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 October 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 $s^\infty$ is said to be $T$-periodic. For a binary sequence $s^\infty$ 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 $s^\infty$. 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 $s^\infty$ 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 $s^\infty$ is the length of the shortest linear feedback shift register which can generate $s^\infty$. It is defined to be the least positive integer $L$ satisfying:

$$s_t = c_1s_{t-1} + c_2s_{t-2} + \cdots + c_Ls_{t-L} \text{ for all } t \geq L,$$

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 \( p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s} \), and introduced a class of new binary sequences whose characteristic set is selected as \( \{ 0 \} \cup \{ \cup_{d \mid n_{1d} > 1} D^{(d)}_1 \} \). 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 \( s \). Results show that the autocorrelation values of these prime cube sequences are seven-valued for \( p \equiv 1 \) (mod 4), and three-valued for \( p \equiv 3 \) (mod 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 linear complexity and the exact linear complexity of prime cube sequences with period \( p^2 \). Results show that the autocorrelation values of these prime cube sequences are seven-valued for \( p \equiv 1 \) (mod 4), and four-valued for \( p \equiv 3 \) (mod 4). The linear complexity of generalized cyclotomic sequences of order 2 and 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 \( D_0^{(p^{n+1})} = \langle g^d \rangle \) be a cyclic subgroup of the multiplicative group \( \mathbb{Z}_{p^{n+1}}^* \). Define \( D_i^{(p^{n+1})} = g^i D_0^{(p^{n+1})} \), \( i = 0, 1, \cdots, d-1 \), \( p^m D_i^{(p^{n+1})} = \{ p^m a : a \in D_i^{(p^{n+1})} \} \), and \( m = 0, 1, \cdots, n \). Then:

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

Edemskiy defined the binary sequence \( s^\infty \) with period \( p^{n+1} \) as follows:

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

where the characteristic set of \( s^\infty \) is selected as:

\[
C = \bigcup_{m=0}^{n} \bigcup_{i \in I_m} p^m D_i^{(p^{n+1})} \cup \{ 0 \}, \quad I_m \subset \{ 0, 1, \cdots, d-1 \}.
\]
He proposed a method for computing the linear complexity of $s^\infty$ and considered some special given $I_m$. In this paper for even $d$ we shall choose special subsets:

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

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:

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

where $p \mid l$ 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:

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

**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:

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

and,
\[
\sum_{m_1=0}^n \sum_{m_2=0}^n \sum_{l=0}^{p^{n+1}-1} (\frac{t}{p^{m_1}}) \left( \frac{t + \tau}{p^{m_2}} \right) = \sum_{m_1=0}^n \sum_{m_2=0}^n \sum_{l=0}^{p^{n+1}-1} (\frac{t}{p^{m_1}}) \left( \frac{t - \tau}{p^{m_2}} \right)
\]

and,

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

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

\[ \sum_{m_1=0}^{n} \sum_{m_2=0}^{n} \sum_{l=0}^{p^{n+1}-1} \left( \frac{l}{p^{m_1}} \right) \left( \frac{l+\tau}{p^{m_2}} \right) = \sum_{m_1=0}^{n} \sum_{m_2=0}^{n} \sum_{l=0}^{p^{n+1}-1} \left( \frac{l}{p^{m_1}} \right) \left( \frac{l+\tau}{p^{m_2}} \right) \]

\[ + \sum_{m_1=0}^{n} \sum_{m_2=0}^{n} \sum_{l=0}^{p^{n+1}-1} \left( \frac{l}{p^{m_1}} \right) \left( \frac{l+\tau}{p^{m_2}} \right) + \sum_{m_1=0}^{n} \sum_{m_2=0}^{n} \sum_{l=0}^{p^{n+1}-1} \left( \frac{l}{p^{m_1}} \right) \left( \frac{l+\tau}{p^{m_2}} \right) \]

\[ = p^{n+1} - p^{n-m_0}(p + 1). \]

\[ \square \]

3. Autocorrelation Values

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

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

\[ C_s(\tau) = \begin{cases} 
  p^{n+1}, & \text{if } \tau = 0, \\
  p^{n+1} - p^{n-m_0}(p + 1) - \left( \frac{-\tau}{p} \right) - \left( \frac{-\tau}{p^{m_1}} \right), & \text{if } \gcd(\tau, p^{n+1}) = p^{m_0}, 
\end{cases} \]

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

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

\[ t \in C \iff \text{there exists } i \in I_m \text{ satisfying } t = p^mD_i^{(p^{n+1})} \]

\[ \iff \text{there exists } i \in I_m \text{ satisfying } t' \in D_i^{(p^{n+1})} \]

\[ \iff \text{there exist } i \in I_m, 0 \leq s \leq p^nR - 1 \text{ satisfying } t' \equiv g^{ds+i} \pmod{p^{n+1}} \]

\[ \iff \frac{1}{\phi(p^{n+1})} \sum_{i \in I_m} \sum_{s=0}^{p^nR-1} \sum_{\chi \mod p^{n+1}} \chi(t')\overline{\chi}(g^{ds+i}) = 1 \]

\[ \iff \frac{1}{d} \sum_{\chi \mod p^{n+1}} \chi(t') \sum_{i \in I_m} \overline{\chi}(g^i) = 1, \]

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

\[
(-1)^{s_1} = - \frac{2}{d} \sum_{\chi \mod p^{n+1}} \left( \sum_{t \in I_m} \overline{\chi}(s^t) \right) \chi(t') = - \frac{2}{d} \sum_{\chi \mod p^{n+1}} \left( \sum_{i=0}^{d-1} \overline{\chi}(s^{2i+1}) \right) \chi(t')
\]

\[
= - \sum_{\chi \mod p^{n+1}} \overline{\chi}(s) \chi(t') = \left( \frac{t}{p} \right),
\]

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

\[
(-1)^{s_1} = \begin{cases} 
\left( \frac{t}{p} \right), & t = p^m t', \ 0 \leq m \leq n, \gcd(t', p) = 1, \\
-1, & p^{n+1} \mid t.
\end{cases}
\] (4)

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

\[
C_s(\tau) = \sum_{t=0}^{p^{n+1}-1} (-1)^{s_1 t + s_1} 
= \sum_{m_1=0}^{n} \sum_{m_2=0}^{n} \sum_{l=0}^{p^{n+1}-1} \left( \frac{t}{p^m} \right) \left( \frac{t + \tau}{p^m} \right) - \sum_{m=0}^{n} \sum_{l=0}^{p^{n+1}-1} \left( \frac{t}{p^m} \right) \left( \frac{t + \tau}{p^m} \right)
\]

\[- \sum_{m=0}^{n} \sum_{t=0}^{p^{n+1}-1} \left( \frac{t + \tau}{p^{m+1} \mid t} \right) + \sum_{m=0}^{n} \sum_{t=0}^{p^{n+1}-1} \left( \frac{t + \tau}{p^{m+1} \mid t} \right)
\]

\[
= \sum_{m_1=0}^{n} \sum_{m_2=0}^{n} \sum_{l=0}^{p^{n+1}-1} \left( \frac{t}{p^m} \right) \left( \frac{t + \tau}{p^m} \right) - \left( \frac{-\tau}{p^m} \right) - \left( \frac{\tau}{p^m} \right).
\]

It follows from Lemma 2 that:

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

which proves Theorem 1. \( \square \)
In the case of $d = 2$, that is, if $s^\infty$ 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:

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

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:

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

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

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

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


