mathematics

MDPI

Article

Linear Complexity and Trace Representation of New Ding Generalized Cyclotomic Sequences with Period pq and Order Two

Jiang Ma, Wei Zhao, Yanguo Jia *, Xiumin Shen 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.); shenxm@ysu.edu.cn (X.S.); jianghy2018@stumail.ysu.edu.cn (H.J.)

* Correspondence: jyg@ysu.edu.cn; Tel.: +86-135-0335-4988

Abstract: Linear complexity is an important property to measure the unpredictability of pseudo-random sequences. Trace representation is helpful for analyzing cryptography properties of pseudo-random sequences. In this paper, a class of new Ding generalized cyclotomic binary sequences of order two with period pq is constructed based on the new segmentation of Ding Helleseth generalized cyclotomy. Firstly, the linear complexity and minimal polynomial of the sequences are investigated. Then, their trace representation is given. It is proved that the sequences have larger linear complexity and can resist the attack of the Berlekamp–Massey algorithm. This paper also confirms that generalized cyclotomic sequences with good randomness may be obtained by modifying the characteristic set of generalized cyclotomy.

Keywords: pseudo-random sequences; stream cipher; Linear complexity; trace representation; generalized cyclotomic sequence

Citation: Ma, J.; Zhao, W.; Jia, Y.; Shen, X.; Jiang, H. Linear Complexity and Trace Representation of New Ding Generalized Cyclotomic Sequences with Period pq and Order Two. *Mathematics* **2021**, *9*, 2285. https://doi.org/10.3390/math9182285

Academic Editor: Yang-Hui He

Received: 9 August 2021
Accepted: 14 September 2021
Published: 16 September 2021

1. Introduction

Pseudo-random sequences are widely used in spread spectrum communication, multiple access communication, radar navigation, software testing, cryptography, and so on. The study keystones of pseudo-random sequence are its construction methods and randomness analysis. As the property of pseudo-random sequences, the linear complexity is defined as the length of the shortest linear shift register, which can generate the sequences [1]. By the Berlekamp–Massey algorithm [2], the linear complexity of a pseudo-random sequence must be greater than the half of its period. Trace representation is an important tool for designing and analyzing pseudo-random sequences [3]. In 1962, Whiteman proposed the Whiteman generalized cyclotomy in search of residual difference sets [4]. Subsequently, Ding et al. [5] presented the Ding–Helleseth generalized cyclotomy. Generalized cyclotomy became a popular method to construct pseudo-random sequences. Based on the Ding–Helleseth generalized cyclotomy of order two, Ding [6] constructed new generalized cyclotomic classes (V_0, V_1). By use of these cyclotomic classes, Liu et al. [7] constructed the generalized cyclotomic sequences, and calculated the linear complexity and autocorrelation values of the sequences. Chen et al. [8] described the trace representations of the sequences by the Mattson–Solomon polynomial. However, these new generalized cyclotomic sequences are almost balanced, and their imbalance is $q - p - 1$.

Li et al. [9] constructed a group of balanced sequences based on Whiteman's generalized cyclotomy, but only gave the lower bound of linear complexity. Bai et al. [10] defined a class of balanced binary sequence based on the Ding–Helleseth generalized cyclotomy and calculated the linear complexity. By the defining pairs of the Legendre sequence, Du et al. determined the trace representation and linear complexity of the generalized cyclotomic sequence of length pq with arbitrary order. It can be seen that Bai et al.'s conclusion is a special case when the order is two [11].

Kim et al. [12] found a general trace representation of Lengendre sequences with any prime period. Qi et al. [13] pointed out that a simpler trace representation of Legendre sequences. In 2015, Lv et al. [14] proofed that generalized cyclotomic sequences of order d can be represented as a sum of d-residue sequences. Especially if d = 2, generalized cyclotomic sequences can be represented as a sum of Legendre sequences. Inspired by these conclusions, we consider that trace representation of generalized cyclotomic binary sequences with period pq can be expressed by trace representation of Legendre sequences with period p and q.

In this paper, we constructed a class of new balanced generalized cyclotomic sequences with an imbalance degree of 1 based on the Ding's new generalized cyclotomic classes (V_0, V_1), and discuss the linear complexity and trace representation of the sequences. According to the definition of the new sequences, their characteristic sets are different from those in [9,11,15], and they belong to different sequences.

2. Preliminaries

Let $S = \{S_i\}$ be a sequence of period N over a finite field $GF(2)$, then the generating polynomial of S can be expressed as

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

where $S^N(x) = s_0 + s_1 x + \cdots + s_{N-1}x^{N-1}$. The minimal polynomial of S is given by $M_S(x) = (x^N - 1)/gcd(S^N(x), x^N - 1)$, and the linear complexity of S is given by

$$LC(S) = deg(M_S(x)) = N - deg(gcd(S^N(x), x^N - 1)) \tag{2}$$

Let m be the order of 2 modulo N. α is a primitive Nth root of unity over the field $GF(2^m)$ of $x^N - 1$. The linear complexity of the sequence $\{S_i\}$ is further derived as

$$LC(S) = N - \left|\left\{k : S(\alpha^k) = 0, 0 \le k \le N - 1\right\}\right| \tag{3}$$

Let p be an odd prime, $gcd(t, p) = 1$. Define

$$\left(\frac{t}{p}\right) = \begin{cases} 1, \ if \ x^2 \equiv t (mod \ p) \ for \ some \ x, \\ -1, \ otherwise. \end{cases}, \tag{4}$$

where $\left(\frac{t}{p}\right)$ is the Lengendre symbol.

The trace function of x from finite field $GF(2^n)$ to $GF(2)$ is defined as

$$tr_1^n(x) = x + x^2 + x^{2^2} + \cdots x^{2^{n-1}} \tag{5}$$

For $\forall a, b \in GF(2)$, $\exists x, y \in GF(2^n)$, trace function $tr_1^n(x)$ satisfy the following properties:

(i) $tr_1^n(x) = tr_1^n\left(x^{2^j}\right)$ for any positive integer j.

(ii) $tr_1^n(x)(ax + by) = atr_1^n(x) + btr_1^n(y)$

These properties show that trace functions are linear functions. See, e.g., [1,3] for details.

3. The Construction of the New Ding Generalized Cyclotomic Binary Sequences

Let p and q be two distinct odd primes with $p < q$. Define $N = pq$, $gcd(p - 1, q - 1) = 2$, and $d = (p - 1)(q - 1)/2$. By the Chinese Remainder Theorem, there exists a common primitive root g of both p and q [10,11,16].

Clearly, $ord_N(g) = lcm(ord_p(g), ord_q(g)) = d$, where $ord_N(g)$ denotes the multiplicative order of g modulo N. Let x be an integer satisfying the simultaneous congruencies:

$x \equiv g(mod\ p), x \equiv 1(mod\ q)$. The existence of x mod pq is guaranteed by the Chinese Remainder Theorem [10,13].

Define the new segmentation of the Ding–Helleseth generalized cyclotomy as follows:

$$V_0 = \left\{g^s x^h : 0 \le s \le d-1, 0 \le h \le 1, 2 \middle| s+h\right\}, V_1 = \left\{g^s x^h : 0 \le s \le d-1, 0 \le h \le 1, 2 \nmid s+h\right\}.$$

Clearly, $V_0 = gV_1$ according to the definitions of V_0 and V_1.

Therefore, the Ding's new generalized cyclotomic classes (V_0, V_1) constitute a segmentation of all invertible elements in Z_N [4], the residue ring module N. It is easy to see that $Z_N^* = V_0 \cup V_1$, $V_0 \cap V_1 = \varnothing$, where Z_N^* denotes multiplicative group of the ring Z_N and $\varnothing$ the empty set.

Define

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

In order to obtain the average segmentation of P and Q by quadratic residues theory, define

$$D_0^{(p)} = \left\{g^{2f} mod\ p : f = 0, 1, \cdots, (p-3)/2\right\},\ D_0^{(q)} = \left\{g^{2f} mod\ q : f = 0, 1, \cdots, (q-3)/2\right\},\ D_1^{(p)} = gD_0^{(p)},$$
$$D_1^{(q)} = gD_0^{(q)},\ R = \{0\},\ P_0 = pD_0^{(q)},\ P_1 = pD_1^{(q)},\ Q_0 = qD_0^{(p)},\ Q_1 = qD_1^{(p)},\ C_0 = P_0 \cup Q_0 \cup V_0 \cup R,$$
$$C_1 = P_1 \cup Q_1 \cup V_1. \text{ Then, } Z_N = C_0 \cup C_1,\ C_0 \cap C_1 = \varnothing.$$

Definition 1. *The new generalized cyclotomic sequences* $\{S_i\}$ *of order two of length* pq *is defined by*

$$S_i = \begin{cases} 0, if (i\ mod\ N) \in C_0, \\ 1, if (i\ mod\ N) \in C_1. \end{cases} \tag{6}$$

Clearly, the sequence $\{S_i\}$ *has least period N. In one period of this sequence, the integer 0 appears* $(pq+1)/2$ *times and the integer 1 appears* $(pq-1)/2$ *times. It is a balance sequence with imbalance degree 1.*

4. Linear Complexity and Minimal Polynomial of the New Sequences

According to the definition of $\{S_i\}$, the generating polynomial $S(x)$ can be expressed as

$$S(x) = \sum_{i \in C_1} x^i = \sum_{i \in P_1 \cup Q_1 \cup V_1} x^i \in GF(2)[x] \tag{7}$$

According to the expression of $S(x)$, $S(1)$ can be reckoned as

$$\begin{aligned} S(1) &= ((p-1)/2 + (q-1)/2 + (p-1)(q-1)/2)(mod\ 2) \\ &= ((p-1)/2 + (q-1)/2)(mod\ 2) \end{aligned} \tag{8}$$

Lemma 1.

$$\sum_{i \in P_0 \cup P_1} \alpha^i = 1, \sum_{i \in Q_0 \cup Q_1} \alpha^i = 1, \sum_{i=0}^{N-1} \alpha^i = \sum_{i \in P \cup Q \cup V_0 \cup V_1} \alpha^i + 1 = 0.$$

Refer to the Equations (4) and (5) in [10] for details.

Lemma 2 ([8]). *Let* $\alpha \in V_j$ *and* $i, j \in \{0, 1\}$, *then* $\alpha V_i \in V_{i+j(mod 2)}$.

Lemma 3.

$$\sum_{i \in V_1} \alpha^{ki} = \begin{cases} \frac{p-1}{2}(mod\ 2), k \in P, \\ 0, k \in Q. \end{cases} \tag{9}$$

Proof. Suppose that $k \in P$, by the definition of x, we have

$$\begin{aligned} V_1(mod\ q) &= \left\{ g^{2f+1}x(mod\ q) : f = 0, 1, \cdots, \frac{(d-2)}{2} \right\} \cup \left\{ g^{2f}(mod\ q) : f = 0, 1, \cdots, \frac{(d-2)}{2} \right\} \\ &= \left\{ g^f\ mod\ q : f = 0, 1, \cdots, d-1 \right\} = \{1, 2, \cdots, q-1\}. \end{aligned} \tag{10}$$

When f ranges over $\{0, 1, \cdots, d-1\}$, $g^f\ mod\ q$ takes on each element of $\{0, 1, \cdots, q-1\}$ $(p-1)/2$ times. It follows from Lemma 2 that

$$\sum_{i \in V_1} \alpha^{ki} = \frac{p-1}{2} \sum_{i \in P} \alpha^i = \frac{p-1}{2} (mod 2) \tag{11}$$

Suppose that $k \in Q$. By symmetry, we get

$$V_1(mod\ p) = \left\{ g^f(mod\ p) : f = 0, 1, \cdots, \frac{(d-2)}{2} \right\} = \left\{ g, g^3, \cdots, g^{p-2} \right\} \tag{12}$$

When f ranges over $\{0, 1, \cdots, d-1\}$, $V_1(mod\ p)$ takes on each element of $D_1^{(p)}$ $q-1$ times. It follows from Lemma 1 that

$$\sum_{i \in V_1} \alpha^{ki} = (q-1) \sum_{i \in P} \alpha^i = 0 \tag{13}$$

□

Lemma 4. *Let the symbols be the same as before. Then,*

$$S(\alpha^k) = \begin{cases} S(\alpha), & k \in Z_N^* \text{ and } k\ mod\ p \in D_0^{(q)}, \\ S(\alpha) + 1, & k \in Z_N^* \text{ and } k\ mod\ p \in D_1^{(q)}, \\ \sum\limits_{i \in P_1} \alpha^{ki}, & k \in P, \\ \sum\limits_{i \in Q_1} \alpha^{ki} + \frac{q-1}{2}, & k \in Q. \end{cases} \tag{14}$$

Proof. By the proof of Lemma 3, we obtain $V_0(mod\ p) = D_0^{(p)}$, $V_1(mod\ p) = D_1^{(p)}$, $V_0(mod\ q) = V_1(mod\ q) = D_0^{(q)} \cup D_1^{(q)} = \{1, 2, \cdots, q-1\}$.

If $k \in V_0$, $kmod\ p \in D_0^{(q)}$, there must exist an integer m such that $k \equiv g^m mod\ pq$, where $m \in \{0, 1, \cdots, d-1\}$. According to the Chinese Remainder Theorem, we can get that $k \equiv g^m mod\ p$ and m must be even. Hence, $kQ_1 = Q_1$, and $kP_1 = P_1$. By Lemma 2, $kV_1 = V_1$. By Lemma 1

$$S(\alpha^k) = \sum_{i \in P_1 \cup Q_1 \cup V_1} \alpha^{ki} = S(\alpha) \tag{15}$$

If $k \in V_0$ and $kmod\ p \in D_1^{(q)}$ then $kP_1 = P_0$, $kQ_1 = Q_1$, $kV_1 = V_1$. By Lemma 1

$$S(\alpha^k) = \sum_{i \in P_1 \cup Q_1 \cup V_1} \alpha^{ki} = \sum_{i \in P_0 \cup Q_0 \cup V_1} \alpha^i = S(\alpha) + 1 \tag{16}$$

If $k \in V_1$ and $kmod\ p \in D_0^{(q)}$ then $kP_1 = P_1$, $kQ_1 = Q_0$, $kV_1 = V_0$. By Lemma 1

$$S(\alpha^k) = \sum_{i \in P_1 \cup Q_1 \cup V_1} \alpha^{ki} = \sum_{i \in P_1 \cup Q_1 \cup V_0} \alpha^i = S(\alpha) \tag{17}$$

If $k \in V_1$ and $kmod\ p \in D_1^{(q)}$ then $kP_1 = P_0$, $kQ_1 = Q_0$, $kV_1 = V_0$. By Lemma 1

$$S(\alpha^k) = \sum_{i \in P_1 \cup Q_1 \cup V_1} \alpha^{ki} = \sum_{i \in P_0 \cup Q_0 \cup V_0} \alpha^i = S(\alpha) + 1 \tag{18}$$

To sum up, if $k \in Z_N^*$, and $kmod\ p \in D_0^{(q)}$ then $S(\alpha^k) = S(\alpha)$; if $k \in Z_N^*$, and $kmod\ p \in D_1^{(q)}$, then $S(\alpha^k) = S(\alpha) + 1$.

If $k \in P$, then by Lemma 3

$$\begin{aligned} S(\alpha^k) &= \sum_{i \in P_1 \cup Q_1 \cup V_1} \alpha^{ki} = \sum_{i \in P_1} \alpha^{ki} + \sum_{i \in D_1^{(p)}} \alpha^{qki} + \sum_{i \in V_1} \alpha^{ki} = \sum_{i \in P_1} \alpha^{ki} + \frac{p-1}{2} + \frac{p-1}{2} \\ &= \sum_{i \in P_1} \alpha^{ki}. \end{aligned} \tag{19}$$

If $k \in Q$, then by Lemma 3

$$S(\alpha^k) = \sum_{i \in P_1 \cup Q_1 \cup V_1} \alpha^{ki} = \sum_{i \in Q_1} \alpha^{ki} + \sum_{i \in D_1^{(q)}} \alpha^{pki} + \sum_{i \in V_1} \alpha^{ki} = \sum_{i \in Q_1} \alpha^{ki} + \frac{q-1}{2} \tag{20}$$

□

Lemma 5. *$S(\alpha) \in \{0, 1\}$ if and only if $q \equiv \pm 1 (mod 8)$.*

Proof. The proof can be referred to Lemma 4 in [10]. □

Lemma 6.

(i) *If $k \in P$, $\sum_{i \in P_1} \alpha^{ki} \in \{0, 1\}$ if and only if $q \equiv \pm 1 (mod 8)$.*

(ii) *If $k \in Q$, $\sum_{i \in Q_1} \alpha^{ki} \in \{0, 1\}$ if and only if $p \equiv \pm 1 (mod 8)$.*

Proof. The proof can be referred to [1,17,18]. □

Note that

if $k \in P_0$, $\sum_{i \in P_1} \alpha^{ki} = 0$, then $k \in P_1$, $\sum_{i \in P_1} \alpha^{ki} = 1$;
if $k \in P_0$, $\sum_{i \in P_1} \alpha^{ki} = 1$, then $k \in P_1$, $\sum_{i \in P_1} \alpha^{ki} = 0$.
if $k \in Q_0$, $\sum_{i \in Q_1} \alpha^{ki} = 0$, then $k \in Q_1$, $\sum_{i \in Q_1} \alpha^{ki} = 1$;
if $k \in Q_0$, $\sum_{i \in Q_1} \alpha^{ki} = 1$, then $k \in Q_1$, $\sum_{i \in Q_1} \alpha^{ki} = 0$.

Considering the symmetry, in this paper, we set that

if $k \in P_0$, then $\sum_{i \in P_1} \alpha^{ki} = 0$, and if $k \in P_1$, then $\sum_{i \in P_1} \alpha^{ki} = 1$;
if $k \in Q_0$, then $\sum_{i \in Q_1} \alpha^{ki} + \frac{q-1}{2} = 0$, and if $k \in Q_1$, then $\sum_{i \in Q_1} \alpha^{ki} + \frac{q-1}{2} = 1$.

Let α be the same as before, then α^p is a primitive qth root of unity, α^q is a primitive pth root of unity. Hence,

$$x^p - 1 = \prod_{i \in R \cup Q} \left(x - \alpha^i\right), x^q - 1 = \prod_{i \in R \cup P} \left(x - \alpha^i\right). \tag{21}$$

In case $q \equiv \pm 1 (mod 8)$, define $P_j(x) = \prod_{i \in p_j} (x - \alpha^i)$, where $j = \{0, 1\}$. It follows that

$$x^q - 1 = P_0(x) P_1(x)(x - 1) \tag{22}$$

In case $p \equiv \pm 1 (mod 8)$, define $Q_j(x) = \prod_{i \in Q_j} (x - \alpha^i)$, where $j = \{0, 1\}$. It follows that

$$x^p - 1 = Q_0(x) Q_1(x)(x - 1) \tag{23}$$

Let $D(x) = \prod_{i \in Z_N^*} (x - \alpha^i)$, $D_j(x) = \prod_{\substack{i \in Z_N^* \\ i(mod\ p) \in D_j^{(q)}}} (x - \alpha^i)$, where $j \in \{0, 1\}$. It follows that

$$D(x) = D_0(x) D_1(x) \tag{24}$$

Theorem 1. *Let notations be the same as before, then the linear complexity of the new generalized cyclotomic sequences $S = \{S_i\}$ satisfies*

(i) If $p \equiv -3(mod 8)$, $q \equiv 3(mod 8)$ or $p \equiv 3(mod 8)$, $q \equiv -3(mod 8)$, then

$$LC(S) = N,\ M_S(x) = x^N - 1.$$

(ii) If $p \equiv 3(mod 8)$,$q \equiv 3(mod 8)$, then

$$LC(S) = N - 1,\ M_S(x) = \frac{x^N - 1}{x - 1}.$$

(iii) If $p \equiv -3(mod 8)$, $q \equiv -1(mod 8)$ or$p \equiv 3(mod 8)$, $q \equiv 1(mod 8)$, then

$$LC(S) = N - \frac{q-1}{2},\ M_S(x) = \frac{x^N - 1}{P_0(x)}.$$

(iv) If $p \equiv 3(mod 8)$, $q \equiv -1(mod 8)$, then

$$LC(S) = N - \frac{q-1}{2} - 1,\ M_S(x) = \frac{x^N - 1}{P_0(x)(x-1)}.$$

(v) If $p \equiv 1(mod 8)$, $q \equiv 3(mod 8)$ or $p \equiv -1(mod 8)$, $q \equiv -3(mod 8)$, then

$$LC(S) = \frac{N+q}{2},\ M_S(x) = \frac{x^N - 1}{Q_0(x) D_0(x)}.$$

(vi) If $p \equiv -1(mod\ 8)$, $q \equiv 3(mod\ 8)$, then

$$LC(S) = \frac{N+q}{2} - 1,\ M_S(x) = \frac{x^N - 1}{Q_0(x) D_0(x)(x-1)}.$$

(vii) If $p \equiv -1(mod 8)$, $q \equiv 1(mod 8)$ or $p \equiv 1(mod 8)$, $q \equiv -1(mod 8)$, then

$$LC(S) = \frac{N+1}{2},\ M_S(x) = \frac{x^N - 1}{P_0(x) Q_0(x) D_0(x)}.$$

(viii) If $p \equiv -1(mod 8)$, $q \equiv -1(mod 8)$, then

$$LC(S) = \frac{N-1}{2},\ M_S(x) = \frac{x^N - 1}{P_0(x) Q_0(x) D_0(x)(x-1)}.$$

Proof. In the two cases of (i), by Lemmas 4–6 and the Equation (8)

$$S(\alpha^k) = \begin{cases} 1, k = 0, \\ \neq 0, k \in Z_{N^*}, \\ \neq 0, k \in P, \\ \neq 0, k \in Q. \end{cases} \tag{25}$$

Hence, $gcd\left(x^N-1, S(x)\right)=1$. It follows that

$$M_S(x)=x^N-1,\ LC(S)=deg(M_S(x))=N. \tag{26}$$

In the case of (ii), by Lemmas 4–6 and the Equation (8),

$$S(\alpha^k)=\begin{cases} 0, k=0, \\ \neq 0, k\in Z_{N^*}, \\ \neq 0, k\in P, \\ \neq 0, k\in Q. \end{cases} \tag{27}$$

Hence, $gcd\left(x^N-1, S(x)\right)=x-1$. It follows that

$$M_S(x)=\frac{x^N-1}{x-1}, LC(S)=deg(M_S(x))=N-1. \tag{28}$$

In the two cases of (iii), by Lemmas 4–6, the Equation (8) and the choice of α

$$S(\alpha^k)=\begin{cases} 1, k=0, \\ \neq 0, k\in Z_{N^*}, \\ 0, k\in P_0, \\ 1, k\in P_1, \\ \neq 0, k\in Q. \end{cases} \tag{29}$$

Hence, $gcd\left(x^N-1, S(x)\right)=P_0(x)$. It follows that

$$M_S(x)=\frac{x^N-1}{P_0(x)},\ LC(S)=deg(M_S(x))=N-\frac{q-1}{2}. \tag{30}$$

In the case of (iv), by Lemmas 4–6, the Equation (8) and the choice of α

$$S(\alpha^k)=\begin{cases} 0, k=0, \\ \neq 0, k\in Z_{N^*}, \\ 0, k\in P_0, \\ 1, k\in P_1, \\ \neq 0, k\in Q. \end{cases} \tag{31}$$

Hence, $gcd\left(x^N-1, S(x)\right)=P_0(x)(x-1)$. It follows that

$$M_S(x)=\frac{x^N-1}{P_0(x)(x-1)},\ LC(S)=deg(M_S(x))=N-\frac{q-1}{2}-1. \tag{32}$$

In the case of (v), by Lemmas 4–6, the Equation (8) and the choice of α

$$S(\alpha^k)=\begin{cases} 1, k=0, \\ 0, k\in Z_{N^*}\ and\ k\ mod\ q\in D_0^{(q)}, \\ 1, k\in Z_{N^*}\ and\ k\ mod\ q\in D_1^{(q)}, \\ \neq 0, k\in P\cup Q_1, \\ 0, k\in Q_0. \end{cases} \tag{33}$$

Hence, $gcd\left(x^N-1, S(x)\right)=Q_0(x)D_0(x)$. It follows that

$$M_S(x)=\frac{x^N-1}{Q_0(x)D_0(x)}, LC(S)=deg(M_S(x))=\frac{N+q}{2}. \tag{34}$$

In the case of (vi), by Lemmas 4–6, the Equation (8) and the choice of α

$$S(\alpha^k) = \begin{cases} 0, & k = 0, \\ 0, & k \in Z_{N^*} \text{ and } k \bmod q \in D_0^{(q)}, \\ 1, & k \in Z_{N^*} \text{ and } k \bmod q \in D_1^{(q)}, \\ \neq 0, & k \in P \cup Q_1, \\ 0, & k \in Q_0. \end{cases} \tag{35}$$

Hence, $gcd\left(x^N - 1, S(x)\right) = Q_0(x)D_0(x)(x-1)$. It follows that

$$M_S(x) = \frac{x^N - 1}{Q_0(x)D_0(x)(x-1)},\ LC(S) = deg(M_S(x)) = \frac{N+q}{2} - 1. \tag{36}$$

In the two cases of (vii), by Lemmas 4–6, the Equation (8) and the choice of α

$$S(\alpha^k) = \begin{cases} 1, & k = 0, \\ 0, & k \in Z_{N^*} \text{ and } k \bmod q \in D_0^{(q)}, \\ 1, & k \in Z_{N^*} \text{ and } k \bmod q \in D_1^{(q)}, \\ 1, & k \in P_0 \cup Q_0, \\ 0, & k \in P_1 \cup Q_1. \end{cases} \tag{37}$$

Hence, $gcd\left(x^N - 1, S(x)\right) = P_0(x)Q_0(x)D_0(x)$. It follows that

$$M_S(x) = \frac{x^N - 1}{P_0(x)Q_0(x)D_0(x)}, LC(S) = deg(M_S(x)) = \frac{N+1}{2}. \tag{38}$$

In the case of (viii), by Lemmas 4–6, the Equation (8) and the choice of α

$$S(\alpha^k) = \begin{cases} 0, k = 0, \\ 0, k \in Z_{N^*} \text{ and } k \bmod q \in D_0^{(q)}, \\ 1, k \in Z_{N^*} \text{ and } k \bmod q \in D_1^{(q)}, \\ 1, k \in P_0 \cup Q_0, \\ 0, k \in P_1 \cup Q_1. \end{cases} \tag{39}$$

Hence, $gcd\left(x^N - 1, S(x)\right) = P_0(x)Q_0(x)D_0(x)(x-1)$. It follows that

$$M_S(x) = \frac{x^N - 1}{P_0(x)Q_0(x)D_0(x)},\ LC(S) = deg(M_S(x)) = \frac{N-1}{2} \tag{40}$$

□

5. Trace Representation of the New Sequences

Lemma 7. *Let p and q be two odd primes, $p \equiv \pm 1 (mod 8)$ and $q \equiv \pm 1 (mod 8)$, n be the order of 2 mod p, and m be the order of 2 mod q. Suppose g is a fixed common primitive root both p and q such that $g^{\frac{p-1}{n}} \equiv 2 (mod\ p)$ and $g^{\frac{q-1}{m}} \equiv 2 (mod\ q)$. Then, there exists a primitive pth root of unity $\beta \in GF(2^n)$ and a primitive qth root of unity $\gamma \in GF(2^m)$ for any positive integer f such that*

$$\sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n\left(\beta^{q^f g^{2i}}\right) = 0,\ \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m\left(\gamma^{p^f g^{2j}}\right) = 0. \tag{41}$$

$$\sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n\left(\beta^{q^f g^{2i} t}\right) = \begin{cases} \frac{p-1}{2}, \ if\ t = 0\ mod\ p \\ \frac{1-\left(\frac{t}{p}\right)}{2}, \ if\ t \neq 0\ mod\ p \end{cases}, \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m\left(\gamma^{p^f g^{2j} t}\right) = \begin{cases} \frac{q-1}{2}, \ if\ t = 0\ mod\ q \\ \frac{1-\left(\frac{t}{q}\right)}{2}, \ if\ t \neq 0\ mod\ q \end{cases} \tag{42}$$

Proof. The proof can be referred to Theorem 2 in [12]. □

Lemma 8. *Let $p > 3$ and $q > 3$ be primes, $p \equiv \pm 3(mod 8)$ and $q \equiv \pm 3(mod 8)$, n be the order of 2 mod p, m be the order of 2 mod q. Suppose g is a fixed common primitive root both p and q such that $g^{\frac{p-1}{n}} \equiv 2(mod\ p)$ and $g^{\frac{q-1}{m}} \equiv 2(mod\ q)$. Let $2^n - 1 = 3px$ and $2^m - 1 = 3qy$ for some positive integer x and y. Let α_1 be a primitive element in $GF(2^n)$, α_2 be a primitive element in $GF(2^m)$. Then, there exists a primitive pth root of unity $\beta \in GF(2^n)$ and a primitive qth root of unity $\gamma \in GF(2^m)$ for any positive integer f such that*

$$\sum_{i=0}^{\frac{p-1}{n}-1} tr_1^n\left(\left(\alpha_1^{px}\right)^{2^i} \beta^{q^f g^i}\right) = 0, \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\left(\alpha_2^{qy}\right)^{2^j} \beta^{p^f g^j}\right) = 0. \tag{43}$$

$$\sum_{i=0}^{\frac{p-1}{n}-1} tr_1^n\left(\left(\alpha_1^{px}\right)^{2^i} \beta^{q^f g^i t}\right) = \begin{cases} tr_1^n\left(\alpha_1^{px}\right), \ if\ t = 0\ mod\ p \\ \frac{1-\left(\frac{t}{p}\right)}{2}, \quad if\ t \neq 0\ mod\ p \end{cases} \tag{44}$$

$$\sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\left(\alpha_2^{qy}\right)^{2^j} \gamma^{p^f g^j t}\right) = \begin{cases} tr_1^m\left(\alpha_2^{qy}\right), \ if\ t = 0\ mod\ q \\ \frac{1-\left(\frac{t}{q}\right)}{2}, \quad if\ t \neq 0\ mod\ q \end{cases} \tag{45}$$

Proof. The proof can be referred to Theorem 4 in [12]. □

Theorem 2. *Let $p \equiv \pm 1(mod 8)$, $q \equiv \pm 1(mod 8)$, $N = pq$, $0 \leq t \leq N-1$, then the sequences $\{S_i\}$ can be expressed as*

$$S(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n\left(\beta^{q g^{2i} t}\right) + \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m\left(\gamma^{p g^{2j} t}\right) + \delta(t) \tag{46}$$

(i) If $p \equiv 1(mod 8)$, $q \equiv -1(mod 8)$, then

$$\delta(t) = \begin{cases} \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m\left(\gamma^{g^{2j} t}\right), t \in Z_N^* \cup \{0\} \\ \sum_{i=0}^{\frac{p-1}{n}-1} tr_1^n\left(\beta^{q g^i t}\right), t \in P \cup Q \end{cases} \tag{47}$$

(ii) If $p \equiv -1(mod 8)$, $q \equiv 1(mod 8)$, then

$$\delta(t) = \begin{cases} 1 + \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m\left(\gamma^{g^{2j+1} t}\right), t \in Z_N^* \cup \{0\} \\ \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\gamma^{p g^j t}\right), t \in P \cup Q \end{cases} \tag{48}$$

(iii) If $p \equiv -1(mod8)$, $q \equiv -1(mod8)$, *then*

$$\delta(t) = \begin{cases} \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m\left(\gamma^{g^{2j}t}\right), & t \in Z_N^* \\ 1, & t \in P \cup Q \\ 0, & t = 0 \end{cases} \tag{49}$$

Proof. (i) Let $a(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n\left(\beta^{qg^{2i}t}\right)$, $b(t) = \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m\left(\gamma^{pg^{2j}t}\right)$.

If $t \in V_0$, then $a(t) = 0$, $b(t) = \frac{1-\left(\frac{t}{q}\right)}{2}$, $\delta(t) = \frac{1-\left(\frac{t}{q}\right)}{2}$. Hence, $S(t) = 0$.

If $t \in V_1$, then $a(t) = 1$, $b(t) = \frac{1-\left(\frac{t}{q}\right)}{2}$, $\delta(t) = \frac{1-\left(\frac{t}{q}\right)}{2}$. Hence, $S(t) = 1$.

If $t \in P$, let $t = pk_1$, where $1 \le k_1 \le q-1$. So, there exists positive integer u such that $t = pg^u$. Then, $a(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n(1) = 0$, $\delta(t) = \sum_{i=0}^{\frac{p-1}{n}-1} tr_1^n(1) = 0$, $b(t)$ is discussed in the following two cases:

If $t \in P_0$, $b(t) = 0$; If $t \in P_1$, $b(t) = 1$.

Hence, if $t \in P_0$, $S(t) = 0$ and if $t \in P_1$, $b(t) = 1$.

If $t \in Q$, let $t = qk_2$, where $1 \le k_2 \le p-1$. Thus, there exists a positive integer v such that $t = qg^v$. Then, $b(t) = \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m(1) = 1$, $\delta(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n\left(\beta^{q^2g^{2i}} + \beta^{q^2g^{2i+1}}\right) = 1$, $a(t)$ is discussed in the following two cases:

If $t \in Q_0$, $a(t) = 0$; If $t \in Q_1$, $a(t) = 1$.

Hence, if $t \in Q_0$, $S(t) = 0$ and if $t \in Q_1$, $S(t) = 1$.

If $t = 0$, then $S(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n(1) + \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m(1) + \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m(1) = 0$.

(ii) and (iii) can be proved similarly.

The theorem is proved. □

Theorem 3. *Let* $p \equiv \pm 3(mod8)$, $q \equiv \pm 3(mod8)$, $N = pq$, $0 \le t \le N-1$, *then the sequences* $\{S_i\}$ *can be expressed as*

$$S(t) = \sum_{i=0}^{\frac{p-1}{n}-1} tr_1^n\left(\left(\alpha_1^{px}\right)^{2^i}\beta^{qg^it}\right) + \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\left(\alpha_2^{qy}\right)^{2^j}\gamma^{pg^jt}\right) + \delta(t) \tag{50}$$

(i) If $p \equiv 3(mod8)$, $q \equiv -3(mod8)$, *then*

$$\delta(t) = \begin{cases} \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\left(\alpha_2^{qy}\right)^{2^j}\gamma^{g^jt}\right), t \in Z_N^* \cup \{0\} \\ \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\gamma^{pg^jt}\right), t \in P \cup Q \end{cases} \tag{51}$$

(ii) If $p \equiv -3(mod8)$, $q \equiv 3(mod8)$, *then*

$$\delta(t) = \begin{cases} 1 + \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\left(\alpha_2^{2qy}\right)^{2^j}\gamma^{g^jt}\right), t \in Z_N^* \cup \{0\} \\ \sum_{i=0}^{\frac{p-1}{n}-1} tr_1^n\left(\beta^{qg^it}\right), t \in P \cup Q \end{cases} \tag{52}$$

(iii) If $p \equiv 3(mod8)$, $q \equiv 3(mod8)$, *then*

$$\delta(t) = \begin{cases} \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\left(\alpha_2^{qy}\right)^{2^j}\gamma^{g^j t}\right), & t \in Z_N^* \\ 1, & t \in P \cup Q \\ 0, & t = 0 \end{cases} \tag{53}$$

Proof. (i) Let $a(t) = \sum_{i=0}^{\frac{p-1}{n}-1} tr_1^n\left(\left(\alpha_1^{px}\right)^{2^i}\beta^{qg^i t}\right)$, $b(t) = \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\left(\alpha_2^{qy}\right)^{2^j}\gamma^{pg^j t}\right)$.

If $t \in V_0$, then $a(t) = 0$, $b(t) = \frac{1-\left(\frac{t}{q}\right)}{2}$, $\delta(t) = \frac{1-\left(\frac{t}{q}\right)}{2}$. Hence $S(t) = 0$.

If $t \in V_1$, then $a(t) = 1$, $b(t) = \frac{1-\left(\frac{t}{q}\right)}{2}$, $\delta(t) = \frac{1-\left(\frac{t}{q}\right)}{2}$. Hence $S(t) = 1$.

If $t \in P$, let $t = pk_1$, where $1 \le k_1 \le q-1$. Thus, there exists a positive integer u such that $t = pg^u$. Then, $a(t) = \sum_{i=0}^{\frac{p-1}{n}-1} tr_1^n\left(\alpha_1^{px}\right) = 1$, $\delta(t) = \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\gamma^{p^2 g^{j+u}}\right) = 1$, $b(t)$ is discussed in the following two cases:

If $t \in P_0$, $b(t) = 0$; If $t \in P_1$, $b(t) = 1$.

Hence, if $t \in P_0$, $S(t) = 0$ and if $t \in P_1$, $b(t) = 1$.

If $t \in Q$, let $t = qk_2$, where $k \le k_2 \le p-1$. Thus, there exists positive integer v such that $t = qg^v$. Then, $b(t) = \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\alpha_2^{qy}\right) = 0$, $\delta(t) = \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m(1) = 0$, $a(t)$ is discussed in the following two cases:

If $t \in Q_0$, $a(t) = 0$; If $t \in Q_1$, $a(t) = 1$.

Hence, if $t \in Q_0$, $S(t) = 0$ and if $t \in Q_1$, $S(t) = 1$.

If $t = 0$, then $S(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n\left(\alpha_1^{px}\right) + \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\alpha_2^{qy}\right) + \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\alpha_2^{qy}\right) = 0$

(ii) and (iii) can be proved similarly.

The theorem is proved. □

Theorem 4. *Let* $p \equiv \pm 1(mod8)$, $q \equiv \pm 3(mod8)$, $N = pq$, $0 \le t \le N-1$, *then the sequences* $\{S_i\}$ *can be expressed as*

$$S(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n\left(\beta^{qg^{2i}t}\right) + \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\left(\alpha_2^{qy}\right)^{2^j}\gamma^{pg^j t}\right) + \delta(t) \tag{54}$$

(i) If $p \equiv 1(mod8)$, $q \equiv 3(mod8)$, *then*

$$\delta(t) = \begin{cases} \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m\left(\gamma^{g^{2j}t}\right), t \in Z_N^* \cup \{0\} \\ \sum_{i=0}^{\frac{p-1}{n}-1} tr_1^n\left(\beta^{qg^i t}\right), t \in P \cup Q \end{cases} \tag{55}$$

(ii) If $p \equiv -1(mod8)$, $q \equiv -3(mod8)$, *then*

$$\delta(t) = \begin{cases} 1 + \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m\left(\gamma^{g^{2j+1}t}\right), t \in Z_N^* \cup \{0\} \\ \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\gamma^{pg^j t}\right), t \in P \cup Q \end{cases} \tag{56}$$

(iii) If $p \equiv -1(mod8)$, $q \equiv 3(mod8)$, *then*

$$\delta(t) = \begin{cases} \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m\left(\gamma^{g^{2j}t}\right), & t \in Z_N^* \\ 1, & t \in P \cup Q \\ 0, & t = 0 \end{cases} \tag{57}$$

Proof. The proof can be referred to Theorem 2 and Theorem 3. □

Theorem 5. *Let* $p \equiv \pm 3(mod8)$, $q \equiv \pm 1(mod8)$, $N = pq$, $0 \le t \le N-1$, *then the sequences* $\{S_i\}$ *can be expressed as*

$$S(t) = \sum_{i=0}^{\frac{p-1}{n}-1} tr_1^n\left(\left(\alpha_1^{px}\right)^{2^i}\beta^{qg^i t}\right) + \sum_{j=0}^{\frac{q-1}{2m}-1} tr_1^m\left(\gamma^{pg^{2j}t}\right) + \delta(t) \tag{58}$$

(i) If $p \equiv 3(mod8)$, $q \equiv 1(mod8)$, *then*

$$\delta(t) = \begin{cases} \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\left(\alpha_2^{qy}\right)^{2^j}\gamma^{g^j t}\right), t \in Z_N^* \cup \{0\} \\ \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\gamma^{pg^j t}\right), t \in P \cup Q \end{cases} \tag{59}$$

(ii) If $p \equiv 3(mod8)$, $q \equiv -1(mod8)$, *then*

$$\delta(t) = \begin{cases} \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\left(\alpha_2^{qy}\right)^{2^j}\gamma^{g^j t}\right), & t \in Z_N^* \\ 1, & t \in P \cup Q \\ 0, & t = 0 \end{cases} \tag{60}$$

(iii) If $p \equiv -3(mod8)$, $p \equiv -1(mod8)$, *then*

$$\delta(t) = \begin{cases} 1 + \sum_{j=0}^{\frac{q-1}{m}-1} tr_1^m\left(\left(\alpha_2^{2qy}\right)^{2^j}\gamma^{g^j t}\right), t \in Z_N^* \cup \{0\} \\ \sum_{i=0}^{\frac{p-1}{n}-1} tr_1^n\left(\beta^{qg^i t}\right), t \in P \cup Q \end{cases} \tag{61}$$

Proof. The proof can be referred to Theorem 2 and Theorem 3. □

6. Conclusions

In this paper, we presented the construction of a class of new balanced generalized cyclotomic binary sequences of order two with period pq based on the Ding's new generalized cyclotomic classes (V_0, V_1). The imbalance degree of the new sequences is 1, which conforms to the Golomb's random principles [3]. We determined the linear complexity and the minimal polynomial of the sequences. The results show that the sequences have good linear complexity to resist the attack of the Berlekamp–Massey algorithm. It is feasible that it serves as key stream in stream ciphers or as pseudo-random sequences in random number generators. By comparison, we can see that the linear complexity of the new sequences approximate to the result in [8], but the similar values are under different conditions with the choices of α. Moreover, the linear complexity of the new sequences in this paper is

better than those in [6,19]. We also give the trace representation of the sequences. The next step is to study the autocorrelation of the sequences [20].

Author Contributions: Conceptualization, J.M. and Y.J.; Data curation, X.S.; Funding acquisition, Y.J. and X.S.; Methodology, J.M.; Project administration, Y.J.; Resources, Y.J.; Software, W.Z.; Validation, W.Z., Y.J. and H.J.; Writing—original draft, J.M.; Writing—review & editing, J.M. and Y.J. All authors have read and agreed to the published version of the manuscript.

Funding: This paper was supported by the National Natural Science Foundation of China (61501395), the Natural Science Foundation of Hebei Province (F2020203043), the Research Project for Science and Technology in Higher Education of Hebei (QN2021144) and Science and Technology Research and Development Program of Qinhuangdao (202005A008).

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

Acknowledgments: The authors would like to thank anonymous referees for helpful suggestions, which greatly improve the presentation quality of this paper.

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

References

1. Cusick, T.W.; Ding, C.S.; Renvall, A. *Stream Ciphers and Number Theory*; Elsevier/North-Holland Mathematical Library: Amsterdam, The Netherlands, 1998.
2. Imamura, K.; Yoshida, W. A simple derivation of the Berlekamp- Massey algorithm and some applications. *IEEE Trans. Inf. Theory* **1987**, *33*, 146–150. [CrossRef]
3. Golomb, S.W.; Gong, G. *Signal Design for Good Correlation*; Cambridge University Press: Cambridge, NY, USA, 2005; pp. 117–119.
4. Whiteman, A.L. A family of difference sets. *Ill. J. Math.* **1962**, *6*, 107–121. [CrossRef]
5. Ding, C.S.; Helleseth, T. New generalized cyclotomy and its applications. *Finite Fields Appl.* **1998**, *4*, 140–166. [CrossRef]
6. Ding, C.S. Cyclotomic constructions of cyclic codes with length being the product of two primes. *IEEE Trans. Inf. Theory* **2012**, *58*, 2231–2236. [CrossRef]
7. Liu, H.N.; Chen, X.L. Autocorrelation Values and Linear Complexity of New Generalized Cyclotomic sequences. *Acta Math. Sin.* **2019**, *3*, 233–246.
8. Chen, Z.X.; Liu, H.N.; Yang, Y. Trace Representation of New Generalized Cyclotomic Sequences Based on RSA Moduli. *Acta Electron. Sin.* **2019**, *47*, 1512–1517.
9. Li, S.Q.; Xiao, G.Z. Study on a Class of Whiteman Generalized Cyclotomic Sequence with Length *pq* and Order Two. *J. Electron. Inf. Technol.* **2009**, *31*, 2205–2208.
10. Bai, E.J.; Liu, X.J.; Xiao, G.Z. Linear complexity of new generalized cyclotomic sequences of order of length pq. *IEEE Trans. Inf. Theory* **2005**, *51*, 1849–1853. [CrossRef]
11. Du, X.; Yan, T.; Xiao, G. Trace representation of some generalized cyclotomic sequences of length pq. *Inf. Sci.* **2008**, *178*, 3307–3316. [CrossRef]
12. Kim, J.H.; Song, H.Y. Trace Representation of Legendre Sequences. *Des. Codes Cryptogr.* **2001**, *24*, 343–348. [CrossRef]
13. Qi, M.; Xiong, S.; Yuan, J.; Rao, W.; Zhong, L. A Simpler Trace Representation of Legendre Sequences. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2015**, *98*, 1026–1031. [CrossRef]
14. Lv, C.; Yan, T.; Xiao, G. Multi-Rate Representation of Generalized Cyclotomic Sequences of Any Odd Period. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2015**, *98*, 2301–2306. [CrossRef]
15. Chen, Z.X.; Li, S.Q. Some Notes on Generalized Cyclotomic Sequences of Length pq. *J. Exp. Algorithmics* **2008**, *23*, 843–850. [CrossRef]
16. Ding, C.S.; Pei, D.; Salomaa, A. *Chinese Remainder Theorem. Applications in Computing, Coding, Cryptography*; World Scientific: Singapore, 1996.
17. Ding, C.; Hesseseth, T.; Shan, W. On linear complexity of Legendre sequences. *IEEE Trans. Inf. Theory* **1998**, *44*, 1276–1278. [CrossRef]
18. Wang, Q.; Lin, D.; Guang, X. On the Linear Complexity of Legendre Sequences over Fq. *IEICE Trans. Fundam.* **2014**, *97*, 1627–1630. [CrossRef]
19. Bo, Y.A.; Du, T.Q.; Xiao, Z.B. Linear Complexity of Generalized Cyclotomic Binary Sequences of Period *pq*. *Acta Math. Sin.* **2020**, *40*, 16–25.
20. Korobeinikov, A.V. Fast algorithm for calculating autocorrelation function in code synthesis tasks by enumerative technique. *Issues Radio Electron.* **2021**, *1*, 13–18. [CrossRef]