ON THE LINEAR COMPLEXITIES OF TWO CLASSES OF QUATERNARY SEQUENCES OF EVEN LENGTH WITH OPTIMAL AUTOCORRELATION

PINHUI KE* AND YUEQIN JIANG
Fujian Provincial Key Laboratory of Network Security and Cryptology
College of Mathematics and Informatics
Fujian Normal University, Fuzhou, Fujian 350117, China

ZHIXIONG CHEN
School of Mathematics
Putian University
Putian, Fujian 351100, China

(Communicated by Zhengchun Zhou)

Abstract. Let $q$ be a prime greater than 4. In this paper, we determine the coefficients of the discrete Fourier transform over the finite field $\mathbb{F}_q$ of two classes of quaternary sequences of even length with optimal autocorrelation. They are quaternary sequence with period $2p$ derived from binary Legendre sequences and quaternary sequence with period $2p(p + 2)$ derived from twin-prime sequences pair. As applications, the linear complexities over the finite field $\mathbb{F}_q$ of both of the quaternary sequences are determined.

1. Introduction

Due to their constant envelope properties, binary and quaternary sequences can be used as spreading sequences in the code division multiple access (CDMA) communication systems [18, 17]. There are three common ways to define a quaternary sequence. The first one is to use trace function over Galois ring [11, 24, 26]. The second one is to use the inverse Gray mapping along two binary sequences [13, 14, 16]. The third one is to define the support sets of a quaternary sequence directly, see [23, 28, 29] for instance.

Most references concentrated on the correlation of the quaternary sequences. Since the linear complexity corresponds to the difficulty of reproducing the sequence from its samples, it is an important criterion for cryptographic application. By the Berlekamp-Massey algorithm, for a sequence with period $N$, if its linear complexity is larger than $\frac{N}{2}$, then it is considered good with respect to the linear complexity [17]. Since a quaternary sequence can also be regarded as a sequence over a general finite field $\mathbb{F}_q$ with $q > 4$, it is needed for us to consider the linear complexity of a quaternary sequence over a general finite field from the viewpoint of cryptography.

2010 Mathematics Subject Classification: Primary: 58F15, 58F17; Secondary: 53C35.

Key words and phrases: Discrete Fourier transform, Legendre sequence, twin-prime sequences pair, linear complexity, quaternary sequences.

The authors are supported by National Natural Science Foundation of China (No. 61772292, 61772476), Natural Science Foundation of Fujian Province (No. 2015J01237), Fujian Normal University Innovative Research Team (No. IRTL1207).

* Corresponding author: Pinhui Ke.
In [7], Du et al. defined a class of quaternary sequence of length $2p$ over $\mathbb{F}_4$ and showed it possesses high linear complexity. Then, Ke et al. defined a class of quaternary sequence of length $2p^m$ over $\mathbb{F}_4$ and showed it has good linear complexity in [12]. Note that for quaternary sequence over $\mathbb{F}_4$, Su et al. introduce the well-distribution measure and correlation measure of order $k$ in [20] recently. Kim et al. also proposed a quaternary sequences of period $2p$ using the Legendre sequences of period $p$ [13]. A sequence with high linear complexity may have low linear complexity when it is considered as sequence over a larger finite field [15]. Since a quaternary sequence can also be treated as a sequence over a general finite field $\mathbb{F}_q$ with $q > 4$, it is necessary for us to consider the linear complexity of a quaternary sequence over a general finite field from the view point of cryptography.

In this work, we aim to revisit two classes of quaternary sequences in the literature. The first one is defined by Kim et al. via two Legendre sequences in [13], where the autocorrelation and the linear complexity of the sequence were studied. The second one is defined via twin-prime sequences pair of period $p(p + 2)$ using the interleaved technique in [21], where the autocorrelation of the sequence was also studied. We will view these sequences over $\mathbb{F}_q$ and determine the linear complexity. The mail tool we used is the discrete Fourier transform.

This paper is organized as follows. In Section 2, we introduce the quaternary sequences proposed by Kim et al. in [13] and the quaternary sequences proposed by Su et al. in [21]. In Sections 3 and 4, we determine the coefficients of the discrete Fourier transform of above mentioned quaternary sequences over $\mathbb{F}_q$, where $q$ is a prime and $q > 4$. Then, the linear complexities of the corresponding quaternary sequences over $\mathbb{F}_q$ can be easily derived. In the last section, we draw some conclusions.

2. Preliminaries

Let $q^\infty = (q(t))$ be a $d$-ary sequence with period $N$. Then the sequence $q^\infty$ is said to be balanced if the difference among numbers of occurrences of each element in a period is less than or equal to one. And the autocorrelation function of $q^\infty$ at the shift phase $\tau$ is defined as

$$R_{q^\infty}(\tau) = \sum_{t=0}^{N-1} w_d^{q(t) - q(t+\tau)}$$

where $0 \leq \tau < N$ and $w_d$ is a complex primitive $d$-th root of unity.

The maximum out-of-phase autocorrelation magnitude of $q^\infty$ is defined as

$$R_{\text{max}}(q^\infty) = \max\{|R_{q^\infty}(\tau)| : 1 \leq \tau < N\}.$$ 

In many applications of the communication systems, it is desirable for the spreading sequences to have the maximum out-of-phase autocorrelation magnitude as low as possible. For the case of even period, a quaternary sequence $q^\infty$ is called optimal if $R_{\text{max}}(q^\infty) = 2$ [22].

Two $d$-ary sequences $a^\infty = (a(t))$ and $b^\infty = (b(t))$ with the same period $N$ are called equivalent if there exists integers $k$, $l$ and $h$ such that $a(t) = l \cdot b(i + k) + h$, for any $i \geq 0$, where $\gcd(l, d) = 1$ and the operation in the bracket is performed modulo $N$. Denote it by $a \sim b$ for abbreviation. It is obvious that if two periodic sequences $a^\infty$ and $b^\infty$ are equivalent, they have the similar autocorrelation distribution. Otherwise, two periodic sequences are distinct.
Let $a(t)$ and $b(t)$ be two binary sequences of period $N$. Then a quaternary sequence $q^\infty = (q(t))_{t=0}^{N-1}$ could be defined by $q(t) = \phi[a(t), b(t)]$, where $\phi$ is the inverse Gray mapping defined by

$$\phi[a, b] = \begin{cases} 
0, & \text{if } (a, b) = (0, 0); \\
1, & \text{if } (a, b) = (0, 1); \\
2, & \text{if } (a, b) = (1, 1); \\
3, & \text{if } (a, b) = (1, 0).
\end{cases}$$

In what follows, we denote it by $q^\infty = \phi[a^\infty, b^\infty]$ for short.

2.1. The quaternary sequences proposed by Kim et al.

For an odd prime $p$, let $QR_p$ and $NQR_p$ be the sets of quadratic residues and quadratic non-residues in the ring of integers modulo $p$, $\mathbb{Z}_p$, respectively. And let $b_0(t)$ and $b_1(t)$ be the binary sequences defined by

$$b_0(t) = \begin{cases} 
0, & \text{if } t = 0; \\
0, & \text{if } t \in QR_p; \\
1, & \text{if } t \in NQR_p,
\end{cases}$$

and

$$b_1(t) = \begin{cases} 
1, & \text{if } t = 0; \\
0, & \text{if } t \in QR_p; \\
1, & \text{if } t \in NQR_p,
\end{cases}$$

respectively.

By using the inverse Gray mapping, Kim et al. constructed two classes of quaternary sequences $q_1^\infty$ and $q_2^\infty$ as follows [13]. For an odd prime $p$ with $p \equiv 1 \pmod{4}$, let $s_0(t)$ and $s_1(t)$ be two binary sequences of period $2p$ defined by

$$s_0(t) = \begin{cases} 
b_0(t), & \text{if } t \equiv 0 \pmod{2}; \\
b_1(t), & \text{if } t \equiv 1 \pmod{2},
\end{cases}$$

and

$$s_1(t) = \begin{cases} 
b_0(t), & \text{if } t \equiv 0 \pmod{2}; \\
b_1(t) \oplus 1, & \text{if } t \equiv 1 \pmod{2},
\end{cases}$$

where $\oplus$ denotes modulo 2 addition. Then

$$q_1^\infty = \phi[s_0^\infty, s_1^\infty].$$

For an odd prime $p$ with $p \equiv 3 \pmod{4}$, let $s_2(t)$ and $s_3(t)$ be two binary sequences of period $2p$ defined by

$$s_2(t) = \begin{cases} 
b_0(t), & \text{if } t \equiv 0 \pmod{2}; \\
b_0(t), & \text{if } t \equiv 1 \pmod{2},
\end{cases}$$

and

$$s_3(t) = \begin{cases} 
b_1(t), & \text{if } t \equiv 0 \pmod{2}; \\
b_1(t) \oplus 1, & \text{if } t \equiv 1 \pmod{2},
\end{cases}$$

Then

$$q_2^\infty = \phi[s_2^\infty, s_3^\infty].$$
In [13], Kim et al. proved that the quaternary sequences $q^\infty_1$ and $q^\infty_2$ are both balanced and the autocorrelation values of the proposed quaternary sequences are optimal.

2.2. INTERLEAVED SEQUENCE. Let $N$ and $P$ be two positive integers. Assume that $a^{(i)} = (a^{(i)}_0, a^{(i)}_1, \ldots, a^{(i)}_{N-1})$ is a sequence of period $N$, $0 \leq i \leq P-1$, and $e = (e_0, e_1, \ldots, e_{P-1})$ is a sequence defined over $\mathbb{Z}_N$. Define an $N \times P$ matrix $U = (u_{i,j})$ as follows

\[
\begin{pmatrix}
  a^{(0)}_0 & a^{(1)}_0 & \cdots & a^{(P-1)}_0 \\
  a^{(0)}_1 & a^{(1)}_1 & \cdots & a^{(P-1)}_1 \\
  \vdots & \vdots & \ddots & \vdots \\
  a^{(0)}_{N-1} & a^{(1)}_{N-1} & \cdots & a^{(P-1)}_{N-1}
\end{pmatrix}
\]

An interleaved sequence $u^\infty$ of period $NP$ is then obtained by concatenating the successive rows of the matrix above. That is,

\[u_{iP+j} = u_{i,j}, 0 \leq i < N, 0 \leq j < P.\]

For convenience, denote it as

\[u^\infty = I(L^0(u^0(a^{(0)}_0)), L^1(u^1(a^{(1)}_0)), \ldots, L^{P-1}(u^{P-1}(a^{(P-1)}_0))),\]

where $I$ is the interleaving operator. The sequence $e$ is called the shift sequence and the sequences $a^{(i)}$, $0 \leq i \leq p-1$ are called column sequences [9].

2.3. THE QUATERNARY SEQUENCES PROPOSED BY SU ET AL. In [21], a generic construction of quaternary sequence with optimal autocorrelation was given by Su et al. The construction consists of following three steps.

(i) Let $n$ be an odd integer, $N = 2n$, and $\lambda = \frac{n+1}{2}$. Generate four sequences $a_i^\infty$ of length $n$, $0 \leq i \leq 3$, and a binary sequence $e^\infty = (e_1, e_2, e_3)$, where $e_i \in \{0, 1\}$, and $e_1 + e_2 + e_3 \equiv 1 \pmod{2}$.

(ii) Define two binary sequences of length $N$,

\[c^\infty = I(a_0^\infty, e_1 + L^\lambda(a_1^\infty)), d^\infty = I(e_2 + a_2^\infty, e_3 + L^\lambda(a_3^\infty)).\]

(iii) Applying inverse Gray mapping to $c^\infty$ and $d^\infty$, we obtain a quaternary sequence $u^\infty$ of length $N$

\[u(t) = \phi[c(t), d(t)].\]

It is proved in [21] that twin-prime sequences pairs, GMW sequences pairs and two, three or four binary sequences defined by cyclotomic classes of order 4 can be chosen as the component sequences $a^\infty_i$ in above generic construction.

2.4. THE LINEAR COMPLEXITY. Let $q^\infty = (q(t))$ be a sequence of period $N$ over $\mathbb{F}_q$. The linear complexity of $q^\infty$ is defined to be the smallest positive integer $l$ such that there are constants $c_0 \neq 0, c_1, \ldots, c_l \in \mathbb{F}_q$ satisfying

\[-c_0q(t) = c_1q(t-1) + \cdots + c_lq(t-l)\]

for all $t \geq l$.

The polynomial $c(x) = c_0 + c_1x + \cdots + c_lx^l$ is called a characteristic polynomial of $q(t)$. A characteristic polynomial with the smallest degree is called a minimal polynomial of the periodic sequence $q(t)$. The degree of a minimal polynomial of $q(t)$ is referred to as the linear complexity of this sequence.

Suppose that $\gcd(N, q) = 1$, let $m$ be the order of $q$ modulo $N$, that is, $m$ is the least positive integer such that $q^m \equiv 1 \pmod{N}$. By Blahut’s Theorem [19], the linear complexity of a periodic sequence can be determined by counting the
number of nonzero coefficients of its discrete Fourier transform. For an \( N \)-periodic quaternary sequence \( q(t) \), then the discrete Fourier transform of \( q(t) \) is defined as

\[
A_i = \frac{1}{N} \sum_{t=0}^{N-1} q(t) \alpha^{-it},
\]

where \( 0 \leq i < N \) and \( \alpha \) is a primitive \( N \)-th root of unity in \( \mathbb{F}_{q^m} \). Hence, if we count the number \( L_0 \) of indices \( i \)'s satisfying \( A_i = 0 \), the linear complexity of \( q(t) \) becomes \( N - L_0 \).

### 3. Linear Complexity of Quaternary Sequence from Legendre Sequence

In [13], Kim et al. determined the linear complexity of the quaternary sequences in (1) and (3)(Section 4, Theorem 17 and Theorem 18 in [13]). To this end, they represented the sequences in (1) and (3) by redefining the intermediate sequence \( s_1(t) \) as follows:

\[
s_1(t) = \frac{1}{2}([1 - \Xi(t) - I(t) - I(t - p)]),
\]

where

\[
\Xi(t) = \begin{cases} 
\eta(t), & 0 \leq t < p; \\
-\eta(t), & p \leq t < 2p,
\end{cases}
\]

and

\[
I(t) = \begin{cases} 
1, & t = 0; \\
0, & t \neq 0.
\end{cases}
\]

In order to avoid confusion, let us denote above mentioned intermediate sequence \( s_1(t) \) as \( s'_1(t) \). Kim et al. believed that the sequences \( s_1(t) \) and \( s'_1(t) \) are the same sequence in different form. However, they are different, which can be confirmed by the following counter example. Let \( p = 17 \), two binary sequences \( b_0(t), b_1(t) \) are given as

\[
b_0(t) = 00010111001110100; \\
b_1(t) = 10010111001110100.
\]

Then, \( s_1(t) \) and \( s'_1(t) \) are obtained as follows

\[
s_1(t) = 0100001001101110011110111001100001; \\
s'_1(t) = 00010111001110100011000110001011.
\]

Computing their autocorrelation functions, we have \( R_{s_1}(\tau) \in \{34, -2, 2, -30\} \). However, \( R_{s'_1}(\tau) \in \{34, -2, -6, -10, -22, -30, 2, 6, 10, 22\} \). Thus, \( s_1(t) \) and \( s'_1(t) \) are not equivalent.

In this section, we will determine the linear complexity of the quaternary sequences (2) and (4) over \( \mathbb{F}_q \) \( (q > 4) \). Before doing this, let us introduce some useful auxiliary lemmas.

**Lemma 3.1.** [25, 5] We have the following basic facts:

1) \( u \mathbb{Q} \mathbb{R}_p = \mathbb{Q} \mathbb{R}_p \) for any quadratic residue \( u \) in \( \mathbb{Z}_p \);

2) \( u \mathbb{N} \mathbb{R}_p = \mathbb{N} \mathbb{R}_p \) for any quadratic non-residue \( u \) in \( \mathbb{Z}_p \).
Let \( q \) be a prime number with \((p, q) = 1\) and \( m \) be the order of \( q \) modulo \( p \). Assume that \( \delta \) is a primitive \( p \)-th root of unity in \( F_q \), denote

\[
\eta_0 = \sum_{t \in \mathbb{Q}_p^\times} \delta^t, \quad \eta_1 = \sum_{t \in \mathbb{Q}_p^\times} \delta^t.
\]

It is obvious that \( \eta_0 + \eta_1 = -1 \).

**Lemma 3.2.** [6, 27] Let the notations be the same as before, then we have

\[
\eta_0 = \begin{cases} 
-1 & \text{if } p \equiv 1 \pmod{4}; \\
- \frac{1 - \sqrt{p}}{2} & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]

For a quaternary sequence \( q^\infty = \phi[a^\infty, b^\infty] \), it can be easily verified that

\[
q(t) = \phi[a(t), b(t)] = 3a(t) + b(t) - 2a(t)b(t).
\]

Note that this representation holds only for \( q \geq 5 \). Then we can compute the discrete Fourier coefficients of the quaternary sequence \( q_1(t) \) as follows.

**Theorem 3.3.** Let \( p \) and \( q \) be two different primes with \( q > 4 \). If \( p \equiv 1 \pmod{4} \), the discrete Fourier transform coefficients over \( F_q \) of the quaternary sequence \( q_1(t) \) defined in (2) are given as

\[
A_{-i} = \frac{1}{2p} \cdot \begin{cases} 
2p, & \text{if } i = 0; \\
-2, & \text{if } i \in \mathbb{Z}_{2p}\setminus\{0\}, \text{ } i \text{ is odd}; \\
2\sqrt{p}, & \text{if } i \in \mathbb{Z}_{2p}\setminus\{0\}, \text{ } i \text{ is even and } 2i \in \mathbb{Q}_p^\times; \\
-2\sqrt{p}, & \text{if } i \in \mathbb{Z}_{2p}\setminus\{0\}, \text{ } i \text{ is even and } 2i \not\in \mathbb{Q}_p^\times.
\end{cases}
\]

**Proof.** By definition, we have \( q_1(t) = \phi[s_0(t), s_1(t)] \). So the coefficient of the discrete Fourier transform of \( q_1(t) \) at \(-i\) can be calculated by

\[
(6) \quad A_{-i} = \frac{1}{2p} \cdot (3 \sum_{t=0}^{2p-1} s_0(t)\alpha^{it} + \sum_{t=0}^{2p-1} s_1(t)\alpha^{it} - 2 \sum_{t=0}^{2p-1} s_0(t)s_1(t)\alpha^{it}),
\]

where \( \alpha \) is a \( 2p \)-th root of unity in \( F_q \). Denote \( \beta = \alpha^2 \), then \( \beta \) is a \( p \)-th root of unity in \( F_q \). By Chinese Remainder Theorem, \( \mathbb{Z}_{2p} \) is isomorphism to \( \mathbb{Z}_2 \times \mathbb{Z}_p \). Thus, for any \( t \in \mathbb{Z}_{2p} \), we could represent it as \( pt_1 + 22_p^{-1}t_2 \), where \( t_1 = t \pmod{2} \), \( t_2 = t \pmod{p} \) and \( 2p^{-1} \) denotes the inverse element of 2 modulo \( p \). Now let us turn to the calculation of (6). Firstly, the first summation in (6) can be rewritten as

\[
\sum_{t=0}^{2p-1} s_0(t)\alpha^{it} = \sum_{t_1=0}^{p-1} \sum_{t_2=0}^{p-1} s_0(pt_1 + 22_p^{-1}t_2)\alpha^{i(pt_1 + 22_p^{-1}t_2)}
\]

\[
= \sum_{t_2=0}^{p-1} s_0(22_p^{-1}t_2)\alpha^{i22_p^{-1}t_2} + \sum_{t_2=0}^{p-1} s_0(p + 22_p^{-1}t_2)\alpha^{i(p + 22_p^{-1}t_2)}.
\]

Then, by the definition of the sequence \( s_0^\infty \), we have

\[
\sum_{t=0}^{2p-1} s_0(t)\alpha^{it} = \sum_{t_2=0}^{p-1} b_0(22_p^{-1}t_2)\alpha^{i22_p^{-1}t_2} + \sum_{t_2=0}^{p-1} b_1(p + 22_p^{-1}t_2)\alpha^{i(p + 22_p^{-1}t_2)}
\]

\[
= \sum_{t_2=0}^{p-1} b_0(22_p^{-1}t_2)\alpha^{i22_p^{-1}t_2} + (-1)^p \sum_{t_2=0}^{p-1} b_1(22_p^{-1}t_2)\alpha^{i22_p^{-1}t_2}
\]

**Advances in Mathematics of Communications** Volume 12, No. 3 (2018), 525–539
where \( t'_2 = 2_p^{-1} t_2 \). If \( 2i \in \mathbb{QR}_p \), by the definitions of \( b_0^\infty \) and \( b_1^\infty \), we have

\[
\sum_{t=0}^{2p-1} s_0(t)\alpha^{it} = \sum_{t'_2 \in \mathbb{NQR}_p} \beta^{it'_2} + (-1)^i (1 + \sum_{t'_2 \in \mathbb{QR}_p} \beta^{it'_2}).
\]

Secondly, the second summation in (6) can be calculated as

\[
\sum_{t=0}^{2p-1} s_1(t)\alpha^{it} = \sum_{t_1=0}^{p-1} s_1(pt_1 + 22_p^{-1} t_2)\alpha^{i(pt_1 + 22_p^{-1} t_2)}
\]

\[
= \sum_{t_2=0}^{p-1} s_1(22_p^{-1} t_2)\alpha^{i22_p^{-1} t_2} + \sum_{t_2=0}^{p-1} s_1(p + 22_p^{-1} t_2)\alpha^{i(p+22_p^{-1} t_2)}
\]

\[
= \sum_{t_2=0}^{p-1} b_0(22_p^{-1} t_2)\alpha^{i22_p^{-1} t_2} + (-1)^i \sum_{t_2=0}^{p-1} (b_1(22_p^{-1} t_2) \oplus 1)\alpha^{i22_p^{-1} t_2}
\]

\[
= \sum_{t'_2=0}^{p-1} b_0(2t'_2)\alpha^{it'_2} + (-1)^i \sum_{t'_2=0}^{p-1} (b_1(2t'_2) \oplus 1)\alpha^{it'_2},
\]

where \( t'_2 = 2_p^{-1} t_2 \). By Lemma 2, we have

\[
\sum_{t=0}^{2p-1} s_1(t)\alpha^{it} = \sum_{t'_2 \in \mathbb{QR}_p} \beta^{it'_2} + (-1)^i \sum_{t'_2 \in \mathbb{QR}_p} \beta^{it'_2}.
\]

Finally, the last summation in (6) can be calculated as

\[
\sum_{t=0}^{2p-1} s_0(t)s_1(t)\alpha^{it} = \sum_{t_1=0}^{p-1} \sum_{t_2=0}^{p-1} s_0(pt_1 + 22_p^{-1} t_2)s_1(pt_1 + 22_p^{-1} t_2)\alpha^{i(pt_1 + 22_p^{-1} t_2)}
\]

\[
= \sum_{t_2=0}^{p-1} s_0(22_p^{-1} t_2)s_1(22_p^{-1} t_2)\alpha^{i22_p^{-1} t_2}
\]

\[
+ \sum_{t_2=0}^{p-1} s_0(p + 22_p^{-1} t_2)s_1(p + 22_p^{-1} t_2)\alpha^{i(p+22_p^{-1} t_2)}
\]

\[
= \sum_{t'_2=0}^{p-1} b_0(2t'_2)\alpha^{it'_2} + (-1)^i \sum_{t'_2=0}^{p-1} (b_1(2t'_2)(b_1(2t'_2) + 1))\alpha^{it'_2}
\]

\[
= \sum_{t'_2 \in \mathbb{NQR}_p} \beta^{it'_2},
\]

where \( t'_2 = 2_p^{-1} t_2 \). In conclusion, we have

\[
A_{-1} = \frac{1}{2p} \cdot (2 \sum_{t'_2 \in \mathbb{QR}_p} \beta^{it'_2} + 2(-1)^i \sum_{t'_2 \in \mathbb{QR}_p} \beta^{it'_2} + 2(-1)^i).
\]
Note that if \( i = 0 \), we have

\[
\sum_{t' \in \text{NQR}_p} 1 = \frac{p-1}{2}.
\]

So, \( A_0 = 1 \). For any odd \( i \in \mathbb{Z}_{2p} \setminus \{0\} \), we have \( A_{-i} = \frac{1}{2p} \cdot (-2) = -\frac{1}{p} \). For any even \( i \in \mathbb{Z}_{2p} \setminus \{0\} \), we have

\[
A_{-i} = \frac{1}{2p} \cdot (4 \sum_{t' \in \text{NQR}_p} \beta^{it'} + 2).
\]

By Lemma 4, we have \( A_{-i} = \frac{1}{2p} \cdot (2\sqrt{p}) \), if \( i \in \mathbb{Q}_p \), otherwise \( A_{-i} = \frac{1}{2p} \cdot (-2\sqrt{p}) \). Thus we complete the proof. \( \square \)

**Remark 1.** It is well known that 2 \( \in \mathbb{Q}_p \) if and only if \( p \equiv \pm 1 \pmod{8} \). Thus, if \( p \equiv 1 \pmod{4} \), we have \( 2i \in \mathbb{Q}_p \) if and only if \( i \in \text{QR}_p \) and \( p \equiv 1 \pmod{8} \) or \( i \in \text{NQR}_p \) and \( p \equiv 5 \pmod{8} \). And if \( p \equiv 1 \pmod{4} \), we similarly have \( 2i \in \text{NQR}_p \) if and only if \( i \in \text{QR}_p \) and \( p \equiv 1 \pmod{8} \) or \( i \in \mathbb{Q}_p \) and \( p \equiv 5 \pmod{8} \).

**Corollary 1.** Let \( p \) and \( q \) be two different primes with \( q > 4 \). For \( p \equiv 1 \pmod{4} \), the linear complexity over \( \mathbb{F}_q \) of the quaternary sequence \( q(t) \) is \( 2p \).

Similar to Theorem 3.3, we compute the discrete Fourier coefficients of the quaternary sequence \( q_2(t) \) as follows.

**Theorem 3.4.** Let \( p \) and \( q \) be two different primes with \( q > 4 \). If \( p \equiv 3 \pmod{4} \), the discrete Fourier transform coefficients of the quaternary sequence \( q_2(t) \) defined in (4) are given as

\[
A_{-i} = \frac{1}{2p} \cdot \begin{cases} 
2p-2, & \text{if } i = 0; \\
2, & \text{if } i \in \mathbb{Z}_{2p} \setminus \{0\}, \text{ } i \text{ is odd}; \\
2\sqrt{-p} - 2, & \text{if } i \in \mathbb{Z}_{2p} \setminus \{0\}, \text{ } i \text{ is even and } 2i \in \mathbb{Q}_p; \\
-2\sqrt{-p} - 2, & \text{if } i \in \mathbb{Z}_{2p} \setminus \{0\}, \text{ } i \text{ is even and } 2i \in \text{NQR}_p.
\end{cases}
\]

**Proof.** Since the proof is similar to that of Theorem 3.3, we omit it. \( \square \)

**Corollary 2.** Let \( p \) and \( q \) be two different primes with \( q > 4 \). If \( p \equiv 3 \pmod{4} \), the linear complexity over \( \mathbb{F}_q \) of the quaternary sequence \( q_2(t) \) is \( 2p \).

4. Linear complexity of quaternary sequence from twin-prime sequence pair

As we have mentioned in Section 2.3, the construction proposed by Su et al. in [21] is generic since different sequences including twin-prime sequences pairs, GMW sequences pairs and two, three or four binary sequences defined by cyclotomic classes of order 4 can be chosen as the component sequences. In this section, we will focus on the case of using twin-prime sequences pairs as the component sequences and investigate the linear complexity of the corresponding quaternary sequence.

Let us begin with the definition of the twin-prime sequences pairs. Let \( p \) and \( p+2 \) be two primes. For \( i = 1, 2, \cdots, p+1 \), define \( e_i = (p+2)^{-1}i \pmod{p} \), \( b_i=1 \) if \( i \in \mathbb{Q}_p \) or \( b_i=0 \) if \( i \in \text{NQR}_p \). Furthermore, for \( i = 1, 2, \cdots, p+1 \), define a set of sequences \( a_i^{\infty} \) with period \( p \) as follows

\[
a_i^{\infty} = \begin{cases} 
l', & \text{if } i \in \mathbb{Q}_p; \\
l, & \text{if } i \in \text{NQR}_p.
\end{cases}
\]
where \( l'\) and \( l\) are the sequences defined by

\[
l'(t) = \begin{cases} 
0, & \text{if } t \equiv 0 \pmod{p}; \\
1, & \text{if } t \in \mathbb{QR}_p; \\
0, & \text{if } t \in \mathbb{NQR}_p,
\end{cases}
\]

and

\[
l(t) = \begin{cases} 
1, & \text{if } t \equiv 0 \pmod{p}; \\
1, & \text{if } t \in \mathbb{QR}_p; \\
0, & \text{if } t \in \mathbb{NQR}_p,
\end{cases}
\]

respectively. Then the sequence \( a^\infty \) and its modified sequence \( b^\infty \), called the twin-prime sequences pair are given by

\[
a^\infty = I(0_p^\infty, L^{e_1}(a_1^\infty) + b_1, \cdots, L^{e_{p+1}}(a_{p+1}^\infty) + b_{p+1})
\]

and

\[
b^\infty = I(1_p^\infty, L^{e_1}(a_1^\infty) + b_1, \cdots, L^{e_{p+1}}(a_{p+1}^\infty) + b_{p+1}),
\]

where \( 0_p^\infty \) and \( 1_p^\infty \) denote the all-zeros and all-ones sequences of length \( p \), respectively. In [21], Su et al. showed that the quaternary sequence \( u^\infty \) defined in (5) possesses optimal autocorrelation if \((a_0^\infty, a_1^\infty, a_2^\infty, a_3^\infty)\) belongs to one of the following cases \((a^\infty, b^\infty, a^\infty, b^\infty), (a^\infty, b^\infty, b^\infty, a^\infty), (b^\infty, a^\infty, a^\infty, b^\infty), \) or \((b^\infty, a^\infty, a^\infty, b^\infty)\).

In this paper, let us assume that \((a_0^\infty, a_1^\infty, a_2^\infty, a_3^\infty) = (a^\infty, b^\infty, a^\infty, b^\infty)\) and \((e_1, e_2, e_2) = (0, 0, 1)\). The remainder cases can be calculated similarly. Denote \( n = p(p+2) \) and \( N = 2n \) and let \( q \) be a prime with \( \gcd(N, q) = 1 \). Define \( m \) to be the order of \( q \) modulo \( N \), then there exists a primitive \( N \)-th root \( \alpha \) of unity in \( \mathbb{F}_q^\infty \). Let \( \beta = \alpha^2 \), then \( \beta \) is an \( n \)-th root of unity.

In [2], it has been demonstrated that twin-prime (TP, for short) sequence is just a special case of modified Jacobi sequence or related-prime(RP, for short) sequence where the difference of the primes is 2. In [10], Green et al. presented the distribution of roots of the generating polynomial of polyphase RP sequence over \( \mathbb{F}_2 \). For our purpose, we need to investigate the distributions of roots of the generating polynomial of TP sequence \( a^\infty \) and its modification sequence \( b^\infty \) over \( \mathbb{F}_q \), instead of \( \mathbb{F}_2 \).

Using the notations in [10], let us define \( H = \{ i | 0 < i < n \text{ and } i \equiv 0 \pmod{p} \} \), \( V = \{ i | 0 < i < n \text{ and } i \equiv 0 \pmod{p+2} \} \), \( P_0 = \{ i | i \in \mathbb{Z}_n^* \text{ and } (\frac{i}{p}) \cdot (\frac{i}{p+2}) = -1 \} \) and \( P_1 = \{ i | i \in \mathbb{Z}_n^* \text{ and } (\frac{i}{p}) \cdot (\frac{i}{p+2}) = 1 \} \), where \((\cdot)\) denotes the Legendre symbol. It is obvious that \( \mathbb{Z}_n = \{ 0 \} \cup H \cup V \cup P_0 \cup P_1 \). Let \( h \in H, c \in V, p_i \in P_i \). Clearly, \( h \cdot H = H, v \cdot V = V \), and \( p_0 \cdot P_0 = P_0 \). Furthermore, \( h \cdot V = v \cdot H = 0, p_i \cdot P_i = P_{i+j} \). Also, \( h \cdot P_1 = H \) reproduced \( p-1 \) times and \( v \cdot P_1 = V \) reproduced \( p+1 \) times. By definition, the generating polynomials of \( a^\infty \) and \( b^\infty \) are

\[
S_{a^\infty}(x) = 0 + 0 \cdot \sum_{t \in V} x^t + \sum_{t \in H} x^t + 0 \cdot \sum_{t \in P_0} x^t + 1 \cdot \sum_{t \in P_1} x^t
\]

and

\[
S_{b^\infty}(x) = 1 + 1 \cdot \sum_{t \in V} x^t + \sum_{t \in H} x^t + 0 \cdot \sum_{t \in P_0} x^t + 1 \cdot \sum_{t \in P_1} x^t,
\]

respectively.
Lemma 4.1. Let $\beta$ be an $n$-th root of unity in $\mathbb{F}_q$. For the generating polynomials of the sequences $a^\infty$ and $b^\infty$, we have

\begin{align}
S_{a^\infty}(\beta^t) &= \begin{cases}
\frac{(p+1)^2}{2}, & \text{if } t = 0; \\
\frac{p+1}{2}, & \text{if } t \in H; \\
\frac{p+1}{2}, & \text{if } t \in V; \\
\sigma_1 - 1, & \text{if } t \in P_0; \\
\sigma_0 - 1, & \text{if } t \in P_1.
\end{cases}
\end{align}

and

\begin{align}
S_{b^\infty}(\beta^t) &= \begin{cases}
\frac{(p+1)^2}{2} + p, & \text{if } t = 0; \\
\frac{p-1}{2}, & \text{if } t \in H; \\
\frac{p+1}{2}, & \text{if } t \in V; \\
\sigma_1 - 1, & \text{if } t \in P_0; \\
\sigma_0 - 1, & \text{if } t \in P_1.
\end{cases}
\end{align}

where $\sigma_i = \sum_{t \in P_i} \beta^t$ for $i = 0, 1$.

Proof. Since the proofs are similar, we only prove (10). According to (8), we have

\[ S_{b^\infty}(\beta^0) = S_{b^\infty}(1) = 1 + (p-1) + (p+1) + \frac{(p-1)(p+1)}{2} = \frac{(p+1)^2}{2} + p. \]

If $h \in H$,

\[ S_{b^\infty}(\beta^h) = 1 + \sum_{t \in V} \beta^{ht} + \sum_{t \in H} \beta^{ht} + 0 \cdot \sum_{t \in P_0} \beta^{ht} + 1 \cdot \sum_{t \in P_1} \beta^{ht} \]

\[ = 1 + (p-1) + \sum_{t \in H} \beta^t + \frac{p-1}{2} \sum_{t \in H} \beta^t = \frac{p-1}{2}, \]

where the last equation holds by the fact that $\sum_{t \in H} \beta^t = -1$, which can be easily seen from

\[ (\beta^p - 1) \sum_{t \in H} \beta^t = (\beta^p - 1)(\beta^p + \beta^{2p} + \cdots + \beta^{(p+1)p}) = 1 - \beta^p. \]

Similarly, we can prove that $\sum_{t \in V} \beta^t = -1$. Now, for any $v \in V$, we have

\[ S_{b^\infty}(\beta^v) = 1 + \sum_{t \in V} \beta^{vt} + \sum_{t \in H} \beta^{vt} + 0 \cdot \sum_{t \in P_0} \beta^{vt} + \sum_{t \in P_1} \beta^{vt} \]

\[ = 1 + \sum_{t \in V} \beta^t + (p+1) + \frac{p+1}{2} \sum_{t \in H} \beta^t = \frac{p+1}{2}. \]

If $p_0 \in P_0$,

\[ S_{b^\infty}(\beta^{p_0}) = 1 + \sum_{t \in V} \beta^{p_0 t} + \sum_{t \in H} \beta^{p_0 t} + 0 \cdot \sum_{t \in P_0} \beta^{p_0 t} + \sum_{t \in P_1} \beta^{p_0 t} \]

\[ = 1 + \sum_{t \in V} \beta^t + \sum_{t \in H} \beta^t + \sum_{t \in P_1} \beta^t = \sigma_1 - 1. \]

Similarly, if $p_1 \in P_1$, we have

\[ S_{b^\infty}(\beta^{p_1}) = 1 + \sum_{t \in V} \beta^{p_1 t} + \sum_{t \in H} \beta^{p_1 t} + 0 \cdot \sum_{t \in P_0} \beta^{p_1 t} + \sum_{t \in P_1} \beta^{p_1 t} \]
The first summation in (11) can be rewritten as
\[
= 1 + \sum_{t_1 \in V} \beta^t + \sum_{t \in H} \beta^t + \sum_{t \in P_0} \beta^t = \sigma_0 - 1.
\]
Thus we complete the proof. \( \square \)

**Theorem 4.2.** Let notations be the same as before. The discrete Fourier transform coefficients of the quaternary sequence \( u(t) \) defined in (5) are given as
\[
NA_{-i} = \begin{cases} 
2(p + 1)^2 + 2p, & \text{if } i = 0; \\
-2p, & \text{if } i = n; \\
(p + 1)(1 + (-1)^i \beta^{-i2n^{-1}}), & \text{if } i \in \mathbb{Z}_{2n} \setminus \{0, n\}, i \equiv 0 \pmod{p + 2}; \\
-(p + 1)^i (p - 1) \beta^{-i2n^{-1}}, & \text{if } i \in \mathbb{Z}_{2n} \setminus \{0, n\}, i \equiv 0 \pmod{p}; \\
2(\alpha_1 - 1)(1 + (-1)^i \beta^{-i2n^{-1}}), & \text{if } i \in \mathbb{Z}_{2n} \setminus \{0, n\}, i \text{ mod } n \in P_0; \\
2(\alpha_0 - 1)(1 + (-1)^i \beta^{-i2n^{-1}}), & \text{if } i \in \mathbb{Z}_{2n} \setminus \{0, n\}, i \text{ mod } n \in P_1,
\end{cases}
\]
where \( n = 2p(p + 2) \) and \( N = 2n \) is the length of the quaternary sequence \( u^\infty \).

**Proof.** The discrete Fourier transform of quaternary sequence \( u(t) \) can be calculated as
\[
(11) \quad NA_{-i} = 3 \sum_{t=0}^{2n-1} c(t)\alpha^{it} + \sum_{t=0}^{2n-1} d(t)\alpha^{it} - 2 \sum_{t=0}^{2n-1} c(t)d(t)\alpha^{it}.
\]

By Chinese Remainder Theorem, \( \mathbb{Z}_{2n} \) is isomorphism to \( \mathbb{Z}_n \times \mathbb{Z}_2 \). Thus, for any \( t \in \mathbb{Z}_{2n} \), we could represent it as \( 22_n^{-1}t_1 + nt_2 \), where \( t_1 = t \pmod{n} \) and \( t_2 = t \pmod{2} \). According to the definitions of \( c(t) \) and \( d(t) \), we have
\[
c(t) = \begin{cases} 
c(22_n^{-1}t_1) = a(2^{-1}t_1), & \text{if } t_2 = 0; \\
c(22_n^{-1}t_1 + n) = b(2^{-1} + 2_n^{-1}t_1), & \text{if } t_2 = 1,
\end{cases}
\]
and
\[
d(t) = \begin{cases} 
c(22_n^{-1}t_1) = a(2^{-1}t_1), & \text{if } t_2 = 0; \\
c(22_n^{-1}t_1 + n) = b(2^{-1} + 2_n^{-1}t_1) \oplus 1, & \text{if } t_2 = 1.
\end{cases}
\]

The calculation of \( NA_{-i} \) in (11) can be divided into following three parts. Firstly, the first summation in (11) can be rewritten as
\[
\sum_{t=0}^{2n-1} c(t)\alpha^{it} = \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{1} c(22_n^{-1}t_1 + nt_2)\alpha^{i22_n^{-1}t_1 + nt_2}
\]
\[
= \sum_{t_1=0}^{n-1} c(22_n^{-1}t_1)\alpha^{22_n^{-1}t_1} + (-1)^t \sum_{t_1=0}^{n-1} c(22_n^{-1}t_1 + n)\alpha^{i22_n^{-1}t_1}
\]
\[
= \sum_{t_1=0}^{n-1} a(2^{-1}t_1)\alpha^{22_n^{-1}t_1} + (-1)^t \sum_{t_1=0}^{n-1} b\left(2^{-1} + 2_n^{-1}t_1\right)\alpha^{i22_n^{-1}t_1}
\]
\[
= \sum_{t_1=0}^{n-1} a(2^{-1}t_1)\alpha^{22_n^{-1}t_1} + (-1)^t \sum_{t_1=0}^{n-1} b(2_n^{-1}(t_1 + n - 1))\alpha^{i22_n^{-1}t_1}
\]
\[
= \sum_{t_1=0}^{n-1} a(2^{-1}t_1)\alpha^{22_n^{-1}t_1} + (-1)^t \sum_{t_1=0}^{n-1} b(2_n^{-1}t_1)\alpha^{i22_n^{-1}(t_1-n+1)}
\]
\[
= \sum_{t_1=0}^{n-1} a(2^{-1}t_1)\alpha^{22_n^{-1}t_1} + (-1)^t \sum_{t_1=0}^{n-1} b(2_n^{-1}t_1)\alpha^{i22_n^{-1}t_1}
\]

The calculation of \( NA_{-i} \) in (11) can be divided into following three parts. Firstly, the first summation in (11) can be rewritten as
\[
\sum_{t=0}^{2n-1} c(t)\alpha^{it} = \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{1} c(22_n^{-1}t_1 + nt_2)\alpha^{i22_n^{-1}t_1 + nt_2}
\]
\[
= \sum_{t_1=0}^{n-1} c(22_n^{-1}t_1)\alpha^{22_n^{-1}t_1} + (-1)^t \sum_{t_1=0}^{n-1} c(22_n^{-1}t_1 + n)\alpha^{i22_n^{-1}t_1}
\]
\[
= \sum_{t_1=0}^{n-1} a(2^{-1}t_1)\alpha^{22_n^{-1}t_1} + (-1)^t \sum_{t_1=0}^{n-1} b\left(2^{-1} + 2_n^{-1}t_1\right)\alpha^{i22_n^{-1}t_1}
\]
\[
= \sum_{t_1=0}^{n-1} a(2^{-1}t_1)\alpha^{22_n^{-1}t_1} + (-1)^t \sum_{t_1=0}^{n-1} b(2_n^{-1}(t_1 + n - 1))\alpha^{i22_n^{-1}t_1}
\]
\[
= \sum_{t_1=0}^{n-1} a(2^{-1}t_1)\alpha^{22_n^{-1}t_1} + (-1)^t \sum_{t_1=0}^{n-1} b(2_n^{-1}t_1)\alpha^{i22_n^{-1}(t_1-n+1)}
\]
\[
= \sum_{t_1=0}^{n-1} a(2^{-1}t_1)\alpha^{22_n^{-1}t_1} + (-1)^t \sum_{t_1=0}^{n-1} b(2_n^{-1}t_1)\alpha^{i22_n^{-1}t_1}
\]
Secondly, the second summation in (11) can be rewritten as
\[
\sum_{t=0}^{2n-1} c(t)d(t)\alpha^t = \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{1} c(2^{2n-1}t_1 + nt_2)d(2^{2n-1}t_1 + nt_2)(\alpha^{t_1}t_1 + \alpha^{t_2}t_2)
\]
\[
= \sum_{t_1=0}^{n-1} c(2^{2n-1}t_1)d(2^{2n-1}t_1)\alpha^{t_1}t_1 + \sum_{t_1=0}^{n-1} c(2^{2n-1}t_1 + nt_2)d(2^{2n-1}t_1 + nt_2)(\alpha^{t_1}t_1 + \alpha^{t_2}t_2)
\]
\[
= \sum_{t_1=0}^{n-1} a(2^{2n-1}t_1)\alpha^{t_1}t_1 + \sum_{t_1=0}^{n-1} b(\frac{n-1}{2} + 2^{n-1}t_1)(\alpha^{t_1}t_1 + \alpha^{t_2}t_2)
\]
\[
= \sum_{t_1=0}^{n-1} a(2^{2n-1}t_1)\alpha^{t_1}t_1.
\]

Finally, the last summation in (11) can be rewritten as
\[
\sum_{t=0}^{2n-1} c(t)d(t)\alpha^t = \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{1} c(2^{2n-1}t_1 + nt_2)d(2^{2n-1}t_1 + nt_2)(\alpha^{t_1}t_1 + \alpha^{t_2}t_2)
\]
\[
= \sum_{t_1=0}^{n-1} c(2^{2n-1}t_1)d(2^{2n-1}t_1)\alpha^{t_1}t_1 + \sum_{t_1=0}^{n-1} c(2^{2n-1}t_1 + nt_2)d(2^{2n-1}t_1 + nt_2)(\alpha^{t_1}t_1 + \alpha^{t_2}t_2)
\]
\[
= \sum_{t_1=0}^{n-1} a(2^{2n-1}t_1)\alpha^{t_1}t_1 + \sum_{t_1=0}^{n-1} b(\frac{n-1}{2} + 2^{n-1}t_1)(\alpha^{t_1}t_1 + \alpha^{t_2}t_2)
\]
\[
= \sum_{t_1=0}^{n-1} a(2^{2n-1}t_1)\alpha^{t_1}t_1.
\]

Putting everything together, we have
\[
NA_i = 2 \sum_{t_1=0}^{n-1} a(2^{2n-1}t_1)\alpha^{t_1}t_1 + 2(-1)^i\alpha^{-i2^{2n-1}} \sum_{t_1=0}^{n-1} b(2^{n-1}t_1)\alpha^{t_1}t_1
\]
\[
= 2 \sum_{t_1=0}^{n-1} a(t_1)\alpha^{2t_1} + 2(-1)^i\alpha^{-i2^{2n-1}} \sum_{t_1=0}^{n-1} b(t_1)\alpha^{2t_1}.
\]

According to our notation, \(\beta = \alpha^2\) is a primitive \(n\)-th root of unity in \(F_{q^n}\). By Lemma (4.1), we have

(i) If \(i = 0\), then
\[
NA_0 = 2 \cdot \frac{(p + 1)^2}{2} + 2 \cdot (\frac{(p + 1)^2}{2} + p) = 2(p + 1)^2 + 2p.
\]

(ii) If \(i = n\), then
\[
NA_n = 2 \cdot \frac{(p + 1)^2}{2} - 2 \cdot (\frac{(p + 1)^2}{2} + p) = -2p.
\]

(iii) If \(i \in \mathbb{Z}_{2n} \setminus \{0, n\}\), we divide them into following four cases.

Case 1: If \(i \equiv 0(\text{mod} \; p + 2)\), then
\[
NA_i = 2 \cdot \frac{p + 1}{2} + 2(-1)^i\beta^{-i2^{2n-1}} \cdot \frac{p + 1}{2} = (p + 1)(1 + (-1)^i\beta^{-i2^{2n-1}}).
\]
Case 2: If \( i \equiv 0 (\text{mod } p) \), then
\[
NA_{-i} = 2 \cdot \left(\frac{-p + 1}{2}\right) + 2(-1)^i \beta^{-i2\cdot n^2} \cdot \frac{p - 1}{2} = -(p + 1) + (-1)^{i(p - 1)}\beta^{-i2\cdot n^2}.
\]

Case 3: If \( i \mod n \in P_0 \), then
\[
NA_{-i} = 2(\sigma_1 - 1) + 2(-1)^i \beta^{-i2\cdot n^2}(\sigma_1 - 1) = 2(\sigma_1 - 1)(1 + (-1)^i\beta^{-i2\cdot n^2}).
\]

Case 4: If \( i \mod n \in P_1 \), then
\[
NA_{-i} = 2(\sigma_0 - 1) + 2(-1)^i \beta^{-i2\cdot n^2}(\sigma_0 - 1) = 2(\sigma_0 - 1)(1 + (-1)^i\beta^{-i2\cdot n^2}).
\]

Thus, we complete the proof.

\[\square\]

**Corollary 3.** If \( q \mid (p + 1) \), the linear complexity of the quaternary sequence \( u^\infty \) over \( \mathbb{F}_q \) equals to \( p^2 + 2p + 3 \) or \( 2p^2 + 2p + 2 \). Otherwise, the linear complexity of the quaternary sequence \( u^\infty \) over \( \mathbb{F}_q \) belongs to \( \{2p^2 + 4p, 2p^2 + 4p - 1, p^2 + 4p + 1, p^2 + 4p\} \).

**Proof.** If \( q \mid (p + 1) \), it is easy to verify that \( NA_{-n} \neq 0 \) for \( i = 0, n \) and \( i \in \mathbb{Z}_{2n} \setminus \{0, n\} \), \( i \equiv 0 (\text{mod } p) \). Furthermore, if \( q \in P_0 \), then \( \sigma_0^q = \sigma_0 \), and then \( \sigma_0 \in \mathbb{F}_q \). Since \( \sigma_0 + \sigma_1 = 1 \), for those \( i \in \mathbb{Z}_{2n} \setminus \{0, n\} \) and \( i \mod n \in P_0 \cup P_1 \), \( NA_{-i} \neq 0 \) hold for at least half of them. Thus, the linear complexity of the quaternary sequence \( u^\infty \) over \( \mathbb{F}_q \) equals to \( p^2 + 2p + 3 \) if only one of \( \sigma_0 \) or \( \sigma_1 \) equals to 0, otherwise it equals to \( 2p^2 + 2p + 2 \) if \( \sigma_i \neq 0 \) for \( i = 0, 1 \). If \( q \) does not divide \( (p + 1) \), \( NA_{-n} \neq 0 \) for \( i = n \), and \( i \in \mathbb{Z}_{2n} \setminus \{0, n\} \), \( i \equiv 0 \pmod{p + 2} \) or \( i \equiv 0 \pmod{p} \). The remainder proof is similar to the case of \( q \mid (p + 1) \). Thus, we complete the proof.

\[\square\]

5. Conclusion

In this paper, we analyze the linear complexities over finite field \( \mathbb{F}_q \) of two classes of quaternary sequences, where \( q \) is a prime greater than 4. These two classes of quaternary sequences we concerned, which were proposed by Kim et al. and Su et al., respectively, are both even length and have optimal autocorrelation properties. Our main method is counting the non-zero coefficients of the discrete Fourier transform of the corresponding quaternary sequences over \( \mathbb{F}_q \).

We mention that it is also interesting to consider the linear complexity of quaternary sequences over \( \mathbb{Z}_4 \). For example, in [8], Edemskiy derived the linear complexity of quaternary sequences with optimal autocorrelation value over the finite ring \( \mathbb{Z}_4 \) and in [3], Chen et al. determined the exact values of the linear complexity of quaternary sequence over \( \mathbb{Z}_4 \) defined from the generalized cyclotomic classes modulo \( 2p \). In [4], Chen et al. defined a family of quaternary sequences over \( \mathbb{Z}_4 \) of length \( pq \), a product of two distinct odd primes, using the generalized cyclotomic classes modulo \( pq \) and calculate the discrete Fourier transform of the sequences. Readers may refer to above mentioned references for the details. As a future work, we will study the linear complexities over \( \mathbb{Z}_4 \) of the quaternary sequences we concerned in this paper. In this case, the analysis will be proceeded in a Galois ring, which will be more challenging than the situation in a finite field.

**Acknowledgments**

The authors would like to thank the reviewers and editors for their detailed and constructive comments, which substantially improved the presentation of the paper.
References

[1] M. Antweiler and L. Bomer, Complex sequences over GF(p) with a two-level autocorrelation
function and a large linear span, IEEE Transaction on Information Theory, 38 (1992), 120–130.
[2] D. Calabro and J. K. Wolf, On the synthesis of two-dimensional arrays with desirable corre-
lation properties, Inform. Contro, 11 (1967), 537–560.
[3] Z. X. Chen and V. Edemskiy, Linear complexity of quaternary sequences over Z4 derived
from generalized cyclotomic classes modulo 2p, International Journal of Network Security, 19 (2017), 613–620.
[4] Z. X. Chen, Linear complexity and trace representation of quaternary sequences over Z4 based
on generalized cyclotomic classes modulo pq, Cryptography and Communications-discrete
Structures, Boolean Functions and Sequences, 9 (2017), 445–458.
[5] C. Ding, T. Helleseth and W. Shan, On the linear complexity of Legendre sequences, IEEE
Transaction on Information Theory, 44 (1998), 1276–1278.
[6] C. Ding, Codes from difference sets, World Scientific Publishing Co. Pte. Ltd., Hackensack,
NJ, 2015.
[7] X. N. Du and Z. X. Chen, Linear complexity of quaternary sequence generated using general-
ized cyclomic classes modulo 2p, IEICE Transactions on Fundamentals, 94 (2011), 1214–1217.
[8] V. Edemskiy and A. Ivanov, The linear complexity of balanced quaternary sequences with
optimal autocorrelation value, Cryptography and Communications, 7 (2015), 485–496.
[9] S. W. Golomb and G. Gong, Signal Design for Good Correlation: For Wireless Communica-
tion, in Cryptography and Radar Cambridge University Press, Cambridge, 2005.
[10] D. H. Green and L. P. Garcia Perera, The linear complexity of related prime sequences, Proc.
R. Soc. Lond. A, 460 (2004), 487–498.
[11] A. Johansen, T. Helleseth and X. Tang, The correlation disibution of quaternary sequences of
period 2(2n − 1), IEEE Transaction on Information Theory, 54 (2008), 3130–3139.
[12] P. H. Ke and S. Y. Zhang, New classes of quaternary cyclotomic sequences of length 2p
with high linear complexity, Information Processing Letters, 112 (2012), 646–650.
[13] Y.-S. Kim, J.-W. Jang, S.-H. Kim and J.-S. No, New quaternary sequences with ideal autocor-
relation constructed from legendre sequences, IEICE Transactions on Fundamentals, E96-A
(2013), 1872–1882.
[14] Y.-S. Kim, J.-W. Jang, S.-H. Kim and J.-S. No, New quaternary sequences with optimal autocorrelation, IEEE International Symposium on Information Theory, (2009), 286–289.
[15] A. Klapper, The vulnerability of geometric sequences based on fields of odd characteristic, Journal of Cryptology, 7 (1994), 33–51.
[16] R. Marzouk and A. Winterhof, On the pseudorandomness of binary and quaternary sequences
linked by the Gray mapping, Periodica Mathematica Hungarica, 60 (2010), 1–11.
[17] J. L. Massey, Shift register synthesis and BCH decoding, IEEE Transaction on Information
Theory, 15 (1969), 122–127.
[18] A. J. Menezes, P. C. Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, CRC
Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997.
[19] R. A. Ruepepe, The Science of Information Integrity, in Stream ciphers, In: Simmons G.J.
ed.) Contemporary Cryptology, IEEE Press, New York, (1992), 65–134.
[20] M. Su and A. Winterhof, On the pseudorandomness of quaternary sequences derived from
sequences over F2, Periodica Mathematica Hungarica, 74 (2017), 79–87.
[21] W. Su, Y. Yang, Z. C. Zhou and X. H. Tang, New quaternary sequence of even length with
optimal autocorrelation, Science China in Information Sciences, 61 (2018), 022308, 13pp.
[22] X. H. Tang and C. Ding, New classes of balanced quaternary and almost balanced binary
sequences with optimal autocorrelation value, IEEE Transaction on Information Theory, 56
(2010), 6398–6405.
[23] X. H. Tang and J. Linder, Almost quaternary sequences with ideal autocorrelation property,
IEEE Signal Process Letters, 16 (2009), 38–40.
[24] X. Tang and P. Udaya, A note on the optimal quadruphase sequences families, IEEE Trans-
action on Information Theory, 53 (2007), 433–436.
[25] R. J. Turyn, The linear complexity of the Legendre sequence, J. Soc. Ind. Appl. Math., 12
(1964), 115–116.
[26] P. Udaya and M. U. Siddiqi, Generalized GMW quadruphase sequences satisfying the Welch bound with equality, Applicable Algebra in Engineering, Communication and Computing, 10 (2000), 203–225.

[27] Q. Wang, Y. Jiang and D. Lin, Linear complexity of binary generalized cyclotomic sequences over $GF(q)$, Journal of Complexity, 31 (2015), 731–740.

[28] Y. Yang and X. H. Tang, Balanced quaternary sequences pairs of odd period with(almost) optimal autocorrelation and cross-correlation, IEEE Communications Letters, 18 (2014), 1327–1330.

[29] Z. Yang and P. H. Ke, Construction of quaternary sequences of length $p$ with low auto-correlation, Cryptography and Communications-discrete Structures, Boolean Functions and Sequences, 3 (2011), 55–64.

Received June 2017; revised January 2018.

E-mail address: keph@fjnu.edu.cn
E-mail address: 1561533288@qq.com
E-mail address: ptczx@126.com