Linear Complexity of Some Binary Interleaved Sequences of Period $4N$

Xiao Ma[1,2], Tongjiang Yan[1,2], Daode Zhang[3], Yanyan Liu[1]
(Corresponding author: Tongjiang Yan)

College of Science, China University of Petroleum, Qingdao, Shandong 266580, China[1]
Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou, Fujian 350117, China[2]
State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences[3]
Beijing 266580, China
(Email: yantoji@163.com)
(Received Nov. 20, 2014; revised and accepted Apr. 20 & July 4, 2015)

Abstract

It is necessary that the linear complexity of a key stream sequence in a stream cipher system is not less than half of a period. This paper puts forward the linear complexity of a class of binary interleaved sequences with period $4N$ over the finite field with characteristic 2. Results show that the linear complexity of some of these sequences satisfies the requirements of cryptography.

Keywords: Interleaved sequence, linear complexity, minimal polynomial, stream cipher

1 Introduction

Sequences with good autocorrelation and large linear complexity have many applications in CDMA communication systems and cryptography [2, 4, 13].

Given two binary sequences $a = a(t)$ and $b = b(t)$ of period n, the periodic correlation between them is defined by

$$R_{a,b}(\tau) = \sum_{t=0}^{n-1} (-1)^{a(t)+b(t+\tau)}, 0 \leq \tau < n,$$

where the addition $t + \tau$ is performed modulo n. If $a = b$, $R_{a,b}(\tau)$ is called the (period) autocorrelation function of a, denoted by $R_a(\tau)$, otherwise, $R_{a,b}(\tau)$ is called the (periodic) cross-correlation function of a and b [12].

Binary sequences with optimal autocorrelation values can be classified into four types as follows according to the remainders of n modulo 4: (1) $R_a(\tau) = -1$ if $n \equiv 3 \bmod 4$; (2) $R_a(\tau) \in \{-2, 2\}$ if $n \equiv 2 \bmod 4$; (3) $R_a(\tau) \in \{1, -3\}$ if $n \equiv 1 \bmod 4$; (4) $R_a(\tau) \in \{0, -4\}$ if $n \equiv 0 \bmod 4$, where $0 < \tau < n$ [5]. In the first case, $R_a(\tau)$ is often called ideal autocorrelation. For more details about optimal autocorrelation, the reader is referred to [1, 4, 11].

The linear complexity of a sequence is often described in terms of the shortest linear feedback shift register (LFSR) that generates the sequence. Generally speaking, a sequence with large linear complexity is favorable for cryptography to resist the well-known Berlekamp-Massey algorithm [7, 16], and the sequence can be recovered easily if it has low linear complexity [5].

Some results have been gotten based on the interleaved structure [8, 15]. More precisely, Tang and Gong investigated the interleaved sequences of the form

$$\begin{aligned} u \;=\; & \mathbf{I}(a_0 + b(0), L^{\frac{1}{4}+\eta}(a_1) + b(1), \\ & L^{\frac{1}{2}}(a_2) + b(2), L^{\frac{3}{4}+\eta}(a_3) + b(3)), \end{aligned} \quad (1)$$

where $\mathbf{I}$ and L denote the interleaved operator and the left cyclic shift operator respectively [5]. $(b(0), b(1), b(2), b(3))$ is a binary perfect sequence which satisfies $R_b(\tau) = 0$ for $0 < \tau < 4$. And $a_i's$, $i = 0, 1, 2, 3$, are binary sequences of period N taken from the following sequence pairs:

- (l, l'): l and l' are the two types of Legendre sequences;
- (t, t'): t is a twin-prime sequence, and t' is its modified version.

Based on the two pairs of sequences, Tang and Gong constructed several kinds of sequences of period $4N$ with optimal autocorrelation value/magnitude, then Li and Tang obtained the linear complexity of these sequences in [5]. But in application, sequences with low autocorrelation values rather than optimal autocorrelation values also play an important role. In this paper, using the interleaved technique, we consider a class of sequences in the form of (t', t, t', t) defined by Equation (1). In [14], Yan and Gong have proved that the autocorrelation values of these sequences are low. Besides, this paper determine both the linear complexity and minimal polynomial of u of period $4N$ with low autocorrelation value/magnitude.

The remainder of this paper is organized as follows. Section 2 gives some preliminaries. Section 3 determines both the minimal polynomials and linear complexities of the sequences u obtained from twin-prime sequences. Conclusions and remarks are given in Section 4.

2 Preliminaries

Let $\{a_0, a_1, \cdots, a_{T-1}\}$ be a set of T sequences of period N. An $N \times T$ matrix U is formed by placing the sequence a_i on the ith column, where $0 \le i \le T-1$. Then one can obtain an interleaved sequence u of period NT by concatenating the successive rows of the matrix U. For simplicity, the interleaved sequence u can be written as

$$u = \mathbf{I}(a_0, a_1, \cdots, a_{T-1}).$$

In this paper, Legendre sequence and two-prime sequence are mentioned. Let $\mathbf{QR}_N$ and $\mathbf{NQR}_N$ denote all the nonzero squares and non-squares in $\mathbb{Z}_N$ respectively, where N is a prime. The Legendre sequence $l = (l(0), l(1), \cdots, l(N-1))$ of period N is defined as

$$l(i) = \begin{cases} 0 \text{ or } 1, & \text{if } i = 0; \\ 1, & \text{if } i \in \mathbf{QR}_N; \\ 0, & \text{if } i \in \mathbf{NQR}_N. \end{cases}$$

Specifically, l is called the first type Legendre sequence if $l(0) = 1$ otherwise the second type Legendre sequence. For simplicity, we employ l and l' to describe the first and second type Legendre sequence, respectively.

Let p and $p+2$ be two primes. The twin-prime sequence $t = (t(0), t(1), \cdots, t(N-1))$ of period $N = p(p+2)$ is defined as

$$t(i) = \begin{cases} 0, & \text{if } i = 0 (\bmod\ p+2); \\ 1, & \text{if } i = 0 (\bmod\ p); \\ l_p(i) + l_{p+2}(i), & \text{otherwise.} \end{cases}$$

where l_p, l_{p+2} are two Legendre sequences of period p and $p+2$ respectively.

Let $s = (s(i))_{i=0}^{\infty}$ be a sequence over a field $\mathbb{F}$. A polynomial of the form

$$f(x) = 1 + c_1 x + c_2 x^2 + \cdots + c_r x^r \in \mathbb{F}[x]$$

is called the characteristic polynomial of the sequence s if

$$s(i) = c_1 s(i-1) + c_2 s(i-2) + \cdots + c_r s(i-r), \forall i \ge r.$$

Among all the characteristic polynomials of s, the monic polynomial $m_s(x)$ with the lowest degree is called its minimal polynomial. The linear complexity of s is defined as the degree of $m_s(x)$, which is described as $\mathrm{LC}(s)$.

Let $s = (s(0), s(1), \cdots, s(n-1))$ be a binary sequence of period n and define the sequence polynomial

$$s(x) = s(0) + s(1)x + \cdots + s(n-1)x^{n-1}. \quad (2)$$

Then, its minimal polynomial and linear complexity can be determined by Lemma 1.

Lemma 1. *[6] Assume a sequence s of period n with sequence polynomial $s(x)$ is defined by Equation (2). Then*

- *The minimal polynomial is* $m_s(x) = \frac{x^n - 1}{\gcd(x^n-1, s(x))}$;
- *The linear complexity is* $\mathrm{LC}(s) = n - \deg(\gcd(x^n - 1, s(x)))$,

where $\gcd(x^n - 1, s(x))$ *denotes the greatest common divisor of* $x^n - 1$ *and* $s(x)$.

For the sequence polynomial, we have the following results.

Lemma 2. *[9] Let a be a binary sequence of period n, and $s_a(x)$ be its sequence polynomial. Then*

1) $s_b(x) = x^{n-\tau} s_a(x)$, *if* $b = L^{\tau}(a)$;
2) $s_b(x) = s_a(x) + \dfrac{x^n - 1}{x - 1}$, *if b is the complement sequence of a;*
3) $s_u(x) = s_a(x^4) + x s_b(x^4) + x^2 s_c(x^4) + x^3 s_d(x^4)$, *if* $u = \mathbf{I}(a, b, c, d)$.

3 Minimal Polynomial and Linear Complexity

If N is an odd integer and m is the order of 2 modulo N, then the finite field $\mathbb{F}_{2^m}$ is the splitting field of $x^N - 1$. Therefore, $\mathbb{F}_{2^m}$ has a primitive Nth root of unity, say β, and the set $\{1, \beta, \cdots, \beta^{N-1}\}$ of roots of $x^N - 1$ can form a cyclic group of order N with respect to the multiplication in $\mathbb{F}_{2^m}$ [5].

Let $u(x)$ be the sequence polynomial of u defined by Equation (1). By Lemma 1, it is equivalent to discuss the $\gcd(x^{4N} - 1, u(x))$ for determining the minimal polynomial and linear complexity of u. Without loss of generality, from now on we assume that the binary perfect sequence is $b = (0, 1, 1, 1)$ and the sequence polynomials of $a_i{}'s$ are $s_{a_i}(x)$, $1 \le i \le 3$.

By 1) and 2) in Lemma 2 and the fact $\frac{1}{4} = \frac{N+1}{4}$ (mod N) if $N \equiv 3$ (mod 4), the sequence polynomials of $L^{\frac{1}{4}+\eta}(a_1) + b(1)$, $L^{\frac{1}{2}}(a_2) + b(2)$, $L^{\frac{3}{4}+\eta}(a_3) + b(3)$ are $x^{N - \frac{N+1}{4} - \eta} s_{a_1}(x) + \frac{x^N - 1}{x - 1}$, $x^{N - \frac{N+1}{2}} s_{a_2}(x) + \frac{x^N - 1}{x - 1}$, $x^{N - \frac{3N+3}{4} - \eta} s_{a_3}(x) + \frac{x^N - 1}{x - 1}$, respectively. Then according to 3) in Lemma 2, the sequence polynomial of u for $N \equiv 3$ (mod 4) is

$$\begin{aligned} u(x) = \; & s_{a_0}(x^4) + x^{N-4\eta} s_{a_1}(x^4) \\ & + x^{2N} s_{a_2}(x^4) + x^{3N-4\eta} s_{a_3}(x^4) \\ & + \frac{x^{4N} - 1}{x^4 - 1}(x + x^2 + x^3). \end{aligned} \quad (3)$$

In what follows, we focus on the discussion of $\gcd(x^{4N} - 1, u(x))$ in terms of $(a_0, a_1, a_2, a_3) = (t', t, t', t)$, then compute both the linear complexity and minimal polynomial of u.

Let $N = pq$ where p and $p+2$ are two primes, and $s(x)$ be the sequence polynomial of twin-prime sequence t of period N. By Lemma 2, the sequence polynomial of modified twin-prime sequence t' is $s(x) + \frac{x^N-1}{x^q-1}$. Then, Equation (3) can be reduced to

$$\begin{aligned} u(x) &= s(x^4)(1+x^{2N})(1+x^{N-4\eta}) \\ &+ \frac{x^{4N}-1}{x^{4q}-1}(1+x^{2N}) \\ &+ \frac{x^{4N}-1}{x^{4q}-1}(x+x^2+x^3). \end{aligned} \quad (4)$$

Since N is odd, we have $u(1) = 1$, i.e., $\gcd(x-1, u(x)) = 1$. Then, Equation (4) can be rewritten as

$$\begin{aligned} & \gcd(x^{4N}-1, u(x)) \\ = & \gcd(\frac{x^{4N}-1}{x^4-1}, u(x)) \\ = & \gcd(\frac{x^{4N}-1}{x^{4q}-1}\frac{x^{4q}-1}{x^4-1}, s(x^4)(1+x^{2N})(1+x^{N-4\eta}) \\ & + \frac{x^{4N}-1}{x^{4q}-1}(1+x^{2N})) \\ = & \frac{x^{2N}-1}{x^{2q}-1}\gcd(\frac{x^{2N}-1}{x^{2q}-1}\frac{x^{4q}-1}{x^4-1}, s(x^4)(x^{2q}-1) \\ & (1+x^{N-4\eta}) + \frac{x^{2N}-1}{x^{2q}-1}(1+x^{2N})) \\ = & \frac{x^{2N}-1}{x^{2q}-1}\frac{x^{2q}-1}{x^2-1}\gcd(\frac{x^{2N}-1}{x^{2q}-1}\frac{x^{2q}-1}{x^2-1}, \\ & s(x^4)(x^2-1)(1+x^{N-4\eta}) + (\frac{x^{2N}-1}{x^{2q}-1})^2(x^2-1)). \end{aligned}$$

It follows from $\gcd(\frac{x^{2N}-1}{x^2-1}, x^2-1) = 1$ that

$$\begin{aligned} & \gcd(x^{4N}-1, u(x)) \\ = & \frac{x^{2N}-1}{x^2-1}\gcd(\frac{x^{2N}-1}{x^2-1}, s(x^4)(1+x^{N-4\eta}) \\ & + (\frac{x^{2N}-1}{x^{2q}-1})^2). \end{aligned} \quad (5)$$

Since N and $N-4\eta$ are odd, x^N-1 and $x^{N-4\eta}-1$ have no repeated roots in their splitting field.

For simplicity, define

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

Lemma 3. *[3] Let $s(x)$ be the sequence polynomial of the twin-prime sequence of period N and D_j be the generalized cyclotomic classes of order 2 with respect to p and $p+2$ for $j = 0, 1$. Then, for $0 \le i \le N-1$,*

1) *If $p \equiv 1 \pmod 4$, $s(\beta^i) = 0$ if $i = 0$, otherwise $s(\beta^i) \ne 0$.*
2) *If $p \equiv 3 \pmod 4$, $s(\beta^i) = 0$ if $i = 0$, $i \in P \cup Q$ or $i \in D_0$ (by choice of β), otherwise $s(\beta^i) \ne 0$.*

Further, $x^N - 1 = \frac{(x^q-1)(x^p-1)d_0(x)d_1(x)}{x-1}$, *where* $d_j(x) = \prod_{i\in D_j}(x-\beta^i) \in \mathbb{F}_2[x]$, $j = 0, 1$.

We discuss the results of Equation (5) by Lemma 3 as follows,

- $(\frac{x^N-1}{x-1})^2|_{\beta^i} = \left(\frac{(x^q-1)(x^p-1)d_0(x)d_1(x)}{(x-1)^2}\right)^2|_{\beta^i} = 0$ if $i \in P \cup Q \cup D_0 \cup D_1$.
- $\left(\frac{x^N-1}{x^q-1}\right)^4|_{\beta^i} = 0$ if $i \in Q \cup D_0 \cup D_1$.

Nextly, we will discuss the roots of $s(x^4)$ and $(1 + x^{N-4\eta})$ according to the distinct values of η and p by Lemma 3, then $\gcd(x^{4N}-1, u(x))$ is determined.

Case 1. $\eta = 0$, $p \equiv 1 \pmod 4$.

By Lemma 3, we have $s(x^4)|_{\beta^i} = 0$ if $i \in \{0\}$, and $(1+x^N)|_{\beta^i} = 0$ if $i \in \{0\} \cup P \cup Q \cup D_0 \cup D_1$. Then

$$\begin{aligned} & \gcd\left(\frac{x^{2N}-1}{x^2-1}, s(x^4)(1+x^N) + \left(\frac{x^{2N}-1}{x^{2q}-1}\right)^2\right) \\ = & \frac{x^N-1}{x^q-1}, \\ & \gcd(x^{4N}-1, u(x)) = \frac{x^{2N}-1}{x^2-1}\frac{x^N-1}{x^q-1} \end{aligned}$$

Case 2. $\eta = 0$, $p \equiv 3 \pmod 4$.

By Lemma 3, we have $s(x^4)|_{\beta^i} = 0$ if $i \in \{0\} \cup P \cup Q \cup D_0$, and $(1+x^N)|_{\beta^i} = 0$ if $i \in \{0\} \cup P \cup Q \cup D_0 \cup D_1$. Then

$$\begin{aligned} & \gcd\left(\frac{x^{2N}-1}{x^2-1}, s(x^4)(1+x^N) + \left(\frac{x^{2N}-1}{x^{2q}-1}\right)^2\right) \\ = & \left(\frac{x^p-1}{x-1}d_0(x)\right)^2 d_1(x), \\ & \gcd(x^{4N}-1, u(x)) \\ = & \frac{x^{2N}-1}{x^2-1}\left(\frac{x^p-1}{x-1}d_0(x)\right)^2 d_1(x) \end{aligned}$$

Case 3. $\eta \in Q$, $p \equiv 1 \pmod 4$.

By Lemma 3, we have $s(x^4)|_{\beta^i} = 0$ if $i \in \{0\}$, and $(1+x^{N-4\eta})|_{\beta^i} = 0$ if $i \in \{0\} \cup P$. Then

$$\begin{aligned} & \gcd\left(\frac{x^{2N}-1}{x^2-1}, s(x^4)(1+x^{N-4\eta}) + \left(\frac{x^{2N}-1}{x^{2q}-1}\right)^2\right) \\ = & 1, \\ & \gcd(x^{4N}-1, u(x)) = \frac{x^{2N}-1}{x^2-1} \end{aligned}$$

Case 4. $\eta \in Q$, $p \equiv 3 \pmod 4$.

By Lemma 3, we have $s(x^4)|_{\beta^i} = 0$ if $i \in \{0\} \cup P \cup Q \cup D_0$, and $(1+x^{N-4\eta})|_{\beta^i} = 0$ if $i \in \{0\} \cup P$. Then

$$\begin{aligned} & \gcd\left(\frac{x^{2N}-1}{x^2-1}, s(x^4)(1+x^{N-4\eta}) + \left(\frac{x^{2N}-1}{x^{2q}-1}\right)^2\right) \\ = & \left(\frac{x^p-1}{x-1}d_0(x)\right)^2, \\ & \gcd(x^{4N}-1, u(x)) = \frac{x^{2N}-1}{x^2-1}\left(\frac{x^p-1}{x-1}d_0(x)\right)^2 \end{aligned}$$

Case 5. $\eta \in P$, $p \equiv 1 \pmod 4$.

By Lemma 3, we have $s(x^4)|_{\beta^i} = 0$ if $i \in \{0\}$, and $(1+x^{N-4\eta})|_{\beta^i} = 0$ if $i \in \{0\} \cup Q$. Then

$$\gcd\left(\frac{x^{2N}-1}{x^2-1}, s(x^4)(1+x^{N-4\eta}) + \left(\frac{x^{2N}-1}{x^{2q}-1}\right)^2\right) = \frac{x^p-1}{x-1},$$

$$\gcd(x^{4N}-1, u(x)) = \frac{x^{2N}-1}{x^2-1}\frac{x^p-1}{x-1}$$

Case 6. $\eta \in P$, $p \equiv 3 \pmod 4$.

By Lemma 3, we have $s(x^4)|_{\beta^i} = 0$ if $i \in \{0\} \cup P \cup Q \cup D_0$, and $(1+x^{N-4\eta})|_{\beta^i} = 0$ if $i \in \{0\} \cup Q$. Then

$$\gcd\left(\frac{x^{2N}-1}{x^2-1}, s(x^4)(1+x^{N-4\eta}) + \left(\frac{x^{2N}-1}{x^{2q}-1}\right)^2\right) = \left(\frac{x^p-1}{x-1}d_0(x)\right)^2,$$

$$\gcd(x^{4N}-1, u(x)) = \frac{x^{2N}-1}{x^2-1}\left(\frac{x^p-1}{x-1}d_0(x)\right)^2$$

In the following two cases, as for $\eta \in Z_N^*$, one can deduce that $(1+x^{N-4\eta})|_{\beta^i} = 0$ for any $1 \le i \le N-1$.

Case 7. $\eta \in Z_N^*$, $p \equiv 1 \pmod 4$.

By Lemma 3, we have $s(x^4)|_{\beta^i} = 0$ if $i \in \{0\}$. Then

$$\gcd\left(\frac{x^{2N}-1}{x^2-1}, s(x^4)(1+x^{N-4\eta}) + \left(\frac{x^{2N}-1}{x^{2q}-1}\right)^2\right) = 1,$$

$$\gcd(x^{4N}-1, u(x)) = \frac{x^{2N}-1}{x^2-1}$$

Case 8. $\eta \in Z_N^*$, $p \equiv 3 \pmod 4$.

By Lemma 3, we have $s(x^4)|_{\beta^i} = 0$ if $i \in \{0\} \cup P \cup Q \cup D_0$. Then

$$\gcd\left(\frac{x^{2N}-1}{x^2-1}, s(x^4)(1+x^{N-4\eta}) + \left(\frac{x^{2N}-1}{x^{2q}-1}\right)^2\right) = \left(\frac{x^p-1}{x-1}d_0(x)\right)^2,$$

$$\gcd(x^{4N}-1, u(x)) = \frac{x^{2N}-1}{x^2-1}\left(\frac{x^p-1}{x-1}d_0(x)\right)^2$$

By Lemma 1, substituting the results discussed above into $m_u(x) = \frac{x^{4N}-1}{\gcd(x^{4N}-1, u(x))}$, we can determine the minimal polynomial and linear complexity of u that obtained from the twin-prime sequence as follows.

Theorem 1. *Let the integer $N = pq$ where p and $q = p+2$ are two primes, $(a_0, a_1, a_2, a_3) = (t', t, t', t)$ and $b = (0,1,1,1)$. Then the interleaved sequence u defined by Equation (1) has the following properties:*

- *The minimal polynomial is*

$$m_u(x) = \begin{cases} (x^N-1)(x^2-1)(x^q-1), \\ \quad \text{if } \eta = 0 \text{ and } p \equiv 1 \pmod 4; \\ \frac{(x^{2N}-1)(x^4-1)}{(x^{2p}-1)d_0^2(x)d_1(x)}, \\ \quad \text{if } \eta = 0 \text{ and } p \equiv 3 \pmod 4; \\ (x^{2N}-1)(x^2-1), \\ \quad \text{if } \eta \in Q \text{ and } p \equiv 1 \pmod 4; \\ \frac{(x^{2N}-1)(x^4-1)}{(x^{2p}-1)d_0^2(x)}, \\ \quad \text{if } \eta \in Q \text{ and } p \equiv 3 \pmod 4; \\ \frac{(x^{2N}-1)(x-1)^3}{x^p-1}, \\ \quad \text{if } \eta \in P \text{ and } p \equiv 1 \pmod 4; \\ \frac{(x^{2N}-1)(x^4-1)}{(x^{2p}-1)d_0^2(x)}, \\ \quad \text{if } \eta \in P \text{ and } p \equiv 3 \pmod 4; \\ (x^{2N}-1)(x^2-1), \\ \quad \text{if } \eta \in Z_N^* \text{ and } p \equiv 1 \pmod 4; \\ \frac{(x^{2N}-1)(x^4-1)}{(x^{2p}-1)d_0^2(x)}, \\ \quad \text{if } \eta \in Z_N^* \text{ and } p \equiv 3 \pmod 4. \end{cases}$$

- *The linear complexity of u is*

$$LC(u) = \begin{cases} p^2+3p+4, \text{if } \eta = 0 \text{ and } p \equiv 1 \pmod 4; \\ \frac{p^2}{2}+2p+\frac{11}{2}, \text{if } \eta = 0 \text{ and } p \equiv 3 \pmod 4; \\ 2p^2+4p+2, \text{if } \eta \in Q \text{ and } p \equiv 1 \pmod 4; \\ p^2+2p+5, \text{if } \eta \in Q \text{ and } p \equiv 3 \pmod 4; \\ 2p^2+3p+3, \text{if } \eta \in P \text{ and } p \equiv 1 \pmod 4; \\ p^2+2p+5, \text{if } \eta \in P \text{ and } p \equiv 3 \pmod 4; \\ 2p^2+4p+2, \text{if } \eta \in Z_N^* \text{ and } p \equiv 1 \pmod 4; \\ p^2+2p+5, \text{if } \eta \in Z_N^* \text{ and } p \equiv 3 \pmod 4. \end{cases}$$

Example 1. *Let $p = 3$ and $q = 5$, then the twin-prime sequence of period $N = 15$ is*

$$t = (0,0,0,1,0,0,1,1,0,1,0,1,1,1,1)$$

and the modified twin-prime sequence is

$$t' = (1,0,0,1,0,1,1,1,0,1,1,1,1,1,1).$$

If one takes $\eta = 5 \in Q$, then $\frac{1}{4}+\eta = 9 \mod 15$, $\frac{1}{2} = 8 \mod 15$, and $\frac{3}{4}+\eta = 2 \mod 15$. By Equation (1), the *sequence u of period $4N = 60$ is*

$$\begin{aligned} t \;=\; & (1,0,1,1,0,1,0,0,0,0,0,1,1,0,0,\\ & 1,0,0,0,0,1,0,0,0,1,1,0,1,1,1,\\ & 0,0,0,1,1,1,1,0,1,0,1,1,0,0,1,\\ & 1,1,0,1,0,0,0,1,0,0,1,1,1,0,1). \end{aligned}$$

By Magma program, the minimal polynomial of u is $m_u(x) = x^{20} + x^{16} + x^{12} + x^6 + x^2 + 1$ and the linear complexity of u is $LC(u) = 20$, which are compatible with the results given by Theorem 1.

Example 2. *Let $p = 5$ and $q = 7$, then the twin-prime sequence of period $N = 35$ is*

$$\begin{aligned} t \;=\; & (0,0,1,0,0,1,1,0,1,0,1,0,0,0,0,1,0,\\ & 0,1,1,1,0,1,1,1,1,1,0,0,0,1,1,1,0,1) \end{aligned}$$

and the modified twin-prime sequence is

$$\begin{aligned} t' \;=\; & (1,0,1,0,0,1,1,1,1,0,1,0,0,0,1,1,0,\\ & 0,1,1,1,1,1,1,1,1,1,0,1,0,1,1,1,0,1). \end{aligned}$$

If one takes $\eta = 7 \in Q$, then $\frac{1}{4} + \eta = 16 \mod 35$, $\frac{1}{2} = 18 \mod 35$, and $\frac{3}{4} + \eta = 34 \mod 35$. By Equation (1), the sequence u of period $4N = 140$ is

$$\begin{aligned} t \;=\; & (1,1,0,0,0,1,0,1,1,0,0,1,0,0,0,0,0,0,0,1,\\ & 1,1,0,1,1,0,0,0,1,0,0,0,1,0,0,1,0,0,1,0,\\ & 1,0,0,1,0,1,1,0,0,1,0,1,0,1,0,1,1,0,0,1,\\ & 1,0,1,1,0,0,0,0,0,1,0,1,1,0,1,1,1,1,0,0,\\ & 1,1,1,0,1,0,1,0,1,1,0,1,1,1,0,0,1,0,0,0,\\ & 1,0,0,0,1,1,1,0,0,0,0,0,1,1,1,1,0,0,1,1,\\ & 1,1,1,1,1,1,0,0,1,1,0,0,0,1,1,0,1,0,1,1). \end{aligned}$$

By Magma program, the minimal polynomial of u is $m_u(x) = x^{72} + x^{70} + x^2 + 1$ and the linear complexity of u is $LC(u) = 72$, which are compatible with the results given by Theorem 1.

4 Conclusion

In this paper, based on the discussion of roots of the sequence polynomials in the splitting field of $x^N - 1$, both the minimal polynomials and linear complexities of the binary interleaved sequences of period $4N$ with low autocorrelation value/magnitude are completely determined. When $p \equiv 1 \pmod 4$ and $\eta \in Q \cup Z_N^*$, the linear complexity of u is greater than half of a period, then it is as strong as the sequences defined by Tang et al. [5].

Most recently, Xiong and Qu investigated 2-adic complexity of some binary sequences with interleaved structure [10]. Similarly, we will compute 2-adic complexity of interleaved sequences defined in this paper.

Acknowledgments

This work was supported by the National Natural Science Foundations of China (No.61170319, No.61103199), the Natural Science Fund of Shandong Province (No.ZR2014FQ005) and the Fundamental Research Funds for the Central Universities (No.15CX08011A, No.15CX02065A).

References

[1] K. T. Arasu, C. Ding, T. Helleseth, P. Kumar, and H. Martinsen, "Almost difference sets and their sequences with optimal autocorrelation," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 2934–2943, 2001.

[2] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*, Amsterdam: Elsevier, 2004.

[3] 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.

[4] S. W. Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar*, New York: Cambridge University Press, 2005.

[5] N. Li and X. Tang, "On the linear complexity of binary sequences of period 4N with optimal autocorrelation value/magnitude," *IEEE Transactions on Information Theory*, vol. 57, no. 11, pp. 7597–7604, 2011.

[6] R. Lidl and H. Niederreiter, *Finite Fields (Encyclopedia of Mathematics and Its Applications)*, New York: Cambridge University Press, 1997.

[7] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.

[8] X. Tang and G. Gong, "New constructions of binary sequences with optimal autocorrelation value/magnitude," *IEEE Transactions on Information Theory*, vol. 56, no. 3, pp. 1278–1286, 2010.

[9] Qi Wang and X. Du, "The linear complexity of binary sequences with optimal autocorrelation," *IEEE Transactions on Information Theory*, vol. 56, no. 12, pp. 6388–6397, 2010.

[10] H. Xiong, L. Qu, and C. Li, "2-adic complexity of binary sequences with interleaved structure," *Finite Fields and Their Applications*, vol. 33, pp. 14–28, 2015.

[11] T. Yan, "New binary sequences of period pq with low values of correlation and large linear complexity," *International Journal of Network Security*, vol. 10, no. 3, pp. 185–189, 2010.

[12] T. Yan, Z. Chen, and B. Li, "A general construction of binary sequences with optimal autocorrelation," *Information Sciences*, vol. 287, pp. 26–31, 2014.

[13] T. Yan, X. Du, and S. Li, "Trace representations and multi-rate constructions of two classes of generalized

cyclotomic sequences," *International Journal of Network Security*, vol. 7, no. 2, pp. 269–272, 2008.

[14] T. Yan and G. Gong, "Some notes on constructions of binary sequences with optimal autocorrelation," 2014. (http://arxiv.org/abs/1411.4340)

[15] N. Y. Yu and G. Gong, "New binary sequences with optimal autocorrelation magnitude," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4771–4779, 2008.

[16] J. Zhou and W. Xiong, "An algorithm for computing m-tight error linear complexity of sequences over GF(p^m) with period p^m," *International Journal of Network Security*, vol. 15, no. 1, pp. 59–63, 2013.

Xiao Ma was born in 1992 in Shandong Province of China. She was graduated from China University of Petroleum. She will study for a postgraduate degree at China University of Petroleum in 2014. And her tutor is Tongjiang YAN. Email:maxiaoupc@163.com

Tongjiang Yan was born in 1973 in Shandong Province of China. He was graduated from the Department of Mathematics, Huaibei Coal-industry Teachers College, China, in 1996. In 1999, he received the M.S. degree in mathematics from the Northeast Normal University, Lanzhou, China. In 2007, he received the Ph.D. degree in Xidian University. He is now a professor of China University of Petroleum. His research interests include cryptography and algebra. Email:yantoji@163.com

Daode Zhang was born in 1991 in Shandong Province of China. He was graduated from China University of Petroleum. He will study for a postgraduate degree at University of Chinese Academy of Sciences in 2014. And his tutor is Bao Li. Email:zhangddmath@163.com

Yanyan Liu was born in 1990 in Shandong Province of China. She was graduated from China University of Petroleum. She will study for a postgraduate degree at China University of Petroleum in 2013. And her tutor is Tongjiang YAN. Email:yanyan_fu@163.com