On the Linear Complexity of New Generalized Cyclotomic Binary Sequences of Order Two and Period $pqr$

Longfei Liu*, Xiaoyuan Yang, Xiaoni Du, and Bin Wei

Abstract: Periodic sequences over finite fields, constructed by classical cyclotomic classes and generalized cyclotomic classes, have good pseudorandom properties. The linear complexity of a period sequence plays a fundamental role in the randomness of sequences. Let $p$, $q$, and $r$ be distinct odd primes with $\gcd(p-1, q-1) = \gcd(p-1, r-1) = \gcd(q-1, r-1) = 2$. In this paper, a new class of generalized cyclotomic sequence with respect to $pqr$ over $GF(2)$ is constructed by finding a special characteristic set. In addition, we determine its linear complexity using cyclotomic theory. Our results show that these sequences have high linear complexity, which means they can resist linear attacks.

Key words: stream cipher; pseudorandom sequence; generalized cyclotomy; linear complexity

1 Introduction

In modern communications, pseudorandom sequences over finite fields are widely used in Bluetooth, military communications, coding theory, and especially as keys in private-key cryptosystems since the 1950s. Pseudorandom sequences are useful for obtaining high linear complexity, low correlation, and large periods[1].

Linear complexity (or linear span) is an important parameter in measuring a sequence or an encoder. In coding theory, we sometimes pursue low encoding complexity[2]. However, we want to obtain high linear complexity of constructed sequences. According to the Berlekamp-Massey algorithm[1], if the linear complexity of a periodic sequence is more than half of the period, this sequence can be considered a good sequence in terms of linear complexity. One method for constructing sequences with high linear complexity uses classical cyclotomic and generalized cyclotomic classes.

Suppose $Z_N$ denotes the ring of integers modulo $N$. Let $Z_N^*$ be the set of all elements coprime with $N$. If a family of sets $\{D_0, D_1, \ldots, D_{d-1}\}$ satisfies

$$D_i \cap D_j = \emptyset$$

for all $i \neq j$,

$$\bigcup_{i=0}^{d-1} D_i = Z_N^*.$$

If $D_0$ is a group with respect to the integer multiplications modulo $N$, and there exist elements $a_1, \ldots, a_{d-1}$ of $Z_N^*$ such that $D_i = a_i D_0$ for all $i$, the cosets $D_i$ are called classical cyclotomic classes of order $d$ when $N$ is prime, and generalized cyclotomic classes of order $d$ when $N$ is composite[1].

The detailed definition of classical cyclotomic classes was first presented in the book, *Disquisitiones Arithmeticae*, that referred to them as Gaussian periods. By the use of classical cyclotomic classes, we obtain a good method of constructing pseudorandom sequences. For instance, the Legendre sequence[4], as the most important classical cyclotomic sequence, has ideal periodic autocorrelation and exhibits large linear complexity.

In recent decades, many families of generalized cyclotomic sequences were obtained. In 1962, the concept of generalized cyclotomy with respect to $pq$ was first proposed by Whiteman[5], and Ding[6]
proved these sequences have several randomness properties. Later, sequences of order four\cite{7} and order $2^k$ (where $k > 1$)\cite{8} were proven to possess high linear complexity and ideal balance. Du et al.\cite{9} completely solved the problem of the linear complexity of a generalized sequence of order $p^n$ by using trace theory. Recently, Chang and Li\cite{10} generalized the length of a Whiteman’ sequence to $2pq$, and derived the linear complexity of this sequence. The linear complexity of generalized sequences of period $pq$ and $2pq$ over the finite field of four elements is presented in Refs. [11, 12]. Fan and Ge\cite{13} introduced a generalized cyclotomy of order $d$ over $\mathbb{Z}_{p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}}$, which includes Whiteman’s and Ding’s generalized cyclotomy as special cases. Thereafter, some applications were found based on generalized cyclotomy, such as cyclic codes, frequency-hopping sequences, and 2-D optical orthogonal codes\cite{14-18}.

Many scholars have focused on the linear complexity of generalized cyclotomic sequences with different characteristic sets, periods, and orders\cite{19, 20}. Some researchers have constructed periodic sequences over special fields or rings, such as over the $\mathbb{Z}_4$\cite{21}, GF(2), GF(3), or even GF(q)\cite{22} where $q = p^n$ and $p$ is an odd prime. Most of the above sequences have high linear complexity, and take on the value $N$ ($N$ denotes the period of the sequence) in some conditions; the lower bound is $N/2$. The periods of these sequences were considered with respect to $pq$ or $2pq$, where $p$ and $q$ are odd primes.

This paper is focused on constructing a new class of generalized cyclotomic sequences, whose period is $N = pq$. Furthermore, we derive the linear complexity of these sequences. Our results show that these new sequences have high linear complexity and may be of vital use in some communication systems.

2 Linear Complexity of a Whiteman’s Generalized Sequence with Period $pq$

2.1 Preliminaries

Let $N = pq$, assume $p$, $q$, and $r$ ($p > q > r$) be odd primes with $\gcd(p - 1, q - 1) = \gcd(p - 1, r - 1) = \gcd(q - 1, r - 1) = 2$ and $r \equiv 1 \mod 4$. Define $e = (p - 1)(q - 1)(r - 1)/4$. Although $N$ does not possess a primitive root, based on the Chinese Remainder Theorem, we can obtain a fixed common root $g$ modulo $N$ of $p$, $q$, and $r$. Otherwise, we have $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r$ under the isomorphism $\psi : \omega \mapsto (\omega(\mod p), \omega(\mod q), \omega(\mod r))^T$. Thus the order of $g$ modulo $N$ $\text{Ord}_N(g) = \text{lcm}(\text{Ord}_p(g), \text{Ord}_q(g), \text{Ord}_r(g)) = e$. Assume $x_1$ and $x_2$ are positive integers which satisfying

\[
\begin{align*}
    x_1 &\equiv g(\mod p), \\
    x_1 &\equiv 1(\mod q), \\
    x_1 &\equiv 1(\mod r), \\
    x_2 &\equiv 1(\mod p), \\
    x_2 &\equiv g(\mod q), \\
    x_2 &\equiv 1(\mod r).
\end{align*}
\]

Define

\[
\begin{align*}
    D_0 &= (g), \\
    D_1 &= x_1D_0, \\
    D_2 &= x_2D_0, \\
    D_3 &= x_1x_2D_0.
\end{align*}
\]

$B_0 = D_0 \cup D_1$, $B_1 = D_2 \cup D_3$.

According to Ref. [23], we get the Whiteman’s subgroup of the multiplicative group $\mathbb{Z}_{pq}^\times = B_0 \cup B_1 = D_0 \cup D_1 \cup D_2 \cup D_3$. $B_0 \cap B_1 = \emptyset$, where $\emptyset$ denotes the empty set.

\[
\begin{align*}
    P &= \{p, 2p, \ldots, (qr - 1)p\}, \\
    P_1 &= \{pq, 2pq, \ldots, (r - 1)pq\}, \\
    P_2 &= \\{pr, 2pr, \ldots, (q - 1)pr\}, \\
    P_3 &= P - P_1 - P_2.
\end{align*}
\]

Note that here we divide $P_3$ into two sets of the generalized cyclotomic sequence of length $qr$ with respect to order $2^4$, then

\[
\begin{align*}
    Z_{qr}^* &= \{g^sx^i : s = 0, 1, \ldots, (p - 1)(q - 1)/2 - 1; \\
    &\quad i = 0, 1\}, \quad (1) \\
    D_0^{(qr)} &= \{g^s : s = 0, 1, \ldots, (p - 1)(q - 1)/2 - 1\}, \\
    D_1^{(qr)} &= \{g^sx : s = 0, 1, \ldots, (p - 1)(q - 1)/2 - 1\}, \\
    \quad P_3 = pD_0^{(qr)} \cup pD_1^{(qr)}.
\end{align*}
\]

Otherwise, we define

\[
\begin{align*}
    Q &= \{q, 2q, \ldots, (pr - 1)q\}, \\
    Q_1 &= \{pq, 2pq, \ldots, (r - 1)pq\}, \\
    Q_2 &= \{qr, 2qr, \ldots, (p - 1)qr\}, \\
    Q_3 &= Q - Q_1 - Q_2. \\
    R &= \{r, 2r, \ldots, (pq - 1)r\} - \{pr, 2pr, \ldots, (q - 1)pr\}, \\
    (q - 1)pr - (qr, 2qr, \ldots, (p - 1)qr\}, \\
    O &= \{0\}.
\end{align*}
\]

So

\[
\begin{align*}
    C_0 &= B_0 \cup Q_3 \cup R, \\
    C_1 &= B_1 \cup P \cup Q_2, \\
    C_0 \cup C_1 &= \mathbb{Z}_{pq}^\times, \quad C_0 \cap C_1 = \emptyset.
\end{align*}
\]

Based on generalized cyclotomy, a binary sequence $s^\infty = s_0s_1 \ldots s_{N-1} \ldots$ is defined as the generalized cyclotomic sequence with respect to $pq$, which yields

Tsinghua Science and Technology, June 2016, 21(3): 295–301
the following:
\[ s_i = \begin{cases} 1, & \text{if } (i \mod N) \in C_1; \\ 0, & \text{if } (i \mod N) \in C_0. \end{cases} \]

Here \( C_1 \) denotes the support or characteristic set of this sequence \( s^\infty \).

### 2.2 Linear complexity

In this subsection, we recall the definition and formula of the linear complexity of a period sequence over a finite field \( F \).

For a sequence \( s^\infty \) with period \( N \) over a finite field \( F \), if \( S^N = s_0 + s_1 x + \cdots + s_{N-1} x^{N-1} \), its linear complexity or linear span\(^{[1]} \) is defined as the smallest positive integer \( l \) such that there exist coefficients \( d_0, d_1, d_2, \ldots, d_l \) satisfying
\[ dq_i + d_1 q_{i-1} + \cdots + d_l q_{i-l} = 0, \]
where \( i \geq 1 \). And the minimal polynomial of this sequence over a finite field is given by \( d(x) = d_0 + d_1 x + \cdots + d_l x^l \).

As linear complexity is an important criterion of periodic sequences, many researchers study how to calculate it. There are a few methods for establishing the linear complexity and minimal polynomial of periodic sequences. For instance, we can establish the linear complexity by calculating the sequence’s trace representation. Here, we choose another method, shown in Eq. (2), to calculate the linear complexity.

\[ L(s^\infty) = N - \deg(\gcd(x^N - 1, S^N(x))) \]
(2)

Assume that \( \eta \) is a primitive \( pq^2r \)-th root of unity over the extension field of \( GF(2) \), then by Eq. (2), we have
\[ L(s^\infty) = N - \left\lfloor \frac{\eta}{\gcd(x^N - 1, S^N(x))} \right\rfloor \]
(3)

where \( S(x) \) is defined by
\[ S(x) = \sum_{i \in C_1} x^i = \left( \sum_{i \in B_0} + \sum_{i \in P} + \sum_{i \in Q_2} \right) x^i \in GF(2)[x] \]
(4)

The main purpose of this subsection is to obtain the exact values of \( S(\eta^j) \) when \( j \) takes on each element of \( \{0, 1, \ldots, N\} \). Our main result is provided in Theorem 1, which requires that we prove a number of lemmas at first.

**Lemma 1** Over the ring of \( GF(2)[x] \),
\[ \sum_{i \in P} \eta^i = \sum_{i \in Q} \eta^i = \sum_{i \in R} \eta^i = 1, \]
\[ \sum_{i \in P_1} \eta^i = \sum_{i \in P_2} \eta^i = \sum_{i \in P_3} \eta^i = 1, \]
\[ \sum_{i \in Q_2} \eta^i = \sum_{i \in Q_3} \eta^i = 1, \]
\[ \sum_{i \in Q_2} \eta^i + \sum_{i \in P} \eta^i = 1. \]
**Proof** From the definition of \( \eta \), we have \( 0 = \eta^{pq} - 1 = (\eta^p - 1)(1 + \eta^p + \eta^{2p} + \cdots + \eta^{(q-1)p}) \). Since \( \eta \) is a primitive \( pq \)-th root of unity, thus \( 1 + \eta^p + \eta^{2p} + \cdots + \eta^{(q-1)p} = 0 \), \( \sum_{i \in P} \eta^i = 1 \). By symmetry this lemma can be proven directly.

On the basis of the above definition, now we calculate the exact values in \( S(\eta) \), including \( \sum_{i \in B_0} \eta^k \), \( \sum_{i \in P} \eta^k \), and \( \sum_{i \in Q_2} \eta^k \).

**Lemma 2** If \( k \in P_1 \cup Q_2 \cup P_2 \), then \( \sum_{i \in B_0} \eta^k = 0 \).

**Proof** Suppose that \( k \in P_1 \), by the definition of \( B_0 \), then
\[ B_0 \mod r = (D_0 \cup D_1) \mod r = \{ g^s \mod r : s = 0, 1, \ldots, e - 1 \} \]
\[ \{ g^s x_1 \mod r : s = 0, 1, \ldots, e - 1 \} \]
\[ \{ g^s \mod r : s = 0, 1, \ldots, r - 2 \} \]
\[ \{ 1, \ldots, r - 1 \} \]
When \( s \) ranges over \( \{0, 1, \ldots, e - 1\} \), the sets of \( \{ g^s \mod r \} \) and \( \{ g^s x_1 \mod r \} \) run on each element of \( \{1, \ldots, r - 1\} \) \((r - 1)/2 \) times. Then
\[ \sum_{i \in B_0} \eta^k = ((r - 1)(r - 1)/2) \sum_{i \in P_1} \eta^k \]
(5)
If \( k \in Q_2 \),
\[ B_0 \mod p = (D_0 \cup D_1) \mod p = \{ g^s \mod p : s = 0, 1, \ldots, e - 1 \} \]
\[ \{ g^s x_1 \mod p : s = 0, 1, \ldots, e - 1 \} \]
\[ \{ g^s \mod p : s = 0, 1, \ldots, e - 1 \} \]
\[ \{ g^{s+1} \mod p : s = 0, 1, \ldots, e - 1 \} \]
\[ \{ 1, \ldots, p - 1 \} \]
When \( s \) ranges over \( \{0, 1, \ldots, e - 1\} \), the sets of \( \{ g^s \mod p \} \) and \( \{ g^s x_1 \mod p \} \) run on each element of \( \{1, \ldots, p - 1\} \) \((r - 1)(r - 1)/2 \) times. Then
\[ \sum_{i \in B_0} \eta^k = ((r - 1)(r - 1)/2) \sum_{i \in P_1} \eta^k \]
(5)
The rest of this lemma can be proved similarly.

**Lemma 3**
\[ \sum_{i \in B_0} \eta^k = \begin{cases} \frac{q - 1}{2} \mod 2, & \text{if } k \in Q_3; \\ \frac{r - 1}{2} \mod 2, & \text{if } k \in R. \end{cases} \]

**Proof** For \( k \in Q_3 \),
\[ B_0 \mod pr = (D_0 \cup D_1) \mod pr = \{ g^s \mod pr : s = 0, 1, \ldots, e - 1 \} \cup \]
\( \{ g^s x_1 \mod pr : s = 0, 1, \ldots, e - 1 \} = \{ g^s \mod pr : s = 0, 1, \ldots, \} \)
\( (p - 1)(r - 1)/2 - 1 \} \cup \{ g^{s+1} \mod pr : s = 0, 1, \ldots, (p - 1)(r - 1)/2 - 1 \} \).

Similar to the method of Eq. (1), we have \( Z_{pr}^* = \{ g^s x^i \mod pr : s = 0, 1, \ldots, (p - 1)(r - 1)/2 - 1 \}; i = 0, 1 \). So, when \( s \) ranges over \( \{ 0, 1, \ldots, e - 1 \} \), the sets of \( \{ g^s \mod r \} \) and \( \{ g^a x_1 \mod r \} \) run on each element of \( Z_{pr}^* \) \( (q - 1)/2 \) times. Then \( B_0 \mod pr = Z_{pr}^* \), and thus
\[
\sum_{i \in B_0} \eta_{ki} = ((q - 1)/2 \mod 2) \sum_{i \in \mathbb{Z}_{pr}^*} \eta_{ij} = (q - 1)/2 \mod 2.
\]

For \( k \in R \),
\( B_0 \mod pq = (D_0 \cup D_1) \mod pq = \{ g^s \mod pq : s = 0, 1, \ldots, e - 1 \} \cup \{ g^a x_1 \mod pq : s = 0, 1, \ldots, e - 1 \} = \{ g^s \mod pq : s = 0, 1, \ldots, (p - 1)(q - 1)/2 - 1 \} \cup \{ g^{s+1} \mod pq : s = 0, 1, \ldots, (p - 1)(q - 1)/2 - 1 \} \).

Similarly, we have
\[
\sum_{i \in B_0} \eta_{ki} = ((r - 1)/2 \mod 2) \sum_{i \in \mathbb{Z}_{pq}^*} \eta_{ij} = (r - 1)/2 \mod 2.
\]

\textbf{Lemma 4} If \( k \in P_3 \cup P_4 \), then \( \sum_{i \in B_0} \eta_{ki} = 0 \).

\textbf{Proof} Since
\( B_0 \mod qr = (D_0 \cup D_1) \mod qr = \{ g^s \mod qr : s = 0, 1, \ldots, e - 1 \} \cup \{ g^a x_1 \mod qr : s = 0, 1, \ldots, e - 1 \} \),
by the definition of \( x_1 \), we have \( x_1 \equiv 1 \mod (qr) \). It follows that
\[
\sum_{i \in B_0} \eta_{ki} = ((p - 1) \mod 2) \sum_{i \in D_0^{(qr)}} \eta_{ij} = 0.
\]

\textbf{Lemma 5}
\[
\sum_{i \in P} \eta_{ki} = \begin{cases} 1, & \text{if } k \in \mathbb{Z}_N^* \cup \mathbb{P} \cup \mathbb{Q}_3 \cup R; \\ 0, & \text{if } k \notin \mathbb{Q}_2 \cup \mathbb{O}. \end{cases}
\]

\textbf{Proof} Here, we discuss the lemma in different situations. By the definition of \( \mathbb{Z}_N^* \) and Lemma 1, it follows:

\textbf{Case 1}
For \( k \in \mathbb{Z}_N^* \), \( kP = P \), \( \sum_{i \in P} \eta_{ki} = \sum_{i \in P} \eta_{ij} = 1 \).

For \( k \in O \), \( kP = O \), \( \sum_{i \in P} \eta_{ki} = (q - r - 1) \mod 2 = 0 \).

\textbf{Case 2}
For \( k \in Q_1 \), \( kP = Q_1 \cup O \),
\[
\sum_{i \in P} \eta_{ki} = (q \mod 2) \sum_{i \in Q_1} \eta_{ij} + (q - 1) \mod 2 = 2.
\]
For \( k \in Q_2 \), \( kP = O \),
\[
\sum_{i \in P} \eta_{ki} = (q - r - 1) \mod 2 = 0.
\]
For \( k \in Q_3 \), \( kP = P_1 \cup O \),
\[
\sum_{i \in P} \eta_{ki} = (q \mod 2) \sum_{i \in P_1} \eta_{ij} + (q - 1) \mod 2 = 1.
\]

\textbf{Case 3}
For \( k \in P_2 \), \( kP = P_2 \cup O \),
\[
\sum_{i \in P} \eta_{ki} = (r \mod 2) \sum_{i \in P_2} \eta_{ij} + (r - 1) \mod 2 = 1.
\]

For \( k \in P_3 \), \( kP = P \),
\[
\sum_{i \in P} \eta_{ki} = \sum_{i \in P} \eta_{ij} = 1.
\]
For \( k \in R \), \( kP = P_2 \cup O \),
\[
\sum_{i \in P} \eta_{ki} = (r \mod 2) \sum_{i \in P_2} \eta_{ij} + (r - 1) \mod 2 = 1.
\]

\textbf{Lemma 6}
\[
\sum_{i \in Q_2} \eta_{ki} = \begin{cases} 1, & \text{if } k \in \mathbb{Z}_N^* \cup \mathbb{Q}_2; \\ 0, & \text{if } k \in \mathbb{Q}_1 \cup \mathbb{Q}_3 \cup \mathbb{P} \cup \mathbb{P}_3 \cup R \cup O. \end{cases}
\]

\textbf{Proof} Here, we discuss the lemma in different situations.

\textbf{Case 1}
For \( k \in \mathbb{Z}_N^* \), \( kQ_2 = Q_2 \),
\[
\sum_{i \in Q_2} \eta_{ki} = \sum_{i \in Q_2} \eta_{ij} = 1.
\]
For \( k \in O \), \( kQ_2 = O \),
\[
\sum_{i \in Q_2} \eta_{ki} = (p - 1) \mod 2 = 0.
\]

\textbf{Case 2}
For \( k \in Q_1 \), \( kQ_2 = O \),
\[
\sum_{i \in Q_2} \eta_{ki} = (p - 1) \mod 2 = 0.
\]
For \( k \in Q_2 \), \( kQ_2 = Q_2 \),
\[
\sum_{i \in Q_2} \eta_{ki} = \sum_{i \in Q_2} \eta_{ij} = 1.
\]
For \( k \in Q_3 \), \( kQ_2 = Q_2 \),
\[
\sum_{i \in Q_2} \eta_{ki} = (r - 1 \mod 2) \sum_{i \in Q_2} \eta_{ij} = 0.
\]

\textbf{Case 3}
For \( k \in P_2 \), \( kQ_2 = O \),
\[
\sum_{i \in Q_2} \eta_{ki} = (p - 1) \mod 2 = 0.
\]
For \( k \in P_3 \), \( kQ_2 = O \),
\[
\sum_{i \in Q_2} \eta_{ki} = (p - 1) \mod 2 = 0.
\]
For $k \in R$, $Q_2 = Q_2$.  
\[ \sum_{i \in Q_2} \eta^{ki} = (q - 1 \mod 2) \sum_{i \in Q_2} \eta^{ki} = 0. \]

On the basis of Lemmas 3–6, we derive the exact value of $S(\eta^k)$.

**Lemma 7**

\[ S(\eta^k) = \begin{cases} 
S(\eta), & \text{if } k \in B_0; \\
S(\eta) + 1, & \text{if } k \in B_1; \\
0, & \text{if } k \in Q_3 \cup O; \\
1, & \text{if } k \in P_2 \cup P_3 \cup Q_1 \cup Q_2 \cup R. 
\end{cases} \]

**Proof** By the definition of $S(\eta^k)$ and Lemmas 1–6, then

**Case 1**

If $k \in B_0$, then $B_0 = B_0$. So 
\[ S(\eta^k) = \left( \sum_{i \in B_0} + \sum_{i \in P} + \sum_{i \in Q_2} \right) \eta^{ki} = \sum_{i \in B_0} \eta^i + 1 + 1 = S(\eta). \]

If $k \in B_1$, then $B_0 = B_1$. Note that, $\sum_{i \in B_0} \eta^i \neq 1$. So 
\[ S(\eta^k) = \left( \sum_{i \in B_0} + \sum_{i \in P} + \sum_{i \in Q_2} \right) \eta^{ki} = \sum_{i \in B_1} \eta^i + 1 + 1 = S(\eta) + 1. \]

**Case 2**

If $k \in Q_1$, then 
\[ S(\eta^k) = \left( \sum_{i \in B_0} + \sum_{i \in P} + \sum_{i \in Q_2} \right) \eta^{ki} = 0 + 1 + 0 = 1. \]

If $k \in Q_2$, then 
\[ S(\eta^k) = \left( \sum_{i \in B_0} + \sum_{i \in P} + \sum_{i \in Q_2} \right) \eta^{ki} = 1 + 0 + 0 = 1. \]

If $k \in Q_3$, then 
\[ S(\eta^k) = \left( \sum_{i \in B_0} + \sum_{i \in P} + \sum_{i \in Q_2} \right) \eta^{ki} = 0 + 1 + \frac{q - 1}{2} = \frac{q + 1}{2}. \]

Note that $r \equiv 1 \mod 4$ and $\gcd(r - 1, q - 1) = 2$. It follows that $q \equiv 3 \mod 4$. Hence, if $k \in Q_3$, 
$S(\eta^k) = 0$.

**Case 3**

If $k \in P_2$, then 
\[ S(\eta^k) = \left( \sum_{i \in B_0} + \sum_{i \in P} + \sum_{i \in Q_2} \right) \eta^{ki} = 0 + 1 + 0 = 1. \]

If $k \in P_3$, then 
\[ S(\eta^k) = \left( \sum_{i \in B_0} + \sum_{i \in P} + \sum_{i \in Q_2} \right) \eta^{ki} = 0 + 1 + 0 = 1. \]

If $k \in R$, then 
\[ S(\eta^k) = \left( \sum_{i \in B_0} + \sum_{i \in P} + \sum_{i \in Q_2} \right) \eta^{ki} = 0 + 1 + \frac{r - 1}{2} = \frac{r + 1}{2}. \]

Since $r \equiv 1 \mod 4$, we see that when $k \in R$, 
$S(\eta^k) = 1$. \[ \]

**Lemma 8**

$2 \in B_0$ if and only if $S(\eta) \in \{0, 1\}$.

**Proof** Since $S(\eta) \in GF(2)[x]$, and the characteristic of the extension field of $GF(2)$ is 2, it follows that 
$S^2(\eta) = S(\eta^2)$. Note that $2 \in Z_{pqr}$, by Lemma 7, we have $S(\eta^2) = S(\eta)$ if and only if $2 \in B_0$.

**Theorem 1**

LC($s(\infty)$) = \[ \begin{cases} 
pqr - \frac{(p - 1)(q + 1)(r - 1)}{2}, & \text{if } 2 \in B_0; \\
pqr - \frac{(p - 1)(r - 1)}{2} - 1, & \text{if } 2 \in B_1. 
\end{cases} \]

**Proof** In the case of $2 \in B_0$, by Lemma 7, we can get that one of $S(\eta)$ and $S(\eta) + 1$ must be zero for a fixed $\eta$. Here we assume $S(\eta)$ is zero. Thus 
\[ S(\eta^k) = \begin{cases} 
0, & \text{if } k \in B_0; \\
1, & \text{if } k \in B_1; \\
0, & \text{if } k \in Q_3 \cup O; \\
1, & \text{if } k \in P_2 \cup P_3 \cup Q_1 \cup Q_2 \cup R. 
\end{cases} \]

Hence, 
\[ \text{LC}(s(\infty)) = \frac{pqr - \frac{(p - 1)(q + 1)(r - 1)}{2}}{2} - 1. \]

In the case of $2 \in B_1$, by Lemmas 7 and 8, 
\[ S(\eta^k) = \begin{cases} 
\neq 0, & \text{if } k \in B_0; \\
\neq 0, & \text{if } k \in B_1; \\
0, & \text{if } k \in Q_3 \cup O; \\
1, & \text{if } k \in P_2 \cup P_3 \cup Q_1 \cup Q_2 \cup R. 
\end{cases} \]

Hence, 
\[ \text{LC}(s(\infty)) = \frac{pqr - \frac{(p - 1)(q + 1)(r - 1)}{2}}{2} - 1. \]
This completes the proof of this theorem.

Remark: According to Ref. [24], since \(\gcd(p - 1, q - 1) = 2\), \(\gcd(p - 1, r - 1) = 2\), \(\gcd(q - 1, r - 1) = 2\), \(r \equiv 1 \mod 4\), and 2 is a quadratic residue modulo \(pqr\), we have \(2 \in B_0\) if and only if \(p \equiv -1(\mod 8)\), \(q \equiv -1(\mod 8)\), and \(r \equiv 1(\mod 8)\).

### 3 Conclusion

The contribution of this paper is to construct a new class of generalized cyclotomic sequences of order two with period \(pqr\) and obtain the linear complexity of this sequence. Meanwhile, we point out that the linear complexity is larger than \(pqr/2\). Thus, the above sequence is a family of valid sequences from the linear complexity viewpoint. Recently, the generalized cyclotomic sequences of order \(pq\) and \(p^m\) have been used to construct cyclic codes, frequency-hopping sequences, and 2-D optical orthogonal codes\[^{14–18}\]. It may be interesting to explore applications based on the generalized cyclotomic sequences of period \(pqr\).

### Acknowledgment

This work was supported by the National Natural Science Foundation of China (Nos. 61272492, 61103231, 61202492, 61202395, 61462077, and 61562077) and the Program for New Century Excellent Talents in University (No. NCET-12-0620).

### References

[1] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*. Elsevier, 1998.

[2] C. Qian, W. Lei, and Z. Wang, Low complexity LDPC decoder with modified sum-product algorithm, *Tsinghua Science and Technology*, vol. 18, no. 1, pp. 57–61, 2013.

[3] C. Gauss, *Disquisitiones Arithmeticae*. Springer-Verlag, 1986.

[4] C. Ding, T. Helleseth, and W. Shan, On the linear complexity of Legendre sequences, *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1276–1278, 1998.

[5] A. Whiteman, A family of difference sets, *Illinois J. Math.*, vol. 6, no. 1, pp. 107–121, 1962.

[6] C. Ding, Linear complexity of generalized cyclotomic binary sequences of order 2, *Finite Fields and Their Applications*, vol. 8, no. 1, pp. 159–174, 1997.

[7] T. Yan, H. Li, and G. Xiao, The linear complexity of new generalized cyclotomic binary sequences of order four, *Information Sciences*, vol. 178, no. 3, pp. 807–815, 2007.

[8] T. Yan, X. Du, G. Xiao, and X. Huang, Linear complexity of binary Whiteman generalized cyclotomic sequences of order \(2^k\), *Information Sciences*, vol. 179, no. 7, pp. 1019–1023, 2009.

[9] X. Du, T. Yan, and G. Xiao, Trace representation of some generalized cyclotomic sequences of length \(pq\), *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3881–3891, 2012.

[10] H. Cai, H. Liang, and X. Tang, Constructions of optimal 2-D optical orthogonal codes via generalized cyclotomic classes, *IEEE Transactions on Information Theory*, vol. 61, no. 1, pp. 688–695, 2015.

[11] X. Zeng, H. Cai, X. Tang, and Y. Yang, Optimal frequency-hopping sequences of odd length, *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 3237–3248, 2013.

[12] H. Cai, Z. Zhou, Y. Yang, and X. Tang, A new construction of frequency-hopping sequences optimal partial hamming correlation, *IEEE Transactions on Information Theory*, vol. 60, no. 9, pp. 5782–5790, 2014.

[13] M. Qi, S. Xiong, J. Yuan, and W. Rao, Linear complexity over \(\mathbb{F}_q\) of generalized cyclotomic quaternary sequences with period \(2p\), *IEEE Transactions on Fundamentals of Electronics*, vol. 61, no. 2, pp. 1326–1336, 2014.

[14] C. Ding, Cyclic codes from the two primes sequences, *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3881–3891, 2012.

[15] Z. Chang and D. Li, On the linear complexity of generalized cyclotomic binary sequences of length \(2pq\), *Concurrency and Computation: Practice and Experience*, vol. 26, no. 8, pp. 1520–1530, 2014.

[16] D. Li, Q. Wen, J. Zhang, and Z. Chang, Linear complexity of generalized cyclotomic quaternary sequences with period \(pq\), *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E97-A, no. 5, pp. 1153–1158, 2014.

[17] Z. Chang and D. Li, On the linear complexity of quaternary cyclotomic sequences with the period \(2pq\), *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E97-A, no. 2, pp. 679–684, 2014.
Longfei Liu received the MEng degree in 2013 from Engineering University of the Armed Police Force. He is currently a teaching assistant at Engineering University of the Armed Police Force. His research interests include network security and stream cipher.

Xiaoyuan Yang received the BS (1982) and MS degrees (1991) in information and electronic system from Xidian University. He is currently a professor and PhD supervisor at Engineering University of Armed Police Force. He is also the director of the Key Lab of Cryptography and Information Security of Armed Police Force. He won the award of “Excellent Professional and Technical Personnel” from the whole military and “Excellent Teachers” from China Education Ministry. He has published about 120 research papers, 4 research books, and 4 teaching materials. His research interests include cryptography protocols and post-quantum cryptography.

Xiaoni Du received the MS degree from Lanzhou University in 2000 and the PhD degree in cryptography from Xidian University in 2008. She is currently a professor at Northwest Normal University. Her research interests include cryptography and information security.

Bin Wei received the PhD degree from Xi’an Jiao Tong University in 2013. He is currently an associate professor at Engineering University of APF. His research interests include cryptography and information security.