mathematics

MDPI

Article

Autocorrelation Values of Generalized Cyclotomic Sequences with Period p^{n+1}

Xiaolin Chen and Huaning Liu *

School of Mathematics, Northwest University, Xi'an 710127, China; xlchen@stumail.nwu.edu.cn
* Correspondence: hnliu@nwu.edu.cn

Received: 17 September 2019; Accepted: 9 Octber 2019; Published: 12 October 2019



Abstract: Recently Edemskiy proposed a method for computing the linear complexity of generalized cyclotomic binary sequences of period p^{n+1}, where $p = dR + 1$ is an odd prime, d, R are two non-negative integers, and $n > 0$ is a positive integer. In this paper we determine the exact values of autocorrelation of these sequences of period p^{n+1} $(n \geq 0)$ with special subsets. The method is based on certain identities involving character sums. Our results on the autocorrelation values include those of Legendre sequences, prime-square sequences, and prime cube sequences.

Keywords: stream cipher; generalized cyclotomy; generalized cyclotomic sequence; autocorrelation value; character sum

MSC: 94A55; 94A60; 11K45; 11B50

1. Introduction

Pseudorandom sequences with good randomness properties are widely applied in simulation, radar systems, spread-spectrum communication systems, ranging systems, software testing, global positioning systems, channel coding, code-division multiple-access (CDMA) systems, and stream ciphers [1–5]. If a sequence $s^\infty = (s_0, s_1, \cdots)$ over a field $\mathbb{F}$ satisfies $s_n = s_{n+T}$, $n \geq 0$, then s^∞ is said to be *T-periodic*. For a binary sequence s^∞ over the binary field $\mathbb{F}_2$, if $s_n = 1$ if and only if $n \in D$, then set D is called the *characteristic set* or *support set* of s^∞. Two important tools for measuring the randomness properties of pseudorandom sequences are autocorrelation values and linear complexity. The *periodic autocorrelation value* $C_s(\tau)$ of a T-periodic binary sequence s^∞ is defined by:

$$C_s(\tau) = \sum_{n=0}^{T-1} (-1)^{s_{n+\tau} + s_n},$$

where $0 \leq \tau \leq T-1$. The periodic autocorrelation value reflects global randomness. The *linear complexity* $L(s^\infty)$ of the sequence s^∞ is the length of the shortest linear feedback shift register which can generate s^∞. It is defined to be the least positive integer L satisfying:

$$s_t = c_1 s_{t-1} + c_2 s_{t-2} + \cdots + c_L s_{t-L} \text{ for all } t \geq L,$$

where $c_1, \cdots, c_L \in \mathbb{F}$.

The construction and randomness properties analysis of pseudorandom sequences are the core problem for pseudorandom sequences theory. Ding and Helleseth [6] introduced a generalized cyclotomy with respect to $p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, and introduced a class of new binary sequences whose characteristic set is selected as $\{0\} \cup [\cup_{d|n,d>1} \frac{n}{d} D_1^{(d)}]$. Several generalized cyclotomic sequences were constructed based on this generalized cyclotomy. Ding [7] obtained lower bounds on the linear complexity of generalized cyclotomic sequences with period p^2. He also determined the exact values of autocorrelation of these sequences by using certain formulas for generalized cyclotomic numbers. Later Ding [8] calculated the linear complexity of these sequences. In contrast to [7], this time he obtained the exact linear complexity, and the results did not require any special requirement for the prime. Park, Hong, and Eun [9] found technical errors in [8], so they corrected the errors and re-established the main results on the linear complexity. Yan, Sun, and Xiao [10] studied new generalized cyclotomic binary sequences with respect to p^2, which are a special case of those whose characteristic set are $\{0\} \cup [\cup_{d|n,d>1} \frac{n}{d} D_1^{(d)}]$ in [6]. Results indicate that these sequences possess high linear complexity. The exact values of autocorrelation are five-valued for $p \equiv 1 \pmod 4$, and three-valued for $p \equiv 3 \pmod 4$. The exact same results on the linear complexity and the exact values of autocorrelation of these new binary sequences were presented in [11,12], respectively. Kim, Jin, and Song [13] calculated the exact values of autocorrelation and linear complexity of prime cube sequences with period p^3. Results show that the autocorrelation values of these prime cube sequences are seven-valued for $p \equiv 1 \pmod 4$, and four-valued for $p \equiv 3 \pmod 4$. The linear complexity of generalized cyclotomic sequences of period p^n for any $n > 0$ is calculated in [14–17]. The autocorrelation values of those sequences of order 2 and period p^n are calculated in [18]. In this paper the described results on autocorrelation values are a generalization of the known ones from [10–13,19]. In contrast to [11–13], we present a simpler proof by using certain identities involving character sums. The proof of the results on autocorrelation values in [11–13] are all based on generalized cyclotomic numbers. The method for computing the autocorrelation values of the binary sequences in [10] is based on their characteristic polynomials. The autocorrelation values of our theorem are entirely consistent with those in [18], but the described results in this paper do not require the restriction $d = 2$. In addition, the parameters of our sequences are more complicated than those in [18], but the proof of our results is shorter and simpler.

In 2011 Edemskiy [20] proposed a method for computing the linear complexity of p^{n+1}-periodic generalized cyclotomic binary sequences. For details, suppose g is a primitive root of p^{n+1}, where $p = dR + 1$ is an odd prime, d, R are two non-negative integers, and $n > 0$ is a positive integer. Let $D_0^{(p^{n+1})} = (g^d)$ be a cyclic subgroup of the multiplicative group $\mathbb{Z}_{p^{n+1}}^*$. Define $D_i^{(p^{n+1})} = g^i D_0^{(p^{n+1})}$, $i = 0, 1, \cdots, d-1$, $p^m D_i^{(p^{n+1})} = \left\{ p^m a : a \in D_i^{(p^{n+1})} \right\}$, and $m = 0, 1, \cdots, n$. Then:

$$\mathbb{Z}_{p^{n+1}}^* = \bigcup_{i=0}^{d-1} D_i^{(p^{n+1})} \qquad \text{and} \qquad \mathbb{Z}_{p^{n+1}} = \bigcup_{m=0}^{n} \bigcup_{i=0}^{d-1} p^m D_i^{(p^{n+1})} \cup \{0\}.$$

Edemskiy defined the binary sequence s^∞ with period p^{n+1} as follows:

$$s_i = \begin{cases} 1, & \text{if } (i \bmod p^{n+1}) \in C, \\ 0, & \text{if } (i \bmod p^{n+1}) \notin C, \end{cases} \tag{1}$$

where the *characteristic set* of s^∞ is selected as:

$$C = \bigcup_{m=0}^{n} \bigcup_{i \in I_m} p^m D_i^{(p^{n+1})} \cup \{0\}, \qquad I_m \subset \{0, 1, \cdots, d-1\}.$$

He proposed a method for computing the *linear complexity* of s^{∞} and considered some special given I_m. In this paper for even d we shall choose special subsets:

$$I_0 = I_1 = \cdots = I_n = \{1, 3, 5, \cdots, d-1\}, \tag{2}$$

and compute the exact values of *autocorrelation* of this special generalized cyclotomic sequence with period p^{n+1} $(n \geq 0)$.

2. Sums Involving Legendre Symbol

We need the following lemma from [21].

Lemma 1. *Let $p > 2$ be a prime, $l \in \mathbb{Z}$, and $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol modulo p. Then we have:*

$$\sum_{t=0}^{p-1} \left(\frac{t(t+l)}{p}\right) = \begin{cases} p-1, & p \mid l, \\ -1, & p \nmid l, \end{cases}$$

where $p|l$ indicates that p is a divisor of l.

Lemma 2. *Let $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol modulo p. For $1 \leq \tau \leq p^{n+1}-1$ with $\gcd(\tau, p^{n+1}) = p^{m_0}$, we have:*

$$\sum_{m_1=0}^{n} \sum_{m_2=0}^{n} \sum_{\substack{t=0 \\ \gcd(t,p^{n+1})=p^{m_1} \\ \gcd(t+\tau,p^{n+1})=p^{m_2}}}^{p^{n+1}-1} \left(\frac{\frac{t}{p^{m_1}}}{p}\right)\left(\frac{\frac{t+\tau}{p^{m_2}}}{p}\right) = p^{n+1} - p^{n-m_0}(p+1).$$

Proof. It is convenient to divide the relations between m_1 and m_2 into three cases according as $m_1 > m_2$ or $m_1 < m_2$ or $m_1 = m_2$. From properties of the Legendre symbols modulo p and complete residue systems, we deduce:

$$\sum_{\substack{m_1=0 \\ m_1>m_2}}^{n} \sum_{m_2=0}^{n} \sum_{\substack{t=0 \\ \gcd(t,p^{n+1})=p^{m_1} \\ \gcd(t+\tau,p^{n+1})=p^{m_2}}}^{p^{n+1}-1} \left(\frac{\frac{t}{p^{m_1}}}{p}\right)\left(\frac{\frac{t+\tau}{p^{m_2}}}{p}\right) = \sum_{\substack{m_1=0 \\ m_1>m_2}}^{n} \sum_{m_2=0}^{n} \sum_{\gcd(p^{m_1}t+\tau,p^{n+1})=p^{m_2}}^{p^{n+1-m_1}-1} \left(\frac{t}{p}\right)\left(\frac{\frac{p^{m_1}t+\tau}{p^{m_2}}}{p}\right)$$

$$= \sum_{\substack{m_1=0 \\ m_1>m_2}}^{n} \sum_{m_2=0}^{n} \sum_{\gcd(p^{m_1}t+\tau,p^{n+1})=p^{m_2}}^{p^{n+1-m_1}-1} \left(\frac{t}{p}\right)\left(\frac{\frac{\tau}{p^{m_2}}}{p}\right) = \sum_{\substack{m_1=0 \\ m_1>m_2 \\ p^{m_2} \| \tau}}^{n} \sum_{m_2=0}^{n} \sum_{t=0}^{p^{n+1-m_1}-1} \left(\frac{t}{p}\right)\left(\frac{\frac{\tau}{p^{m_2}}}{p}\right) = 0,$$

and,

$$\sum_{\substack{m_1=0\\ m_1<m_2}}^{n}\sum_{m_2=0}^{n}\sum_{\substack{t=0\\ \gcd(t,p^{n+1})=p^{m_1}\\ \gcd(t+\tau,p^{n+1})=p^{m_2}}}^{p^{n+1}-1}\left(\frac{t}{p^{m_1}}\right)\left(\frac{t+\tau}{p^{m_2}}\right)=\sum_{\substack{m_1=0\\ m_1<m_2}}^{n}\sum_{m_2=0}^{n}\sum_{\substack{t=0\\ \gcd(t-\tau,p^{n+1})=p^{m_1}\\ \gcd(t,p^{n+1})=p^{m_2}}}^{p^{n+1}-1}\left(\frac{t-\tau}{p^{m_1}}\right)\left(\frac{t}{p^{m_2}}\right)$$

$$=\sum_{\substack{m_1=0\\ m_1<m_2}}^{n}\sum_{m_2=0}^{n}\sum_{\substack{t=0\\ \gcd(p^{m_2}t+\tau,p^{n+1})=p^{m_1}}}^{p^{n+1-m_2}-1}\left(\frac{t}{p}\right)\left(\frac{\frac{p^{m_2}t-\tau}{p^{m_1}}}{p}\right)=\sum_{\substack{m_1=0\\ m_1<m_2}}^{n}\sum_{m_2=0}^{n}\sum_{\substack{t=0\\ \gcd(p^{m_2}t+\tau,p^{n+1})=p^{m_1}}}^{p^{n+1-m_2}-1}\left(\frac{t}{p}\right)\left(\frac{\frac{-\tau}{p^{m_1}}}{p}\right)$$

$$=\sum_{\substack{m_1=0\\ m_1<m_2\\ p^{m_1}\|\tau}}^{n}\sum_{m_2=0}^{n}\sum_{t=0}^{p^{n+1-m_2}-1}\left(\frac{t}{p}\right)\left(\frac{\frac{-\tau}{p^{m_1}}}{p}\right)=0,$$

and,

$$\sum_{\substack{m_1=0\\ m_1=m_2}}^{n}\sum_{m_2=0}^{n}\sum_{\substack{t=0\\ \gcd(t,p^{n+1})=p^{m_1}\\ \gcd(t+\tau,p^{n+1})=p^{m_2}}}^{p^{n+1}-1}\left(\frac{t}{p^{m_1}}\right)\left(\frac{t+\tau}{p^{m_2}}\right)=\sum_{m=0}^{n}\sum_{\substack{t=0\\ \gcd(p^{m}t+\tau,p^{n+1})=p^{m}}}^{p^{n+1-m}-1}\left(\frac{t}{p}\right)\left(\frac{\frac{p^{m}t+\tau}{p^{m}}}{p}\right)$$

$$=\sum_{\substack{m=0\\ p^{m}\|\tau}}^{n}\sum_{\substack{t=0\\ \gcd(t+\frac{\tau}{p^{m}},p)=1}}^{p^{n+1-m}-1}\left(\frac{t}{p}\right)\left(\frac{t+\frac{\tau}{p^{m}}}{p}\right)+\sum_{\substack{m=0\\ p^{m+1}|\tau}}^{n}\sum_{\substack{t=0\\ \gcd(t,p)=1}}^{p^{n+1-m}-1}\left(\frac{t}{p}\right)\left(\frac{t+\frac{\tau}{p^{m}}}{p}\right)$$

$$=\sum_{\substack{m=0\\ p^{m}\|\tau}}^{n}\sum_{t=0}^{p^{n+1-m}-1}\left(\frac{t}{p}\right)\left(\frac{t+\frac{\tau}{p^{m}}}{p}\right)+\sum_{\substack{m=0\\ p^{m+1}|\tau}}^{n}p^{n-m}(p-1)$$

$$=\sum_{\substack{m=0\\ p^{m}\|\tau}}^{n}(-p^{n-m})+\sum_{\substack{m=0\\ p^{m+1}|\tau}}^{n}p^{n-m}(p-1)$$

$$=\begin{cases}-p^{n}, & \text{if } m_0=0,\\ -p^{n-m_0}+p^{n-m_0+1}(p^{m_0}-1), & \text{if } 1\le m_0\le n,\end{cases}$$

$$=p^{n+1}-p^{n-m_0}(p+1),$$

by Lemma 1. The combined results in these three cases yield:

$$\sum_{m_1=0}^{n}\sum_{m_2=0}^{n}\sum_{\substack{t=0\\ \gcd(t,p^{n+1})=p^{m_1}\\ \gcd(t+\tau,p^{n+1})=p^{m_2}}}^{p^{n+1}-1}\left(\frac{\frac{t}{p^{m_1}}}{p}\right)\left(\frac{\frac{t+\tau}{p^{m_2}}}{p}\right)=\sum_{\substack{m_1=0\\ m_1>m_2}}^{n}\sum_{m_2=0}^{n}\sum_{\substack{t=0\\ \gcd(t,p^{n+1})=p^{m_1}\\ \gcd(t+\tau,p^{n+1})=p^{m_2}}}^{p^{n+1}-1}\left(\frac{\frac{t}{p^{m_1}}}{p}\right)\left(\frac{\frac{t+\tau}{p^{m_2}}}{p}\right)$$

$$+\sum_{\substack{m_1=0\\ m_1<m_2}}^{n}\sum_{m_2=0}^{n}\sum_{\substack{t=0\\ \gcd(t,p^{n+1})=p^{m_1}\\ \gcd(t+\tau,p^{n+1})=p^{m_2}}}^{p^{n+1}-1}\left(\frac{\frac{t}{p^{m_1}}}{p}\right)\left(\frac{\frac{t+\tau}{p^{m_2}}}{p}\right)+\sum_{\substack{m_1=0\\ m_1=m_2}}^{n}\sum_{m_2=0}^{n}\sum_{\substack{t=0\\ \gcd(t,p^{n+1})=p^{m_1}\\ \gcd(t+\tau,p^{n+1})=p^{m_2}}}^{p^{n+1}-1}\left(\frac{\frac{t}{p^{m_1}}}{p}\right)\left(\frac{\frac{t+\tau}{p^{m_2}}}{p}\right)$$

$$=p^{n+1}-p^{n-m_0}(p+1).$$

□

3. Autocorrelation Values

The object of this section is to compute the autocorrelation values of s^∞ and the main results are stated as follows.

Theorem 1. *Let s^∞ be defined as in Equation (1) with $I_m=\{1,3,5,\cdots,d-1\}$ for $m=0,1,\cdots,n$. For $0\le\tau\le p^{n+1}-1$, the autocorrelation values of s^∞ are:*

$$C_s(\tau)=\begin{cases} p^{n+1}, & \text{if } \tau=0,\\ p^{n+1}-p^{n-m_0}(p+1)-\left(\frac{\frac{-\tau}{p^{m_0}}}{p}\right)-\left(\frac{\frac{\tau}{p^{m_0}}}{p}\right), & \text{if } \gcd(\tau,p^{n+1})=p^{m_0},\end{cases}$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol modulo p.

Proof. For $t\in\mathbb{Z}$, let $\gcd(t,p^{n+1})=p^m$, $0\le m\le n$ and write $t=p^mt'$, $\gcd(t',p)=1$. Observe that by $C=\bigcup_{m=0}^{n}\bigcup_{i\in I_m}p^mD_i^{(p^{n+1})}\bigcup\{0\}$ and make use of the orthogonality relation for characters modulo p^{n+1}, we have:

$$\begin{aligned} t\in C &\iff \text{there exists } i\in I_m \text{ satisfying } t\in p^mD_i^{(p^{n+1})}\\ &\iff \text{there exists } i\in I_m \text{ satisfying } t'\in D_i^{(p^{n+1})}\\ &\iff \text{there exist } i\in I_m,\ 0\le s\le p^nR-1 \text{ satisfying } t'\equiv g^{ds+i}\pmod{p^{n+1}}\\ &\iff \frac{1}{\phi(p^{n+1})}\sum_{i\in I_m}\sum_{s=0}^{p^nR-1}\sum_{\chi \bmod p^{n+1}}\chi(t')\overline{\chi}(g^{ds+i})=1\\ &\iff \frac{1}{d}\sum_{\substack{\chi \bmod p^{n+1}\\ \chi(g^d)=1}}\chi(t')\sum_{i\in I_m}\overline{\chi}(g^i)=1, \end{aligned}\tag{3}$$

where the sum $\sum_{\chi \bmod p^{n+1}}$ is over all multiplicative characters modulo p^{n+1}. With the aid of Equation (3) and the definition of I_m we now get:

$$\begin{aligned}(-1)^{s_t} &= -\frac{2}{d}\sum_{\substack{\chi \bmod p^{n+1}\\ \chi(g^d)=1\\ \chi\neq\chi_0}}\left(\sum_{i\in I_m}\overline{\chi}(g^i)\right)\chi(t') = -\frac{2}{d}\sum_{\substack{\chi \bmod p^{n+1}\\ \chi(g^d)=1\\ \chi\neq\chi_0}}\left(\sum_{i=0}^{\frac{d}{2}-1}\overline{\chi}(g^{2i+1})\right)\chi(t')\\ &= -\sum_{\substack{\chi \bmod p^{n+1}\\ \chi(g^d)=1\\ \chi(g^2)=1\\ \chi\neq\chi_0}}\overline{\chi}(g)\chi(t') = \left(\frac{t'}{p}\right),\end{aligned}$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol modulo p. Then for $0 \le t \le p^{n+1}-1$, we have:

$$(-1)^{s_t} = \begin{cases} \left(\frac{t'}{p}\right), & t = p^m t',\ 0 \le m \le n,\ \gcd(t',p)=1,\\ -1, & p^{n+1} \mid t. \end{cases} \tag{4}$$

For $1 \le \tau \le p^{n+1}-1$ with $\gcd(\tau, p^{n+1}) = p^{m_0}$, by means of Equation (4) we have:

$$\begin{aligned}C_s(\tau) &= \sum_{t=0}^{p^{n+1}-1}(-1)^{s_{t+\tau}+s_t}\\ &= \sum_{m_1=0}^{n}\sum_{m_2=0}^{n}\sum_{\substack{t=0\\ \gcd(t,p^{n+1})=p^{m_1}\\ \gcd(t+\tau,p^{n+1})=p^{m_2}}}^{p^{n+1}-1}\left(\frac{\frac{t}{p^{m_1}}}{p}\right)\left(\frac{\frac{t+\tau}{p^{m_2}}}{p}\right) - \sum_{m=0}^{n}\sum_{\substack{t=0\\ \gcd(t,p^{n+1})=p^{m}\\ p^{n+1}\mid t+\tau}}^{p^{n+1}-1}\left(\frac{\frac{t}{p^{m}}}{p}\right)\\ &\quad - \sum_{m=0}^{n}\sum_{\substack{t=0\\ p^{n+1}\mid t\\ \gcd(t+\tau,p^{n+1})=p^{m}}}^{p^{n+1}-1}\left(\frac{\frac{t+\tau}{p^{m}}}{p}\right) + \sum_{\substack{t=0\\ p^{n+1}\mid t\\ p^{n+1}\mid t+\tau}}^{p^{n+1}-1}1\\ &= \sum_{m_1=0}^{n}\sum_{m_2=0}^{n}\sum_{\substack{t=0\\ \gcd(t,p^{n+1})=p^{m_1}\\ \gcd(t+\tau,p^{n+1})=p^{m_2}}}^{p^{n+1}-1}\left(\frac{\frac{t}{p^{m_1}}}{p}\right)\left(\frac{\frac{t+\tau}{p^{m_2}}}{p}\right) - \left(\frac{\frac{-\tau}{p^{m_0}}}{p}\right) - \left(\frac{\frac{\tau}{p^{m_0}}}{p}\right).\end{aligned}$$

It follows from Lemma 2 that:

$$C_s(\tau) = \begin{cases} p^{n+1}, & \text{if } \tau = 0,\\ p^{n+1} - p^{n-m_0}(p+1) - \left(\frac{\frac{-\tau}{p^{m_0}}}{p}\right) - \left(\frac{\frac{\tau}{p^{m_0}}}{p}\right), & \text{if } \gcd(\tau,p^{n+1}) = p^{m_0}, \end{cases}$$

which proves Theorem 1. □

In the case of $d = 2$, that is, if s^∞ is defined by the quadratic residue classes, then the autocorrelation values are entirely consistent with those when $n = 0$ in [19], $n = 1$ in [10–12], and $n = 2$ in [13]. As a consequence, we get the following two corollaries for two special cases.

Corollary 1. *If $d = 2$, $n = 1$, $I_m = \{1\}$, $m = 0, 1$, that is:*

$$s_i = \begin{cases} 1, & \text{if } (i \bmod p^2) \in D_1^{(p^2)} \cup pD_1^{(p^2)} \cup \{0\}, \\ 0, & \text{if } (i \bmod p^2) \in D_0^{(p^2)} \cup pD_0^{(p^2)}. \end{cases}$$

Then for $p \equiv 1 \pmod 4$ we have:

$$C_s(\tau) = \begin{cases} p^2, & \text{if } \tau = 0, \\ -p-2, & \text{if } \tau \in D_0^{(p^2)}, \\ -p+2, & \text{if } \tau \in D_1^{(p^2)}, \\ p^2-p-3, & \text{if } \tau \in pD_0^{(p^2)}, \\ p^2-p+1, & \text{if } \tau \in pD_1^{(p^2)}, \end{cases}$$

and for $p \equiv 3 \pmod 4$ we have:

$$C_s(\tau) = \begin{cases} p^2, & \text{if } \tau = 0, \\ -p, & \text{if } \tau \in \mathbb{Z}_{p^2}^*, \\ p^2-p-1, & \text{if } \tau \in p\mathbb{Z}_p^*. \end{cases}$$

Corollary 2. *If $d = 2$, $n = 2$, $I_m = \{1\}$, $m = 0, 1, 2$, that is:*

$$s_i = \begin{cases} 1, & \text{if } (i \bmod p^3) \in D_1^{(p^3)} \cup pD_1^{(p^3)} \cup p^2D_1^{(p^3)} \cup \{0\}, \\ 0, & \text{if } (i \bmod p^2) \in D_0^{(p^3)} \cup pD_0^{(p^3)} \cup p^2D_0^{(p^3)}. \end{cases}$$

Then for $p \equiv 1 \pmod 4$ we have:

$$C_s(\tau) = \begin{cases} p^3, & \text{if } \tau = 0, \\ -p^2-2, & \text{if } \tau \in D_0^{(p^3)}, \\ -p^2+2, & \text{if } \tau \in D_1^{(p^3)}, \\ p^3-p^2-p-2, & \text{if } \tau \in pD_0^{(p^3)}, \\ p^3-p^2-p+2, & \text{if } \tau \in pD_1^{(p^3)}, \\ p^3-p-3, & \text{if } \tau \in p^2D_0^{(p^3)}, \\ p^3-p+1, & \text{if } \tau \in p^2D_1^{(p^3)}, \end{cases}$$

and for $p \equiv 3 \pmod 4$ we have:

$$C_s(\tau) = \begin{cases} p^3, & \text{if } \tau = 0, \\ -p^2, & \text{if } \tau \in D_0^{(p^3)} \cup D_1^{(p^3)}, \\ p^3-p^2-p, & \text{if } \tau \in pD_0^{(p^3)} \cup pD_1^{(p^3)}, \\ p^3-p-1, & \text{if } \tau \in p^2D_0^{(p^3)} \cup p^2D_1^{(p^3)}. \end{cases}$$

4. Conclusions

In this paper we computed the exact values of autocorrelation of generalized cyclotomic binary sequences of any order d and period p^{n+1} $(n \geq 0)$. Theorem 1 included the results of the autocorrelation values of Legendre sequences, prime-square sequences, and prime cube sequences from [10–13,19]. The autocorrelation values of our theorem were entirely consistent with those in [18]. In contrast to [18], our main results did not need the restriction $d = 2$, and the proof of our theorem was based on certain identities involving character sums while the proof in [18] used the generalized cyclotomic numbers.

Author Contributions: Conceptualization, X.C. and H.L.; methodology, X.C. and H.L.; writing—original draft preparation, X.C. and H.L.; writing—review and editing, X.C. and H.L.

Funding: This research was funded by National Natural Science Foundation of China grant number 11571277, and the Science and Technology Program of Shaanxi Province of China grant number 2016GY-080 and 2016GY-077.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cusick, T.W.; Ding, C.; Renvall, A. *Stream Ciphers and Number Theory*; North-Holland Mathematical Library, North-Holland Publishing Co.: Amsterdam, The Netherlands, 1998.
2. Ding, C. Autocorrelation values of generalized cyclotomic sequences of order two. *IEEE Trans. Inf. Theory* **1998**, *44*, 1699–1702. [CrossRef]
3. Gong, X.; Zhang, B.; Feng, D.; Yan, T. Autocorrelation values of new generalized cyclotomic sequences of order six over $\mathbb{Z}_{pq}$. In *Information Security and Cryptology*; Lecture Notes in Computer Science; Springer: Berlin, Germany, 2014; Volume 8567, pp. 86–98.
4. Li, S.; Chen, Z.; Fu, X.; Xiao, G. Autocorrelation values of new generalized cyclotomic sequences of order two and length pq. *J. Comput. Sci. Technol.* **2007**, *22*, 830–834. [CrossRef]
5. Wang, Q. The linear complexity of some binary sequences with three-level autocorrelation. *IEEE Trans. Inf. Theory* **2010**, *56*, 4046–4052. [CrossRef]
6. Ding, C.; Helleseth, T. New generalized cyclotomy and its applications. *Finite Fields Their Appl.* **1998**, *4*, 140–166. [CrossRef]
7. Ding, C. Binary cyclotomic generators. In *Fast Software Encryption*; Lecture Notes in Computer Science; Preneel, B., Ed.; Springer: Berlin, Germany, 1995; Volume 1008, pp. 29–60.
8. Ding, C. Linear complexity of some generalized cyclotomic sequences. *Int. J. Algebra Comput.* **1998**, *8*, 431–442. [CrossRef]
9. Park, Y.-H.; Hong, D.; Eun, H. On the linear complexity of some generalized cyclotomic sequences. *Int. J. Algebra Comput.* **2004**, *14*, 431–439. [CrossRef]
10. Yan, T.; Sun, R.; Xiao, G. Autocorrelation and linear complexity of the new generalized cyclotomic sequences. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2007**, *E90-A*, 857–864. [CrossRef]
11. Bai, E.; Liu, X. Some notes on prime-square sequences. *J. Comput. Sci. Technol.* **2007**, *22*, 481–486. [CrossRef]
12. Yan, T.; Huang, B.; Xiao, G. Cryptographic properties of some binary generalized cyclotomic sequences with the length p^2. *Inf. Sci.* **2008**, *178*, 1078–1086. [CrossRef]
13. Kim, Y.-J.; Jin, S.-Y.; Song, H.-Y. Linear complexity and autocorrelation of prime cube sequences. In *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*; Lecture Notes in Computer Science; Springer: Berlin, Germany, 2007; Volume 4851, pp. 188–197.
14. Du, X.; Yan, T.; Shi, Y. Linear complexity of generalized cyclotomic sequences with period p^m. *J. Electron. Inf. Technol.* **2010**, *32*, 821–824. (In Chinese) [CrossRef]
15. Kim, Y.-J.; Song, H.-Y. Linear complexity of prime n-square sequences. In Proceedings of the IEEE International Symposium on Information Theory, Toronto, ON, Canada, 6–11 July 2008; pp. 2405–2408.
16. Shi, Y.; Du, X.; Yan, T.; Li, X. Study of linear complexity of generalized cyclotomic sequences with period p^m. *Comput. Eng.* **2013**, *39*, 189–193. (In Chinese)

17. Yan, T.; Li, S.; Xiao, G. On the linear complexity of generalized cyclotomic sequences with the period p^m. *Appl. Math. Lett.* **2008**, *21*, 187–193. [CrossRef]
18. Jin, S.-Y.; Kim, Y.-J.; Song, H.-Y. Autocorrelation of new generalized cyclotomic sequences of period p^n. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2010**, *E93-A*, 2345–2348. [CrossRef]
19. Golomb, S.W.; Gong, G. *Sequence Design for Good Correlation*; Cambridge University Press: Cambridge, UK, 2005.
20. Edemskiy, V. About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1}. *Des. Codes Cryptogr.* **2011**, *61*, 251–260. [CrossRef]
21. Mullen, G.L.; Panario, D. *Handbook of Finite Fields*; Chapman and Hall/CRC: New York, NY, USA, 2013. [CrossRef]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).