information

Article

New Generalized Cyclotomic Quaternary Sequences with Large Linear Complexity and a Product of Two Primes Period

Jiang Ma, Wei Zhao, Yanguo Jia * and Haiyang Jiang

School of Information Science and Engineering, Yanshan University, Qinhuangdao 066004, China; mj2021@stumail.ysu.edu.cn (J.M.); lrjw@ysu.edu.cn (W.Z.); jianghy2018@stumail.ysu.edu.cn (H.J.)
* Correspondence: jyg@ysu.edu.cn; Tel.: +86-135-0335-4988

Abstract: Linear complexity is an important criterion to characterize the unpredictability of pseudo-random sequences, and large linear complexity corresponds to high cryptographic strength. Pseudo-random Sequences with a large linear complexity property are of importance in many domains. In this paper, based on the theory of inverse Gray mapping, two classes of new generalized cyclotomic quaternary sequences with period *pq* are constructed, where *pq* is a product of two large distinct primes. In addition, we give the linear complexity over the residue class ring Z_4 via the Hamming weights of their Fourier spectral sequence. The results show that these two kinds of sequences have large linear complexity.

Keywords: stream ciphers; finite field; quaternary sequence; Fourier spectral sequence; linear complexity

Citation: Ma, J.; Zhao, W.; Jia, Y.; Jiang, H. New Generalized Cyclotomic Quaternary Sequences with Large Linear Complexity and a Product of Two Primes Period. *Information* **2021**, *12*, 193. https://doi.org/10.3390/info12050193

Academic Editor: Giorgio Kaniadakis

Received: 29 March 2021
Accepted: 26 April 2021
Published: 28 April 2021

1. Introduction

Pseudo-random sequences with large linear complexity and low nontrivial autocorrelation values are widely applied in spread spectrum communication, radar navigation, cryptography, code division multiple access, especially stream cipher. The linear complexity of a sequence is defined as the smallest order of linear feedback shift register that can generate the whole sequence. According to the Berlekamp–Massey algorithm, a large linear complexity should be no less than a half of the period of the sequence [1,2]. Binary sequences with good pseudo-random properties have been studied in depth in recent decades [2]. Compared with binary sequences, quaternary sequences have a higher transmission rate, and a code element can represent more bits of information. Moreover, quaternary sequences have important applications in the four-phase spread spectrum system [3]. Therefore, quaternary sequences are attracting more and more researchers to consider them. Most references have concentrated on the linear complexity of quaternary sequences over F_4 [4–7]. However, there has been less attention to the linear complexity of sequences over Z_4 due to the phenomenon of zero divisors in Z_4 [8].

Inverse Gray mapping is one of the main methods for constructing quaternary sequences [9]. Given two arbitrary binary sequences of equal length, a unique quaternary sequence can be determined by inverse Gray mapping. Kim et al. constructed a class of quaternary sequences with period $2p$ over Z_4 by the use of a Legendre sequence pair. They analyzed the autocorrelation properties and the linear complexity of these sequences [10,11]. Yang et al. defined a class of quaternary sequence on Z_4 by using the Whiteman generalized cyclotomic binary sequence pair and calculated the autocorrelation values [12]. Li et al. analyzed the linear complexity of the sequence which was constructed in [12] by considering the weights of Fourier spectral sequence of the sequence [13,14]. Wang et al. established a class of quaternary sequence on Z_4 based on the balanced Whiteman generalized cyclotomic binary sequence pair and gave the linear complexity of the sequence [15]. Wei et al. introduced the quaternary sequence on Z_4 based on the Ding generalized cyclotomic binary sequence pair and discussed the linear complexity of the sequence [16,17]. The quaternary sequences mentioned above all are constructed by selecting two homogeneous binary sequences. It is necessary to confirm whether the quaternary sequences constructed by binary sequences with greater distinction have large linear complexity.

First, this paper proposes a new class of quaternary sequences with period pq based on the Whiteman generalized cyclotomic binary sequence and the Ding generalized cyclotomic binary sequence, which can be denoted by the first class of the generalized cyclotomic quaternary sequence. Second, this paper proposes a new class of quaternary sequences with period pq based on the Ding generalized cyclotomic binary sequence and the new Ding generalized cyclotomic binary sequence [17,18], which can be denoted by the second class of the generalized cyclotomic quaternary sequence. Moreover, the linear complexity of the two quaternary sequences is computed by considering the Hamming weight of their Fourier spectral sequences.

2. Preliminaries

Suppose that $S = \{S_i\}$ is a sequence over F_r with period N, where r is an odd prime, F_r is the finite field with r elements, and N divides $r^m - 1$ ($m \geq 1$, m is a positive integer). The linear complexity $LC(S)$ of the sequence S is the smallest positive integer L satisfying

$$s_i + c_1 s_{i-1} + \cdots + c_{L-1} s_{i-L+1} + c_L s_{i-L} = 0, \ \ for \ \ L \leq i \leq N. \tag{1}$$

where the coefficients $c_1, c_2, \cdots c_L \in F_r$. The generating polynomial of S is defined by

$$s(x) \ = \sum_{i=0}^{N-1} s_i x^i \in F_r[x] \tag{2}$$

Definition 1. *[1] Let θ be an element inF_{r^m} of order N. Then the discrete Fourier Transform of S* is defined as

$$A_k = \sum_{t=0}^{N-1} S(t) \ \ \theta^{tk}, \ \ 0 \leq k \leq N-1 \tag{3}$$

The inverse formula of Equation (1) is given by

$$S(t) \ = \frac{1}{N} \sum_{t=0}^{N-1} A_k \theta^{-tk}, \ \ 0 \leq t \leq N-1 \tag{4}$$

where A_k is called a Fourier spectrum of the sequence S. Note that $A = \{A_k\}$ is called a Fourier spectrum sequence with period N of S.

Lemma 1. *[1]* $\sum_{i=0}^{N-1} \theta^{di} = \begin{cases} 0, & if \ d \equiv 0 \ (modN) \\ N, & otherelse \end{cases}$.

Lemma 2. *[14] Let$A = \{A_k\}$ be the Fourier spectrum sequence of S. Then the linear complexity of S* is given by

$$LC(S) \ = \ |\{k | A_k \neq 0, \ \ 0 \leq k \leq N-1\}| \tag{5}$$

The linear complexity of S is further derived as

$$LC(S) \ = \ N - |\{k | A_k \neq 0, \ \ 0 \leq k \leq N-1\}| \tag{6}$$

Definition 2. *Let$a(t)$ and$b(t)$ be a binary sequence with period N. Let $\psi[x,y]$* be the inverse Gray mapping defined by

$$\psi[a(t), b(t)] \ = \begin{cases} 0, \ if \ (a,b) & = \ (0,0) \\ 1, \ if \ (a,b) & = \ (0,1) \\ 2, \ if \ (a,b) & = \ (1,1) \\ 3, \ if \ (a,b) & = \ (1,0) \end{cases} . \tag{7}$$

Definition 3. *Indicator functions $I_p(t)$ and $I_q(t)$ are defined as*

$$I_p(t) = \begin{cases} 1, & if \ t \equiv 0 \, (\mathrm{mod} p), \\ 0, & \text{otherwise.} \end{cases} \qquad I_q(t) = \begin{cases} 1, & if \ t \equiv 0 \, (\mathrm{mod} q), \\ 0, & \text{otherwise.} \end{cases} . \tag{8}$$

Definition 4. *The quadratic characters $\eta_p(t)$ and $\eta_q(t)$ are defined as*

$$\eta_p(t) = \begin{cases} 0, & t \equiv 0(\mathrm{mod} p) \\ 1, & t \in QR_p \\ -1, & t \in NQR_p \end{cases} \qquad \eta_q(t) = \begin{cases} 0, & t \equiv 0(\mathrm{mod} q) \\ 1, & t \in QR_p \\ -1, & t \in NQR_p \end{cases} \tag{9}$$

where QR_p and NQR_p are the sets of quadratic residues and quadratic non-residues in the set of integers modulo p, respectively; By symmetry, QR_p and NQR_p are defined similarly.

3. The Linear Complexity of the First Class of Generalized Cyclotomic Quaternary Sequences

Let p and q be two distinct odd primes and set $N = pq$. Define that $P = \{p, 2p, 3p, \cdots (q-1)p\}$, $Q = \{q, 2q, 3q, \cdots (p-1)q\}$, then the residue ring $Z_N = \{0\} \cup P \cup Q \cup Z_N^*$, where Z_N^* denotes the set of all invertible elements in Z_N. According to the Chinese remainder theorem, we can get $Z_N \cong Z_p \times Z_q$, $t \mapsto (t_1, t_2)$ for $\forall t \in Z_N$, where $t = t_1(\mathrm{mod} p)$, $t = t_2(\mathrm{mod} q)$.

The two generalized cyclotomic binary sequences are presented as follows.

$$S_1(t) = \begin{cases} 1, & t \in P \\ 0, & t \in \{0\} \cup Q \\ \frac{1-\eta_p(t)\eta_q(t)}{2}, & t \in Z_N^* \end{cases} \quad S_2(t) = \begin{cases} 1, & t \in P \\ 0, & t \in \{0\} \cup Q \\ \frac{1-\eta_q(t)}{2}, & t \in Z_N^* \end{cases} \tag{10}$$

where $S_1(t)$ is the Whiteman generalized cyclotomic binary sequences of order two with period pq [17], $S_2(t)$ is the Ding generalized cyclotomic binary sequences of order two with period pq [2]. Then, the first class of the generalized cyclotomic quaternary sequence can be expressed by $S'(t) = \psi[S_1(t), S_2(t)]$. Clearly that the sequence $S'(t)$ is different from those in references [12,15,16]. Moreover, when t ranges over Z_N^*, every element in $S'(t)$ takes on the same times.

The linear complexity of a periodic sequence can be determined by counting the number of nonzero coefficients of its discrete Fourier transform, which is defined over a finite field [11]. Therefore, a proper field should be found for the linear representation [11].

Let θ be a primitive pq-th root of unity in F_{r^m} where $r \geq 5$ is the odd prime which is not equal to p or q and F_{r^m} is the splitting field of $x^{pq} - 1$. Suppose that $\alpha = \theta^q$, $\beta = \theta^p$ is the pth and qth primitive root of unity in the field F_{r^m}, respectively.

According to the definitions of indicator function and quadratic character, the sequences $S_1(t)$ and $S_2(t)$ can be expressed as

$$S_1(t) = \frac{1}{2}\left[1 - \eta_p(t_1)\eta_q(t_2) + I_p(t_1) - I_q(t_2) - I_p(t_1)I_q(t_2)\right] \tag{11}$$

$$S_2(t) = \frac{1}{2}\left\{1 - \left[1 - I_p(t_1)\right]\left[1 - I_q(t_2)\right]\eta_q(t_2) + I_p(t_1) - I_q(t_2) - I_p(t_1)I_q(t_2)\right\} \tag{12}$$

Then we can derive the representation of $S'(t)$

$$\begin{aligned} S'(t) &= \psi[S_1(t), S_2(t)] = 3S_1(t) + S_2(t) - 2S_1(t)S_2(t) = \tfrac{1}{2}\big[3 - 2\eta_p(t_1)\eta_q(t_2) \\ &+ I_p(t_1) - 3I_q(t_2) - I_p(t_1)I_q(t_2) - \eta_p(t_1)\eta_q^2(t_2) - I_q(t_2)\eta_p(t_1)\eta_q(t_2) + \\ &I_p(t_1)\eta_p(t_1)\eta_q(t_2) - I_p(t_1)I_q(t_2)\eta_p(t_1)\eta_q(t_2) + I_p(t_1)\eta_p(t_1)\eta_q^2(t_2) - \\ &I_p(t_1)I_q(t_2)\eta_p(t_1)\eta_q^2(t_2) + I_q(t_2)\eta_p(t_1)\eta_q^2(t_2)\big] \end{aligned} \tag{13}$$

Note that the representation holds for $r \geq 5$.

The term of Fourier spectral sequence $A' = (A'_k)$ of sequence $S'(t)$ is defined by

$$\begin{aligned} A' = \sum_{t=0}^{N-1} S'(t)\theta^{tk} = \frac{1}{2}\Bigg[3\sum_{t=0}^{N-1}\theta^{tk} - 2\sum_{t=0}^{N-1}\eta_p(t_1)\eta_q(t_2)\theta^{tk} + \sum_{t=0}^{N-1} I_p(t_1)\theta^{tk} \\ -3\sum_{t=0}^{N-1} I_q(t_2)\theta^{tk} - \sum_{t=0}^{N-1} I_p(t_1)I_q(t_2)\theta^{tk} - \sum_{t=0}^{N-1}\eta_p(t_1)\eta_q^2(t_2)\theta^{tk} \end{aligned} \tag{14}$$

Lemma 3. *[6] Let θ be such a primitive pqth root of unity over F_{r^m}*, then

$$\sum_{t \in Z_N}^{N-1} \theta^i = 0, \sum_{t \in pZ_q^*}^{N-1} \theta^i = -1(\mathrm{mod} r), \sum_{t \in qZ_p^*}^{N-1} \theta^i = -1(\mathrm{mod} r). \tag{15}$$

Lemma 4. *[13]*

$$\sum_{t=0}^{N-1} \eta_p(t_1)\eta_q(t_2)\theta^{tk} = \begin{cases} 0, & k \in \{0\} \cup pZ_q^* \cup qZ_p^* \\ \pm(S_p - S_{Np})(S_q - S_{Nq}), & k \in Z_N^*, \eta_p(k)\eta_q(k) = \pm 1 \end{cases} \tag{16}$$

where $S_p = \sum_{i \in QR_p} \alpha^i$, $S_{Np} = \sum_{i \in NQR_p} \alpha^i$; $S_q = \sum_{i \in QR_q} \beta^i$, $S_{Nq} = \sum_{i \in NQR_q} \beta^i$.

Lemma 5. *[13]*

$$\sum_{t=0}^{N-1} I_p(t_1)\theta^{tk} = \begin{cases} q(\mathrm{mod} r), & k \in \{0\} \cup qZ_p^* \\ 0, & k \in Z_N^* \cup pZ_q^* \end{cases} \tag{17}$$

$$\sum_{t=0}^{N-1} I_q(t_2)\theta^{tk} = \begin{cases} p(\mathrm{mod} r), & k \in \{0\} \cup pZ_q^* \\ 0, & k \in Z_N^* \cup qZ_p^* \end{cases}. \tag{18}$$

Lemma 6. *[13]*

$$\sum_{t=0}^{N-1} I_p(t_1)I_q(t_2)\theta^{tk} = 1, 0 \leq k \leq N-1. \tag{19}$$

Lemma 7.

$$\sum_{t=0}^{N-1} \eta_p(t_1)\eta_q^2(t_2)\theta^{tk} = \begin{cases} 0, & k = 0 \\ \pm(S_p - S_{Np}), & k \in Z_N^* \\ 0, & k \in pZ_q^* \\ \pm(S_p - S_{Np}) * (q-1)(\mathrm{mod} r), & k \in qZ_p^* \end{cases}. \tag{20}$$

Proof. By Chinese Remainder Theorem, we know $t = qq_p^{-1}t_1 + pp_q^{-1}t_2(\mathrm{mod} pq)$, where q_p^{-1} represents the inverse element of $q(\mathrm{mod} p)$, and p_q^{-1} represents the inverse element of $p(\mathrm{mod} q)$. Then

$$\begin{aligned} \sum_{t=0}^{N-1} \eta_p(t_1)\eta_q^2(t_2)\theta^{tk} &= \sum_{t_1 \in Z_p^*} \eta_p(t_1)\theta^{kqq_p^{-1}t_1} \sum_{t_2 \in Z_q^*} \eta_q^2(t_2)\theta^{kpp_q^{-1}t_2} \\ &= \sum_{t_2 \in Z_q^*} \beta^{kt_2}\left(\sum_{t_1 \in QR_p} \alpha^{kt_1} - \sum_{t_1 \in NQR_p} \alpha^{kt_1}\right) \end{aligned} \tag{21}$$

Note that $p \nmid q_p^{-1}$, then $\theta^{qq_p^{-1}}$ is the pth primitive root of unity, denoted as α. Similarly, $\theta^{pp_q^{-1}}$ is the qth primitive root of unity, denoted as β.

If $k=0$, $\sum_{t=0}^{N-1}\eta_p(t_1)\eta_q^2(t_2)\theta^{tk}=(q-1)\cdot 0(\text{mod}r)=0$.

If $k\in pZ_q^*$, $\sum_{t=0}^{N-1}\eta_p(t_1)\eta_q^2(t_2)\theta^{tk}=0*(-1)(\text{mod}r)=0$.

If $k\in qZ_p^*$, $\sum_{t=0}^{N-1}\eta_p(t_1)\eta_q^2(t_2)\theta^{tk}=\pm(S_p-S_{Np})*(q-1)(\text{mod}r)$.

If $k\in Z_N^*$ and $k(\text{mod}p)\in QR_p$, $\sum_{t=0}^{N-1}\eta_p(t_1)\eta_q^2(t_2)\theta^{tk}=-(S_p-S_{Np})$.

If $k\in Z_N^*$ and $k(\text{mod}p)\in NQR_p$, $\sum_{t=0}^{N-1}\eta_p(t_1)\eta_q^2(t_2)\theta^{tk}=(S_p-S_{Np})$. □

Lemma 8. *Let* $(S_p-S_{Np})=\delta$ *and* $(S_p-S_{Np})=\xi$. *Then*

$$A_k'=\begin{cases}\frac{(3p+1)(q-1)}{2}, & if\ k=0\\ \frac{-2\delta\xi-(1\pm\delta)}{2}, & if\ k\in Z_N^*,\eta_p(k)\eta_q(k)=1\\ \frac{2\delta\xi-(1\pm\delta)}{2}, & if\ k\in Z_N^*,\eta_p(k)\eta_q(k)=-1\\ \frac{-(3p+1)}{2}, & if\ k\in pZ_q^*\\ \frac{(q-1)(1\pm\delta)}{2}, & if\ k\in qZ_p^*\end{cases} \tag{22}$$

Proof. The proof is omitted because A' can be easily obtained by the lemmas 3–7. □

Lemma 9. *[13]* $S_p\in F_r$ *if and only if* $r\in QR_p$; $S_q\in F_r$ *if and only if* $r\in QR_q$.

Theorem 1. *Suppose that* $r\geq 5$ *, the linear complexity of the generalized cyclotomic quaternary sequence* $S'(t)$ with period pq is calculated as follows.

(1) *If r satisfies one of two cases:* $\eta_p(r)\eta_q(r)=-1$; $\eta_p(r)\eta_q(r)=1$ *and* $\pm 2\delta\xi\neq(1\pm\delta)(\text{mod}r)$. *Then*

$$LC(S')=\begin{cases}pq, & if r\nmid(3p+1),r\nmid(q-1),r\nmid(1\pm\delta)\\ pq-p+1, & if r\nmid(3p+1),r\nmid(q-1),r|(1\pm\delta)\\ pq-p, & if r\nmid(3p+1),r|(q-1)\\ pq-q, & if r|(3p+1),r\nmid(q-1),r\nmid(1\pm\delta)\\ pq-p-q+1, & otherwise.\end{cases} \tag{23}$$

(2) *If r satisfies one of two cases:* $\eta_p(r)\eta_q(r)=1$ *and* $-2\delta\xi=(1\pm\delta)(\text{mod}r)$; $\eta_p(r)\eta_q(r)=1$ *and* $2\delta\xi=(1\pm\delta)(\text{mod}r)$. *Then*

$$LC(S')=\begin{cases}(pq+p+q-1)/2, if\ r\nmid(3p+1),r\nmid(q-1),r\nmid(1\pm\delta)\\ (pq-p+q+1)/2, if\ r\nmid(3p+1),r\nmid(q-1),r|(1\pm\delta)\\ (pq-p+q-1)/2, if\ r\nmid(3p+1),r|(q-1)\\ (pq+p-q-1)/2, if\ r|(3p+1),r\nmid(q-1),r\nmid(1\pm\delta)\\ (pq-p-q+1)/2, otherwise.\end{cases} \tag{24}$$

Proof. (1) If r meets $\eta_p(r)\eta_q(r)=-1$, then $\delta\xi\in F_{r^m}\backslash F_r$, when $k\in Z_N^*$. That is, $\pm 2\delta\xi-(1\pm\delta)\neq 0(\text{mod}r)$ for $k\in Z_N^*$.

If r meets $\eta_p(r)\eta_q(r) = 1$, then $\delta\xi \in F_r$. We know $\pm 2\delta\xi \neq (1 \pm \delta)(\mathrm{mod}\, r)$. Easily, we get

$$A'_k = \begin{cases} \frac{(3p+1)(q-1)}{2}, & if\ k = 0 \\ \frac{\pm 2\delta\xi - (1\pm\delta)}{2} \neq 0, & if\ k \in Z_N^* \\ \frac{-(3p+1)}{2}, & if\ k \in pZ_q^* \\ \frac{(q-1)(1\pm\delta)}{2}, & if\ k \in qZ_p^* \end{cases} \tag{25}$$

The result is clear.

(2) Similar proof is omitted. □

4. The Linear Complexity of the Second Class of Generalized Cyclotomic Quaternary Sequences

In order to construct cyclic codes, Ding described a new generalized cyclotomy (V_0, V_1), which is a new segmentation of the Ding–Helleseth generalized cyclotomy of order two [2]. By use of this cyclotomic class, Liu et al. constructed a generalized cyclotomic sequence [19]. Let the symbols and the functions be the same as before. It is easy to see that this sequence can be expressed as

$$S_3(t) = \begin{cases} 1, & t \in P \\ 0, & t \in \{0\} \cup Q \\ \frac{1-\eta_p(t)}{2}, & t \in Z_N^* \end{cases} \tag{26}$$

Define the second class of generalized cyclotomic quaternary sequence with period $N = pq$ as $S''(t) = \psi[S_2(t), S_3(t)]$. Clearly, the sequence $S''(t)$ is different from those in references [12,15,16]. Moreover, when t ranges over Z_N^*, every element in $S''(t)$ takes on the same times.

According to the definitions of indicator function and quadratic character, the sequences $S_3(t)$ can be expressed as

$$S_3(t) = \frac{1}{2}\{1 - [1 - I_p(t_1)][1 - I_q(t_2)]\eta_p(t_1) + I_p(t_1) - I_q(t_2) - I_p(t_1)I_q(t_2)\} \tag{27}$$

Then we can derive the representation of $S''(t)$

$$\begin{aligned} S''(t) &= \psi[S_2(t), S_3(t)] = 3S_2(t) + S_3(t) - 2S_2(t)S_3(t) \\ &= \tfrac{1}{2}[3 + I_p(t_1) - 3I_q(t_2) - 2\eta_q(t_2) + 2I_q(t_2)\eta_q(t_2) + 2I_p(t_1)\eta_q(t_2) \\ &\quad - I_p(t_1)I_q(t_2) - \eta_p(t_1)\eta_q(t_2) + I_q(t_2)\eta_p(t_1)\eta_q(t_2) + I_p(t_1)\eta_p(t_1) \\ &\quad \eta_q(t_2) - 2I_p(t_1)I_q(t_2)\eta_q(t_2) - I_p(t_1)I_q(t_2)\eta_p(t_1)\eta_q(t_2)] \end{aligned} \tag{28}$$

The term of Fourier spectral sequence $A'' = (A'')$ of sequence $S''(t)$ is defined by

$$\begin{aligned} A'' &= \sum_{t=0}^{N-1} S''(t)\theta^{tk} = \frac{1}{2}\Big[3\sum_{t=0}^{N-1}\theta^{tk} + \sum_{t=0}^{N-1} I_p(t_1)\theta^{tk} - 3\sum_{t=0}^{N-1} I_q(t_2)\theta^{tk} - 2\sum_{t=0}^{N-1}\eta_q(t_2)\theta^{tk} \\ &\quad + 2\sum_{t=0}^{N-1} I_p(t_1)\eta_q(t_2)\theta^{tk} - \sum_{t=0}^{N-1} I_p(t_1)I_q(t_2)\theta^{tk} - \sum_{t=0}^{N-1}\eta_p(t_1)\eta_q(t_2)\theta^{tk}\Big] \end{aligned} \tag{29}$$

Lemma 10. *[16]*

$$\sum_{t=0}^{N-1} \eta_q(t_2)\theta^{tk} = \begin{cases} 0, & k \in \{0\} \cup qZ_p^* \cup Z_N^* \\ p\xi, & k \in pZ_q^*, k \in QR_q \\ -p\xi, & k \in pZ_q^*, k \in NQR_q \end{cases}. \tag{30}$$

Lemma 11. [16]

$$\sum_{t=0}^{N-1} I_p(t_1)\eta_q(t_2)\theta^{tk} = \begin{cases} 0, & k \in \{0\} \cup qZ_p^* \\ \xi, & k \in Z_N^* \cup pZ_q^*, k \in QR_q \\ -\xi, & k \in Z_N^* \cup pZ_q^*, k \in NQR_q \end{cases}. \tag{31}$$

Lemma 12. *Let* $2\xi(p-1)+(3p+1)=\sigma$, *then*

$$A'' = \begin{cases} \frac{(3p+1)(q-1)}{2}, & if\ k=0 \\ \frac{\xi(2\pm\delta)-1}{2}, & if\ k \in Z_N^*, \eta_p(k)=1 \\ \frac{-\xi(2\pm\delta)-1}{2}, & if\ k \in Z_N^*, \eta_p(k)=-1 \\ \frac{\pm\sigma}{2}, & if\ k \in pZ_q^* \\ \frac{q-1}{2}, & if\ k \in qZ_p^* \end{cases} \tag{32}$$

Proof. The proof is omitted because A'' can be easily obtained by the lemmas 3–6, 10,11. □

Theorem 2. *Suppose that* $r \geq 5$, *the linear complexity of generalized cyclotomic quaternary sequence* $S''(t)$ *with period pq is calculated as follows.*

(1) If r satisfies one of two cases:

$\eta_p(r)\eta_q(r)=-1; \eta_p(r)\eta_q(r)=1$ and $\pm\xi(2\pm\delta)\neq 1(\mathrm{mod} r)$. Then

$$LC(S'') = \begin{cases} pq, & if\ r \nmid (3p+1), r \nmid (q-1), r \nmid \pm\sigma \\ pq-q+1, & if\ r \nmid (3p+1), r \nmid (q-1), r | \pm\sigma \\ pq-p-q+1, & if\ r | (q-1), r | \pm\sigma \\ pq-p, & if\ r | (q-1), r \nmid \pm\sigma \\ pq-1, & if\ r | (3p+1), r \nmid (q-1), r \nmid \pm\sigma \\ pq-q, & if\ r | (3p+1), r \nmid (q-1), r | \pm\sigma \end{cases} \tag{33}$$

(2) If r satisfies cases:

$\eta_p(r)\eta_q(r)=1$ and $\pm\xi(2\pm\delta)=1(\mathrm{mod} r)$. Then

$$LC(S'') = \begin{cases} (pq+p+q-1/2, if\ r \nmid (3p+1), r \nmid (q-1), r \nmid \pm\sigma \\ (pq+p-q+1)/2, if\ r \nmid (3p+1), r \nmid (q-1), r | \pm\sigma \\ (pq-p-q+1)/2, if\ r | (q-1), r | \pm\sigma \\ (pq-p+q-1)/2, if\ r | (q-1), r \nmid \pm\sigma \\ (pq+p+q-3)/2, if\ r | (3p+1), r \nmid (q-1), r \nmid \pm\sigma \\ (pq+p-q-1)/2, if\ r | (3p+1), r \nmid (q-1), r | \pm\sigma \end{cases} \tag{34}$$

Proof. (1) If r meets $\eta_p(r)\eta_q(r)=-1$, then $\delta\xi \in F_{r^m} \backslash F_r$, when $k \in Z_N^*$. That is, $\pm\xi(2\pm\delta)\neq 1(\mathrm{mod} r)$ for $k \in Z_N^*$

If r meets $\eta_p(r)\eta_q(r)=1$, then $\delta\xi \in F_r$. So, $\pm\xi(2\pm\delta)\neq 1(\mathrm{mod} r)$. Easily, we get

$$A'' = \begin{cases} \frac{(3p+1)(q-1)}{2}, & if\ k=0 \\ \frac{\pm\xi(2\pm\delta)-1}{2} \neq 0, & if\ k \in Z_N^* \\ \frac{\pm\delta}{2}, & if\ k \in pZ_q^* \\ \frac{q-1}{2}, & if\ k \in qZ_p^* \end{cases} \tag{35}$$

The result is clear.

(2) Similar proof is omitted. □

5. Conclusions

Pseudorandom sequences with period *pq* have been taken seriously, as *pq* is the RSA modulus, which involves the complex problem of large integer factorization. This paper constructs two classes of new generalized cyclotomic quaternary sequences with period *pq* over Z_4 by choosing different kinds of generalized cyclotomic binary sequence pairs, and investigates the linear complexity respectively by counting the number of nonzero terms of their Fourier spectral sequence. More quaternary pseudorandom sequences can be constructed according to this idea. We estimate that most of them have large linear complexity, and some of them may have low autocorrection.

In view of symmetry, we suppose that $p < q$. The results show that, the first class of the generalized cyclotomic quaternary sequence has lower linear complexity only if $\eta_p(r)\eta_q(r) = 1$, $\pm 2\delta\xi = (1 \pm \delta)(\text{mod} r)$ and $r|(3p+1)$; the second one has lower linear complexity only if $\eta_p(r)\eta_q(r) = 1$, $\pm\xi(2 \pm \delta) = 1(\text{mod} r)$ and $r|\pm\sigma$. In other cases, the linear complexity of the two classes of quaternary sequences is greater than half of the period. Therefore, the two classes of the new sequences in this paper have a large linear complexity in resisting the attack of the Berlekamp–Massey algorithm. Compared with references [12,15,16], the linear complexity of the quaternary sequences constructed in this paper have more values, which make them adapt to more kinds of Linear feedback shift register with different orders. The next step planned is to study the autocorrelation of the two classes of the new quaternary sequences.

Author Contributions: Conceptualization, J.M. and Y.J.; methodology, J.M.; software, W.Z.; validation, Y.J., W.Z. and H.J.; resources, Y.J.; writing—original draft preparation, J.M.; writing—review and editing, J.M. and Y.J.; project administration, Y.J.; funding acquisition, Y.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (61501395, 61601401), the Natural Science Foundation of Hebei Province (F2016203293, F2018203057) and the research project for science and technology in Higher education of Hebei (QN2021144).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used to support the findings of this study are included within the article.

Conflicts of Interest: The authors declare that they have no conflict of interest.

References

1. Golomb, S.W.; Gong, G. *Signal Design for Good Correlation: For Wireless Communications, Cryptography and Radar Application*; Cambridge University Press: Cambridge, UK, 2005.
2. Cusick, T.W.; Ding, C.; Renvall, A. *Stream Ciphers and Number Theory*; Elsevier: Amsterdam, The Netherlands, 2004.
3. Hu, L.; Yue, Q. Gauss periods and codebooks from generalized cyclotomic sets of order four. *Des. Codes Crypt.* **2013**, *69*, 233–246. [CrossRef]
4. Du, X.; Chen, Z. Linear complexity of quaternary sequence generated using generalized cyclotomic classes modulo 2p. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2011**, *94*, 1214–1217.
5. Ke, P.; Zhang, S. New classes of quaternary cyclotomic sequence of length $2p^m$ with high linear complexity. *Inf. Process. Lett.* **2012**, *112*, 646–650. [CrossRef]
6. Chang, Z.; Li, D. On the linear complexity of the quaternary cyclotomic sequences with the period 2pq. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2014**, *97-A*, 679–684.
7. Edemskiy, V.; Ivanov, A. Linear complexity of quaternary sequences of length pq with low autocorrelation. *J. Comput. Appl. Math.* **2014**, *259B*, 555–560. [CrossRef]
8. Chen, Z. Linear complexity and trace representation of quaternary sequences over Z_4 based on generalized cyclotomic classes modulo pq. *Cryptogr. Commun.* **2017**, *9*, 445–458. [CrossRef]
9. Krone, S.M.; Sarwate, D.V. Quadriphase sequences for spread spectrum multiple-access communication. *IEEE Trans. Inf. Theory* **1984**, *IT-30*, 520–529. [CrossRef]
10. Kim, Y.S.; Jang, J.W.; Kim, S.H.; No, J.S. New construction of quaternary sequences with ideal autocorrelation from Legendre sequences. *IEEE Int. Symp. Inf. Theory* **2009**, 282–285. [CrossRef]

11. Kim, Y.S.; Jang, J.W.; Kim, S.H.; No, J.S. Linear complexity of quaternary sequences constructed from binary Legendre sequences. In Proceedings of the 2012 International Symposium on Information Theory and Its Applications, IEEE, Honolulu, HI, USA, 28–31 October 2013.
12. Zheng, Y.; Pinhui, K. Construction of quaternary sequences of length pq with low auto- correlation. *Cryptogr. Commun.* **2011**, *3*, 55–64.
13. Li, D.D.; Wen, Q.Y.; Zhang, J.; Chang, Z.L. Linear Complexity of Generalized Cyclotomic Quaternary Sequences with Period pq. *IEICE Trans. Fundam.* **2014**, *97*, 1153–1158. [CrossRef]
14. Blahut, R.E. Transform techniques for error control codes. *IBM J. Res. Develop.* **1979**, *23*, 299–315. [CrossRef]
15. Wang, G.H.; Du, X.N.; Wan, Y.Q.; Li, Z.X. Linear complexity of balanced quaternary generalized cyclotomic sequences with Period pq. *J. Shandong Univ.* **2016**, *51*, 145–150.
16. Wei, W.Y.; Du, X.N.; Li, Z.X.; Wan, Y.Q. Linear Complexity of Quaternary Generalized Cyclotomic Sequences with Period pq. *Comput. Sci.* **2017**, *44*, 174–176.
17. Ding, C. Autocorrelation values of generalized cyclotomic sequences. *IEEE Trans. Inf. Theory* **1998**, *44*, 1699–1702. [CrossRef]
18. Ding, C. Cyclotomic constructions of cyclic codes with length being the product of two primes. *IEEE Trans. Inf. Theory* **2012**, *58*, 2231–2236. [CrossRef]
19. Liu, H.; Chen, X. Autocorrelation Values and Linear Complexity of New Generalized Cyclotomic squences. *Acta Math. Sin.* **2019**, *3*, 233–246.