Hindawi
Journal of Mathematics
Volume 2021, Article ID 5535887, 10 pages
https://doi.org/10.1155/2021/5535887

Research Article

Autocorrelation and Linear Complexity of Binary Generalized Cyclotomic Sequences with Period *pq*

Yan Wang, Liantao Yan, Qing Tian, and Liping Ding

School of Science, Xi'an University of Architecture and Technology, Xi'an 710055, China

Correspondence should be addressed to Liantao Yan; yanliantao@xauat.edu.cn

Received 26 February 2021; Revised 27 March 2021; Accepted 3 April 2021; Published 26 April 2021

Academic Editor: Tianping Zhang

Ding constructed a new cyclotomic class (V_0, V_1). Based on it, a construction of generalized cyclotomic binary sequences with period pq is described, and their autocorrelation value, linear complexity, and minimal polynomial are confirmed. The autocorrelation function $C_S(w)$ is 3-level if $p \equiv 3\text{mod}4$, and $C_S(w)$ is 5-level if $p \equiv 1\text{mod}4$. The linear complexity $\text{LC}(S) > (pq/2)$ if $p \equiv 1 \bmod 8$, $p > q + 1$, or $p \equiv 3\text{mod}4$ or $p \equiv -3\text{mod}8$. The results show that these sequences have quite good cryptographic properties in the aspect of autocorrelation and linear complexity.

1. Introduction

Pseudorandom sequences with good cryptography properties have wide applications in CDMA, global positing systems, and stream ciphers. The security of stream ciphers depends on the randomness of the key stream, which makes the construction of pseudorandom sequences to be an important research direction. Many researchers focused on cyclotomic sequences, which have good balance property. Linear complexity and autocorrelation are important criteria for measuring unpredictability of cyclotomic sequences.

Let F_l denote a finite field with l elements, where l is a prime power. A sequence $S = \{s_i\}$ is periodic if there exists a positive integer N such that $s_{j+N} = s_j$ for all $j \geq 0$.

Let $S = \{s_i\}$ be a periodic sequence over F_l with period N. The periodic autocorrelation function of binary sequence S is defined by

$$C_S(w) = \sum_{i=0}^{N-1} (-1)^{s_{i+w}+s_i}, \tag{1}$$

where $0 \leq w \leq N-1$.

Autocorrelation function measures the amount of similarity between sequence S and a shift of S by w shifts. Only when the values of $C_S(w)$ distribute flat and low, sequence S is easy to distinguish from each time shifted version of itself. The autocorrelation function with the ideal distribution of values is two-valued, which is given as

$$C_S(w) = \begin{cases} N & \text{if } w = 0, \\ 1, & \text{otherwise.} \end{cases} \tag{2}$$

Sequences with ideal autocorrelation functions have many applications in cryptography, coding, and other communication engineering.

Linear complexity of S, denoted by $\text{LC}(S)$, is the least integer L of a linear recurrence relation over F_l satisfied by S:

$$-c_0 s_{i+L} = c_1 s_{i+L-1} + \cdots + c_L s_i, \quad i \geq 0, \tag{3}$$

where $c_0, c_1, \ldots, c_L \in F_l$. The linear complexity of a sequence is also defined to be the length of the shortest linear feedback shift register which can generate the sequence. It is an important criterion of randomness of sequences in stream ciphers. To resist the attack from Berlekamp–Massey algorithm, the sequences used in cipher systems should have large linear complexity. If $\text{LC}(S) \geq (N/2)$, where N is the least period of S, then S is considered to be good from the viewpoint of linear complexity.

The minimal polynomial $m(x)$ of S is

$$m(x) = \frac{x^N - 1}{\gcd\left(x^N - 1, S(x)\right)}, \tag{4}$$

and the linear complexity $\mathrm{LC}(S)$ of S is given by $N - \deg(\gcd(x^N - 1, S(x)))$, where $S(x)$ is the generating polynomial of S, that is,

$$S(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_{N-1} x^{N-1}. \tag{5}$$

Sequences from cyclotomic and generalized cyclotomic are important families of pseudorandom sequences.

For an integer $N \geq 2$, let $Z_N = \{0, 1, \ldots, N-1\}$ denote the residue class ring of integers modulo N and Z_N^* be the multiplicative group consisting of all invertible elements in Z_N. A partition $\left\{D_0^{(N)}, D_1^{(N)}, \ldots, D_{d-1}^{(N)}\right\}$ of Z_N^* is a family of sets satisfying $D_i^{(N)} \cap D_j^{(N)} = \varnothing$ for all $i \neq j$ and $Z_N^* = \cup_{i=0}^{d-1} D_i^{(N)}$. Suppose $D_0^{(N)}$ is a multiplicative subgroup of Z_N^* and there exist elements $g \in Z_N^*$ such that $D_i^{(N)} = g^i D_0^{(N)}$ for all $i = 1, \ldots, d-1$; then, $D_i^{(N)}$ are called classical cyclotomic classes of order d with respect to N when N is prime and generalized cyclotomic classes of order d with respect to N when N is composite. The sequences constructed by them are called classical cyclotomic sequences and generalized cyclotomic sequences, respectively. Gauss [1] first proposed the concept of cyclotomic, divided the multiplicative group Z_p^*, and then divided the residual class ring Z_p to construct Gauss classical cyclotomic. Whiteman [2] divided the multiplicative group Z_{pq}^* and then divided the residual class ring Z_{pq} to construct Whiteman generalized cyclotomic. Ding and Helleseth [3] divided the multiplicative group $Z_{p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}}^*$ and then divided the residual class ring $Z_{p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}}$ to construct the Ding generalized cyclotomic. The above three kinds of cyclotomic theories are the most representative and the most widely used cyclotomic theories.

Classical cyclotomic sequences include Legendre sequences, d-degree residual sequences, and Hall sextic residue sequences. Damgaard [4] determined the autocorrelation value of Legendre sequences, and then Ding et al. [5] determined their linear complexity. Kim and Song [6] determined the linear complexity of Hall sextic residue sequences.

Ding [7] constructed Whiteman generalized cyclotomic sequences of order 2 and confirmed their linear complexity. And Ding [8] determined the autocorrelation value of Whiteman generalized cyclotomic sequences of order 2. Bai [9] constructed Whiteman generalized cyclotomic sequences of order 4 and determined their linear complexity. Yan et al. [10] extended Whiteman generalized cyclotomic sequences to the case of order 2^k.

Bai [9] determined the autocorrelation value of Ding generalized cyclotomic sequences with period pq of order 2. And Bai et al. [11] confirmed they had high linear complexity. Yan et al. [12] constructed Ding generalized cyclotomic sequences with period p^m and confirmed they had high linear complexity. Edemskiy [13] constructed a kind of balanced binary generalized cyclotomic sequences with period p^{n+1}. Zhang et al. [14] determined the linear complexity of generalized cyclotomic sequences with period $2p^m$. Hu et al. [15] constructed generalized cyclotomic sequences with period $p^{m+1}q^{n+1}$ and determined their linear complexity. Ke et al. [16] determined the linear complexity and the autocorrelation value of Ding generalized cyclotomic sequences with period $2p^m$. Chang et al. [17] constructed binary generalized cyclotomic sequences with period pqr and determined their linear complexity and minimal polynomial.

Ding [18] constructed a new cyclotomic class (V_0, V_1) and obtained a kind of cyclic code from it. Liu and Chen [19] determined binary generalized cyclotomic sequences with period pq based on the new cyclotomic class (V_0, V_1) and determined their autocorrelation value, linear complexity, and minimal polynomial.

In this paper, based on Ding's new cyclotomic class (V_0, V_1), a simple construction of binary generalized cyclotomic sequences with period pq is constructed, and their autocorrelation value, linear complexity, and minimal polynomial are confirmed. The remainder of this paper is organized as follows. Section 2 proposes a construction of generalized cyclotomic binary sequences. Section 3 calculates the autocorrelation value, linear complexity, and minimal polynomial of the new sequences and compares our results with [19]. Section 4 concludes this paper.

2. Preliminaries

Lemma 1 (see [20]). *Let $m_1 > 0, m_2 > 0, a_1$, and a_2 be integers. The system of congruences,*

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \end{cases} \tag{6}$$

has solutions if and only if $\gcd(m_1, m_2) | a_1 - a_2$.

If the above condition is satisfied, the solution is unique modulo $lcm(m_1, m_2)$.

Let $N = pq$, where p and q are two distinct odd primes. Let g be the unique common primitive root of p and q. The existence and uniqueness of g are guaranteed by Lemma 1. Similarly, there exists a unique integer x which satisfies the following system of congruences:

$$\begin{cases} x \equiv g \pmod{p}, \\ x \equiv 1 \pmod{q}. \end{cases} \tag{7}$$

Let $d = \gcd(p-1, q-1)$ and $e = (\gcd(p-1)(q-1)/d)$. According to Whiteman [2], Whiteman generalized cyclotomic class of order d is

$$D_i = \left\{g^s x^i \colon s = 0, 1, \ldots, e-1\right\}, \quad i = 0, 1, \ldots, d-1. \tag{8}$$

It can be easily seen that $D_i \cap D_j^{(N)} = \varnothing$ for all $i \neq j$ and $Z_N^* = \cup_{i=0}^{d-1} D_i$.

Define two sets

$$P = \{p, 2p, \ldots, (q-1)p\},$$
$$Q = \{q, 2q, \ldots, (p-1)q\}. \tag{9}$$

Then,

$$Z_{pq} = \bigcup_{i=0}^{d-1} D_i \cup P \cup Q \cup \{0\}. \tag{10}$$

Lemma 2 (see [7]). *Let*

$$d = \gcd(p-1, q-1) = 2,$$
$$C_0 = \{0\} \cup Q \cup D_0, \tag{11}$$
$$C_1 = P \cup D_1.$$

And a new binary generalized cyclotomic sequence S of order 2 is

$$s_i = \begin{cases} 0, & \text{if } i \in C_0, \\ 1, & \text{if } i \in C_1. \end{cases} \tag{12}$$

Let $m = ord_{pq}(2)$ and α be a primitive pqth root of unity in finite field F_{2^m}, $d_i(x) = \prod_{j \in D_i}(x - \alpha^i)$, $i = 0, 1$. Then,

(1) When $p \equiv 1 \bmod 8$, $q \equiv 3 \bmod 8$ or $p \equiv -3 \bmod 8$, $q \equiv -1 \bmod 8$,

$$\mathrm{LC}(S) = pq - 1,$$
$$m(x) = \frac{x^{pq} - 1}{x - 1}. \tag{13}$$

(2) When $p \equiv -1 \bmod 8$, $q \equiv 3 \bmod 8$ or $p \equiv 3 \bmod 8$, $q \equiv -1 \bmod 8$,

$$\mathrm{LC}(S) = (p-1)q,$$
$$m(x) = \frac{x^{pq} - 1}{x^q - 1}. \tag{14}$$

(3) When $p \equiv -1 \bmod 8$, $q \equiv -3 \bmod 8$ or $p \equiv 3 \bmod 8$, $q \equiv 1 \bmod 8$,

$$\mathrm{LC}(S) = pq - p - q + 1,$$
$$m(x) = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}. \tag{15}$$

(4) When $p \equiv 1 \bmod 8$, $q \equiv -1 \bmod 8$ or $p \equiv -3 \bmod 8$, $q \equiv 3 \bmod 8$,

$$\mathrm{LC}(S) = \frac{pq + p + q - 3}{2},$$
$$m(x) = \frac{x^{pq} - 1}{(x-1)d_0(x)}. \tag{16}$$

(5) When $p \equiv -1 \bmod 8$, $q \equiv 1 \bmod 8$ or $p \equiv 3 \bmod 8$, $q \equiv -3 \bmod 8$,

$$\mathrm{LC}(S) = \frac{(p-1)(q-1)}{2},$$
$$m(x) = d_1(x). \tag{17}$$

(6) When $p \equiv -1 \bmod 8$, $q \equiv 1 \bmod 8$ or $p \equiv 3 \bmod 8$, $q \equiv 3 \bmod 8$,

$$\mathrm{LC}(S) = \frac{(p-1)(q+1)}{2},$$
$$m(x) = \frac{(x^p - 1)d_1(x)}{x - 1}. \tag{18}$$

Lemma 3 (see [8]). *Let*

$$d = \gcd(p-1, q-1) = 2,$$
$$C_0 = \{0\} \cup Q \cup D_0, \tag{19}$$
$$C_1 = P \cup D_1.$$

And a binary generalized cyclotomic sequence S of order 2 is defined by

$$s_i = \begin{cases} 0, & \text{if } i \in C_0, \\ 1, & \text{if } i \in C_1. \end{cases} \tag{20}$$

Then,

(1) When $((p-1)(q-1)/4)$ is even,

$$C_S(w) = \begin{cases} q - p - 3, & w \in P, \\ 1 + p - q, & w \in Q, \\ -1, & w \in Z_N^*. \end{cases} \tag{21}$$

(2) When $((p-1)(q-1)/4)$ is odd,

$$C_S(w) = \begin{cases} q - p - 3, & w \in P, \\ 1 + p - q, & w \in Q, \\ -3, & w \in D_0, \\ 1, & w \in D_1. \end{cases} \tag{22}$$

Lemma 4 (see [9]). *Let*

$$d = \gcd(p-1, q-1) = 4,$$
$$C_0 = \{0\} \cup Q \cup D_0 \cup D_2, \tag{23}$$
$$C_1 = P \cup D_1 \cup D_3.$$

And a binary generalized cyclotomic sequence S of order 4 is defined by

$$s_i = \begin{cases} 0 & \text{if } i \in C_0, \\ 1 & \text{if } i \in C_1. \end{cases} \tag{24}$$

(1) If $2 \in D_0$ or $2 \in D_2$, then

$$\mathrm{LC}(S) = \frac{(p+1)(q-1)}{2}. \tag{25}$$

If $2 \in D_1$ or $2 \in D_3$, then

$$\mathrm{LC}(S) = p(q-1). \tag{26}$$

(2) When $p \equiv -1 \bmod 8$, $q \equiv 3 \bmod 8$ or $p \equiv 3 \bmod 8$, $q \equiv -1 \bmod 8$,

$$C_S(w) = \begin{cases} pq, & w \in 0, \\ q-p-3, & w \in P, \\ 1+p-q, & w \in Q, \\ 1, & w \in D_0 \cup D_2, \\ -3, & w \in D_1 \cup D_3. \end{cases} \tag{27}$$

Lemma 5 (see [10]). *Let*

$$\begin{aligned} d &= \gcd(p-1, q-1) = 2^k, \\ C_0 &= \{0\} \cup Q \cup \left(\bigcup_{i=0}^{2^{k-1}-1} D_i \right), \\ C_1 &= P \cup \left(\bigcup_{i=2^{k-1}}^{2^k-1} D_i \right). \end{aligned} \tag{28}$$

And a binary generalized cyclotomic sequence S of order 2^k is defined by

$$s_i = \begin{cases} 0, & \text{if } i \in C_0, \\ 1, & \text{if } i \in C_1. \end{cases} \tag{29}$$

Let $m = ord_{pq}(2)$ and α be a pqth primitive root of unity in finite field F_{2^m},

$$\begin{aligned} S_i(x) &= \sum_{j \in P \cup \left(\cap_{t=2^{k-1}+i}^{2^k-1+i} D_t \right)} x^j, \quad i = 0, 1, \ldots, 2^k - 1, \\ \Lambda &= \left\{ i_j \colon S_{i_j}(\alpha) = 0, \quad j = 0, 1, \ldots, 2^{k-1} - 1 \right\}. \end{aligned} \tag{30}$$

Then,

(1) If for all s, $g^s \equiv 2 \bmod pq$ is true,

$$\begin{aligned} \mathrm{LC}(S) &= (p-1)q, \\ m(x) &= \frac{x^{pq}-1}{x^q-1}. \end{aligned} \tag{31}$$

(2) When there exists s such that $g^s \equiv 2 \bmod pq$,

$$\begin{aligned} \mathrm{LC}(S) &= \frac{(p+1)(q-1)}{2}, \\ m(x) &= \frac{x^{pq}-1}{(x^p-1)\left(\prod_{i \in \Lambda} d_i(x)\right)}, \end{aligned} \tag{32}$$

where $d_i(x) = \prod_{j \in D_i} (x - \alpha^j)$.

The following are Ding's new cyclotomic class (V_0, V_1).

Assume $d = \gcd(p-1, q-1) = 2$; let

$$\begin{aligned} V_0 &= \left\{ g^s x^l \colon 0 \le s \le e-1, \quad 0 \le l \le d-1, 2 \mid s+l \right\}, \\ V_1 &= \left\{ g^s x^l \colon 0 \le s \le e-1, \quad 0 \le l \le d-1, 2 \nmid s+l \right\}. \end{aligned} \tag{33}$$

With the above preparations, a partition of Z_N^* is

$$Z_N^* = V_0 \cup V_1, \tag{34}$$

Then,

$$Z_{pq} = V_0 \cup V_1 \cup P \cup Q \cup \{0\}. \tag{35}$$

Let

$$\begin{aligned} C_0 &= \{0\} \cup Q \cup V_0, \\ C_1 &= P \cup V_1. \end{aligned} \tag{36}$$

And a binary generalized cyclotomic sequence S with period pq constructed in [19] is

$$s_i = \begin{cases} 0, & \text{if } i \in C_0, \\ 1, & \text{if } i \in C_1. \end{cases} \tag{37}$$

Lemma 6 (see [19]). *Let $S = \{s_i\}$ be the binary sequences defined. Then, the autocorrelation of S is*

$$C_S(w) = \begin{cases} pq - 2p - 2, & w \in P, \\ 1 + p - q - (q-1)\eta_w\left((-1)^{(p-1/2)} + 1 \right), & w \in Q, \\ -q - (q-2)\eta_w\left((-1)^{(p-1/2)} + 1 \right), & w \in Z_N^*. \end{cases} \tag{38}$$

Lemma 7 (see [19]). *Let $d_i(x) = \prod_{j \in V_i} (x - \alpha^j)$, $i = 0, 1$. Then,*

(1) When $p \equiv 1 \bmod 8$,

$$\mathrm{LC}(S) = \frac{pq+q-p-1}{2}. \tag{39}$$

(2) When $p \equiv -1 \bmod 8$,

$$\mathrm{LC}(S) = \frac{pq-p-q+1}{2}. \tag{40}$$

(3) When $p \equiv 3 \bmod 8$,

$$\mathrm{LC}(S) = pq - p - q + 1. \tag{41}$$

(4) When $p \equiv -3 \bmod 8$,

$$\mathrm{LC}(S) = pq - p. \tag{42}$$

Now, let

$$C_0 = \{0\} \cup P \cup V_0,$$
$$C_1 = Q \cup V_1. \tag{43}$$

A new binary cyclotomic sequence $S = \{s_i\}$ with period pq is defined by

$$s_i = \begin{cases} 0 & \text{if } (i \bmod pq) \in C_0, \\ 1 & \text{if } (i \bmod pq) \in C_1. \end{cases} \tag{44}$$

3. Main Results

3.1. Autocorrelation of Our New Sequences. Let

$$\eta_i = \begin{cases} 1 & \text{if } i \text{ is the quadratic residue of module } p, \\ -1 & \text{if } i \text{ is not the quadratic residue of module } p. \end{cases} \tag{45}$$

Lemma 8 (see [19]). *Let V_0 and V_1 be the sets defined above; then,*

(1) $2 \in V_0$ if and only if $p \equiv \pm 1 \pmod 8$

(2) $2 \in V_1$ if and only if $p \equiv \pm 3 \pmod 8$

Lemma 9 (see [19]). *Let V_0 be the sets defined above; then, $n \in V_0$ if and only if $(1/2)(1+\eta_n) = 1$, $0 \le n \le N-1$.*

Lemma 10. *Let $1 \le w \le N-1$; then,*

(1) $\sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ \gcd(i+w,pq)=1}}^{N-1} \eta_{i(i+w)} = \begin{cases} (q-2)(p-1), & w \in P, \\ 1-q, & w \in Q, \\ 2-q, & w \in Z_N^*. \end{cases}$

(2) $\sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ p|i+w}}^{N-1} \eta_i = \begin{cases} 0, & w \in P, \\ (q-1)\eta_{-w}, & w \notin P. \end{cases}$

(3) $\sum_{\substack{i=0 \\ p|i \\ \gcd(i+w,pq)=1}}^{N-1} \eta_{i+w} = \begin{cases} 0, & w \in P, \\ (q-1)\eta_w, & w \notin P. \end{cases}$

(4) $\sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ q|i+w, pq\nmid i+w}}^{N-1} \eta_i = \begin{cases} -\eta_{-w} & w \in Z_N^*, \\ 0 & w \notin Z_N^*, \end{cases}$

(5) $\sum_{\substack{i=1 \\ q|i \\ \gcd(i+w,pq)=1}}^{N-1} \eta_{i+w} = \begin{cases} -\eta_w & w \in Z_N^*, \\ 0 & w \notin Z_N^*. \end{cases}$

(6) $\sum_{\substack{i=0 \\ p|i \\ p|i+w}}^{N-1} 1 = \begin{cases} q, & w \in P, \\ 0, & w \notin P. \end{cases}$

(7) $\sum_{\substack{i=1 \\ q|i \\ p|i+w}}^{N-1} 1 = \begin{cases} 0, & w \in P, \\ 1, & w \notin P. \end{cases}$

(8) $\sum_{\substack{i=0 \\ p|i, q|i+w \\ pq\nmid i+w}}^{N-1} 1 = \begin{cases} 0, & w \in P, \\ 1, & w \notin P. \end{cases}$

(9) $\sum_{\substack{i=1 \\ q|i, q|i+w \\ pq\nmid i+w}}^{N-1} 1 = \begin{cases} p-2, & w \in Q, \\ 0, & w \notin Q. \end{cases}$

Proof. For the proof of (1) and (6)–(9), one can refer to in [19]; we just prove (2)–(5).

$$\begin{aligned}
&\sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ p|i+w}}^{N-1} \eta_i = \sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ p|i+w}}^{N-1} \eta_{-w} = \eta_{-w} \sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ p|i+w}}^{N-1} 1 = \begin{cases} 0, & w \in P, \\ (q-1)\eta_{-w}, & w \notin P, \end{cases} \\
&\sum_{\substack{i=0 \\ p|i \\ \gcd(i+w,pq)=1}}^{N-1} \eta_{i+w} = \sum_{\substack{i=0 \\ p|i \\ \gcd(i+w,pq)=1}}^{N-1} \eta_w = \eta_w \sum_{\substack{i=0 \\ p|i \\ \gcd(i+w,pq)=1}}^{N-1} 1 = \begin{cases} 0, & w \in P, \\ (q-1)\eta_w, & w \notin P, \end{cases} \\
&\sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ q|i+w, pq\nmid i+w}}^{N-1} \eta_i = \sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ q|i+w}}^{N-1} \eta_i - \sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ q|i+w, pq\nmid i+w}}^{N-1} \eta_i = 0 - \sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ q|i+w, pq\nmid i+w}}^{N-1} \eta_{-w} = -\eta_{-w} \sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ q|i+w, pq\nmid i+w}}^{N-1} 1 = \begin{cases} -\eta_{-w} & w \in Z_N^*, \\ 0 & w \notin Z_N^*, \end{cases} \\
&\sum_{\substack{i=1 \\ q|i \\ \gcd(i+w,pq)=1}}^{N-1} \eta_{i+w} = \sum_{\substack{i=0 \\ q|i \\ \gcd(i+w,pq)=1}}^{N-1} \eta_{i+w} - \sum_{\substack{i=0 \\ q|i \\ \gcd(i+w,pq)=1}}^{N-1} \eta_{i+w} = 0 - \sum_{\substack{i=0 \\ q|i \\ \gcd(i+w,pq)=1}}^{N-1} \eta_w = -\eta_w \sum_{\substack{i=0 \\ q|i \\ \gcd(i+w,pq)=1}}^{N-1} 1 = \begin{cases} -\eta_w & w \in Z_N^*, \\ 0 & w \notin Z_N^*. \end{cases}
\end{aligned} \tag{46}$$

□

Theorem 1. *Let $S = \{s_i\}$ be the new binary sequences defined in (44); then, the autocorrelation of S is*

$$C_S(w) = \begin{cases} pq - 2p + 2, & w \in P, \\ p - q - 3 + (q-1)\eta_w\left((-1)^{(p-1/2)} + 1\right), & w \in Q, \\ -q + q\eta_w\left((-1)^{(p-1/2)} + 1\right), & w \in Z_N^*. \end{cases} \tag{47}$$

Proof. By the definition of S,

$$(-1)^{S_n} = \begin{cases} \eta_n, & \gcd(n, pq) = 1, \\ 1, & p|n, \\ -1, & q|n, n > 0. \end{cases} \tag{48}$$

Let $1 \le w \le N-1$; then,

$$\begin{aligned} C_S(w) &= \sum_{i=0}^{N-1} (-1)^{s_{i+w}+s_i} = \sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ \gcd(i+w,pq)=1}}^{N-1} \eta_{i(i+w)} + \sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ p|i+w}}^{N-1} \eta_i - \sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ q|i+w, pq\nmid i+w}}^{N-1} \eta_i - \sum_{\substack{i=1 \\ q|i \\ \gcd(i+w,pq)=1}}^{N-1} \eta_{i+w} \\ &\quad - \sum_{\substack{i=1 \\ q|i \\ p|i+w}}^{N-1} 1 + \sum_{\substack{i=1 \\ q|i, q|i+w \\ pq\nmid i+w}}^{N-1} 1 + \sum_{\substack{i=0 \\ p|i \\ \gcd(i+w,pq)=1}}^{N-1} \eta_{i+w} + \sum_{\substack{i=0 \\ p|i \\ p|i+w}}^{N-1} 1 - \sum_{\substack{i=0 \\ p|i, q|i+w \\ pq\nmid i+w}}^{N-1} 1 \\ &= \begin{cases} pq - 2p + 2 & \text{if } w \in P, \\ p - q - 3 + (q-1)\eta_w\left((-1)^{(p-1/2)} + 1\right) & \text{if } w \in Q, \\ -q + q\eta_w\left((-1)^{(p-1/2)} + 1\right) & \text{if } w \in Z_N^*. \end{cases} \end{aligned} \tag{49}$$

The autocorrelation function of the new sequences $C_S(w)$ is 5-level if $p \equiv 1 \bmod 4$. $C_S(w)$ is 3-level. □

3.2. Linear Complexity and Minimal Polynomial of Our New Sequences

Lemma 11 (see [19]). *Let V_0 and V_1 be the sets defined above; then,*

$$\begin{cases} tV_0 \in V_0,\ tV_1 \in V_1, & \text{if } t \in V_0, \\ tV_0 \in V_1,\ tV_1 \in V_0, & \text{if } t \in V_1. \end{cases} \tag{50}$$

Denote

$$\begin{aligned} S(x) &= s_0 + s_1 x + s_2 x^2 + \cdots + s_{N-1} x^{N-1} \\ &= \sum_{i \in C_1} x^i = \sum_{i \in Q} x^i + \sum_{i \in V_1} x^i. \end{aligned} \tag{51}$$

Assume $m = \mathrm{ord}_{pq}(2)$ and α is a pqth primitive root of unity in finite field F_{2^m}. According to the Blahut theorem, the linear complexity of sequence $S = \{s_i\}$ is

$$\mathrm{LC}(S) = pq - \left|\left\{t\colon S\left(\alpha^t\right) = 0, \quad 0 \le t \le pq-1\right\}\right|. \tag{52}$$

Lemma 12. *Let $1 \le t \le N-1$; then,*

$$S\left(\alpha^t\right) = \begin{cases} S(\alpha), & t \in V_0, \\ 1 + S(\alpha), & t \in V_1, \\ \dfrac{p-1}{2} \bmod 2, & t \in P, \\ 1, & t \in Q, \\ 0, & t \in \{0\}. \end{cases} \tag{53}$$

Proof. Let $t \in V_0$; then, by Lemma 11,

$$\begin{aligned} S\left(\alpha^t\right) &= \sum_{i \in Q} \alpha^{ti} + \sum_{i \in V_1} \alpha^{ti} \\ &= \sum_{i \in tQ} \alpha^i + \sum_{i \in tV_1} \alpha^i \\ &= \sum_{i \in Q} \alpha^i + \sum_{i \in V_1} \alpha^i = S(\alpha). \end{aligned} \tag{54}$$

Let $t \in V_1$,

$$\begin{aligned} 0 &= \alpha^{pq} - 1 = (\alpha - 1)\left(1 + \alpha + \cdots + \alpha^{pq-1}\right) \\ &= (\alpha - 1)\left(1 + \sum_{i \in V_0} \alpha^i + \sum_{i \in V_1} \alpha^i + \sum_{i \in P} \alpha^i + \sum_{i \in Q} \alpha^i\right). \end{aligned} \tag{55}$$

Then, by Lemma 11,

$$\begin{aligned} S(\alpha^t) &= \sum_{i\in Q}\alpha^{ti} + \sum_{i\in V_1}\alpha^{ti} \\ &= \sum_{i\in tQ}\alpha^{i} + \sum_{i\in tV_1}\alpha^{i} \\ &= \sum_{i\in Q}\alpha^{i} + \sum_{i\in V_0}\alpha^{i} \\ &= \sum_{i\in Q}\alpha^{i} - \sum_{i\in V_1}\alpha^{i} + 1 \\ &\equiv (S(\alpha)+1)(\mathrm{mod}2). \end{aligned} \tag{56}$$

Let $t \in P$; then,

$$\begin{aligned} V_1 \mathrm{mod} q &= \left\{g^s x^l \mathrm{mod} q\colon 0 \le s \le e-1, 0 \le l \le 1, 2\nmid s+l\right\} \\ &= \left\{g^{2s} x \mathrm{mod} q\colon 0 \le s \le \frac{e}{2}-1\right\} \cup \left\{g^{2s+1} \mathrm{mod} q\colon 0 \le s \le \frac{e}{2}-1\right\} \\ &= \left\{g^{2s} \mathrm{mod} q\colon 0 \le s \le \frac{e}{2}-1\right\} \cup \left\{g^{2s+1} \mathrm{mod} q\colon 0 \le s \le \frac{e}{2}-1\right\} = \{1, 2, \ldots, q-1\}. \end{aligned} \tag{57}$$

When s runs through $\{0, 1, \ldots, e-1\}$, l runs through $\{0, 1\}$, and $2\nmid s+l$, the set V_1 mod q takes on each element in $\{1, 2, \ldots, q-1\}$ exactly $(p-1/2)$ times. Therefore,

$$\begin{aligned} S(\alpha^t) &= \sum_{i\in Q}\alpha^{ti} + \sum_{i\in V_1}\alpha^{ti} = ((p-1)\mathrm{mod}2) + \left(\frac{p-1}{2}\mathrm{mod}2\right) \\ &\cdot \sum_{i\in P}\alpha^{i} = \frac{p-1}{2}\mathrm{mod}2. \end{aligned} \tag{58}$$

Let $t \in Q$; then,

$$\begin{aligned} V_1 \mathrm{mod}\, p &= \left\{g^s x^l \mathrm{mod}\, p\colon 0 \le s \le e-1, 0 \le l \le 1, 2\nmid s+l\right\} \\ &= \left\{g^{2s} x \mathrm{mod}\, p\colon 0 \le s \le \frac{e}{2}-1\right\} \\ &\cup \left\{g^{2s+1} \mathrm{mod}\, p\colon 0 \le s \le \frac{e}{2}-1\right\} \\ &= \left\{g^{2s+1} \mathrm{mod}\, p\colon 0 \le s \le \frac{e}{2}-1\right\} = \left\{g^1, g^3, \ldots, g^{p-2}\right\}. \end{aligned} \tag{59}$$

When s runs through $\{0, 1, \ldots, e-1\}$, l runs through $\{0, 1\}$, and $2\nmid s+l$, the set V_1 mod p takes on each element in $\{g^1, g^3, \ldots, g^{p-2}\}$ exactly $q-1$ times. Therefore,

$$\begin{aligned} S(\alpha^t) &= \sum_{i\in Q}\alpha^{ti} + \sum_{i\in V_1}\alpha^{ti} = \sum_{i\in Q}\alpha^{i} + ((q-1)\mathrm{mod}2) \\ &\cdot \sum_{i\in\{g^1, g^3, \ldots, g^{p-2}\}}\alpha^{i} = -1 \equiv 1\mathrm{mod}2. \end{aligned} \tag{60}$$

Let $t \in \{0\}$; then,

$$\begin{aligned} S(\alpha^t) &= S(1) = p - 1 + \frac{(p-1)(q-1)}{2} \\ &= \frac{(p-1)(q+1)}{2}\mathrm{mod}2 = 0. \end{aligned} \tag{61}$$

□

Lemma 13. *Let V_0 and V_1 be the sets defined above; then, $2 \in V_0$ if and only if $S(\alpha) \in \{0, 1\}$.*

Proof. Since the characteristic of finite field F_{2^m} is 2, $(S(\alpha))^2 = S(\alpha^2)$.

Let $2 \in V_0$; then, $2V_i = V_i$, $i = 0, 1$.

$$\begin{aligned} (S(\alpha))^2 = S(\alpha^2) &= \sum_{i\in Q}\alpha^{2i} + \sum_{i\in V_1}\alpha^{2i} \\ &= \sum_{i\in Q}\alpha^{i} + \sum_{i\in V_1}\alpha^{i} = S(\alpha). \end{aligned} \tag{62}$$

Therefore, $S(\alpha) \in \{0, 1\}$.

Let $2 \in V_1$; then, $2V_i = V_{(i+1)mod2}$, $i = 0, 1$.

$$\begin{aligned} (S(\alpha))^2 = S(\alpha^2) &= \sum_{i\in Q}\alpha^{2i} + \sum_{i\in V_1}\alpha^{2i} \\ &= \sum_{i\in Q}\alpha^{i} + \sum_{i\in V_0}\alpha^{i} = S(\alpha) + 1. \end{aligned} \tag{63}$$

Therefore, $S(\alpha) \notin \{0, 1\}$.

Since $2 \notin P \cup Q$, $2 \in V_0$ if and only if $S(\alpha) \in \{0, 1\}$. □

Theorem 2. *Let $d_i(x) = \prod_{j\in V_i}(x - \alpha^i)$, $i = 0, 1$. Then,*

(1) When $p \equiv 1\mathrm{mod}8$,

$$\mathrm{LC}(S) = \frac{pq + p - q - 1}{2}, \quad m(x) = \frac{x^{pq} - 1}{(x^q - 1)d_i(x)}. \tag{64}$$

(2) When $p \equiv -1 \bmod 8$,

$$\mathrm{LC}(S) = \frac{pq + p + q - 3}{2}, \quad m(x) = \frac{x^{pq} - 1}{(x^q - 1)d_i(x)}. \tag{65}$$

(3) When $p \equiv 3 \bmod 8$,

$$\mathrm{LC}(S) = pq - 1, \quad m(x) = \frac{x^{pq} - 1}{x - 1}. \tag{66}$$

(4) When $p \equiv -3 \bmod 8$,

$$\mathrm{LC}(S) = pq - q, \quad m(x) = \frac{x^{pq} - 1}{x^q - 1}. \tag{67}$$

Proof. Let α be a pqth primitive root of unity in finite field F_{2^m}. Then,

$$x^p - 1 = \prod_{i \in \{0\} \cup Q} \left(x - \alpha^i\right), \quad x^q - 1 = \prod_{i \in \{0\} \cup P} \left(x - \alpha^i\right). \tag{68}$$

Define $d_i(x) = \prod_{j \in V_i} (x - \alpha^j)$, $i = 0, 1$. It can be easily seen that

$$x^N - 1 = (x - 1)(x - \alpha) \ldots \left(x - \alpha^{N-1}\right) = \frac{(x^p - 1)(x^q - 1)d_0(x)d_1(x)}{x - 1}. \tag{69}$$

□

Case 1. $p \equiv 1 \bmod 8$: choose α such that $S(\alpha) = 0$. Then,

$$S\left(\alpha^t\right) = \begin{cases} 1, & t \in Q \cup V_1, \\ 0, & t \in 0 \cup P \cup V_0. \end{cases} \quad LC(S) = pq - q - \frac{(p-1)(q-1)}{2} = \frac{pq + p - q - 1}{2}, m(x) = \frac{x^{pq} - 1}{(x^q - 1 d_0 x)}. \tag{70}$$

Case 2. $p \equiv -1 \bmod 8$: choose α such that $S(\alpha) = 0$. Then,

$$S\left(\alpha^t\right) = \begin{cases} 1, & t \in P \cup Q \cup V_1, \\ 0, & t \in \{0\} \cup V_0, \end{cases} \quad \mathrm{LC}(S) = pq - 1 - \frac{(p-1)(q-1)}{2} = \frac{pq + p + q - 3}{2}, m(x) = \frac{x^{pq} - 1}{(x - 1)d_0(x)}. \tag{71}$$

Case 3. $p \equiv 3 \bmod 8$. Then,

$$S\left(\alpha^t\right) \begin{cases} \neq 0, & t \in P \cup Q \cup V_0 \cup V_1, \\ = 0, & t \in \{0\}, \end{cases} \quad \mathrm{LC}(S) = pq - 1, \quad m(x) = \frac{x^{pq} - 1}{x - 1}. \tag{72}$$

Case 4. $p \equiv -3 \bmod 8$. Then,

$$S\left(\alpha^t\right) \begin{cases} \neq 0, & t \in Q \cup V_0 \cup V_1, \\ = 0, & t \in \{0\} \cup P, \end{cases} \quad \mathrm{LC}(S) = pq - q, \quad m(x) = \frac{x^{pq} - 1}{x^q - 1}. \tag{73}$$

The linear complexity of the new sequences is $\mathrm{LC}(S) > (pq/2)$ if $p \equiv 1 \bmod 8$, $p > q + 1$, or $p \equiv -1 \bmod 8$; $\mathrm{LC}(S) = pq - q$ or $pq - 1$ if $p \equiv \pm 3 \bmod 8$, which is very close to period pq.

The following are some examples.

Example 1. Let $p = 7$ and $q = 3$. Then,

$$P = \{7, 14\}, \quad Q = \{3, 6, 9, 12, 15, 18\}, \quad V_0 = \{1, 2, 4, 8, 11, 16\}, \quad V_1 = \{5, 10, 13, 17, 19, 20\}. \tag{74}$$

Our corresponding new binary sequence of period 21 is as follows: 000101100110110101111.

By using Magma, the autocorrelation value of the above sequence is 3-level, which is consistent with the case $p \equiv 3 \bmod 4$ in Theorem 1. And the linear complexity of the

Table 1: Comparison of autocorrelation $C_S(w)$.

$C_S(w)$	Sequences of Liu and Chen	New sequences
$w \in P$	$pq-2p-2$	$pq-2p+2$
$w \in Q$	$1+p-q-(q-1)\eta_w((-1)^{(p-1/2)}+1)$	$p-q-3+(q-1)\eta_w((-1)^{(p-1/2)}+1)$
$w \in Z_N^*$	$-q-(q-2)\eta_w((-1)^{(p-1/2)}+1)$	$-q+q\eta_w((-1)^{(p-1/2)}+1)$

Table 2: Comparison of linear complexity LC(S).

LC(S)	Sequences of Liu and Chen	New sequences
$p \equiv 1 \bmod 8$	$(pq-p+q-1)/2$	$(pq+p-q-1)/2$
$p \equiv -1 \bmod 8$	$((p-1)(q-1))/2$	$(pq+p+q-3)/2$
$p \equiv 3 \bmod 8$	$pq-p-q+1$	$pq-1$
$p \equiv -3 \bmod 8$	$pq-p$	$pq-q$

above sequence is equal to 14, which is consistent with the case $p \equiv -1 \bmod 8$ in Theorem 2.

Example 2. Let $p = 11$ and $q = 3$. Then,

$$\begin{aligned} P &= \{11, 22\}, \\ Q &= \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30\}, \\ V_0 &= \{1, 4, 5, 14, 16, 20, 23, 25, 26, 31\}, \\ V_1 &= \{2, 7, 8, 10, 13, 17, 19, 28, 29, 32\}. \end{aligned} \tag{75}$$

Our corresponding new binary sequence of period 33 is as follows: 001100111110110101110100100111101.

By using Magma, the autocorrelation value of the above sequence is 3-level, which is consistent with the case $p \equiv 3 \bmod 4$ in Theorem 1. And the linear complexity of the above sequence is equal to 32, which is consistent with the case $p \equiv 3 \bmod 8$ in Theorem 2.

Example 3. Let $p = 13$ and $q = 3$. Then,

$$\begin{aligned} P &= \{13, 26\}, \\ Q &= \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36\}, \\ V_0 &= \{1, 4, 10, 14, 16, 17, 22, 23, 25, 29, 35, 38\}, \\ V_1 &= \{2, 5, 7, 8, 11, 19, 20, 28, 31, 32, 34, 37\}. \end{aligned} \tag{76}$$

Our corresponding new binary sequence of period 39 is as follows: 001101111101100100111100100110111110110.

By using Magma, the autocorrelation value of the above sequence is 5-level, which is consistent with the case $p \equiv 1 \bmod 4$ in Theorem 1. And the linear complexity of the above sequence is equal to 36, which is consistent with the case $p \equiv -3 \bmod 8$ in Theorem 2.

Example 4. Let $p = 17$ and $q = 3$. Then,

$$\begin{aligned} P &= \{17, 34\}, \\ Q &= \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48\}, \\ V_0 &= \{1, 2, 4, 8, 13, 16, 19, 25, 26, 32, 35, 38, 43, 47, 49, 50\}, \\ V_1 &= \{5, 7, 10, 11, 14, 20, 22, 23, 28, 29, 31, 37, 40, 41, 44, 46\}. \end{aligned} \tag{77}$$

Our corresponding new binary sequence of period 51 is as follows: 000101110111101100101111100111110100110111101110100.

By using Magma, the linear complexity of the above sequence is equal to 32, which is consistent with the case $p \equiv 1 \bmod 8$ in Theorem 1, but the autocorrelation value of the above sequence is 4-level, which is consistent with the case $p \equiv 1 \bmod 4$ in Theorem 2.

3.3. Comparisons of Results. The comparisons of our results with [19] are listed in Tables 1 and 2.

The comparisons show the following:

(i) When $p \equiv 3 \bmod 4$, the autocorrelation $C_S(w)$ of the two sequences is unequal, but they are 3-level. When $p \equiv 1 \bmod 4$, the autocorrelation of the two sequences is unequal, but both of them are 5-level.

(ii) When $p \equiv 1 \bmod 4$, $p > q$, or $p \equiv 3 \bmod 4$, the linear complexity of our new sequences is larger.

4. Conclusion

This paper presents a construction of generalized cyclotomic binary sequences with period pq based on Ding's new cyclotomic class (V_0, V_1). And the autocorrelation value, linear complexity, and minimal polynomial of our new sequences are determined. The autocorrelation function $C_S(w)$ is 5-level if $p \equiv 1 \bmod 4$. $C_S(w)$ is 3-level, and S has almost optimal autocorrelation if $p \equiv 3 \bmod 4$. The linear complexity $\mathrm{LC}(S) > (pq/2)$ if $p \equiv 1 \bmod 8$, $p > q+1$, or $p \equiv -1 \bmod 8$; $\mathrm{LC}(S) = pq-q$ or $pq-1$ if $p \equiv \pm 3 \bmod 8$, which is very close to the period. The results show that our

new sequences have quite good cryptographic properties in the aspect of autocorrelation and linear complexity.

Data Availability

All the data used to support the findings of this study are included in Section 3.2 of this article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 61902304) and the National Statistical Science Project (2019LY36).

References

[1] C. F. Gauss, *Disquisitiones Arithmaticae*, Britannica, Leipzig, Germay, 1801.

[2] A. L. Whiteman, "A family of difference sets," *Illinois Journal of Mathematics*, vol. 6, no. 2, pp. 107–121, 1962.

[3] C. Ding and T. Helleseth, "New generalized cyclotomy and its applications," *Finite Fields and their Applications*, vol. 4, no. 2, pp. 140–166, 1998.

[4] I. Damgaard, "On the randomness of Legendre and Jacobi sequences," in *Advances in Cryptology; CRYPTO'88, LNCS 403,* Springer-Verlag, Berlin, Germany, 1990.

[5] 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.

[6] 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.

[7] C. Ding, "Linear complexity of generalized cyclotomic binary sequences of order 2," *Finite Fields and their Applications*, vol. 3, no. 2, pp. 159–174, 1997.

[8] C. Ding, "Autocorrelation values of generalized cyclotomic sequences of order two," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1699–1702, 1998.

[9] E. Bai, *Study on Construction and Randomness Analysis of Pseudorandom Sequences*, Xidian University, Xian, China, 2004.

[10] 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.

[11] E. Bai, X. Liu, and G. Xiao, "Linear complexity of new generalized cyclotomic sequences of order two of Length pq," *IEEE Transactions on Information Theory*, vol. 51, no. 5, pp. 1849–1853, 2005.

[12] T. Yan, S. Li, and G. Xiao, "On the linear complexity of generalized cyclotomic sequences of length p^m," *Applied Mathematics Letters*, vol. 221, no. 2, pp. 187–193, 2008.

[13] V. Edemskiy, "About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1}," *Designs, Codes and Cryptography*, vol. 61, pp. 251–260, 2011.

[14] 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.

[15] L. Hu, Q. Yue, and M. Wang, "The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$," *IEEE Transactions on Information Theory*, vol. 58, no. 8, pp. 5534–5543, 2012.

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

[17] Z. Chang, Y. Zhou, and P. Ke, "Linear complexity of new generalized cyclotomic sequences of order two and length pqr," *Acta Electronica Sinica*, vol. 43, no. 1, p. 166, 2015.

[18] C. Ding, "Cyclotomic constructions of cyclic codes with length being the product of two primes," *IEEE Transactions on Information Theory*, vol. 58, no. 4, pp. 2231–2236, 2011.

[19] H. Liu and X. Chen, "Autocorrelation values and linear complexity of new generalized cyclotimic sequences," *Acta Mathematica Sinica (Chinese Series)*, vol. 62, no. 2, pp. 233–246, 2019.

[20] D. Pei, A. Salomaa, and C. Ding, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*, World Scientific, Singapore, Asia, 1996.