. We can write

$$\begin{aligned} S(\alpha^v) &= (\mu+1) + \sum_{j=1}^{m}\left(S_{1-k\ (\mathrm{mod}4)}^{(j)}(\alpha^v) + R_2^{(j)}(\alpha^v)\right) + (\mu+1) \\ &\sum_{j=1}^{m}\left(S_{2-k\ (\mathrm{mod}4)}^{(j)}(\alpha^v) + R_3^{(j)}(\alpha^v)\right) + \mu\sum_{j=1}^{m}\left(S_{3-k\ (\mathrm{mod}4)}^{(j)}(\alpha^v) + R_0^{(j)}(\alpha^v)\right). \end{aligned} \tag{25}$$

According to Lemma 3, if $v = tp^i$, $1 \le v \le p^m - 1$, we have

$$\begin{aligned} S(\alpha^v) &= (\mu+1) + \sum_{j=1}^{i}(1+\mu+1+\mu)\cdot\frac{p^{j-1}(p-1)}{2} + S_{1-k(\mathrm{mod}4)}^{(i+1)}(\alpha^v) \\ &\quad + R_2^{(i+1)}(\alpha^v) + (\mu+1)\cdot\left(S_{2-k(\mathrm{mod}4)}^{(i+1)}(\alpha^v) + R_3^{(i+1)}(\alpha^v)\right) \\ &\quad + \mu\left(S_{3-k(\mathrm{mod}4)}^{(i+1)}(\alpha^v) + R_0^{(i+1)}(\alpha^v)\right) \\ &= \mu + 1 + \sum_{u\in D_1^{(p)}}\theta^{tu} + \sum_{u\in D_2^{(p)}}\theta^{tu} + \sum_{u\in D_2^{(p)}}\theta^{tu} + \sum_{u\in D_3^{(p)}}\theta^{tu} \\ &\quad + \mu\left(\sum_{u\in D_2^{(p)}}\theta^{tu} + \sum_{u\in D_3^{(p)}}\theta^{tu} + \sum_{u\in D_3^{(p)}}\theta^{tu} + \sum_{u\in D_0^{(p)}}\theta^{tu}\right) \\ &= \mu + 1 + T_2(\theta^{tg}) + \mu T_2(\theta^t) \\ &= \mu + (1+\mu)T_2(\theta^t), \end{aligned} \tag{26}$$

where the last equality follows from the fact that $T_2(\theta^{tg}) = 1 + T_2(\theta^t)$.

(1) If $p \equiv 1 (\mathrm{mod}\ 8)$, by Lemmas 4 and 5, we obtain $S(\alpha^v) \in \{1, \mu\}$. In other words, $S(\alpha^v) \ne 0$ when $1 \le v \le p^m - 1$.

(2) If $p \equiv 5 (\mathrm{mod}\ 8)$, by Lemmas 4 and 5 again, we know that $2 \in D_1^{(P)}$ (if not, then we can simply replace g with g^{-1}). So,

$$T_2(\theta^t) = \begin{cases} \mu, & \text{if } t \in D_0^{(p)} \cup D_2^{(p)}; \\ \mu+1, & \text{if } t \in D_1^{(p)} \cup D_3^{(p)}. \end{cases} \tag{27}$$

Thus, if $t \in D_0^{(p)} \cup D_2^{(p)}$, then $S(\alpha^v) = \mu+1$; if $t \in D_1^{(p)} \cup D_3^{(p)}$, then $S(\alpha^v) = 0$.

To complete the proof, we should verify that if $\alpha^v (1 \le v \le p^m - 1)$ is a multiple root of $S(x)$ when $t \in D_1^{(p)} \cup D_3^{(p)}$.

$$S'(x) = (\mu+1)x^{p^m-1} + \sum_{j=1}^{m}\left[\sum_{u\in H_2^{(2p^j)}} x^{u-1} + \sum_{u\in H_3^{(2p^j)}} x^{u-1} + \mu\left(\sum_{u\in H_3^{(2p^j)}} x^{u-1} + \sum_{u\in H_0^{(2p^j)}} x^{u-1}\right)\right]. \tag{28}$$

According to Lemma 3, if $v = tp^i, 1 \le v \le p^m - 1$, we have

$$\begin{aligned} S'(\alpha^v) &= \alpha^{-v}\left[(\mu+1) + \sum_{j=1}^{m}\left[R_2^{(j)}(\alpha^v) + R_3^{(j)}(\alpha^v) + \mu\left(R_3^{(j)}(\alpha^v) + R_0^{(j)}(\alpha^v)\right)\right]\right] \\ &= \alpha^{-v}\left[(\mu+1) + \sum_{j=1}^{i}(1+1+\mu+\mu)\cdot\frac{p^{j-1}(p-1)}{2} + \left[R_2^{(i+1)}(\alpha^v) + R_3^{(i+1)}(\alpha^v) + \mu\left(R_3^{(i+1)}(\alpha^v) + R_0^{(i+1)}(\alpha^v)\right)\right]\right] \\ &= \alpha^{-v}\left[\mu + 1 + T_4\left(\theta^{tg^2}\right) + T_4\left(\theta^{tg^3}\right) + \mu\left(T_4\left(\theta^{tg^3}\right) + T_4\left(\theta^t\right)\right)\right]. \end{aligned} \tag{29}$$

As it was shown in [14], if $t \in D_k^{(p)}$, then $T_4(\theta^t) = \zeta^{2^k}$ or $T_4(\theta^t) = \zeta^{2^{4-k}}$, where ζ satisfies the relation $\zeta^8 + \zeta^4 + \zeta^2 + \zeta = 1$ and $\zeta^4 + \zeta = \mu$ over $\mathbb{F}_4$.

(i) When $t \in D_1^{(p)}$, without loss of generality, suppose that $T_4(\theta^t) = \zeta^2$. By Lemma 6, we can write $T_4(\theta^{tg^2}) = \zeta^8, T_4(\theta^{tg^3}) = \zeta$. Obviously, $\alpha^{-v} \ne 0$ for any $v = tp^i, 1 \le v \le p^m - 1$. Since

$$\begin{aligned} &\mu + 1 + T_4\left(\theta^{tg^2}\right) + T_4\left(\theta^{tg^3}\right) + \mu\left(T_4\left(\theta^{tg^3}\right) + T_4\left(\theta^t\right)\right) \\ &= \mu + 1 + \zeta^8 + \zeta + \mu\left(\zeta + \zeta^2\right) \\ &= \mu + 1 + \left(1 + \zeta^4 + \zeta^2\right) + \mu\left(\zeta + \zeta^2\right) \\ &= (\mu+1)\left(\zeta^2 + \zeta\right), \end{aligned} \tag{30}$$

and $\mu + 1 \ne 0$, then we get $\zeta^2 + \zeta = 0$ if $S'(\alpha^v) = 0$. But, this means that $\zeta^2 = \zeta$, we get a contradiction. Thus, we have $S'(\alpha^v) \ne 0$ for any $v = tp^i$, $1 \le v \le p^m - 1$.

(ii) When $t \in D_3^{(p)}$, without loss of generality, suppose that $T_4(\theta^t) = \zeta^8$. By Lemma 6, we can write $T_4(\theta^{tg^2}) = \zeta^2, T_4(\theta^{tg^3}) = \zeta^4$. Obviously, $\alpha^{-v} \ne 0$ for any $v = tp^i, 1 \le v \le p^m - 1$. Similarly, since

$$\begin{aligned} &\mu + 1 + T_4\left(\theta^{tg^2}\right) + T_4\left(\theta^{tg^3}\right) + \mu\left(T_4\left(\theta^{tg^3}\right) + T_4\left(\theta^t\right)\right) \\ &= \mu + 1 + \zeta^2 + \zeta^4 + \mu\left(\zeta^4 + \zeta^8\right) \\ &= \mu + 1 + \zeta^2 + (\mu + \zeta) + \mu\left(1 + \zeta + \zeta^2\right) \\ &= (\mu+1)\left(1 + \zeta^2 + \zeta\right), \end{aligned} \tag{31}$$

and $\mu + 1 \ne 0$, we derive that $1 + \zeta^2 + \zeta = 0$ if $S'(\alpha^v) = 0$. But, this means that $\zeta^2 + \zeta = 1$. By $\zeta^8 + \zeta^4 + \zeta^2 + \zeta = 1$, we get $\zeta^8 = \zeta^4$, i.e., $\zeta^2 = \zeta$. It is also a contradiction. Thus, we have $S'(\alpha^v) \ne 0$ for any $v = tp^i, 1 \le v \le p^m - 1$.

In conclusion, we know $S'(\alpha^v) \ne 0$ for all $v = tp^i, 1 \le v \le p^m - 1$. Then, we complete the proof. □

Theorem 2. *Let $p \equiv 1 \pmod 4$ be an odd prime. Let $\{b_2(u)\}_{u\ge 0}$ be a generalized cyclotomic quaternary sequence of period $2p^m$ defined in (10). Then, the linear complexity of $\{b_2(u)\}_{u\ge 0}$ over $\mathbb{F}_4$ is given by*

$$L(\{b_2(u)\}) = 2p^m. \tag{32}$$

Proof. The proof of this theorem is similar to that of Theorem 1. Thus, we omit it here. □

4. Linear Complexity of the Sequence over $\mathbb{Z}_4$

Let $s_u = (s_0, \cdots, s_T)$ be a quaternary sequence of period T over $\mathbb{Z}_4$, and its linear complexity $L(\{s_u\})$ is the smallest order L of a linear feedback shift register (LFSR) in $\mathbb{Z}_4$, for which there exist constants $c_1, c_2, \cdots, c_L \in \mathbb{Z}_4$ such that

$$s_j + c_1 s_{j-1} + c_2 s_{j-2} + \cdots + c_L s_{j-L} = 0, \quad j \ge L. \tag{33}$$

Also, $C(X) = 1 + c_1 X + \cdots + c_L X^L$ is called that connection polynomial. $S(X) = s_0 + s_1 X + \cdots + s_{T-1}X^{T-1} \in \mathbb{Z}_4[X]$ is called the generating polynomial of the sequence. Then, an LFSR with a connection polynomial $C(X)$ generates $\{s_u\}$ if and only if [22]

$$S(X)C(X) \equiv 0 \pmod{X^T - 1}, \tag{34}$$

where $C(X) \in \mathbb{Z}_4[X]$ satisfies $C(0) = 1$. That is,

$$\begin{aligned} L(\{s_u\}) = \min\{&\deg(C(X)) \colon C(X) \in \mathbb{Z}_4[X], \\ &C(0) = 1, S(X)C(X) \equiv 0 \pmod{X^T - 1}\}. \end{aligned} \tag{35}$$

Let $R = GR(4^r, 4)$ be a Galois ring of characteristic 4 and cardinality 4^r, where r is the order of 2 modulo p [23]. Let $R^* = R/2R$ be the group of units of R, and it contains a cyclic subgroup of order $2^r - 1$ [23]. Then, let $\beta \in R$ be of order p. We can write $\gamma = 3\beta$, and then the order of γ is $2p^m$ and

$\gamma^{p^m} = -1$. By [23], we know that $2R$ is the maximal ideal of ring R. The natural homomorphism $R \longrightarrow \overline{R} = R/2R$ will be denoted by "-" and the image $r \in R$ in $\overline{R} = R/2R$ by $\overline{r}$.

Notice that, in the ring R, the number of roots of a polynomial can be greater than its degree. Hence, we need some lemmas.

Lemma 7 (see [13]). *Let $P(x) \in \mathbb{Z}_4[x]$ be a nonconstant polynomial. If $a \in R$ is a root of polynomial $P(x)$, then there exists a polynomial $Q_1(x) \in \mathbb{Z}_4[x]$ such that*

$$P(x) = (x-a)Q_1(x). \tag{36}$$

Moreover, if $b \in R$ is also the root of $P(x)$ and $a - b \in R^*$, then

$$P(x) = (x-a)(x-b)Q_2(x), \tag{37}$$

where $Q_1(x) = (x-b)Q_2(x)$.

Lemma 8 (see [13]). *Let $P(x) \in \mathbb{Z}_4[x]$ be a nonconstant polynomial. If $P(\gamma^v) = 0$ for all $v = 1, 3, \cdots, 2p^m - 1$, then there exists polynomial $P_1(x) \in \mathbb{Z}_4[x]$ such that*

$$P(x) = P_1(x)\left(x^{p^m} + 1\right). \tag{38}$$

If $P(\gamma^v) = 0$ for all $v = 0, 2, \cdots, 2p^m - 2$, then there exists polynomial $P_2(x) \in \mathbb{Z}_4[x]$ such that

$$P(x) = P_2(x)\left(x^{p^m} - 1\right). \tag{39}$$

Theorem 3. *Let $p \equiv 1 (mod\, 4)$ be an odd prime. Let $\{s_1(u)\}_{u \geq 0}$ be a generalized cyclotomic quaternary sequence of period $2p^m$ defined in (10). Then, the linear complexity of $\{s_1(u)\}_{u \geq 0}$ over $\mathbb{Z}_4$ is given by*

$$L(\{s_1(u)\}) = 2p^m. \tag{40}$$

Proof. With notations defined as before, let $\gamma \in R^*$ be of order $2p^m$ and $\gamma^{p^m} = -1$. It is easy to know that $(x^{p^m} - 1)/(x-1) = \prod_{i=1}^{p^m-1}(1-\gamma^{2i})$. Then, $p^m = \prod_{i=1}^{p^m-1}(1-\gamma^i)\ (1+\gamma^i)$. Hence, when $j, l = 0, \cdots, p^m - 1$, we have $\gamma^j - \gamma^l \in R^*$.

By the definition of the connection polynomial and linear complexity over $\mathbb{Z}_4$, we have $L(\{s_u\}) \leq 2p^m$.

Without loss of generality, assume that $L(\{s_u\}) < 2p^m$; then, there exists a connection polynomial $C(x)$, and it satisfies

$$S(x)C(x) \equiv 0 \left(\mathrm{mod}\left(x^{2p^m} - 1\right)\right), \tag{41}$$

where the degree of $C(x)$ is less than $2p^m$.

By the definition of γ, we have $\overline{\gamma}^{p^m} = 1$ and $\overline{\gamma} \neq 0, 1$. Then, in the ring $\overline{R}$, $\sum_{j=1}^{p^m-1}\overline{\gamma}^j = 1$ holds.

By (4), we get

$$\begin{aligned} S(x) = {} & 2x^{p^m} + \sum_{j=1}^{m}\left(S_{1-k\,(\mathrm{mod}\,4)}^{(j)}(x) + R_2^{(j)}(x)\right) \\ & + 2\sum_{j=1}^{m}\left(S_{2-k\,(\mathrm{mod}\,4)}^{(j)}(x) + R_3^{(j)}(x)\right) \\ & + 3\sum_{j=1}^{m}\left(S_{3-k\,(\mathrm{mod}\,4)}^{(j)}(x) + R_0^{(j)}(x)\right). \end{aligned} \tag{42}$$

If $2 \in D_k^{(p)}, 0 \leq k \leq 3$, and by Lemma 1, we obtain

$$\begin{aligned} S(\overline{\gamma}^v) &= \sum_{j=1}^{m}\left(\sum_{u \in H_1^{(p^j)}}\overline{\gamma}^{vu} + \sum_{u \in H_2^{(p^j)}}\overline{\gamma}^{vu} + \sum_{u \in H_3^{(p^j)}}\overline{\gamma}^{vu} + \sum_{u \in H_0^{(p^j)}}\overline{\gamma}^{vu}\right) \\ &= \sum_{l=1}^{p^m-1}\overline{\gamma}^l = 1. \end{aligned} \tag{43}$$

According to (41), we have $C(\gamma^v) = 0$ for all $v = 0, 1, \cdots, 2p^m - 1, v \neq p$. Then, $(x^{p^m} - 1/x - 1) | C(x)$, which implies that there exists a polynomial $Q(x) \in \mathbb{Z}_4[x], 2Q(x) \neq 0$ such that

$$C(x) = Q(x)\frac{\left(x^{p^m-1} - 1\right)}{(x-1)}. \tag{44}$$

Moreover, it is easily seen that

$$\left|D_l^{(p^j)}\right| = \left|D_l^{(2p^j)}\right| = \frac{\varphi(p^j)}{2}, \tag{45}$$

where $l = 0, 1, 2, 3$, $j = 1, 2, \cdots, m$, and $\varphi(\cdot)$ is Euler function. Then,

$$\begin{aligned} S(1) &= 2 + (1+2+3)\sum_{j=1}^{m}\left(\frac{\varphi(p^j)}{2} + \frac{\varphi(p^j)}{2}\right) \\ &= 2 + 4\sum_{j=1}^{m}\varphi\left(p^j\right) = 2. \end{aligned} \tag{46}$$

Thus, $C(1) \in \{0, 2\}$ and $Q(1) \in \{0, 2\}$; this means that

$$\begin{aligned} Q(x) &= (x-1)F(x) + q, \quad q \in \{0, 2\}, \\ C(x) &= \frac{\left(x^{p^m} - 1\right)F(x) + q\left(x^{p^m} - 1\right)}{(x-1)}. \end{aligned} \tag{47}$$

Hence, when $v = 1, 3, \cdots, 2p^m - 1$, we have

$$C(\gamma^v) = \frac{\left(\gamma^{vp^m} - 1\right)F(\gamma^v) + q\left(\gamma^{vp^m} - 1\right)}{\left(\gamma^v - 1\right)} = -2F(\gamma^v) = 0. \tag{48}$$

In other words, when $v = 1, 3, \cdots, 2p^m - 1$, we have $2F(\gamma^v) = 0$. Then, by Lemma 8, we get $(x^{p^m} + 1) \mid 2F(x)$. But, this means that $\deg(F(x)) \geq p^m$, which is contrary to our assumption. The proof is thus completed. □

Theorem 4. *Let $p \equiv 1 (mod 4)$ be an odd prime. Let $\{s_2(u)\}_{u \geq 0}$ be a generalized cyclotomic quaternary sequence of period $2p^m$ defined in (5). Then, the linear complexity of $\{s_2(u)\}_{u \geq 0}$ over $\mathbb{Z}_4$ is given by*

$$L(\{s_2(u)\}) = 2p^m. \tag{49}$$

Proof. The proof of this theorem is similar to that of Theorem 3. Thus, we omit it here. □

5. Conclusions

This paper presented new classes of quaternary generalized cyclotomic sequences with order 4 and period $2p^m$, where p is an odd prime and $p \equiv 1 \pmod 4$. We computed their linear complexity over finite field $\mathbb{F}_4$ as well as $\mathbb{Z}_4$. The results indicated that the sequences proposed in this paper possess high linear complexities. Autocorrelation is another important measure of a sequence. For quaternary sequence s with even period over $\mathbb{Z}_4$, the optimal maximum out-of-phase autocorrelation magnitude, denoted by $R_{\max}(s)$, has been shown to be 2 [24]. For the new proposed sequence, when the period is $2p$, Edemskiy has proved that $R_{\max}(s) = 2\sqrt{2}$ if $p \equiv 5 \pmod 8$ and $R_{\max}(s) = 4$ if $p \equiv 1 \pmod 8$, respectively. However, for the general case, the autocorrelation properties of the new proposed sequences are not known. Hence, as a further work, it is valuable to analyze the autocorrelation values of the new proposed sequences.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (nos. 61772292 and 61772476), the Natural Science Foundation of Fujian Province (no. 2019J01273), and Fujian Normal University Innovative Research Team (no. IRTL1207).

References

[1] G. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communications, Cryptography and Radar Applications*, Cambridge University Press, Cambridge, UK, 2005.

[2] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.

[3] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, UK, 1997.

[4] C. Ding, T. Helleseth, and W. Shan, "On the linear complexity of legendre sequences," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1276–1278, 1998.

[5] J.-H. Kim and H.-Y. Song, "On the linear complexity of Hall's sextic residue sequences," *IEEE Transactions on Information Theory*, vol. 47, no. 5, pp. 2094–2096, 2001.

[6] T. Yan, X. Du, G. Xiao, and X. Huang, "Linear complexity of binary Whiteman generalized cyclotomic sequences of order 2k," *Information Sciences*, vol. 179, no. 7, pp. 1019–1023, 2009.

[7] X. Zeng, H. Cai, X. Tang, and Y. Yang, "Optimal frequency hopping sequences of odd length," *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 3237–3248, 2013.

[8] Z. Xiao, X. Zeng, C. Li, and T. Helleseth, "New generalized cyclotomic binary sequences of period p^2," *Designs, Codes and Cryptography*, vol. 86, no. 7, pp. 1483–1497, 2017.

[9] V. Edemskiy, C. Li, X. Zeng, and T. Helleseth, "The linear complexity of generalized cyclotomic binary sequences of period p^r," *Designs, Codes and Cryptography*, pp. 1–15, 2018.

[10] Z. Ye, P. Ke, and C. Wu, "A further study of the linear complexity of new binary cyclotomic sequence of length p^r," *Applicable Algebra in Engineering, Communication and Computing*, vol. 30, no. 3, pp. 217–231, 2019.

[11] Y. Ouyang and X. Xie, "Linear complexity of generalized cyclotomic sequences of period $2p^m$," *Designs, Codes and Cryptography*, vol. 87, no. 5, pp. 1–12, 2019.

[12] Y.-J. Kim, Y.-P. Hong, and H.-Y. Song, "Autocorrelation of some quaternary cyclotomic sequences of length $2p$," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E91-A, no. 12, pp. 3679–3684, 2008.

[13] 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*, vol. 19, no. 4, pp. 613–622, 2017.

[14] X. Du and Z. Chen, "Linear complexity of quaternary sequences generated using generalized cyclotomic classes modulo $2p$," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E94-A, no. 5, pp. 1214–1217, 2011.

[15] P. Ke, Z. Yang, and J. Zhang, "On the autocorrelation and linear complexity of some 2p periodic quaternary cyclotomic sequences over F4," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E94-A, no. 11, pp. 2472–2477, 2011.

[16] P. Ke and S. Zhang, "New classes of quaternary cyclotomic sequence of length with high linear complexity," *Information Processing Letters*, vol. 112, no. 16, pp. 646–650, 2012.

[17] L. Liu, X. Yang, B. Wei, and L. Wu, "A new class of quaternary generalized cyclotomic sequences of order 2d and length 2pm with high linear complexity," *International Journal of Wavelets, Multiresolution and Information Processing*, vol. 16, no. 1, Article ID 1850006, 2018.

[18] X. Zhou, X. Li, J. Xiao, Y. Tang, R. Abbasi, and L. Xu, "Linear complexity of generalized cyclotomic binary sequences of order $2d$ and length $2p^m$," *International Journal of Wavelets, Multiresolution and Information Processing*, vol. 14, no. 5, Article ID 1650040, 2016.

[19] V. Edemskiy and A. Ivanov, "Autocorrelation and linear complexity of quaternary sequences of period $2p$ based on cyclotomic classes of order four," in *Proceedings of the IEEE International Symposium on Information Theory*, pp. 3120–3124, Istanbul, Turkey, July 2013.

[20] J. Zhang, C.-A. Zhao, and X. Ma, "Linear complexity of generalized cyclotomic binary sequences of length 2p m," *Applicable Algebra in Engineering, Communication and Computing*, vol. 21, no. 2, pp. 93–108, 2010.

[21] J. Michel and Q. Wang, "Some new balanced and almost balanced quaternary sequences with low autocorrelation," *Cryptography and Communications*, vol. 11, no. 2, pp. 191–206, 2019.

[22] P. Udaya and M. U. Siddiqi, "Generalized GMW quadriphase sequences satisfying the Welch bound with equality," *Applicable Algebra in Engineering, Communication and Computing*, vol. 10, no. 3, pp. 203–225, 2000.

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

[24] X. Tang and C. Ding, "New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value," *IEEE Transactions on Information Theory*, vol. 56, no. 12, pp. 6398–6405, 2010.