Vol. 40 (2020)
No. 2

数 学 杂 志
J. of Math. (PRC)

LINEAR COMPLEXITY OF GENERALIZED CYCLOTOMIC BINARY SEQUENCES OF PERIOD pq

YANG Bo[1,2], DU Tian-qi[2], XIAO Zi-bi[2]

(*1.Hubei Province Key Laboratory of Systems Science in Metallurgical Process, Wuhan University of Science and Technology, Wuhan 430081, China*)

(*2.College of Science, Wuhan University of Science and Technology, Wuhan 430081, China*)

Abstract: In this paper, a class of generalized cyclotomic binary sequences of period pq is proposed, where p and q are two distinct odd primes. By using Whiteman's generalized cyclotomy of order 4 and classic cyclotomy of order 2, the sequences are almost balanced and the exact value of their linear complexity is calculated, which shows that the proposed sequences are quite good in terms of the linear complexity.

Keywords: binary sequence; linear complexity; cyclotomy; generalized cyclotomic sequence

2010 MR Subject Classification: 11T22; 11T55; 94A55; 94A60

Document code: A **Article ID:** 0255-7797(2020)02-0139-10

1 Introduction

Pseudo-random sequences were widely used in communication and cryptographic systems. For the application of stream cipher, the keystream sequences had unpredictability and randomness [1]. One of the important indexes for measuring these properties is linear complexity of sequence, which is defined to be the length of the shortest linear feedback shift register that can generate the given sequence. Generally speaking, a sequence with large linear complexity (at least a half of its period) is considered to be favorable for cryptography to resist the well-known Berlekamp-Massey algorithm.

For an integer $N \geq 2$, let $\mathbb{Z}_N = \{0, 1, \cdots, N-1\}$ denote the ring of integers modulo N and $\mathbb{Z}_N^*$ denote the set of all invertible elements of $\mathbb{Z}_N$. Let $\{D_0, D_1, \cdots, D_{d-1}\}$ be a partition of $\mathbb{Z}_N^*$. If D_0 is a multiplicative subgroup of $\mathbb{Z}_N^*$ and there exist elements $g_i \in \mathbb{Z}_N^*$ such that $D_i = g_i D_0$ for all $i \in \{1, 2, \cdots, d-1\}$, then for prime (composite) N, these D_i are called classical (generalized) cyclotomic classes of order d with respect to N.

Using classical cyclotomy or generalized cyclotomy to construct sequences is an effective method to obtain sequences with large linear complexity. The linear complexity and autocorrelation property of generalized cyclotomic sequences with various period were extensively

* **Received date:** 2018-11-11 **Accepted date:** 2019-02-20

Foundation item: Supported by Hubei Province Key Laboratory of Systems Science in Metallurgical Process (Wuhan University of Science and Technology) (Y201707).

Biography: Yang Bo(1973–), male, born at Xiaogan, Hubei, associate professor, major in algebraic coding theory and cryptography.

studied in the literature (see [2–7]). In this paper, we focus on the generalized cyclotomic binary sequences of period pq.

The generalized cyclotomic binary sequences of period pq are by far constructed on the basis of Whiteman's generalized cyclotomic classes or Ding-Helleseth generalized cyclotomic classes which are proposed in [8] and [9], respectively. Most of these sequences have large linear complexity. A brief review of these sequences are provided in Section 2. In this paper, a class of new generalized cyclotomic binary sequences of period pq based on Whiteman's generalized cyclotomy of order 4 and classic cyclotomy of order 2 is proposed. By using the classic method for calculating the linear complexity described in [10], we determine the exact value of the linear complexity of such sequences. Our results show that the proposed sequences have large linear complexity.

2 Preliminary

In this section, we first recall the two types of generalized cyclotomy with respect to pq and the known generalized cyclotomic sequences of period pq, and then define a class of new generalized cyclotomic sequences of period pq.

Let $N = pq$, where p and q are distinct odd primes with $\gcd(p-1, q-1) = d$. Define $e = \frac{(p-1)(q-1)}{d}$. Let g be a fixed primitive root of both p and q. Then $\mathrm{ord}_N(g) = \mathrm{lcm}(p-1, q-1) = e$. Let x be an integer satisfying $x \equiv g \pmod{p}$, $x \equiv 1 \pmod{q}$. Whiteman proved in [8] that

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

Whiteman's generalized cyclotomic classes of order d with respect to pq are defined by [8]

$$D_i = \left\{ g^s x^i \pmod{pq} \ :\ s = 0, 1, \cdots, e-1 \right\}, \quad i = 0, 1, \cdots, d-1. \tag{2.1}$$

Ding-Helleseth generalized cyclotomic classes of order d with respect to pq are defined by [9]

$$D_i' = \left\{ g^{ds+i} x^j \pmod{pq} \ :\ s = 0, 1, \cdots, \frac{e}{d} - 1;\ j = 0, 1, \cdots, d-1 \right\}, \quad i = 0, 1, \cdots, d-1.$$

On the basis of these two generalized cyclotomies of even order d, many generalized cyclotomic sequences of period pq were constructed.

Let $P = p\mathbb{Z}_q^* = \{p, 2p, \cdots, (q-1)p\}$, $Q = q\mathbb{Z}_p^* = \{q, 2q, \cdots, (p-1)q\}$, $R = \{0\}$. It is easily verified that $\mathbb{Z}_N = \mathbb{Z}_N^* \cup P \cup Q \cup R$. Using Whiteman's generalized cyclotomy of order 2 with respect to pq, Ding first constructed a class of generalized cyclotomic binary sequences which admits $D_1 \cup P$ as the characteristic set, i.e., the sequences $(s_0, s_1, s_2, \cdots)$ are given by $s_i = 1$ if $i \pmod{pq} \in D_1 \cup P$ and $s_i = 0$ otherwise. The linear complexity and autocorrelation property of these sequences were investigated in [10] and [11]. This kind of sequences was extended to the cases of $d = 4$ and $d = 2^k$ in [12] and [13], respectively, where the linear complexity of the binary sequences with the characteristic sets $\bigcup_{i=\frac{d}{2}}^{d-1} D_i \cup P$ was

calculated. Based on Ding-Helleseth generalized cyclotomy, the binary sequences with the characteristic sets $\bigcup_{i=\frac{d}{2}}^{d-1} D_i' \cup P$ for $d = 2$ were proposed in [14] and the linear complexity and autocorrelation values of these sequences were determined.

It is easily seen that the difference between the numbers of ones and zeros is $q - p - 1$ in all the above sequences, i.e., they are not balanced unless $q = p + 2$ (note that in the case where the difference is equal to ± 1 the sequences are called almost balanced). In [9] Ding and Helleseth introduced a new method to construct almost balanced sequences, that is, using the classic cyclotomy to divide the sets P and Q. Let d_1 be a divisor of d, and $p - 1 = d_1 f_1$, $q - 1 = d_1 f_2$. For $i = 0, 1, \cdots, d_1 - 1$, define

$$\begin{aligned} D_i^{(p)} &= \{g^{d_1 s+i} \,(\mathrm{mod}\, p) \,:\, s = 0, 1, \cdots, f_1 - 1\}, \\ D_i^{(q)} &= \{g^{d_1 s+i} \,(\mathrm{mod}\, q) \,:\, s = 0, 1, \cdots, f_2 - 1\}. \end{aligned} \tag{2.2}$$

Then $D_i^{(p)}$ and $D_i^{(q)}$ with $i \in \{0, 1, \cdots, d_1 - 1\}$ are the classic cyclotomic classes of order d_1 with respect to p and q, respectively. Let $P_i = pD_i^{(q)}$, $Q_i = qD_i^{(p)}$. Then $P = \bigcup_{i=0}^{d_1-1} P_i$, $Q = \bigcup_{i=0}^{d_1-1} Q_i$. The binary sequences based on Ding-Helleseth generalized cyclotomy and classic cyclotomy corresponding to $d = d_1 = 2$, 4 and 6 were considered in [15–17], respectively, where the linear complexity of the binary sequences with the characteristic set $\bigcup_{i=\frac{d}{2}}^{d-1} (D_i' \cup P_i \cup Q_i)$ was determined. The general case of $d = d_1 = 2k$ was discussed in [18] and a lower bound on the linear complexity of the sequences was given. Almost balanced binary sequences based on Whiteman's generalized cyclotomy with the characteristic set $D_1 \cup P_1 \cup Q_1$ for $d = d_1 = 2$ were investigated in [19–21], where the lower bound of the linear complexity of the sequences was given in [19] and the exact values of the linear complexity and autocorrelation of these sequences were calculated respectively in [20, 21]. In [22], the linear complexity of the sequences with the characteristic set $D_2 \cup D_3 \cup P_2 \cup P_3 \cup Q_2 \cup Q_3$ was determined.

In the following, we define a family of generalized cyclotomic binary sequences of period $N = pq$, where p and q are distinct odd primes with $\gcd(p - 1, q - 1) = 4$. Let D_i with $i \in \{0, 1, 2, 3\}$ be Whiteman's generalized cyclotomic classes of order 4 defined in (2.1), $D_i^{(p)}$ and $D_i^{(q)}$ with $i \in \{0, 1\}$ be the classical cyclotomic classes of order 2 defined in (2.2). Let $P_i = pD_i^{(q)}$, $Q_i = qD_i^{(p)}$, $R = \{0\}$. Then

$$\mathbb{Z}_N = \mathbb{Z}_N^* \cup P \cup Q \cup R = \bigcup_{i=0}^{3} D_i \bigcup_{i=0}^{1} P_i \bigcup_{i=0}^{1} Q_i \cup R.$$

Define two sets

$$C_0 = D_{a+2} \cup D_{a+3} \cup P_0 \cup Q_0 \cup R \;\text{ and }\; C_1 = D_a \cup D_{a+1} \cup P_1 \cup Q_1,$$

where a is an arbitrary integer with $0 \le a \le 3$, and the subscripts i in D_i are assumed to be taken modulo 4. For simplicity, the modulo operation is omitted in this paper. It is easy

to see that $\{C_0, C_1\}$ forms a partition of $\mathbb{Z}_N$ and $|C_0| - |C_1| = 1$. Now we define a family of almost balanced binary sequences of period pq which admits C_1 as the characteristic set, i.e., the sequences $\mathbf{s}^\infty = (s_0, s_1, s_2, \cdots)$ are given by

$$s_i = \begin{cases} 0, & i \,(\mathrm{mod}\, pq) \in C_0, \\ 1, & i \,(\mathrm{mod}\, pq) \in C_1. \end{cases} \tag{2.3}$$

3 Linear Complexity

Let $\mathbf{s}^\infty = (s_0, s_1, s_2, \cdots)$ be a periodic infinite sequence over a field $\mathbb{F}$. The linear complexity of $\mathbf{s}^\infty$ is defined to be the least positive integer L such that there are constants $c_0 = 1,\ c_1, \cdots, c_L \in \mathbb{F}$ satisfying $-s_i = c_1 s_{i-1} + c_2 s_{i-2} + \cdots + c_L s_{i-L}$ for all $i \geq L$. The polynomial $c(x) = c_0 + c_1 x + \cdots c_L x^L$ is called the minimal polynomial of $\mathbf{s}^\infty$. Let N be the period of $\mathbf{s}^\infty$. It is well known that

$$c(x) = \frac{x^N - 1}{\gcd(x^N - 1, s(x))},$$

where $s(x) = s_0 + s_1 x + \cdots + s_{N-1} x^{N-1}$ is the generating polynomial of the sequence $\mathbf{s}^\infty$. The linear complexity of $\{s_i\}$ is given by

$$L(\mathbf{s}^\infty) = N - \deg(\gcd(x^N - 1, s(x))). \tag{3.1}$$

In this section, we use (3.1) to determine the linear complexity of the new generalized cyclotomic binary sequences of period pq defined by (2.3).

For a with $0 \leq a \leq 3$, denote

$$s_a(x) = \sum_{i \in C_1} x^i = (\sum_{i \in P_1} + \sum_{i \in Q_1} + \sum_{i \in D_a} + \sum_{i \in D_{a+1}})x^i \in GF(2)[x]. \tag{3.2}$$

Then the generating polynomial of a sequence defined by (2.3) for a given integer a is $s_a(x)$. Let m be the order of 2 modulo N. Then there exists a primitive Nth root of unity α over the splitting field $GF(2^m)$ of $x^N - 1$. Thus the linear complexity of the sequence is given by

$$L(\mathbf{s}^\infty) = N - |\{j \,:\, s_a(\alpha^j) = 0\}|. \tag{3.3}$$

That is to say, the problem of determining the linear complexity of the sequence defined by (2.3) is reduced to that of counting the number of roots in the set $\{\alpha^j \,:\, j = 0, 1, \cdots, pq-1\}$ of the generating polynomial given in (3.2).

To determine the linear complexity of the sequences defined by (2.3), we need the following lemmas.

Lemma 2.1 (see [23]) Let the symbols be the same as before. Then

(i) if $a \in D_i$, then $aD_j = D_{(i+j)(\mathrm{mod}\, 4)}$, where $i, j \in \{0, 1, 2, 3\}$;

(ii) for any odd prime p, if $t \,(\mathrm{mod}\, p) \in D_i^{(p)}$, then $tD_j^{(p)} = D^{(p)}_{(i+j)\,(\mathrm{mod}\, 2)}$, where $i, j \in \{0, 1\}$.

Lemma 2.2 (see [15]) Let the symbols be the same as before. Then
(i) $\sum\limits_{i\in P}\alpha^i=\sum\limits_{i=1}^{q-1}\alpha^{pi}=1$; (ii) $\sum\limits_{i\in Q}\alpha^i=\sum\limits_{i=1}^{p-1}\alpha^{qi}=1$; (iii) $\sum\limits_{i\in Z_{pq}^*}\alpha^i=1$.

Lemma 2.3 (see [12]) Let the symbols be the same as before. Then

$$\sum_{i\in D_j}\alpha^{ti}=\begin{cases}\frac{p-1}{4}\,(\mathrm{mod}\,2), & \text{if } t\in P,\\ \frac{q-1}{4}\,(\mathrm{mod}\,2), & \text{if } t\in Q.\end{cases}$$

Lemma 2.4 Let the symbols be the same as before. Then
(i) if $t\,(\mathrm{mod}\,p)\in D_0^{(p)}$, then $\sum\limits_{i\in Q_1}\alpha^{ti}=\sum\limits_{i\in Q_1}\alpha^i$;
(ii) if $t\,(\mathrm{mod}\,p)\in D_1^{(p)}$, then $\sum\limits_{i\in Q_1}\alpha^{ti}=1+\sum\limits_{i\in Q_1}\alpha^i$;
(iii) if $t\,(\mathrm{mod}\,q)\in D_0^{(q)}$, then $\sum\limits_{i\in P_1}\alpha^{ti}=\sum\limits_{i\in P_1}\alpha^i$;
(iv) if $t\,(\mathrm{mod}\,q)\in D_1^{(q)}$, then $\sum\limits_{i\in P_1}\alpha^{ti}=1+\sum\limits_{i\in P_1}\alpha^i$.

Proof (i) If $t\,(\mathrm{mod}\,p)\in D_0^{(p)}$, then by Lemma 2.1 (ii), we have $tQ_1=tqD_1^{(p)}=qD_1^{(p)}=Q_1$, thus

$$\sum_{i\in Q_1}\alpha^{ti}=\sum_{i\in Q_1}\alpha^i.$$

(ii) If $t\,(\mathrm{mod}\,p)\in D_1^{(p)}$, then $tQ_1=tqD_1^{(p)}=qD_0^{(p)}=Q_0$, it follows from Lemma 2.2 (ii) that

$$\sum_{i\in Q_1}\alpha^{ti}=\sum_{i\in Q_0}\alpha^i=1+\sum_{i\in Q_1}\alpha^i.$$

The assertions in (iii) and (iv) can be similarly proved, so we omit them here.

Lemma 2.5 Let the symbols be the same as before. For $t\in Z_{pq}^*$, let $t\,(\mathrm{mod}\,p)\in D_i^{(p)}$ and $t\,(\mathrm{mod}\,q)\in D_j^{(q)}$, where $i,j\in\{0,1\}$. Then $t\in D_0\cup D_2$ if and only if $i=j$, and $t\in D_1\cup D_3$ if and only if $i\neq j$.

Proof Let $t\in D_k$ with $k\in\{0,1,2,3\}$. Then there exists a uniquely determined integer u_0 with $0\le u_0\le e-1$ such that $t\equiv g^{u_0}x^k\,(\mathrm{mod}\,pq)$. Since $x\equiv g\,(\mathrm{mod}\,p)$ and $x\equiv 1\,(\mathrm{mod}\,q)$, we have $t\equiv g^{u_0+k}\equiv g^{(u_0+k)\,(\mathrm{mod}\,p-1)}\,(\mathrm{mod}\,p)$ and $t\equiv g^{u_0}\equiv g^{u_0\,(\mathrm{mod}\,q-1)}\,(\mathrm{mod}\,q)$. It is easily verified that k is even if and only if u_0+k and u_0 have the same parity, or equivalently, if and only if $(u_0+k)\,(\mathrm{mod}\,p-1)$ and $u_0\,(\mathrm{mod}\,q-1)$ have the same parity since $p-1$ and $q-1$ are both even. Therefore, $t\,(\mathrm{mod}\,p)$ and $t\,(\mathrm{mod}\,q)$ are either quadratic residues of both p and q or quadratic nonresidues of both p and q, and the desired result for even k follows immediately from the definition of the classical cyclotomic classes of order 2. The case of odd k can be proved in the similar way.

Lemma 2.6 Let the symbols be the same as before. Then

$$s_a(\alpha^t)=\begin{cases}s_a(\alpha), & t\in D_0,\\ 1+s_{a+1}(\alpha), & t\in D_1,\\ 1+s_a(\alpha), & t\in D_2,\\ s_{a+1}(\alpha), & t\in D_3.\end{cases}$$

Proof For $t \in D_0 \cup D_2$, it follows from Lemma 2.5 that $t \,(\mathrm{mod}\ p) \in D_0^{(p)}$ and $t \,(\mathrm{mod}\ q) \in D_0^{(q)}$ or $t \,(\mathrm{mod}\ p) \in D_1^{(p)}$ and $t \,(\mathrm{mod}\ q) \in D_1^{(q)}$. Then by Lemma 2.4, we always have

$$(\sum_{i\in P_1} + \sum_{i\in Q_1})\alpha^{ti} = (\sum_{i\in P_1} + \sum_{i\in Q_1})\alpha^{i}.$$

For $t \in D_1 \cup D_3$, it follows from Lemma 2.5 that $t \,(\mathrm{mod}\, p) \in D_0^{(p)}$ and $t \,(\mathrm{mod}\, q) \in D_1^{(q)}$ or $t \,(\mathrm{mod}\, p) \in D_1^{(p)}$ and $t \,(\mathrm{mod}\, q) \in D_0^{(q)}$. Then by Lemma 2.4, we always have

$$(\sum_{i\in P_1} + \sum_{i\in Q_1})\alpha^{ti} = 1 + (\sum_{i\in P_1} + \sum_{i\in Q_1})\alpha^{i}.$$

Moreover, by Lemma 2.1 we have $tD_a = D_{a+k}$, $tD_{a+1} = D_{a+k+1}$ for $t \in D_k$ with $k \in \{0, 1, 2, 3\}$, so that

$$(\sum_{i\in D_a} + \sum_{i\in D_{a+1}})\,\alpha^{ti} = (\sum_{i\in D_{a+k}} + \sum_{i\in D_{a+k+1}})\,\alpha^{i}.$$

Thus, when $t \in D_0$,

$$s_a(\alpha^t) = (\sum_{i\in P_1} + \sum_{i\in Q_1} + \sum_{i\in D_a} + \sum_{i\in D_{a+1}})\alpha^{i} = s_a(\alpha);$$

when $t \in D_1$,

$$s_a(\alpha^t) = 1 + (\sum_{i\in P_1} + \sum_{i\in Q_1} + \sum_{i\in D_{a+1}} + \sum_{i\in D_{a+2}})\alpha^{i} = 1 + s_{a+1}(\alpha);$$

When $t \in D_2$, by Lemma 2.2 (iii), we have

$$(\sum_{i\in D_a} + \sum_{i\in D_{a+1}} + \sum_{i\in D_{a+2}} + \sum_{i\in D_{a+3}})\alpha^{i} = \sum_{i\in \mathbb{Z}_{pq}^*} \alpha^{i} = 1.$$

It follows then that

$$s_a(\alpha^t) = (\sum_{i\in P_1} + \sum_{i\in Q_1} + \sum_{i\in D_{a+2}} + \sum_{i\in D_{a+3}})\alpha^{i} = 1 + (\sum_{i\in P_1} + \sum_{i\in Q_1} + \sum_{i\in D_a} + \sum_{i\in D_{a+1}})\alpha^{i} = 1 + s_a(\alpha).$$

By the same arguments, for the case $t \in D_3$, we have

$$\begin{aligned} s_a(\alpha^t) &= 1 + (\sum_{i\in P_1} + \sum_{i\in Q_1})\alpha^{i} + (\sum_{i\in D_{a+3}} + \sum_{i\in D_a})\alpha^{i} \\ &= 1 + (\sum_{i\in P_1} + \sum_{i\in Q_1})\alpha^{i} + 1 + (\sum_{i\in D_{a+1}} + \sum_{i\in D_{a+2}})\alpha^{i} \\ &= s_{a+1}(\alpha). \end{aligned}$$

The proof is completed.

Lemma 2.7 Let the symbols be the same as before. Then

$$s_a(\alpha^t) = \begin{cases} \sum\limits_{i\in P_1} \alpha^{ti}, & t \in P, \\ \sum\limits_{i\in Q_1} \alpha^{ti}, & t \in Q. \end{cases}$$

Proof When $t \in P$, for any $i \in Q_1$, $ti \pmod{pq} = 0$, so that

$$\sum_{i \in Q_1} \alpha^{ti} = |Q_1| = \frac{p-1}{2} \pmod 2.$$

Then by Lemma 2.3, we get

$$s_a(\alpha^t) = (\sum_{i \in P_1} + \sum_{i \in Q_1} + \sum_{i \in D_a} + \sum_{i \in D_{a+1}})\alpha^{ti} = \sum_{i \in P_1} \alpha^{ti} + (\frac{p-1}{4} + \frac{p-1}{4} + \frac{p-1}{2}) \pmod 2 = \sum_{i \in P_1} \alpha^{ti}.$$

When $t \in Q$, for any $i \in P_1$, $ti \pmod{pq} = 0$, it follows that

$$\sum_{i \in P_1} \alpha^{ti} = |P_1| = \frac{q-1}{2} \pmod 2.$$

Again by Lemma 2.3, we obtain

$$s_a(\alpha^t) = (\sum_{i \in P_1} + \sum_{i \in Q_1} + \sum_{i \in D_2} + \sum_{i \in D_3})\alpha^{ti} = \sum_{i \in Q_1} \alpha^{ti} + (\frac{q-1}{4} + \frac{q-1}{4} + \frac{q-1}{2}) \pmod 2 = \sum_{i \in Q_1} \alpha^{ti}.$$

Lemma 2.8 For any $a \in \{0,1,2,3\}$, $s_a(\alpha) \in \{0,1\}$ if and only if $2 \in D_0$.

Proof If $2 \in D_0$, then by Lemma 2.6, $s_a(\alpha^2) = s_a(\alpha)$ for any $a \in \{0,1,2,3\}$. Since the characteristic of the field $GF(2^m)$ is 2, it follows that $s_a(\alpha^2) = [s_a(\alpha)]^2$. Thus we get $[s_a(\alpha)]^2 = [s_a(\alpha)]$, and so $s_a(\alpha) \in \{0,1\}$.

To prove the necessity, we suppose, by way of contradiction, that $2 \notin D_0$.

If $2 \in D_1$, then it follows from Lemma 2.6 that $s_a(\alpha^2) = 1 + s_{a+1}(\alpha)$. On the other hand, since $s_a(\alpha) \in \{0,1\}$, $s_a(\alpha) = [s_a(\alpha)]^2 = s_a(\alpha^2)$. Thus $s_a(\alpha) = 1 + s_{a+1}(\alpha)$, which implies $s_{a+1}(\alpha) \in \{0,1\}$. By the same argument, $s_{a+1}(\alpha) = [s_{a+1}(\alpha)]^2 = s_{a+1}(\alpha^2) = 1 + s_{a+2}(\alpha)$, and so $s_a(\alpha) = s_{a+2}(\alpha)$. But from (3.2) and Lemma 2.2 (iii), it follows that

$$s_a(\alpha) + s_{a+2}(\alpha) = \sum_{j=a}^{a+3} \sum_{i \in D_j} \alpha^i = \sum_{i \in Z_{pq}^*} \alpha^i = 1,$$

and so we arrive at a contradiction.

If $2 \in D_2$, then by Lemma 2.6, $s_a(\alpha) = [s_a(\alpha)]^2 = s_a(\alpha^2) = 1 + s_a(\alpha)$, an obvious contradiction.

Similarly, if $2 \in D_3$, then $s_a(\alpha) = [s_a(\alpha)]^2 = s_a(\alpha^2) = s_{a+1}(\alpha)$ and $s_{a+1}(\alpha) = [s_{a+1}(\alpha)]^2 = s_{a+1}(\alpha^2) = s_{a+2}(\alpha)$. It follows that $s_a(\alpha) = s_{a+2}(\alpha)$, a contradiction.

Lemma 2.9 (see [15]) Let the symbols be the same as before. Then

(i) For any $t \in P$, $\sum\limits_{i \in P_1} \alpha^{ti} \in \{0,1\}$ if and only if $q \equiv \pm 1 \pmod 8$.

(ii) For any $t \in Q$, $\sum\limits_{i \in Q_1} \alpha^{ti} \in \{0,1\}$ if and only if $p \equiv \pm 1 \pmod 8$.

Lemma 2.10 (see [24]) $2 \in D_0^{(p)}$ if and only if $p \equiv \pm 1 \pmod 8$.

Now the results on the linear complexity of the sequences defined by (2.3) are summarized in the following three theorems.

Theorem 2.11 Let $p \equiv 1 \pmod 8$ and $q \equiv -3 \pmod 8$. Then $L(s^\infty) = \frac{2pq-p-1}{2}$.

Proof By eq.(3.3), it suffices to count the number of roots in $\{\alpha^j : j = 0, 1, \cdots, pq-1\}$ of $s_a(x)$. For $t \in R = \{0\}$, it is easily verified that

$$s_a(\alpha^t) = \frac{pq-1}{2} \pmod 2 = 0.$$

Since $p \equiv 1 \pmod 8$ and $q \equiv -3 \pmod 8$, it follows from Lemma 2.10 that $2 \in D_0^{(p)}$ and $2 \in D_1^{(q)}$, and so $2 \in D_1 \cup D_3$ by Lemma 2.5. Thus $s_a(\alpha^t) \neq 0$ for any $t \in \mathbb{Z}_{pq}^*$ by Lemma 2.6 and Lemma 2.8. In addition, for any $t \in P$ we have $s_a(\alpha^t) \neq 0$ by Lemma 2.7 and Lemma 2.9 (i), but for any $t \in Q$ we have $s_a(\alpha^t) = \sum_{i \in Q_1} \alpha^{ti} \in \{0, 1\}$ by Lemma 2.7 and Lemma 2.9 (ii). We now distinguish the cases $t \in Q_0$ and $t \in Q_1$. It is obvious $\sum_{i \in Q_1} \alpha^{ti} = \sum_{i \in D_1^{(p)}} (\alpha^{q^2})^i$ when $t \in Q_0$ and $\sum_{i \in Q_1} \alpha^{ti} = \sum_{i \in D_0^{(p)}} (\alpha^{q^2})^i$ when $t \in Q_1$. Since

$$\sum_{i \in D_1^{(p)}} (\alpha^{q^2})^i + \sum_{i \in D_0^{(p)}} (\alpha^{q^2})^i = \sum_{i=1}^{p-1} (\alpha^{q^2})^i = 1,$$

it follows that $s_a(\alpha^t) = 0$ either for all $t \in Q_0$ or for all $t \in Q_1$. In conclusion, the size of the set $\{s_a(\alpha^t) = 0 : t \in \mathbb{Z}_{pq}\}$ is $\frac{p-1}{2} + 1$, then by (3.3) we get that $L(s^\infty) = pq - \frac{p-1}{2} - 1 = \frac{2pq-p-1}{2}$.

Theorem 2.12 Let $p \equiv -3 \pmod 8$ and $q \equiv 1 \pmod 8$. Then $L(s^\infty) = \frac{2pq-q-1}{2}$.

Proof When $p \equiv -3 \pmod 8$ and $q \equiv 1 \pmod 8$, we have $2 \in D_1 \cup D_3$ by Lemma 2.5, and hence $s_a(\alpha^t) \neq 0$ for any $t \in \mathbb{Z}_{pq}^*$ by Lemma 2.6 and Lemma 2.8. By the same arguments as in Theorem 2.11, $s_a(\alpha^t) \neq 0$ for any $t \in Q$ and $s_a(\alpha^t) = 0$ for half of $t \in P$. Therefore, by (3.3) we have $L(s^\infty) = pq - \frac{q-1}{2} - 1 = \frac{2pq-q-1}{2}$.

Theorem 2.13 Let $p \equiv -3 \pmod 8$ and $q \equiv -3 \pmod 8$. Then

$$L(\mathbf{s}^\infty) = \begin{cases} \frac{pq+p+q-3}{2}, & 2 \in D_0, \\ pq-1, & 2 \notin D_0. \end{cases}$$

Proof Since $p \equiv -3 \pmod 8$ and $q \equiv -3 \pmod 8$, it follows from Lemmas 2.7 and 2.9 that $s_a(\alpha^t) \neq 0$ for any $t \in P$ and $t \in Q$.

If $2 \in D_0$, then $s_a(\alpha^t) = 0$ for half of $t \in \mathbb{Z}_{pq}^*$ by Lemma 2.6. If $2 \notin D_0$, then $s_a(\alpha^t) \neq 0$ for any $t \in \mathbb{Z}_{pq}^*$ by Lemma 2.6. So the desired result follows immediately from (3.3).

4 Conclusion

In this paper, new class of almost balanced binary sequences of period pq is constructed via Whiteman's generalized cyclotomy of order 4 and classic cyclotomy of order 2. The linear complexity of these sequences is determined. The results show that the proposed sequences have large linear complexity. In addition, since the parameter a in the characteristic set

could be any integers in the range of 0 to 3, our construction can generate a number of binary sequences with large linear complexity.

References

[1] Rueppel R. Analysis and design of stream ciphers [M]. New York: Springer-Verlag, 1986.

[2] Ding C S. Binary cyclotomic generators[A]. Preneel B. Fast Software Encryption, LNCS 1008[C]. Berlin, Heidelberg: Springer-Verlag, 1995: 29–60.

[3] Du X N, Chen Z X. A generalization of the Hall's sextic residue sequences[J]. Information Sciences, 2013, 222: 784–794.

[4] Hu L Q, Yue Q, Wang M H. The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$[J]. IEEE Trans. Inf. Theory, 2012, 58(8): 5534–5543.

[5] Ke P H, Zhang J, Zhang S Y. On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^m$[J]. Des. Codes Cryptogr., 2013, 67(3): 325–339.

[6] Kim Y J, Jin S Y, Song H Y. Linear complexity and autocorrelation of prime cube sequences[A]. Boztas S, Lu HF. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, LNCS 4851[C]. Berlin Heidelberg: Springer-Verlag, 2007: 188–197.

[7] Liu L F, Yang X Y, Du X N, Wei B. On the linear complexity of new generalized cyclotomic binary sequences of order two and period pqr[J]. Tsinghua Sci. Technol., 2016, 21: 295–301.

[8] Whiteman A L. A family of difference sets[J]. Illionis J. Math., 1962, 6(1): 107–121.

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

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

[11] Ding C S. Autocorrelation values of generalized cyclotomic sequences of order two[J]. IEEE Trans. Inf. Theory, 1998, 44(4): 1699–1702.

[12] Bai E J, Fu X T, Xiao G Z, Huang X L. On the linear complexity of generalized cyclotomic sequences of order four over Z_{pq}^*[J]. IEICE Trans. Fundam., 2005, E88-A(1): 392–395.

[13] Yan T J, Du X N, Xiao G Z. Linear complexity of binary Whiteman-Generalized cyclotomic sequences of order 2^k[J]. Information Science, 2009, 179(7): 1019–1023.

[14] Li S Q, Chen Z X, Sun R, Xiao G Z. On the randomness of generalized cyclotomic sequence of order two and length pq[J]. IEICE Trans. Fundam., 2007, E90-A(9): 2037–2041.

[15] 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. Inf. Theory, 2005, 51(5): 1849–1853.

[16] Yan T J, Hong L, Xiao G Z. The linear complexity of new generalized cyclotomic binary sequences of order four[J]. Information Science, 2008, 178(3): 807–815.

[17] Vladimir E, Olga A. On the linear complexity of Ding-Helleseth generalized cyclotomic binary sequences of order four and six[J]. European Journal of Pure and Applied Mathematics, 2014, 7(3): 256–266.

[18] Yan T J, Xu P. Linear complexity of two classed of binary generalized cyclotomic sequences of any order[J]. Journal of Convergence Information Technology, 2012, 7(14): 98–106.

[19] Li S Q, Zhou L, Xiao G Z. Study on a class of Whiteman-generalized cyclotomic sequence with length pq and order two[J]. Journal of Electronics & Information Technology, 2009, 31(9): 2205–2208.

[20] Hu L Q, Yue Q, Zhu X M. Linear complexity of second-order whiteman generalized cyclotomic sequence of period pq[J]. Journal of Gansu Sciences, 2015, 27(5): 1–5.

[21] Hu L Q, Yue Q, Zhu X M. Autocorrelation value of generalized cyclotomic sequences with period pq[J]. Journal of Nanjing University of Science and Technology, 2015, 39(5): 550–555.

[22] Liu L F, Yang X Y, Chen H B. Linear complexity of Whiteman-generalized cyclotomic sequence with order four[J]. Application Research of Computers, 2011, 28(11): 4350–4352.

[23] Cusick T, Ding C S, Renvall A. Stream ciphers and number theory[M]. Amsterdam, Netherlands: North-Holland Publishing CO., 1998.

[24] Ireland K, Rosen M. A classical introduction to modern number theory[M]. New York: Springer-Verlag, 1990.

周期pq的广义分圆二元序列线性复杂度

杨 波 [1,2], 杜天奇 [2], 肖自碧 [2]

(1.武汉科技大学冶金工业过程系统科学湖北省重点实验室, 湖北 武汉 430081)

(2.武汉科技大学理学院, 湖北 武汉 430081)

摘要: 本文构造了一类周期为pq（p和q是不同的奇素数）的几乎平衡的二元序列, 基于4阶Whiteman-广义分圆和2阶经典分圆我们确定了这类序列的线性复杂度. 研究结果表明该类序列从线性复杂度的角度来看是非常好的.

关键词: 二元序列; 线性复杂度; 分圆; 广义分圆序列

MR(2010)**主题分类号**: 11T22; 11T55; 94A55; 94A60 **中图分类号**: O157.4