Linear Complexity of New Generalized Cyclotomic Sequences of Length $2pq$

Wang Hongwei(王宏伟)[1*], *Ge Wu*(葛武)[2]

1. Civil Construction Engineering Department, Hubei Polytechnic University, Huangshi, 435003, P. R. China;
2. Zhejiang Education Publishing House, Hangzhou, 310013, P. R. China

(Received 3 April 2014; revised 9 May, 2014; accepted 20 May 2014)

Abstract: The linear complexity and minimal polynomial of new generalized cyclotomic sequences of order two are investigated. A new generalized cyclotomic sequence S of length $2pq$ is defined with an imbalance $p+1$. The results show that this sequence has high linear complexity.

Key words: generalized cyclotomic sequence; linear complexity; minimal polynomial

CLC number: O157.4; O236.2 **Document code**: A **Article ID**: 1005-1120(2014)06-0710-07

1 Introduction

Pseudo-random sequences used for stream ciphers are required to be unpredictable. The linear span or linear complexity of a sequence is the main component that indicates this feature. The linear complexity $L(S^\infty)$ of sequence $\{S^\infty\}$ over F_{p^n} (F_{p^n} is a finite field of order p^n) is defined as the length of the shortest linear feedback shift register that can generate the sequence, which is the smallest value of L to satisfy the feedback function $s_j + c_1 s_{j-1} + \cdots + c_L s_{j-L} = 0, j \geqslant L$, with coefficients $c_1, c_2, \cdots, c_L \in F_{p^n}$. The Berlekamp-Massey algorithm[1] states that if $L(S^\infty) > N/2$ (N is the least period of $\{S^\infty\}$), $\{S^\infty\}$ will be considered good with respect to its linear complexity. Let $S(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_{N-1} \cdot x^{N-1}$. If N is the period of $\{S^\infty\}$, then

$$m(x) = (1 - x^N)/\gcd(S(x), 1 - x^N)$$

is called the minimal polynomial of $\{S^\infty\}$[2,3]. Thus the linear complexity of $\{S^\infty\}$ with the period N can be calculated by

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

The generalized cyclotomic numbers were first introduced in 1962 by Whiteman[4] in order to investigate the existence of cyclic difference sets in ring Z_{pq} and the integer ring modulo pq, here, p, q are two odd primes. A difference set in a group G is a combinatorial structure which admits a regular automorphism group. The development of a difference set is a symmetric design. At first, people use these structures to present some experiments designs. In 1970's, it was found that these objects could be used to construct some new sequences with some cryptographic properties, for example, to defense the differential and correlation attack. Following this approach, Ding and Helleseth[5] presented generalized cyclotomy with respect to a positive integer n and gave some applications of these cyclotomic sequences. Since then, a large number of cyclotomic sequences have been constructed and the linear complexity and the autocorrelation values of these generalized cyclotomic sequences have been obtained. For example, Ding, Helleseth, and Shan[6] determined the linear complexity of Legendre sequences were actually based on cyclotomic classes of order two. The linear complexity of some generalized cyclotomic sequences of length pq were obtained by Ding[7] and Bai[8,9],

Foundation items: Supported by the Natural Science Foundation of Hubei Province (2009CDZ004); the Scientific Research Fund of Hubei Provincial Education Department (B20104403).

* **Corresponding author**: Wang Hongwei, Associate Professor, E-mail: hswhw123@163.com.

respectively. Yan, et al[10] calculated the linear complexity of generalized cyclotomic sequence with period p^m. Yan[11] also determined the linear complexity of a new prime-square sequence and a two-prime sequence. The linear complexity of generalized cyclotomic sequence with period p^{n+1} was determined recently by Edemskiy[12], Zhang, et al.[13] also calculated the linear complexity of generalized cyclotomic sequence with period $2p^m$.

In this paper, we introduce a generalized cyclotomic binary sequence S of order two with the length of $2pq$. Then, we calculate its linear complexity and minimal polynomial. The results show that the linear complexity of the sequences S is high.

The main difference between the presented work and the previous researches is that we deal with the even factor 2 of the length of the sequences. As we all know that, in most cases, how to deal with the even factor 2 is a hard work. The high light of our work is to show that there exists a common primitive element g of Z_p, Z_q, Z_{2p} and Z_{2q}, where g is an odd number. Using this fact, we can find the decomposition of the units group in the rings Z_p, Z_q, Z_{2p} and Z_{2q}, respectively, and then, we can construct our sequences explicitly. By a detailed analysis on the represents of the elements in the sequences, the linear complexity of these sequences can be obtained.

2 New Generalized Cyclotomy and Sequence

We use Z_N to denote the ring $Z_N=\{0,1,2,\cdots,n-1\}$ with integer addition modulo N and integer multiplication modulo N as the ring operations. By Z_N^* we denote the set of all invertible elements of the residue class ring Z_N. It is well-known that Z_N^* is a cyclic group if and only if $N=2,4,p^m,2p^m$ for a prime number p and a positive integer m. Further, if $Z_N^*=(g)$ is generated by an element g, then g is called a primitive element of Z_N. Let p and q be two distinct odd primes with $\gcd(p-1,q-1)=2$. Define $N=2pq$ and $e=(p-1)(q-1)/2$.

The following so called generalized chinese remainder theorem will be used frequently in our discussion.

Lemma 1 Generalized chinese remainder theorem: Let $m_1,\cdots,m_t$ be positive integers. For a set of integers $a_1,\cdots,a_t$, the system of congruencies: $x\equiv a_i \bmod m_i, i=1,\cdots,t$, has solutions if and only if

$$a_i\equiv a_j \bmod \gcd(m_i,m_j), i\neq j, 1\leqslant i,j\leqslant t$$

If Lemma 1 is satisfied, the solution is unique modulo $\mathrm{lcm}(m_1,\cdots,m_t)$.

The proof of Lemma 1 is detailed in Ref. [14].

By Lemma1, there exists a common primitive element g of Z_p, Z_q and Z_{2p} and Z_{2q}, and g is an odd number. Therefore, $\mathrm{ord}_N(g)=\mathrm{lcm}(\mathrm{ord}_p(g),\mathrm{ord}_{2q}(g))=\mathrm{lcm}(p-1,q-1)=(p-1)(q-1)/2=e$, where $\mathrm{ord}_N(g)$ denotes the order of g modulo N. Let x be an integer satisfying $x\equiv g \bmod 2p$ and $x\equiv 1 \bmod 2q$. The existence and uniqueness of $x \bmod 2pq$ is guaranteed by the generalized chinese remainder theorem. It is easy to prove that $x\equiv g \bmod p$ and $x\equiv 1 \bmod q$, then $x\equiv 1 \bmod 2$.

Whiteman proved that[11]

$$Z_N^*=\{g^s x^i: s=0,1,\cdots,e-1; i=0,1\}$$

Ding and Helleseth's generalized cyclotomic classes $D_0^{(N)}$ and $D_1^{(N)}$ of order two are defined by

$$D_0^{(N)}=\{g^{2s}: s=0,1,\cdots,(e-2)/2\}\cup\{g^{2s}x: s=0,1,\cdots,(e-2)/2\}$$

$$D_1^{(N)}=\{g^{2s+1}: s=0,1,\cdots,(e-2)/2\}\cup\{g^{2s+1}x: s=0,1,\cdots,(e-2)/2\}$$

where the multiplication is that of Z_N. It is easy to prove that

$$Z_N^*=D_0^{(N)}\cup D_1^{(N)},\ D_0^{(N)}\cap D_1^{(N)}=\varphi$$

where φ denotes the empty set. Similarly

$$Z_{pq}^*=\{g^s x^i: s=0,1,\cdots,e-1; i=0,1\}$$

$$D_0^{(pq)}=\{g^{2s}: s=0,1,\cdots,(e-2)/2\}\cup\{g^{2s}x: s=0,1,\cdots,(e-2)/2\}$$

$$D_1^{(pq)}=\{g^{2s+1}: s=0,1,\cdots,(e-2)/2\}\cup\{g^{2s+1}x: s=0,1,\cdots,(e-2)/2\}$$

where the operation is that of Z_{pq}. It is easy to prove that

$$Z_{pq}^*=D_0^{(pq)}\cup D_1^{(pq)}, D_0^{(pq)}\cap D_1^{(pq)}=\varphi$$

The above decompositions are detailed in

Ref. [5].

Let F be a subset of Z_N and let a be an element of Z_N. Define

$$a+F=\{a+f:f\in F\}$$
$$a\cdot F=\{a\cdot f:f\in F\}$$

and

$$D_0^{(P)}=\{g^{2s}:s=0,1,\cdots,(p-3)/2\}$$
$$D_0^{(q)}=\{g^{2s}:s=0,1,\cdots,(q-3)/2\}$$
$$D_0^{(2p)}=\{g^{2s}:s=0,1,\cdots,(p-3)/2\}$$
$$D_0^{(2q)}=\{g^{2s}:s=0,1,\cdots,(q-3)/2\}$$
$$D_1^{(p)}=gD_0^{(P)},\ D_1^{(q)}=gD_0^{(q)}$$
$$D_1^{(2p)}=gD_0^{(2p)},\ D_1^{(2q)}=gD_0^{(2q)}$$

Denote

$$P_0=pD_0^{(2q)},\ P_1=pD_1^{(2q)},\ P'_0=2pD_0^{(q)}$$
$$P'_1=2pD_1^{(q)},\ Q_0=qD_0^{(2p)},\ Q_1=qD_1^{(2p)}$$
$$Q'_0=2qD_0^{(P)},\ Q'_1=2qD_1^{(p)},\ D_0=D_0^{(N)}$$
$$D_1=D_1^{(N)},\ D'_0=2D_0^{(pq)},\ D'_1=2D_1^{(pq)}$$

and

$$P=P_0\cup P_1,\ P'=p'_0\cup p'_1$$
$$Q=Q_0\cup Q_1,\ Q'=Q'_0\cup Q'_1$$

It is easy to prove that

$$Z_N=Z_N^*\cup P\cup P'\cup Q\cup Q'\cup 2Z_{pq}^*\cup\{pq\}\cup\{0\}$$

where $Z_N^*,P,P',Q,Q',2Z_{pq}^*,\{pq\},\{0\}$ are pairwise null-intersection.

Define

$$C_0=P_0\cup p'_0\cup Q\cup Q'_0\cup D_0\cup D'_0\cup\{pq\}\cup\{0\}$$
$$C_1=P_1\cup p'_1\cup Q'_1\cup D_1\cup D'_1$$

Then

$$C_0\cup C_1=Z_N,C_0\cap C_1=\varphi$$

We define a new generalized cyclotomic sequences $S=\{s_i\}$ of order two of length $2pq$ as

$$s_i=\begin{cases}0 & i \bmod N\in C_0\\ 1 & \text{Otherwise}\end{cases}$$

The sequence S has period N. In one period of sequence S, there are $pq+(p+1)/2$ zeroes and $pq(p+1)/2$ ones. Thus, the sequence S has an imbalance $p+1$.

3 Linear Complexity and Minimal Polynomial of S

Now we begin to calculate the linear complexity and minimal polynomial of the new generalized cyclotomic sequence S. Let the symbols be the same as before. Then for S, the corresponding $S(x)$ is given by

$$S(x)=\sum_{i\in C_1}x^i=$$
$$(\sum_{i\in P_1}+\sum_{i\in P'_1}+\sum_{i\in Q'_1}+\sum_{i\in D_1}+\sum_{i\in D'_1})x^i\in F_2[x]$$

Let m be the order of 2 modulo pq. Then there exists a primitive pq-th root of unity α over the splitting field F_{2^m} of $x^{pq}-1$. The linear complexity of the sequence is then given by $L(S)=N-|\{j:S(\alpha_j)=0,0\leqslant j\leqslant N-1\}|$. Note that

$$0=\alpha^{pq}-1=\alpha^N-1=(\alpha^{2p})^q-1=$$
$$(\alpha^p-1)(1+\alpha^p+\alpha^{2p}+\cdots+\alpha^{(2q-1)p})$$

And it follows that

$$\sum_{i\in p}\alpha^i=(\sum_{i\in p_0}+\sum_{i\in P_1})\alpha^i=1$$

By symmetry, we obtain

$$\sum_{i\in P'}\alpha^i=(\sum_{i\in P'_0}+\sum_{i\in P'_1})\alpha^i=1$$
$$\sum_{i\in Q}\alpha^i=(\sum_{i\in Q_0}+\sum_{i\in Q_1})\alpha^i=1$$
$$\sum_{i\in Q'}\alpha^i=(\sum_{i\in Q'_0}+\sum_{i\in Q'_1})\alpha^i=1$$
$$\sum_{i\in p_q^*}\alpha^i=(\sum_{i\in pD_0^{(q)}}+\sum_{i\in pD_1^{(q)}})\alpha^i=1$$
$$\sum_{i\in q_p^*}\alpha^i=(\sum_{i\in qD_0^{(p)}}+\sum_{i\in qD_1^p})\alpha^i=1$$

Lemma 2 Let $a\in D_j$. Then $aD_i=D_{(i+j)\bmod 2}$, where $i,j=0,1$[5].

Similar to Lemma 2 in Ref. [2], we have the following result.

Lemma 3 Let the symbols be the same as before. Then

$$\sum_{i\in D_1}\alpha^{ti}=$$
$$\begin{cases}0 & t\in P\cup P'\cup\{pq\}\\ (q-1)/2(b \bmod 2) & t\in Q\cup Q'\end{cases}$$

Proof Suppose that $t\in P$. Since g is a common primitive root of both p and $2q$ and the order of g modulo pq is e, by the definition of x we have

$$D_1 \bmod q=\{g^{2s+1} \bmod q:s=0,1,\cdots,(e-2)/2\}\cup\{g^{2s+1}x \bmod q:s=0,1,\cdots,(e-2)/2\}=\{g^{2s+1}:s=0,1,\cdots,(e-2)/2\} \bmod q=D_1^{(q)}$$

When s ranges over $\{0,1,\cdots,(e-2)/2\}$,

$D_1 \bmod q$ takes on each element of $D_1^{(q)}$ $(p-1)$ times.

It follows

$$\sum_{i\in D_1}\alpha^{ti}=((p-1) \bmod 2)\sum_{i\in D_1^{(q)}}\alpha^{ti}=0$$

Similarly, suppose $t\in P'$, then

$$D_1 \bmod q=$$
$$\{g^{2s+1} \bmod q: s=0,1,\cdots,(e-2)/2\}\cup$$
$$\{g^{2s+1}x \bmod q: s=0,1,\cdots,(e-2)/2\}=$$
$$\{g^{2s+1}: s=0,1,\cdots,(e-2)/2\} \bmod q=D_1^{(q)}$$

When s ranges over $\{0,1,\cdots,(e-2)/2\}$, $D_1 \bmod q$ takes on each element of $D_1^{(q)}$ $(p-1)$ times.

We have

$$\sum_{i\in D_1}\alpha^{ti}=((p-1) \bmod 2)\sum_{i\in D_1^{(q)}}\alpha^{ti}=0$$

Suppose $t\in Q$, then

$$D_1 \bmod p=\{g^{2s+1} \bmod p:$$
$$s=0,1,\cdots,(e-2)/2\}\cup$$
$$\{g^{2s+1}x \bmod p: s=0,1,\cdots,(e-2)/2\}=$$
$$\{g^{2s+1}: s=0,1,\cdots,(e-2)/2\}(\bmod p)\cup$$
$$\{g^{2s+2}: s=0,1,\cdots,(e-2)/2\}(\bmod p)=Z_p^*$$

When s ranges over $\{0,1,\cdots,(e-2)/2\}$, $D_1 \bmod p$ takes on each element of Z_p^* $(q-1)/2$ times.

Hence, $\sum_{i\in D_1}\alpha^{ti}=((q-1)/2 \bmod 2)\sum_{i\in qZ_p^*}\alpha^{i}=(q-1)/2 \bmod 2$.

Suppose $t\in Q'$, then

$$D_1 \bmod p=\{g^{2s+1} \bmod p:$$
$$s=0,1,\cdots,(e-2)/2\}\cup$$
$$\{g^{2s+1}x \bmod p: s=0,1,\cdots,(e-2)/2\}=$$
$$\{g^{2s+1}: s=0,1,\cdots,(e-2)/2\} \bmod p\cup$$
$$\{g^{2s+2}: s=0,1,\cdots,(e-2)/2\} \bmod p=Z_p^*$$

When s ranges over $\{0,1,\cdots,(e-2)/2\}$, $D_1 \bmod p$ takes on each element of Z_p^* $(q-1)/2$ times.

Therefore

$$\sum_{i\in D_1}\alpha^{ti}=((q-1)/2 \bmod 2)\sum_{i\in Q'}\alpha^{i}=$$
$$(q-1)/2 \bmod 2$$

Suppose $t=pq$, then

$$\sum_{i\in D_1}\alpha^{ti}=\sum_{i\in D_1}1=e \bmod 2=0$$

Lemma 4 Let the symbols be defined as the same as before. Then

$$\sum_{i\in D_1'}\alpha^{ti}=$$
$$\begin{cases}0 & t\in P\cup P'\cup\{pq\}\\ (q-1)/2 \bmod 2 & t\in Q\cup Q'\end{cases}$$

Proof It can be proved in the same way as that for Lemma 3.

Lemma 5 Let the symbols be the same as before. If $t\in Z_N^*\cup 2Z_{pq}^*$, then

$$S(\alpha^t)=$$
$$\begin{cases}S(\alpha) & t\in Z_N^*\cup 2Z_{pq}^*,\ t \bmod p\in D_0^{(p)}\\ S(\alpha)+1 & t\in Z_N^*\cup 2Z_{pq}^*,\ t \bmod p\in D_1^{(p)}\end{cases}$$

Proof Similar to the proof for Lemma 3, we omit it here.

Lemma 6 $S(\alpha)\in\{0,1\}$ if and only if $p\equiv\pm1 \bmod 8$.

Proof Since the characteristic of the field F_{2^m} is 2, it follows that $[S(\alpha)]^2=S(\alpha^2)$. From Lemma 5, we obtain $S(\alpha^2)=S(\alpha)$ if and only if $2\in D_0^{(p)}$. Hence, $S(\alpha)\in\{0,1\}$ if and only if $2\in D_0^{(p)}$. Note that $D_0^{(p)}$ is the set of quadratic residues modulo p, thus, $2\in D_0^{(p)}$ if and only if $p\equiv\pm1 \bmod 8$

Lemma 7

(1) If $t\in P\cup P'$, $\sum_{i\in P_1'}\alpha^{ti}\in\{0,1\}$ if and only if $q\equiv\pm1 \bmod 8$, $\sum_{i\in pD_1^{(q)}}\alpha^{ti}\in\{0,1\}$ if and only if $q\equiv\pm1 \bmod 8$.

(2) If $t\in Q\cup Q'$, $\sum_{i\in Q'_1}\alpha^{ti}\in\{0,1\}$ if and only if $p\equiv\pm1 \bmod 8$, $\sum_{i\in qD_1^{(p)}}\alpha^{ti}\in\{0,1\}$ if and only if $p\equiv\pm1 \bmod 8$.

Proof If $t\in P$, $\sum_{i\in P_1'}\alpha^{ti}=\sum_{i\in D_1^{(q)}}(\alpha^{2p^2})^{si}$ $(s\in Z_{2q}^*)$. Let $\beta=\alpha^{2p^2}$, then β is a primitive qth root of unity in the splitting field of x^q-1. Since the characteristic of the field F_{2^m} is 2, it follows that $(\sum_{i\in P_1'}\alpha^{ti})^2=\sum_{i\in P_1'}\alpha^{2ti}=\sum_{i\in 2p\cdot 2D_1^{(q)}}\alpha^{ti}$. Note that $\sum_{i\in 2p\cdot 2D_1^{(q)}}\alpha^{ti}=\sum_{i\in 2p2D_1^{(q)}}\alpha^{ti}=\sum_{i\in P_1'}\alpha^{ti}$ if and only if $2\in D_0^{(q)}$, also note that $D_0^{(q)}$ is the set of quadratic residues modulo q. Thus, we obtain $\sum_{i\in P_1'}\alpha^{ti}\in\{0,1\}$ if and only if $q\equiv\pm1 \bmod 8$. The rest of the

conclusion of this lemma can be similarly proved.

Lemma 8

$$S(\alpha^t)=\begin{cases}(\sum_{i\in pD_1^{(q)}}+\sum_{i\in P_1'})\alpha^{ti}+(p-1)/2 \bmod 2 & t\in P\cup P'\\ \sum_{i\in Q_1'}\alpha^{ti} & t\in Q\cup Q'\\ (p-1)/2(b \bmod 2) & t=pq \text{ or } 0\end{cases}$$

Proof If $t\in P\cup P'$, from Lemmas 3－5 and $|D_1^{(2q)}|=|D_1^{(q)}|$, $D_1^{(2q)} \bmod q = D_1^{(q)}$, we obtain

$$S(\alpha^t)=(\sum_{i\in P_1}+\sum_{i\in P_1'}+\sum_{i\in Q_1'}+\sum_{i\in D_1}+\sum_{i\in D_1'})\alpha^{ti}=$$
$$\sum_{i\in P_1}\alpha^{ti}+\sum_{i\in P_1'}\alpha^{ti}+\sum_{i\in D_1^{(p)}}1+0+0=$$
$$\sum_{i\in P_1}\alpha^{ti}+\sum_{i\in P_1'}\alpha^{ti}+(p-1)/2+0+0=$$
$$\sum_{i\in pD_1^{(q)}}\alpha^{ti}+\sum_{i\in P_1'}\alpha^{ti}+(p-1)/2=$$
$$(\sum_{i\in pD_1^{(q)}}+\sum_{i\in P_1'})\alpha^{ti}+(p-1)/2$$

Therefore, if $t\in P\cup P'$, $S(\alpha^t)=(\sum_{i\in pD_1^{(q)}}+\sum_{i\in P_1'})\alpha^{ti}+(p-1)/2$.

If $t\in Q\cup Q'$, from Lemmas 3－5 and $|D_1^{(2p)}|=|D_1^{(p)}|$, $D_1^{(2p)} \bmod p = D_1^{(p)}$, we know that

$$S(\alpha^t)=(\sum_{i\in P_1}+\sum_{i\in P_1'}+\sum_{i\in Q_1'}+\sum_{i\in D_1}+\sum_{i\in D_1'})\alpha^{ti}=$$
$$\sum_{i\in D_1^{(2q)}}1+\sum_{i\in D_1^q}1+\sum_{i\in Q_1'}\alpha^{ti}+(q-1)/2+(q-1)/2=$$
$$(q-1)/2+(q-1)/2+\sum_{i\in Q_1'}\alpha^{ti}+(q-1)/2+$$
$$(q-1)/2=\sum_{i\in Q_1'}\alpha^{ti}$$

Thus, If $t\in Q\cup Q'$, $S(\alpha^t)=\sum_{i\in Q_1'}\alpha^{ti}$.

If $t=pq$, from Lemmas 3－5, we get

$$S(\alpha^t)=(\sum_{i\in P_1}+\sum_{i\in P_1'}+\sum_{i\in Q_1'}+\sum_{i\in D_1}+\sum_{i\in D_1'})\alpha^{ti}=$$
$$(q-1)/2+(q-1)/2+(p-1)/2+0+0=$$
$$(p-1)/2 \bmod 2$$

We also note that

$S(1)=(q-1)/2+(q-1)/2+(p-1)/2+e+e=(p-1)/2 \bmod 2$

This completes the Proof.

The main results of sequence S are summarized in the following two theorems.

Define

$$d_1(x)=\prod_{i\in P\cup P'}(x-\alpha^i)$$

Theorem 1

(1) If $p\equiv 3 \bmod 8$, then

$$L(S)=2pq,\ m(x)=x^{2pq}-1$$

(2) If $p\equiv 5 \bmod 8$ and $q\equiv\pm 3 \bmod 8$, then

$$L(S)=2pq-2,\ m(x)=(x^{2pq}-1)/(x^2+1)$$

(3) If $p\equiv 5 \bmod 8$ and $q\equiv\pm 1 \bmod 8$, then

$$L(S)=2pq-2q,\ m(x)=(x^{2pq}-1)/(x^2+1)d_1(x)$$

Proof For case (1) in Theorem 1 suppose $p\equiv 3 \bmod 8$ and $q\equiv\pm 3 \bmod 8$, using Lemmas 5－8, we obtain $\gcd(x^{2pq}-1, S(x))=1$, then $m(x)=x^{2pq}-1$, $L(S)=2pq$. Suppose $p\equiv 3 \bmod 8$ and $q\equiv\pm 1 \bmod 8$, then $2\in D_1^{(p)}$, $2\in D_0^{(q)}$. From the discussion of Ref. [6], for all α, exactly one of $\sum_{i\in pD_1^{(q)}}\alpha^{ti}(t\in P_0\cup P'_0)$ and $\sum_{i\in pD_1^{(q)}}\alpha^{ti}(t\in P_1\cup P'_1)$ is zero.

We fix α such that $\sum_{i\in pD_1^{(q)}}\alpha^{ti}=0$ $(t\in P_0\cup P'_0)$, then $\sum_{i\in pD_1^{(q)}}\alpha^{ti}=1$ $(t\in P_1\cup P'_1)$. Note $\sum_{i\in p'}\alpha^{ti}=(\sum_{i\in pD_1^{(q)}}\alpha^{ti})^2$ from Lemma 8 we obtain

$$S(\alpha^t)=(\sum_{i\in pD_1^{(q)}}+\sum_{i\in P_1'})\alpha^{ti}+(p-1)/2 \bmod 2=1 \quad t\in P_0\cup P'_0$$
$$S(\alpha^t)=(\sum_{i\in pD_1^{(q)}}+\sum_{i\in P_1'})\alpha^{ti}+(p-1)/2 \bmod 2=1 \quad t\in P_1\cup P'_1$$

Using Lemmas 5－8, we obtain

$$S(\alpha^t)\begin{cases}\neq 0 & t\in 2Z_{pq}^*\cup Z_N^*\cup Q\cup Q'\\ =1 & t\in P\cup P' \text{(by the choice of } \alpha)\\ =1 & t=pq \text{ or } 0\end{cases}$$

Hence, $\gcd(x^{2pq}-1, S(x))=1$, then $m(x)=x^{2pq}-1$, $L(S)=2pq$.

For case (2) in Theorem 1, suppose $p\equiv 5 \bmod 8$ and $q\equiv\pm 3 \bmod 8$, using Lemmas 5－8, we obtain

$$S(\alpha^t)\begin{cases}=0 & t=pq \text{ or } 0\\ \neq 0 & \text{Otherwise}\end{cases}$$

Therefore $\gcd(x^{2pq}-1, S(x))=(x^2+1)$, then $m(x)=(x^{2pq}-1)/(x^2+1)$, $L(S)=2pq-2$.

For case (3) in Theorem 1, suppose $p\equiv 5 \bmod 8$ and $q\equiv\pm 1 \bmod 8$, then $2\in D_1^{(p)}$, $2\in D_0^{(q)}$.

From the discussion of Ref. [6], for all α, exactly

one of $\sum_{i\in pD_1^{(q)}}\alpha^{ti}(t\in P_0\cup P_0')$ and $\sum_{i\in pD_1^{(q)}}\alpha^{ti}(t\in P_1\cup P_1')$ is zero.

We fix α such that $\sum_{i\in pD_1^{(q)}}\alpha^{ti}=0, t\in P_1\cup P_1'$, then $\sum_{i\in pD_1^{(q)}}\alpha^{ti}=1, t\in P_0\cup P_0'$. Note $\sum_{i\in P_1'}\alpha^{ti}=\left(\sum_{i\in pD_1^{(q)}}\alpha^{ti}\right)^2$ from Lemma 8, we obtain

$$S(\alpha^t)=\left(\sum_{i\in pD_1^{(q)}}+\sum_{i\in P_1'}\right)\alpha^{ti}+(p-1)/2 \bmod 2=0 \quad (t\in P_0\cup P_0')$$

$$S(\alpha^t)=\left(\sum_{i\in pD_1^{(q)}}+\sum_{i\in P_1'}\right)\alpha^{ti}+(p-1)/2 \bmod 2=0 \quad (t\in P_1\cup P_1')$$

Using Lemmas 5—8, we obtain

$$S(\alpha^t)\begin{cases}\neq 0 & t\in 2Z_{pq}^*\cup Z_N^*\cup Q\cup Q'\\ =0 & t\in P\cup P'\text{(by the choice of }\alpha)\end{cases}$$

Therefore, $\gcd(x^{2pq}-1, S(x))=(x^2+1)d_1(x)$, then $m(x)=(x^{2pq}-1)/(x^2+1)d_1(x)$, $L(S)=2pq-2q$.

Define

$$d_2(x)=\prod_{i\in 2Z_{pq}^*\cup Z_N^*, i \bmod p\in D_0^{(p)}}(x-\alpha^i), d_3(x)=\prod_{i\in Q_1\cup Q_1'}(x-\alpha^i)$$

Theorem 2 (1) If $p\equiv 1 \bmod 8$ and $q\equiv\pm 3 \bmod 8$, then

$$L(S)=2pq-2e-p-1$$

$$m(x)=(x^{2pq}-1)/(x^2+1)d_2(x)d_3(x)$$

(2) If $p\equiv 1 \bmod 8$ and $q\equiv\pm 1 \bmod 8$, then

$$L(S)=pq-q, m(x)=(x^{2pq}-1)/(x^2+1)d_1(x)d_2(x)d_3(x)$$

(3) If $p\equiv 7 \bmod 8$, then

$$L(S)=2pq-2e-p+1, m(x)=(x^{2pq}-1)/d_2(x)d_3(x)$$

Proof Similar to the proof of Theorem 1, the detail of which is omitted.

Note that since the coefficients of $d_1(x)$, $d_2(x)$ and $d_3(x)$ are invariant under the Frobenius action, $d_1(x), d_2(x), d_3(x)\in F_2[x]$.

4 Efficiency Validation

By using Magma, we check every case in our paper. In the following, one example of the sequence is given to illustrate the efficiency of our method; the experimental results coincide with the results presented in the article completely.

Let $p=19, q=17, g=3, x=307$. Then it is easy to verify this meet all the conditions of Theorem 1 case (1) that we need. In this case, the sequence is

$S=[0,0,0,1,0,1,1,1,0,0,1,1,1,0,1,0,0,$
$0,0,0,1,0,1,1,1,0,0,1,1,1,0,1,0,0,0,0,0,1,$
$0,1,1,1,0,0,1,1,1,0,1,0,0,0,0,0,1,0,1,1,1,$
$0,0,1,1,1,0,1,0,0,1,0,0,1,0,1,1,1,0,0,1,1,$
$1,0,1,0,0,0,0,0,1,0,1,1,1,0,0,1,1,1,0,1,0,$
$0,1,0,0,1,0,1,1,1,0,0,1,1,1,0,1,0,0,0,0,0,$
$1,0,1,1,1,0,0,1,1,1,0,1,0,0,0,0,0,1,0,1,1,$
$1,0,0,1,1,1,0,1,0,0,0,0,0,1,0,1,1,1,0,0,1,$
$1,1,0,1,0,0,0,0,0,1,0,1,1,1,0,0,1,1,1,0,1,$
$0,0,0,0,0,1,0,1,1,1,0,0,1,1,1,0,1,0,0,0,0,$
$0,1,0,1,1,1,0,0,1,1,1,0,1,0,0,0,0,0,1,0,1,$
$1,1,0,0,1,1,1,0,1,0,0,0,0,0,1,0,1,1,1,0,0,$
$1,1,1,0,1,0,0,0,0,0,1,0,1,1,1,0,0,1,1,1,0,$
$1,0,0,1,0,0,1,0,1,1,1,0,0,1,1,1,0,1,0,0,0,$
$0,0,1,0,1,1,1,0,0,1,1,1,0,1,0,0,0,0,0,1,0,$
$1,1,1,0,0,1,1,1,0,1,0,0,0,0,0,1,0,1,1,1,0,$
$0,1,1,1,0,1,0,0,1,0,0,1,0,1,1,1,0,0,1,1,1,$
$0,1,0,0,0,0,0,1,0,1,1,1,0,0,1,1,1,0,1,0,0,$
$0,0,0,1,0,1,1,1,0,0,1,1,0,0,0,0,0,0,0,0,0,$
$0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,1,0,1,1,1,$
$0,0,1,1,1,0,1,0,0,0,0,0,1,0,1,1,1,0,0,1,1,$
$1,0,1,0,0,1,0,0,1,0,1,1,1,0,0,1,1,1,0,1,0,$
$0,0,0,0,1,0,1,1,1,0,0,1,1,1,0,1,0,0,0,0,0,$
$1,0,1,1,1,0,0,1,1,1,0,1,0,0,0,0,0,1,0,1,1,$
$1,0,0,1,1,1,0,1,0,0,1,0,0,1,0,1,1,1,0,0,1,$
$1,1,0,1,0,0,0,0,0,1,0,1,1,1,0,0,1,1,1,0,1,$
$0,0,0,0,0,1,0,1,1,1,0,0,1,1,1,0,1,0,0,0,0,$
$0,1,0,1,1,1,0,0,1,1,1,0,1,0,0,0,0,0,1,0,1,$
$1,1,0,0,1,1,1,0,1,0,0,0,0,0,1,0,1,1,1,0,0,$
$1,1,1,0,1,0,0,1,0,0,1,0,1,1,1,0,0,1,1,1,0,$
$1,0,0,0,0,0,1,0,1,1,1,0,0,1,1,1,0,1,0,0]$

The minimal polynomial of sequence as above is $m(x)=x^{646}-1$ and the linear complexity is $L(S)=646$.

5 Conclusions

We propose a new generalized cyclotomic binary sequence of length $2pq$. Then, we determined its linear complexity and minimal polyno-

mial. The results show that the linear complexity of the sequences S depends on the values of (p mod 8) and (q mod 8). Consequently, the proposed sequence is "good" in terms of its linear complexity and may be attractive for applications in cryptography and communication.

Acknowledgement

We would like to express our grateful thankfulness to the two reviewers for their valuable comments and suggestions.

References:

[1] Massey J L. Shift register synthesis and BCH decoding[J]. IEEE Trans Inform Theory, 1969, 15: 122-127.

[2] Ding C S, Xiao G Z, Shan W J. The stability theory of stream cipher [M]. LNCS 561, Heidelberg: Springer-Verlag, 1991: 251-321.

[3] Lidl R, Niederreiter H. Finite fields [M]. Second edition. UK: Cambridge University Press, 1997: 394-438.

[4] Whiteman A L. A family of difference sets[J]. Illinois J, 1962, 6(1): 107-121.

[5] Ding C S, Helleseth T. New generalized cyclotomy and its applications[J]. Finite Fields Appl, 1998, 4(2): 140-166.

[6] Ding C S, Helleseth T, Shan W J. On the linear complexity of Legendre sequences[J]. IEEE Trans Inform Theory, 1998, 44(3): 1276-1278.

[7] Ding C S. Linear complexity of generalized cyclotomic binary sequences of order 2[J]. Finite Fields Appl, 1997, 3(2): 159-174.

[8] Bai E J, Liu X J, Xiao G Z. Linear complexity of new generalized cyclotomic sequences of order two of length pq[J]. IEEE Trans Inform Theory, 2005, 51(1): 1849-1854.

[9] Bai E J, Fu X T, Xiao G Z. On the linear complexity of new generalized cyclotomic sequences of order four over Z_{pq}^{*}[J]. IEICE Trans Fund, 2005, 88(1): 392-395.

[10] Yan T J, Li S Q, Xiao G Z. On the linear complexity of generalized cyclotomic sequences with period p^m[J]. Mathematics Letters, 2008, 21(2): 187-193.

[11] Yan T J, Sun R, Xiao G Z. Autocorrelation and linear complexity of the new generalized cyclotomic sequences[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2007, 9(4): 857-864

[12] Edemskiy V. About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1}[J]. Des Codes Cryptogr, 2011, 61(3): 251-260.

[13] Zhang J W, Zhao C A, Ma X. Linear complexity of generalized cyclotomic binary sequences of length $2p^m$[J]. AAECC, 2010, 21(2): 93-108.

[14] Ding C S, Pei T, Salomaa A. Chinese remainder theorem: Applications in computing, coding, crypotography[M]. Singapore: World Scientific, Section 2.4, 1996: 2-10.

(Executive editor: Zhang Bei)