Tsinghua Science and Technology

Volume 21 | Issue 3 Article 5

2016

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

Longfei Liu
Key Laboratory of Network & Information Security of APF, Engineering College of APF, Xi'an 710086, China.

Xiaoyuan Yang
Key Laboratory of Network & Information Security of APF, Engineering College of APF, Xi'an 710086, China.

Xiaoni Du
College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, China.

Bin Wei
Key Laboratory of Network & Information Security of APF, Engineering College of APF, Xi'an 710086, China.

TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 05/11 pp295–301
Volume 21, Number 3, June 2016

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

$$D_i \bigcap D_j = \varnothing$$

for all $i \neq j$,

$$\bigcup_{i=0}^{d-1} D_i = \mathbf{Z}_N^*.$$

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 $\mathbf{Z}_N^*$ 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*[3], 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]

• Longfei Liu, Xiaoyuan Yang, and Bin Wei are with Key Laboratory of Network & Information Security of APF, Engineering College of APF, Xi'an 710086, China. E-mail: ya_zhou_521@163.com.
• Xiaoni Du is with College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, China.
* To whom correspondence should be addressed.
Manuscript received: 2016-01-15; accepted: 2016-03-07

proved these sequences have several randomness properties. Later, sequences of order four[7] and order 2^k (where $k>1$)[8] were proven to possess high linear complexity and ideal balance. Du et al.[9] completely solved the problem of the linear complexity of a generalized sequence of order p^m by using trace theory. Recently, Chang and Li[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[13] introduced a generalized cyclotomy of order d over $\mathbf{Z}_{p_1^{e_1},p_2^{e_2},\ldots,p_n^{e_n}}$, 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[14–18].

Many scholars have focused on the linear complexity of generalized cyclotomic sequences with different characteristic sets, periods, and orders[19, 20]. Some researchers have constructed periodic sequences over special fields or rings, such as over the Z_4[21], GF(2), GF(3), or even GF(q)[22] where $q=p^m$ 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 $N=pqr$. 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 *pqr*

2.1 Preliminaries

Let $N=pqr$, 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 $r\equiv 1 \bmod 4$. 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 $\mathbf{Z}_{pqr}\cong\mathbf{Z}_p\times\mathbf{Z}_q\times\mathbf{Z}_r$ under the isomorphism $\psi:\omega\mapsto(\omega(\mathrm{mod}\,p),\omega(\mathrm{mod}q),\omega(\mathrm{mod}r))$[1]. Thus the order of g modulo N $\mathrm{Ord}_N(g)$ is $\mathrm{lcm}(\mathrm{Ord}_p(g),\mathrm{Ord}_q(g),\mathrm{Ord}_r(g))=e$. Assume x_1 and x_2 are positive integers which satisfying

$$\begin{cases} x_1\equiv g(\mathrm{mod}\ p),\\ x_1\equiv 1(\mathrm{mod}\ q),\\ x_1\equiv 1(\mathrm{mod}\ r).\end{cases}$$

$$\begin{cases} x_2\equiv 1(\mathrm{mod}\ p),\\ x_2\equiv g(\mathrm{mod}\ q),\\ x_2\equiv 1(\mathrm{mod}\ r).\end{cases}$$

Define

$$D_0=(g),\ D_1=x_1D_0,$$
$$D_2=x_2D_0,\ D_3=x_1x_2D_0.$$
$$B_0=D_0\bigcup D_1,$$
$$B_1=D_2\bigcup D_3.$$

According to Ref. [23], we get the Whiteman's subgroup of the multiplicative group $\mathbf{Z}_{pqr}^*=B_0\bigcup B_1=D_0\bigcup D_1\bigcup D_2\bigcup D_3$. $B_0\bigcap B_1=\varnothing$, where $\varnothing$ denotes the empty set.

$$P=\{p,2p,\ldots,(qr-1)p\},$$
$$P_1=\{pq,2pq,\ldots,(r-1)pq\},$$
$$P_2=\{pr,2pr,\ldots,(q-1)pr\},$$
$$P_3=P-P_1-P_2.$$

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

$$\mathbf{Z}_{qr}^*=\{g^sx^i:s=0,1,\ldots,(p-1)(q-1)/2-1;\ i=0,1\}\quad(1)$$
$$D_0^{(qr)}=\{g^s:s=0,1,\ldots,(p-1)(q-1)/2-1\},$$
$$D_1^{(qr)}=\{g^sx:s=0,1,\ldots,(p-1)(q-1)/2-1\},$$
$$P_3=pD_0^{(qr)}\bigcup pD_1^{(qr)}.$$

Otherwise, we define

$$Q=\{q,2q,\ldots,(pr-1)q\},$$
$$Q_1=\{pq,2pq,\ldots,(r-1)pq\},$$
$$Q_2=\{rq,2rq,\ldots,(p-1)rq\},$$
$$Q_3=Q-Q_1-Q_2.$$
$$R=\{r,2r,\ldots,(pq-1)r\}-\{pr,2pr,\ldots,(q-1)pr\}-\{qr,2qr,\ldots,(p-1)qr\},$$
$$O=\{0\}.$$

So

$$C_0=B_0\bigcup Q_3\bigcup R,$$
$$C_1=B_1\bigcup P\bigcup Q_2,$$
$$C_0\bigcup C_1=\mathbf{Z}_{pqr},\ C_0\bigcap C_1=\varnothing.$$

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 pqr, which yields

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^∞.

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^∞ 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

$$d_0 s_i + d_1 s_{i-1} + \cdots + d_l s_{i-l} = 0,$$

where $i \geqslant 1$. And the minimal polynomial of this sequence over a finite filed 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.

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

Assume that η is a primitive pqr-th root of unity over the extension field of GF(2), then by Eq. (2), we have

$$L(s^\infty) = N - \left|\{j : S(\eta^j) = 0, 0 \leqslant j \leqslant N-1\}\right| \quad (3)$$

where $S(x)$ is defined by

$$S(x) = \sum_{i \in C_1} x^i = \left(\sum_{i \in B_0} + \sum_{i \in P} + \sum_{i \in Q_2} \right) x^i \in \mathrm{GF}(2)[x] \quad (4)$$

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],

$$\sum_{i \in P} \eta^i = \sum_{i \in Q} \eta^i = \sum_{i \in R} \eta^i = 1,$$

$$\sum_{i \in P_1} \eta^i = \sum_{i \in P_2} \eta^i = \sum_{i \in P_3} \eta^i = 1,$$

$$\sum_{i \in Q_2} \eta^i = \sum_{i \in Q_3} \eta^i = 1.$$

Proof From the definition of η, we have $0 = \eta^{pqr} - 1 = (\eta^p - 1)(1 + \eta^p + \eta^{2p} + \ldots + \eta^{(qr-1)q})$. Since η is a primitive pqr-th root of unity, thus $1 + \eta^p + \eta^{2p} + \cdots + \eta^{(qr-1)q} = 0$, $\sum_{i \in P} \eta^i = 1$. 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 $\sum_{i \in B_0} \eta^{ki}$, $\sum_{i \in P} \eta^{ki}$, and $\sum_{i \in Q_2} \eta^{ki}$.

Lemma 2 If $k \in P_1 \bigcup Q_2 \bigcup P_2$, then $\sum_{i \in B_0} \eta^{ki} = 0$.

Proof Suppose that $k \in P_1$, by the definition of B_0, then

$$\begin{aligned} B_0 \bmod r &= (D_0 \bigcup D_1) \bmod r = \\ &\{g^s \bmod r : s = 0, 1, \ldots, e-1\} \bigcup \\ &\{g^s x_1 \bmod r : s = 0, 1, \ldots, e-1\} = \\ &\{g^s \bmod r : s = 0, 1, \ldots, r-2\} = \\ &\{1, \ldots, r-1\}. \end{aligned}$$

When s ranges over $\{0, 1, \ldots, e-1\}$, the sets of $\{g^s \bmod r\}$ and $\{g^s x_1 \bmod r\}$ run on each element of $\{1, \ldots, r-1\}$ $(p-1)(q-1)/2$ times. Then

$$\sum_{i \in B_0} \eta^{ki} = ((p-1)(q-1)/2 \bmod 2) \sum_{i \in P_1} \eta^i = 0.$$

If $k \in Q_2$,

$$\begin{aligned} B_0 \bmod p &= (D_0 \bigcup D_1) \bmod p = \\ &\{g^s \bmod p : s = 0, 1, \ldots, e-1\} \bigcup \\ &\{g^s x_1 \bmod p : s = 0, 1, \ldots, e-1\} = \\ &\{g^s \bmod p : s = 0, 1, \ldots, e-1\} \bigcup \\ &\{g^{s+1} \bmod p : s = 0, 1, \ldots, e-1\} = \\ &\{1, \ldots, p-1\}. \end{aligned}$$

When s ranges over $\{0, 1, \ldots, e-1\}$, the sets of $\{g^s \bmod p\}$ and $\{g^s x_1 \bmod p\}$ run on each element of $\{1, \ldots, p-1\}$ $(q-1)(r-1)/2$ times. Then

$$\sum_{i \in B_0} \eta^{ki} = ((q-1)(r-1)/2 \bmod 2) \sum_{i \in Q_2} \eta^i = 0.$$

The rest of this lemma can be proved similarly. ■

Lemma 3

$$\sum_{i \in B_0} \eta^{ki} = \begin{cases} \dfrac{q-1}{2} (\bmod 2), & \text{if } k \in Q_3; \\ \dfrac{r-1}{2} (\bmod 2), & \text{if } k \in R. \end{cases}$$

Proof For $k \in Q_3$,

$$\begin{aligned} B_0 \bmod pr &= (D_0 \bigcup D_1) \bmod pr = \\ &\{g^s \bmod pr : s = 0, 1, \ldots, e-1\} \bigcup \end{aligned}$$

$$\{g^s x_1 \bmod pr : s = 0, 1, \ldots, e-1\} = \{g^s \bmod pr : s = 0, 1, \ldots, (p-1)(r-1)/2-1\} \bigcup \{g^{s+1} \bmod pr : s = 0, 1, \ldots, (p-1)(r-1)/2-1\}.$$

Similar to the method of Eq. (1), we have $\mathbf{Z}_{pr}^* = \{g^s x^i \bmod pr : s = 0, 1, \ldots, (p-1)(r-1)/2-1; i = 0, 1\}$. So, when s ranges over $\{0, 1, \ldots, e-1\}$, the sets of $\{g^s \bmod r\}$ and $\{g^s x_1 \bmod r\}$ run on each element of $\mathbf{Z}_{pr}^*$ $(q-1)/2$ times. Then $B_0 \bmod pr = \mathbf{Z}_{pr}^*$, and thus

$$\sum_{i \in B_0} \eta^{ki} = ((q-1)/2 \bmod 2) \sum_{i \in Z_{pr}^*} \eta^{iq} = (q-1)/2 \bmod 2.$$

For $k \in R$,

$$B_0 \bmod pq = (D_0 \bigcup D_1) \bmod pq = \{g^s \bmod pq : s = 0, 1, \ldots, e-1\} \bigcup \{g^s x_1 \bmod pq : s = 0, 1, \ldots, e-1\} = \{g^s \bmod pq : s = 0, 1, \ldots, (p-1)(q-1)/2-1\} \bigcup \{g^{s+1} \bmod pq : s = 0, 1, \ldots, (p-1)(q-1)/2-1\}.$$

Similarly, we have

$$\sum_{i \in B_0} \eta^{ki} = ((r-1)/2 \bmod 2) \sum_{i \in Z_{pq}^*} \eta^{ir} = (r-1)/2 \bmod 2.$$

■

Lemma 4 If $k \in P_3 \bigcup P_4$, then $\sum_{i \in B_0} \eta^{ki} = 0$.

Proof Since

$$B_0 \bmod qr = (D_0 \bigcup D_1) \bmod qr = \{g^s \bmod qr : s = 0, 1, \ldots, e-1\} \bigcup \{g^s x_1 \bmod qr : s = 0, 1, \ldots, e-1\},$$

by the definition of x_1, we have $x_1 \equiv 1 (\bmod qr)$. It follows that

$$\sum_{i \in B_0} \eta^{ki} = ((p-1) \bmod 2) \sum_{i \in D_0^{(qr)}} \eta^{ir} = 0.$$

■

Lemma 5

$$\sum_{i \in P} \eta^{ki} = \begin{cases} 1, & \text{if } k \in \mathbf{Z}_N^* \bigcup P \bigcup Q_3 \bigcup R; \\ 0, & \text{if } k \in Q_2 \bigcup O. \end{cases}$$

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

Case 1

For $k \in \mathbf{Z}_N^*, kP = P, \sum_{i \in P} \eta^{ki} = \sum_{i \in P} \eta^i = 1$.

For $k \in O, kP = O, \sum_{i \in P} \eta^{ki} = (qr-1) \bmod 2 = 0$.

Case 2

For $k \in Q_1, kP = Q_1 \bigcup O$,

$$\sum_{i \in P} \eta^{ki} = (q \bmod 2) \sum_{i \in Q_1} \eta^{ik} + (q-1) \bmod 2 = 1.$$

For $k \in Q_2, kP = O$,

$$\sum_{i \in P} \eta^{ki} = (qr-1) \bmod 2 = 0.$$

For $k \in Q_3, kP = P_1 \bigcup O$,

$$\sum_{i \in P} \eta^{ki} = (q \bmod 2) \sum_{i \in P_1} \eta^{ik} + (q-1) \bmod 2 = 1.$$

Case 3

For $k \in P_2, kP = P_2 \bigcup O$.

$$\sum_{i \in P} \eta^{ki} = (r \bmod 2) \sum_{i \in P_2} \eta^{ik} + (r-1) \bmod 2 = 1.$$

For $k \in P_3, kP = P$.

$$\sum_{i \in P} \eta^{ki} = \sum_{i \in P} \eta^{ik} = 1.$$

For $k \in R, kP = P_2 \bigcup O$.

$$\sum_{i \in P} \eta^{ki} = (r \bmod 2) \sum_{i \in P_2} \eta^{ik} + (r-1) \bmod 2 = 1.$$

■

Lemma 6

$$\sum_{i \in Q_2} \eta^{ki} = \begin{cases} 1, & \text{if } k \in \mathbf{Z}_N^* \bigcup Q_2; \\ 0, & \text{if } k \in Q_1 \bigcup Q_3 \bigcup P_2 \bigcup P_3 \bigcup R \bigcup O. \end{cases}$$

Proof Here, we discuss the lemma in different situations.

Case 1

For $k \in \mathbf{Z}_N^*, kQ_2 = Q_2$,

$$\sum_{i \in Q_2} \eta^{ki} = \sum_{i \in Q_2} \eta^i = 1.$$

For $k \in O, kQ_2 = O$,

$$\sum_{i \in Q_2} \eta^{ki} = (p-1) \bmod 2 = 0.$$

Case 2

For $k \in Q_1, kQ_2 = O$,

$$\sum_{i \in Q_2} \eta^{ki} = (p-1) \bmod 2 = 0.$$

For $k \in Q_2, kQ_2 = Q_2$,

$$\sum_{i \in Q_2} \eta^{ki} = \sum_{i \in Q_2} \eta^i = 1.$$

For $k \in Q_3, kQ_2 = Q_2$.

$$\sum_{i \in Q_2} \eta^{ki} = (r-1 \bmod 2) \sum_{i \in Q_2} \eta^{ik} = 0.$$

Case 3

For $k \in P_2, kQ_2 = O$,

$$\sum_{i \in Q_2} \eta^{ki} = (p-1) \bmod 2 = 0.$$

For $k \in P_3, kQ_2 = O$,

$$\sum_{i \in Q_2} \eta^{ki} = (p-1) \bmod 2 = 0.$$

For $k \in R, kQ_2 = Q_2$,

$$\sum_{i\in Q_2} \eta^{ki} = (q-1 \bmod 2)\sum_{i\in Q_2} \eta^{ik} = 0. \quad \blacksquare$$

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

Lemma 7

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

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

Case 1

If $k \in B_0$, then $kB_0 = B_0$. 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 $kB_0 = B_1$. Note that, $\sum_{i\in B_0} \eta^i + \sum_{i\in B_1} \eta^i = 1$. 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 $r \equiv 1 \bmod 4$ and $\gcd(r-1, q-1) = 2$. It follows that $q \equiv 3 \bmod 4$. 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 $r \equiv 1 \bmod 4$, we see that when $k \in R$, $S(\eta^k) = 1$. $\blacksquare$

Lemma 8 $2 \in B_0$ if and only if $S(\eta) \in \{0, 1\}$.

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

Theorem 1

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

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 η. Here we assume $S(\eta)$ is zero. Thus

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

Hence,

$$\mathrm{LC}(s^\infty) = pqr - \frac{(p-1)(q-1)(r-1)}{2} - (p-1)(r-1) - 1 = pqr - \frac{(p-1)(q+1)(r-1)}{2} - 1.$$

In the case of $2 \in B_1$, by Lemmas 7 and 8,

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

Hence,

$$\mathrm{LC}(s^\infty) = pqr - (p-1)(r-1) - 1.$$

This completes the proof of this theorem. ■

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

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, *Information Sciences*, vol. 178, no. 16, pp. 3307–3316, 2008.

[10] 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.

[11] 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.

[12] 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.

[13] C. Fan and G. Ge, A unified approach to Whiteman's and Ding-Helleseth's generalized cyclotomy over residue class rings, *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1326–1336, 2014.

[14] C. Ding, Cyclic codes from cyclotomic sequences of order four, *Finite Fields and Their Applications*, vol. 23, no. 1, pp. 8–34, 2013.

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

[16] 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.

[17] 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.

[18] 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.

[19] M. Qi, S. Xiong, J. Yuan, and W. Rao, Linear complexity over Fq of generalized cyclotomic quaternary sequences with period 2p, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E98-A, no. 7, pp. 1569–1575, 2015.

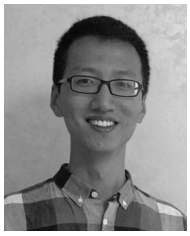
[20] L. Wang and Y. Gao, Linear complexity and correlation of a class of binary cyclotomic sequences, *Applicable Algebra in Engineering, Communication and Computing*, vol. 25, no. 1, pp. 67–97, 2014.

[21] V. Edemskiy and A. Ivanov, Linear complexity of quaternary sequences of length with low autocorrelation, *Journal of Computational and Applied Mathematics*, vol. 259, no. 3, pp. 555–560, 2014.

[22] Q. Wang, Y. Jiang, and D. Lin, Linear complexity of binary generalized cyclotomic sequences over GF(q), *Journal of Complexity*, vol. 31, no. 5, pp. 731–740, 2015.

[23] J. Cao, Q. Yue, and L. Hu, Whiteman's generalized cyclotomic numbers with respect to t primes, *Finite Fields and Their Applications*, vol. 18, no. 3, pp. 634–644, 2012.

[24] D. Burton, *Elementary Number Theory, Fourth ed.* McGraw-Hill International Editions, 1998.



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.