Linear Complexity of Generalized Cyclotomic Sequences with Period $p^n q^m$

Vladimir Edemskiy[1] and Chenhuang Wu[2(✉)]

[1] Department of Applied Mathematics and Informatics, Yaroslav-the-Wise Novgorod State University, Veliky Novgorod 173003, Russia
vladimir.edemsky@novsu.ru

[2] Fujian Key Laboratory of Financial Information Processing, Putian University, Putian, Fujian 351100, China
ptuwch@163.com

Abstract. Linear complexity is a very important merit factor for measuring the unpredictability of pseudo-random sequences for applications. The higher the linear complexity, the better the unpredictability of a sequence. In this paper, we continue the investigation of generalized cyclotomic sequences constructed by new generalized cyclotomy presented by Zeng et al. In detail, we consider the new generalized cyclotomic sequence with period $p^n q^m$ where p, q are odd distinct primes and n, m are natural numbers. It is shown that these sequences have high linear complexity. Finally, we also give some examples to illustrate the correctness of our results.

Keywords: Binary sequences · Generalized cyclotomy · Linear complexity

1 Introduction

Linear complexity is a very important merit factor for measuring the unpredictability of pseudo-random sequences. The linear complexity of a sequence may be defined as the length of the shortest linear feedback shift register which generates the sequence [1]. According to Berlekamp- Massey algorithm, if the linear complexity of the sequence is l, then $2l$ consecutive terms of the sequence can be used to restore the whole sequence. Hence, a "high" linear complexity should be no less than one-half of the length (or minimum period) of the sequence [2]. For cryptographic applications, sequences with high linear complexity are required.

An important method of designing sequences with high linear complexity uses classical cyclotomic classes and generalized cyclotomic classes to construct sequences. Cyclotomy is related to difference sets, sequences, coding theory, and cryptography [3]. Classical cyclotomy was first considered in detail by Gauss. Later, Whiteman presented the generalized cyclotomy of order d with respect to the product of two distinct

V. Edemskiy was supported by Russian Science Foundation according to the research project No. 22-21-00516, https://rscf.ru/en/project/22-21-00516/. C. Wu was partially supported by the Projects of International Cooperation and Exchange NSFC-RFBR No. 61911530130, by the Natural Science Foundation of Fujian Province No. 2020J01905.

S. Mesnager and Z. Zhou (Eds.): WAIFI 2022, LNCS 13638, pp. 320–333, 2023.
https://doi.org/10.1007/978-3-031-22944-2_21

odd primes, which is not consistent with classical cyclotomy [4]. It was extended to odd integers in [5]. Further, a new generalized cyclotomy that includes classical cyclotomy as a special case was introduced by Ding and Helleseth [3]. Fan and Ge proposed a unified approach that determines both Whiteman's and Ding-Helleseth's generalized cyclotomy [6]. In the past decades, the linear complexity of binary and nonbinary Whiteman's and Ding-Helleseth's generalized cyclotomic sequences has been extensively studied [7–12] (see also references therein).

Zeng et al. in [13] presented a new approach and suggested a new generalized cyclotomy. Further, this new generalized cyclotomy was discussed in [14]. Based on the generalized cyclotomic classes from [13], Xiao et al.[15] presented a new family of cyclotomic binary sequences of period p^n and determined the linear complexity of the sequences for the case when $n = 2$ and $f = 2^r$. Later, these results were generalized in [16,17]. The use of new generalized cyclotomic classes for constructing sequences with high linear complexity and even periods $2p^n, 2^m p^n$ was considered in [18,19]. In this paper, we will study the linear complexity of new generalized cyclotomic sequences with period $p^n q^m$. These sequences are defined using new generalized cyclotomic classes from [13]. Thus, we continue the study of new generalized cyclotomic sequences started in [15–17].

The rest of the paper is organized as follows. The definition of sequences and the main result are introduced in Sect. 2. In Sect. 3 we discuss some subsidiary statements about the sequence polynomial and in Sect. 4 we prove our main result. We conclude the paper in Sect. 5.

2 Definitions of Sequences

First of all, we recall the definition of new generalized cyclotomic classes presented in [13] for $N = p^n q^m$, where p and q are odd distinct primes, $n > 0, m > 0$. Suppose e divides $p-1$ and $q-1$; then $p-1 = ef$ and $q-1 = eh$. It is well known that there exists primitive roots η and ξ modulo p^2 and q^2 respectively. In this case, η is the primitive root modulo p^k, $k = 1,2,\ldots,n$ and ξ is the primitive root modulo q^l, $l = 1,2,\ldots,m$ [20].

Let $v = p^k q^l, v \neq 1$, where $k = 0,1,\ldots,n$; $l = 0,1,\ldots,m$.

According to the Chinese Remainder Theorem, there exists g_v such that

$$g_v \equiv \eta^{fp^{k-1}} \pmod{p^k} \text{ when } k \geq 1 \text{ and } g_v \equiv \xi^{hq^{l-1}} \pmod{q^l} \text{ when } l \geq 1. \quad (1)$$

Also there exist ζ_p, ζ_q such that

$$\zeta_p \equiv \begin{cases} \eta \pmod{p^n}, \\ 1 \pmod{q^m}, \end{cases} \quad \text{and } \zeta_q \equiv \begin{cases} \xi \pmod{q^m}, \\ 1 \pmod{p^n}. \end{cases} \quad (2)$$

Throughout this paper, we let $\mathbb{Z}_v$ be the ring of integers modulo v for a positive integer v, and $\mathbb{Z}_v^*$ be the multiplicative group of $\mathbb{Z}_v$. According to [13] we know that $D^{(v)} = \{g_v^s \mid s = 0,\ldots,e-1\}$ is the subgroup of $\mathbb{Z}_v^*$.

Define

$$\Psi_v = \begin{cases} \mathbb{Z}_{fp^{k-1}} \times \mathbb{Z}_{(q-1)q^{l-1}}, & \text{if } k \geq 1, l \geq 1, \\ \mathbb{Z}_{fp^{k-1}} \times \{0\}, & \text{if } l = 0, \\ \{0\} \times \mathbb{Z}_{hq^{l-1}}, & \text{if } k = 0. \end{cases}$$

Let $I = (i_1, i_2) \in \Psi_v$ and $D_I^{(v)} = \zeta_p^{i_1} \zeta_q^{i_2} D^{(v)}$.

By [13] we have the following partitions

$$\mathbb{Z}_v^* \setminus \{0\} = \bigcup_{I \in \Psi_v} D_I^{(v)} \text{ and } \mathbb{Z}_N \setminus \{0\} = \bigcup_{v|N, v>1} \bigcup_{I \in \Psi_v} \frac{N}{v} D_I^{(v)}.$$

It is necessary to note that for $v = p^k$ (or $v = q^l$) we obtain a partition of $\mathbb{Z}_{p^k}^*$ as in [15] and in this case $\eta^t D^{(p^k)}$ is equal to $D_t^{(p^k)} = \{\eta^{t+fp^{k-1}i} \bmod p^k \mid i = 0, 1, \ldots, e-1\}$, $t = 0, 1, \ldots, fp^{k-1} - 1$. The properties of $D_t^{(p^k)}$ were studied in [15,16].

Let f and h be even numbers and b, c be integers such that $0 \leq b < fp^{n-1}$, $0 \leq c < hq^{m-1}$. Then define

$$\Psi_v^{(1)} = \begin{cases} \{(i_1 + b, i_2) \in \Psi_v \mid 0 \leq i_1 < p^{k-1} f/2 - 1\}, & \text{if } k \geq 1, \\ \{(0, i_2 + c) \in \Psi_v \mid 0 \leq i_2 < q^{l-1} h/2 - 1\}, & \text{if } k = 0. \end{cases}$$

Let

$$C_1^{(v)} = \bigcup_{I \in \Psi_v^{(1)}} D_I^{(v)} \text{ and } C_0^{(v)} = \bigcup_{I \in \Psi_v \setminus \Psi_v^{(1)}} D_I^{(v)}.$$

Then we see that

$$|C_j^{(v)}| = \begin{cases} p^{k-1}(p-1)q^{l-1}(q-1)/2, & \text{if } k \geq 1, l \geq 1, \\ p^{k-1}(p-1)/2, & \text{if } k \geq 1, l = 0, \\ q^{l-1}(q-1)/2, & \text{if } k = 0, l \geq 1. \end{cases} \tag{3}$$

for $v = p^k q^l$, $j = 0, 1$.

Define

$$C_j = \bigcup_{v|N, v>1} \frac{N}{v} C_j^{(v)}, j = 0, 1$$

or, in more detail

$$C_j = \bigcup_{k=1}^{n} \bigcup_{l=1}^{m} p^{n-k} q^{m-l} C_j^{(p^k q^l)} \cup \bigcup_{k=1}^{n} p^{n-k} q^m C_j^{(p^k)} \cup \bigcup_{l=1}^{m} p^n q^{m-l} C_j^{(q^l)}. \tag{4}$$

By definition we get $\mathbb{Z}_N \setminus \{0\} = C_0 \cup C_1$ and $C_0 \cap C_1 = \oslash$.

Then we can define a balanced binary sequence s^∞ with period N as follows:

$$s_i = \begin{cases} 1, & \text{if } i \mod N \in C_1 \cup \{0\}, \\ 0, & \text{if } i \mod N \in C_0. \end{cases} \tag{5}$$

A sequence is called balanced if the numbers of 1's and 0's in one minimum period differ by no more than one. Earlier, new generalized cyclotomic classes were used to construct sequences with period p^n. It is necessary to note that for $N = p^2$ this sequence is the same as in [15].

We conclude this section by recalling the notion of the linear complexity and one method of studying the linear complexity. For a N-periodic sequence $s^\infty = \{s_i\}_{i\geq 0}$ over the $\mathbb{F}_2$ (the finite field of two elements), we recall that the linear complexity over $\mathbb{F}_2$, denoted by $\mathrm{LC}(s^\infty)$, is the least order L such that $\{s_i\}$ satisfies

$$s_{i+L} = c_{L-1}s_{i+L-1} + \ldots + c_1 s_{i+1} + c_0 s_i \quad \text{for } i \geq 0,$$

where $c_0 \neq 0, c_1, \ldots, c_{L-1} \in \mathbb{F}_2$.

It is well known (see, for instance, [21]) that if $S(x) = s_0 + s_1 x + \cdots + s_{N-1}x^{N-1}$ then the linear complexity of s^∞ is given by

$$\mathrm{LC}(s^\infty) = N - \deg\Big(\gcd\left(x^N - 1, S(x)\right)\Big).$$

Thus, if α is a primitive root of order N of unity in the extension of the field $\mathbb{F}_2$, then in order to find the linear complexity of a sequence, it is sufficient to study the zeros of $S(x)$ in the set $\{\alpha^i \mid i = 0, 1, \ldots, N-1\}$.

In this paper, we will study the linear complexity of s^∞ defined by (5). The values $S(\alpha^i)$ we will consider in the following section.

2.1 Main Result

To begin with, we introduce some new notations. Let $\mathrm{ord}_p(2)$ be the order[1] of 2 modulo p and

$$l_k = \begin{cases} k, & \text{if } q^m \in D^{(p^k)} \text{ or } q^m \in \eta^{p^{k-1}f/2} D^{(p^k)}, \\ 0, & \text{otherwise} \end{cases}$$

for $k = 1, 2, \ldots, n$. Let $k_0 = \max\limits_{1\leqslant k\leqslant n} l_k$.

A prime p is called a Wieferich prime if $2^{p-1} \equiv 1 \pmod{p^2}$. It is well known that there are only two Wieferich primes, 1093 and 3511, up to 6×10^{17}. Bellow, we will consider only non-Wieferich primes. Our main contribution is the following statement.

Theorem 1. *Let* $2^{p-1} \not\equiv 1 \pmod{p^2}$, $2^{q-1} \not\equiv 1 \pmod{q^2}$, $\gcd(p, q-1) = \gcd(p-1, q) = 1$ *and let* s^∞ *be a sequence defined by* (5). *Then*

(i) $\mathrm{LC}(s^\infty) = N - r_p \cdot \mathrm{ord}_p(2) - p^{k_0} r_q \cdot \mathrm{ord}_q(2) - \delta$ *for* $k_0 > 0$, *where* r_p, r_q *are integers satisfying inequalities* $0 \leq r_p \leq \frac{p-1}{2\,\mathrm{ord}_p(2)}$, $0 \leq r_q \leq \frac{q-1}{2\,\mathrm{ord}_q(2)}$ *and*

$$\delta = \begin{cases} 1, & \text{if } (p^n q^m + 1)/2 \text{ is even}, \\ 0, & \text{if } (p^n q^m + 1)/2 \text{ is odd}. \end{cases}$$

[1] The order of 2 modulo p is the least positive integer T such that $2^T \equiv 1 \pmod{p}$.

(ii) $\mathrm{LC}(s^\infty) = N - r_N \cdot \mathrm{ord}_{pq}(2) - r_p \cdot \mathrm{ord}_p(2) - r_q \cdot \mathrm{ord}_q(2) - \delta$ *for* $k_0 = 0$, *where* r_N *is an integer satisfying inequality* $0 \le r_N \le \frac{(p-1)(q-1)}{2\,\mathrm{ord}_{pq}(2)}$.

According to Theorem 1 the considered sequences have high linear complexity.

Remark 1. We will show that the value r_N also depends on n, m and is not defined only by p, q.

3 Subsidiary Lemmas

In this section we prove a few lemmas and discuss the properties of the generating polynomial of s^∞.

Lemma 1. *Let* $v = p^k q^l$, $k = 1, \dots, n$; $l = 1, \dots, m$. *Then*

(i) $C_1^{(v)} \bmod p^k = C_1^{(p^k)}$;
(ii) $C_1^{(v)} \bmod q^l = \mathbb{Z}_{q^l}^*$.

Proof. Suppose $i \in C_1^{(v)}$; then there exist u, t, s such that $i = \zeta_p^{u+b} \zeta_q^{t+c} g_v^s$ and $0 \le u < p^{k-1} f/2, 0 \le t < q^{l-1}(q-1),\ 0 \le s < e$. So, by (1), (2) and the definition of $C_1^{(v)}$ we get that $i \bmod p^k = \eta^{u+b} \eta^{sp^{k-1}f}$, i.e., $i \bmod p^k \in C_1^{(p^k)}$. Further, it is obvious that $i \pmod{q^l} \in \mathbb{Z}_{q^l}^*$. Moreover, it is clear that if $j \in C_1^{(v)}, j \ne i$ then $j \not\equiv i \pmod{p^k}$ or $j \not\equiv i \pmod{q^l}$. Since by (3) we have

$$|C_1^{(v)}| = \frac{p^{k-1}(p-1)}{2} \cdot q^{l-1}(q-1) = |C_1^{(p^k)}| \cdot |\mathbb{Z}_{q^l}^*|,$$

it follows that the conclusion of the lemma holds. □

Let $S(X) = \sum_{i=0}^{N-1} s_i X^i$ be the generating polynomial of s^∞. Define as in [15,16] the subsidiary polynomials, i.e.,

$$T_b^{(p^k)}(X) = \sum_{i \in C_1^{(p^k)}} X^i,\ k = 1, 2, \dots, n \text{ and } T_c^{(q^l)}(X) = \sum_{i \in C_1^{(q^l)}} X^i, l = 1, 2, \dots, m.$$

Define

$$S_b^{(p^n)}(X) = \sum_{k=1}^{n} T_b^{(p^k)}(X^{p^{n-k}}) \text{ and } S_c^{(q^m)}(X) = \sum_{l=1}^{m} T_c^{(q^l)}(X^{q^{m-l}}).$$

As noted before, the sequence s^∞ defined by (5) for $N = p^2$ is the same as in [15]. In this case, $S_b^{(p^n)}(X) + 1$ is the polynomial of generalized cyclotomic sequence with period p^n considered in [16]. The properties of this polynomial are studied in [15,16].

In the next lemma, we will recall the properties of this polynomial that are necessary in what follows.

Let α be a primitive N-th root of unity in the extension of $\mathbb{F}_2$. Since $\gcd(p^n, q^m) = 1$ then there exist integers x, y such that $xp^n + yq^m = 1$. Define $\beta = \alpha^{yq^m}$ and $\gamma = \alpha^{xp^n}$. Then $\alpha = \beta\gamma$, also β and γ are primitive p^n-th and q^m-th roots of unity, respectively. Denote $\beta_k = \beta^{p^{n-k}}$, $k = 1, 2 \dots, n$ and $\gamma_l = \gamma^{q^{m-l}}$, $l = 1, 2 \dots, m$.

Lemma 2 *[16]. For any $a \in \eta^t C^{(p^k)}$, we see that*

(i) $S_i^{(p^k)}(\beta_k^{p^d a}) = S_{i+t}^{(p^{k-d})}(\beta_{k-d}) + (p^d - 1)/2 \bmod 2$ *for* $0 \le d < k$.

(ii) $S_i^{(p^k)}(\beta_k^a) + S_{i+d_k/2}^{(p^k)}(\beta_k^a) = 1$, *where* $d_k = p^{k-1} f/2$.

(iii) Let p be a non-Wieferich prime. Then $S_i^{(p^k)}(\beta_k) \notin \{0,1\}$ for $k > 1$.

(iv) Let p be a non-Wieferich prime. Then $S_i^{(p^k)}(\beta_k) + S_{i+f/2}^{(p^k)}(\beta_k) \neq 1$ for $k > 1$.

(v)

$$\begin{aligned}&|\{j \mid S_i^{(p^k)}(\beta_k) = 0 \text{ (or } 1),\ j = 1,2,\ldots,p^k - 1)\}| \\ &= |\{j \mid S_i^{(p)}(\beta_1^j) = 0 \text{ (or } 1), j = 1,2,\ldots,p-1\}| = r_p \cdot \mathrm{ord}_p(2),\end{aligned}$$

where r_p is an integer satisfying inequality $0 \le r_p \le \frac{p-1}{2\,\mathrm{ord}_p(2)}$.

Similarly, $S_c^{(q^m)}(X) + 1$ is the generating polynomial of sequence defined by (5) for $v = q^m$. Hence, the properties of $S_c^{(q^m)}(X)$ are the same as those of $S_b^{(p^n)}(X)$ (of course, we need to use q^m instead of p^n).

3.1 The Values of Subsidiary Polynomials

In this subsection we will show that the values of subsidiary polynomials define the values of $S(\alpha^j)$. Here and further we always suppose that $\gcd(p, q-1) = \gcd(p-1, q) = 1$.

Lemma 3. *Let $v = p^k q^l, k = 1,2,\ldots,n;\ l = 1,2,\ldots,m$ and $j \in \mathbb{Z}_N, j \neq 0$. Then*

$$\sum_{i \in \frac{N}{v} C_1^{(v)}} \alpha^{ij} = \begin{cases} T_b^{(p^k)}(\beta^{jp^{n-k}q^{m-l}}), & \text{if } j \equiv 0 \pmod{q^{l-1}} \text{ and } j \not\equiv 0 \pmod{q^l}, \\ 0, & \text{otherwise}. \end{cases}$$

Proof. According to the choice of α, β, γ we obtain that

$$\sum_{i \in p^{n-k}q^{m-l} C_1^{(v)}} \alpha^{ij} = \sum_{u \in C_1^{(v)}} \beta^{ujp^{n-k}q^{m-l}} \gamma^{\mu jp^{n-k}q^{m-l}}.$$

Since by Lemma 1 $C_1^{(v)} \bmod p^k = C_1^{(p^k)}$ and $C_1^{(v)} \bmod q^l = \mathbb{Z}_{q^l}^*$, it follows that

$$\sum_{i \in p^{n-k}q^{m-l} C_1^{(v)}} \alpha^{ij} = \sum_{u \in C_1^{(p^k)}} \beta^{ujp^{n-k}q^{m-l}} \cdot \sum_{u \in \mathbb{Z}_{q^l}^*} \gamma^{\mu jp^{n-k}q^{m-l}}.$$

Denote $\gamma^{p^{n-k}q^{m-l}}$ by $\tilde{\gamma}_l$. Then $\tilde{\gamma}_l$ is a primitive q^l-th root of unity since $\gcd(p-1, q) = 1$.

Let $A_l = \sum_{u \in \mathbb{Z}_{q^l}^*} \tilde{\gamma}_l^{\mu j}$. It is clear

$$A_1 \pmod 2 = \begin{cases} 1, & \text{if } j \not\equiv 0 \pmod q, \\ 0, & \text{if } j \equiv 0 \pmod q. \end{cases}$$

Suppose $l > 1$; then

$$A_l = \sum_{u \in \mathbb{Z}_{q^l}} \tilde{\gamma}_l^{\mu j} - \sum_{u \in q\mathbb{Z}_{q^{l-1}}} \tilde{\gamma}_l^{\mu j} = \sum_{u \in \mathbb{Z}_{q^l}} \tilde{\gamma}_l^{\mu j} - \sum_{u \in \mathbb{Z}_{q^{l-1}}} \tilde{\gamma}_l^{\mu jq}.$$

We consider the following three cases.

(i) Let $j \not\equiv 0 \pmod{q^{l-1}}$. Obviously here $A_l = 0$.
(ii) Let $j \equiv 0 \pmod{q^{l-1}}$ and $j \not\equiv 0 \pmod{q^l}$. In this case $A_l \equiv 0 - q^{l-1} \equiv 1 \pmod 2$.
(iii) Suppose $j \equiv 0 \pmod{q^l}$; then $A_l = q^l - q^{l-1}$ and $A_l \bmod 2 = 0$.

This completes the proof of this lemma.

□

Lemma 4. *Let $j = q^a j_0$ and $\gcd(j_0, q) = 1$, $0 \le a \le m$. Then*

$$\sum_{k=1}^{n} \sum_{l=1}^{m} \sum_{i \in p^{n-k} q^{m-l} C_1^{(p^k q^l)}} \alpha^{ij} = \begin{cases} S_b^{(p^n)}(\beta^{jq^{m-a-1}}), & \text{if } a < m, \\ 0, & \text{if } a = m. \end{cases}$$

Proof. If $a = m$ then $j \equiv 0 \pmod{q^l}$ for $l = 1, 2, \ldots, m$ and by Lemma 3 we observe that $\sum_{l=1}^{m} \sum_{i \in p^{n-k} q^{m-l} C_1^{(p^k q^l)}} \alpha^{ij} = 0$.

Let $a < m$. In this case $j \equiv 0 \pmod{q^a}$ and $j \not\equiv 0 \pmod{q^{a+1}}$. Then again by Lemma 3 we have

$$\sum_{l=1}^{m} \sum_{i \in p^{n-k} q^{m-l} C_1^{(p^k q^l)}} \alpha^{ij} = \sum_{i \in p^{n-k} q^{m-a-1} C_1^{(p^k q^{a+1})}} \alpha^{ij} = T_b^{(p^k)}(\beta^{jp^{n-k} q^{m-a-1}}).$$

Thus, by definitions of $T_b^{(p^k)}(X)$ and $S_b^{(p^n)}(X)$ we see that

$$\sum_{k=1}^{n} \sum_{l=1}^{m} \sum_{i \in p^{n-k} q^{m-l} C_1^{(p^k q^l)}} \alpha^{ij} = \sum_{k=1}^{n} T_b^{(p^k)}(\beta^{jp^{n-k} q^{m-a-1}}) = S_b^{(p^n)}(\beta^{jq^{m-a-1}}).$$

□

Lemma 5. *Let $j = q^a j_0$ and $\gcd(j_0, q) = 1$, $0 \le a \le m$. Then*

(i) $S(\alpha^j) = S_b^{(p^n)}(\beta^{jq^{m-a-1}}) + S_b^{(p^n)}(\beta^{jq^m}) + S_c^{(q^m)}(\gamma^{jp^n}) + 1$ *for* $a < m$,
(ii) $S(\alpha^j) = S_b^{(p^n)}(\beta^{jq^m}) + (q^m + 1)/2$ *for* $a = m$.

Proof. By (4) and (5) we see that

$$S(\alpha^j) = \sum_{k=1}^{n} \sum_{l=1}^{m} \sum_{i \in p^{n-k} q^{m-l} C_1^{(p^k q^l)}} \alpha^{ij} + \sum_{k=1}^{n} \sum_{i \in p^{n-k} q^m C_1^{(p^k)}} \alpha^{ij} + \sum_{l=1}^{m} \sum_{i \in p^n q^{m-l} C_1^{(q^l)}} \alpha^{ij} + 1.$$

The first sum in the last relation is studied in Lemma 4. Using the definition of subsidiary polynomials and equality $\alpha = \beta\gamma$ we get that

$$\sum_{k=1}^{n} \sum_{i \in p^{n-k} q^m C_1^{(p^k)}} \alpha^{ij} = \sum_{k=1}^{n} \sum_{j \in C_1^{(p^k)}} \beta^{jp^{n-k}q^m} \gamma^{jp^{n-k}q^m} = \sum_{k=1}^{n} \sum_{i \in C_k^{(p^k)}} \beta^{ip^{n-k}q^m} = S_b^{(p^n)}(\beta^{jq^m}).$$

and

$$\sum_{l=1}^{m} \sum_{i \in p^n q^{m-l} C_1^{(q^l)}} \alpha^{ij} = \sum_{l=1}^{m} \sum_{j \in C_1^{(q^l)}} \beta^{jp^n q^{m-l}} \gamma^{jp^n q^{m-l}} = \sum_{l=1}^{m} \sum_{i \in C_1^{(q^l)}} \gamma^{jp^n q^{m-l}} = S_c^{(q^m)}(\gamma^{jp^n}).$$

Then the statement of this lemma follows from Lemma 4. □

3.2 The Values of Generating Polynomial

Here and further we will always suppose that $2^{p-1} \not\equiv 1 \pmod{p^2}$, $2^{q-1} \not\equiv 1 \pmod{q^2}$ and $\gcd(p, q-1) = \gcd(p-1, q) = 1$.

As usual, we denote by $\mathbb{F}_2(\beta_k)$ a simple extension of $\mathbb{F}_2$ obtained by adjoining an algebraic element β_k and by $[\mathbb{F}_2(\beta_k) : \mathbb{F}_2]$ the dimension of the vector space $\mathbb{F}_2(\beta_k)$ over $\mathbb{F}_2$ [2]. Here $\beta_k = \beta^{p^{n-k}}, k = 1, \ldots, n$ and $\gamma_l = \gamma^{q^{m-l}}, l = 1, \ldots, m$, as before. It is well known that if $r_1 = [\mathbb{F}_2(\beta_1) : \mathbb{F}_2]$ then r_1 divides $p-1$ and if $t_1 = [\mathbb{F}_2(\gamma_1) : \mathbb{F}_2]$ then t_1 divides $q-1$ [2]. Let $\mathbb{K} = \mathbb{F}_2(\beta_1) \cap \mathbb{F}_2(\gamma_1)$. Then $\mathbb{K}$ is a finite field and $[\mathbb{K} : \mathbb{F}_2] = \gcd(r_1, t_1)$.

Lemma 6. *With notations as above, we have* $\mathbb{F}_2(\beta_k) \cap \mathbb{F}_2(\gamma_l) = \mathbb{K}$ *for* $k = 1, \ldots, n; l = 1, \ldots, m$.

Proof. Let $\mathbb{F} = \mathbb{F}_2(\beta_k) \cap \mathbb{F}_2(\gamma_l)$. Then $[\mathbb{F} : \mathbb{F}_2]$ divides $[\mathbb{F}_2(\beta_k) : \mathbb{F}_2]$ and $[\mathbb{F}_2(\gamma_l) : \mathbb{F}_2]$. According to [16] we know that $[\mathbb{F}_2(\beta_k) : \mathbb{F}_2] = p^{k-1} r_1$ and $[\mathbb{F}_2(\gamma_l) : \mathbb{F}_2] = q^{l-1} t_1$ for p, q such that $2^{p-1} \not\equiv 1 \pmod{p^2}$, $2^{q-1} \not\equiv 1 \pmod{q^2}$. Hence $[\mathbb{F} : \mathbb{F}_2]$ divides $\gcd(p^{k-1} r_1, q^{m-1} t_1)$. By the condition $\gcd(p, q-1) = \gcd(p-1, q) = 1$, then $[\mathbb{F} : \mathbb{F}_2]$ divides $\gcd(r_1, t_1)$. Thus, we get $[\mathbb{F} : \mathbb{F}_2]$ divides $[\mathbb{K} : \mathbb{F}_2]$. Since $\mathbb{K} \subset \mathbb{F}$, this completes the proof of this lemma.

□

Lemma 7. *Let notations be as above and* $S_c^{(q^m)}(\gamma^j) \in \mathbb{K}$ *for* $m > 1$. *Then* $j \equiv 0 \pmod{q^{m-1}}$.

Proof. By Lemma 2 (i) it is clear that without loss of generality it is enough to consider the case $c = 0$. Let u be an integer such that $2 \equiv g^u \pmod{q^m}$. Denote by r degree $[\mathbb{K} : \mathbb{F}_2]$. Since $S_c^{(q^m)}(\gamma^j) \in \mathbb{K}$, it follows that $S_0^{(q^m)}(\gamma^j) = S_0^{(q^m)}(\gamma^j)^{2^r}$. Then again by Lemma 2 (i) we get

$$S_0^{(q^m)}(\gamma^j) = S_0^{(q^m)}(\gamma^j)^{2^{ir}} = S_0^{(q^m)}(\gamma^{j2^{ir}}) = S_{iur}^{(q^m)}(\gamma^j) \text{ for } i = 0, 1, \ldots \tag{6}$$

Let $w=\gcd(q^{m-1}h,ur)$, where $h=(q-1)/e$ as before. There exist integers x,y such that $xq^{m-1}h+yur=w$. Then we see from (6) and Lemma 2 (i) that $S_0^{(q^m)}(\gamma^j)=S_{iw}^{(q^m)}(\gamma^j)$ for $i=0,1,\dots$. By [16] $\gcd(u,q)=1$ for $2^{q-1}\not\equiv 1 \pmod{q^2}$ and $\gcd(q,r)=1$ here. Hence $w=\gcd(h,ur)$ and w divides h. So, we observe that $S_0^{(q^m)}(\gamma^j)=S_{ih}^{(q^m)}(\gamma^j)$ for $i=0,1,\dots$.

Further, $S_t^{(q^m)}(\gamma^j)+S_{t+q^{m-1}h/2}^{(q^m)}(\gamma^j)=1$ for $t=0,1,\dots$ by Lemma 2 (ii). Thus,

$$S_{q^{m-1}h/2}^{(q^m)}(\gamma^j)=S_{q^{m-1}h/2+ih}^{(q^m)}(\gamma^j)$$

for $i=0,1,\dots$. Since

$$S_{q^{m-1}h/2+(q^{m-1}+1)h/2.}^{(q^m)}(\gamma^j)=S_{q^{m-1}h+h/2}^{(q^m)}(\gamma^j)=S_{h/2}^{(q^m)}(\gamma^j),$$

it follows that $S_0^{(q^m)}(\gamma^j)+S_{h/2}^{(q^m)}(\gamma^j)=1$. According to Lemma 2 (iii), in this case $j\equiv 0 \pmod{q^{m-1}}$.

□

Let k_0 be the same as before, i.e., $k_0=0$ or $k_0>0$ is the largest integer such that $q^m\in D^{(p^{k_0})}$ or $q^m\in\eta^{p^{k_0-1}f/2}D^{(p^{k_0})}$.

Lemma 8. *Let* $j\in p^{n-k}q^{m-1}\mathbb{Z}^*_{p^kq^{m-1}}, 1\le k\le n$ *and* $S_b^{(p^n)}(\beta^j)+S_b^{(p^n)}(\beta^{jq^m})\in\mathbb{K}$ *for* $n>1$. *Then* $j\equiv 0 \pmod{p^{n-1}}$ *or* $k\le k_0$.

Proof. Without loss of generality it is enough to consider the case $b=0$. Let $j=p^{n-k}q^{m-1}t$, where $\gcd(t,pq)=1$. If $k=1$ then $j\equiv 0 \pmod{p^{n-1}}$. So, this lemma is right for $k=1$.

Let $k>1$ and denote $\beta^{p^{n-k}q^{m-1}t}$ by $\tilde{\beta}_k$. Then $\tilde{\beta}_k$ is a primitive p^k-th root of unity and $S_0^{(p^k)}(\tilde{\beta}_k)+S_0^{(p^k)}(\tilde{\beta}_k^{q^m})\in\mathbb{K}$ by Lemma 2 (i).

Suppose $k>k_0$; then $q^m\in\eta^z D^{(p^k)}$ for $z\ne 0$ and $z\ne p^{k-1}f/2$. By Lemma 2 (i) we get that $S_0^{(p^k)}(\tilde{\beta}_k)+S_z^{(p^k)}(\tilde{\beta}_k)\in\mathbb{K}$.

We can show in the same way as in Lemma 7 that

$$S_0^{(p^k)}(\tilde{\beta}_k)+S_z^{(p^k)}(\tilde{\beta}_k)=S_{f/2}^{(p^k)}(\tilde{\beta}_k)+S_{z+f/2}^{(p^k)}(\tilde{\beta}_k).$$

Using the definitions of $S_i^{(p^k)}(X)$ and $T_i^{(p^k)}(X)$ we obtain that

$$T_0^{(p^k)}(\tilde{\beta}_k)+T_{f/2}^{(p^k)}(\tilde{\beta}_k)+T_z^{(p^k)}(\tilde{\beta}_k)+T_{z+f/2}^{(p^k)}(\tilde{\beta}_k)\in\mathbb{F}_2(\beta_{k-1}).$$

Let $\mathscr{D}=D^{(p^k)}\cup\dots\cup\eta^{f/2-1}D^{(p^k)}\cup\eta^{p^{k-1}f/2}D^{(p^k)}\cup\dots\cup\eta^{p^{k-1}f/2+f/2-1}D^{(p^k)}$ and $\mathscr{C}=\eta^z\mathscr{D}$. Then

$$T_0^{(p^k)}(\tilde{\beta}_k)+T_{f/2}^{(p^k)}(\tilde{\beta}_k)=\sum_{i\in\mathscr{D}}\tilde{\beta}_k^i$$

and

$$T_z^{(p^k)}(\tilde{\beta}_k) + T_{z+f/2}^{(p^k)}(\tilde{\beta}_k) = \sum_{i \in \mathscr{C}} \tilde{\beta}_k^i.$$

It is clear that $|\mathscr{D}| = |\mathscr{C}| = p-1$ and $\mathscr{D} \pmod p = \mathscr{C} \pmod p = \mathbb{Z}_p^*$.

Denote by $x_i \in \mathscr{D}$ and $y_i \in \mathscr{C}$, respectively, such that $x_i \mod p = y_i \mod p = i$, $i = 1, \ldots, p-1$. Then

$$\sum_{i \in \mathscr{D}} \tilde{\beta}_k^i = \sum_{i=1}^{p-1} \tilde{\beta}_{k-1}^{(x_i - i)/p} \cdot \tilde{\beta}_k^i \text{ and } \sum_{i \in \mathscr{C}} \tilde{\beta}_k^i = \sum_{i=1}^{p-1} \tilde{\beta}_{k-1}^{(y_i - i)/p} \cdot \tilde{\beta}_k^i.$$

Suppose that for any i we have $\tilde{\beta}_{k-1}^{(x_i-i)/p} = \tilde{\beta}_{k-1}^{(y_i-i)/p}$. Then $x_i \equiv y_i \pmod{p^k}$ for $i = 1, 2, \ldots, p-1$. Hence $\mathscr{D} = \mathscr{C}$. Then $z = 0$ or $z = p^{k-1} f/2$. This is impossible because $k > k_0$. Thus, we have that the polynomial $f(X) = \sum_{i=0}^{p-1} (\tilde{\beta}_{k-1}^{(x_i-i)/p} + \tilde{\beta}_{k-1}^{(y_i-i)/p}) X^i$ has at least one nonzero coefficient and $f(\tilde{\beta}_k) \in \mathbb{F}_2(\beta_{k-1})$. This is impossible since $\deg f(X) < p$ and $[\mathbb{F}_2(\beta_k) : \mathbb{F}_2(\beta_{k-1})] = p$ for $k > 1$. So, $k \le k_0$. □

4 The Proof of Main Theorem

In this section we finish the proof of Theorem 1 in the following two Lemmas.

Lemma 9. *Let notation be as above and $k_0 > 0$. Let $2^{p-1} \not\equiv 1 \pmod{p^2}$, $2^{q-1} \not\equiv 1 \pmod{q^2}$, $\gcd(p, q-1) = \gcd(p-1, q) = 1$ and let s^∞ be defined by (5). Then*

$$\mathrm{LC}(s^\infty) = N - r_p \cdot \mathrm{ord}_p(2) - p^{k_0} r_q \cdot \mathrm{ord}_q(2) - \delta,$$

where

$$\delta = \begin{cases} 1, & \text{if } (p^n q^m + 1)/2 \text{ is even}, \\ 0, & \text{if } (p^n q^m + 1)/2 \text{ is odd} \end{cases}$$

and $0 \le r_p \le \frac{p-1}{2\,\mathrm{ord}_p(2)}$, $0 \le r_q \le \frac{q-1}{2\,\mathrm{ord}_q(2)}$.

Proof. As noted before we have

$$\mathrm{LC}(s^\infty) = N - \Big| \{ j \mid S(\alpha^j) = 0,\ j = 0, 1, \ldots, N-1 \} \Big|.$$

First of all we note that by definition $S(1) = (p^n q^m + 1)/2$. Further, according to Lemma 5 we have

$$S(\alpha^j) = S_b^{(p^n)}(\beta^{j q^{m-a-1}}) + S_b^{(p^n)}(\beta^{j q^m}) + S_c^{(q^m)}(\gamma^{j p^n}) + 1 \tag{7}$$

for $j = q^a j_0$, $a < m$, $\gcd(j_0, q) = 1$ and

$$S(\alpha^j) = S_b^{(p^n)}(\beta^{j q^m}) + (q^m + 1)/2$$

for $j = q^m j_0$.

Let $S(\alpha^j)=0,\ 1\le j\le N-1$. We consider a few cases.

(i) Suppose $j\equiv 0 \pmod{q^m}$; then $S(\alpha^j)=S_b^{(p^n)}(\beta^{jq^m})$ for even $(q^m+1)/2$ and $S(\alpha^j)=S_b^{(p^n)}(\beta^{jq^m})+1$ for odd $(q^m+1)/2$. By Lemma 2 (v) we get

$$|\{j|\ S(\alpha^j)=0,\ j=q^m,\dots,(p^n-1)q^m\}|=$$
$$|\{j|\ S_b^{(p)}(\beta_1^j)=0,\ (\text{ or } 1), j=1,2,\dots,p-1\}|=r_p\cdot \mathrm{ord}_p(2).$$

(ii) Let $j\not\equiv 0 \pmod{q^m}$. According to (7) we see that

$$S_b^{(p^n)}(\beta^{jq^{m-a-1}})+S_b^{(p^n)}(\beta^{jq^m})=-S_c^{(q)}(\gamma^{jp^n})-1.$$

Hence $S_c^{(q^m)}(\gamma^{jp^n})\in\mathbb{F}_2(\beta)$. Then by Lemma 6 we get

$$S_c^{(q^m)}(\gamma^{jp^n})\in\mathbb{K}=\mathbb{F}_2(\beta_1)\cap\mathbb{F}_2(\gamma_1).$$

In this case, by Lemma 7 we have $j\equiv 0 \pmod{q^{m-1}}$. Hence $j\in p^{n-k}q^{m-1}\mathbb{Z}^*_{p^kq}$ for $k:\ 1\le k\le n$ and the sum $S_b^{(p^n)}(\beta^j)+S_b^{(p^n)}(\beta^{jq^m})$ also belongs to $\mathbb{K}$. Further by Lemma 8 we get $k\le k_0$ or $j\equiv 0 \pmod{p^{n-1}}$. If $j\equiv 0 \pmod{p^{n-1}}$ then $k=1$ and since $k_0>0$, it follows that $k\le k_0$ in any case.

By choosing k_0 we see that $q^m\in D^{(p_0^k)}$ or $q^m\in\eta^{p^{k_0-1}f/2}D^{(p_0^k)}$. Hence for any $j:$ $j\equiv 0 \pmod{p^{n-k_0}}$ we have

$$S_b^{(p^n)}(\beta^{jq^m})=\begin{cases}S_b^{(p^n)}(\beta^j), & \text{if } q^m\in D^{(p_0^k)},\\ S_{b+p^{k-1}f/2}^{(p^n)}(\beta^j), & \text{if } q^m\in\eta^{p^{k_0-1}f/2}D^{(p_0^k)}.\end{cases}$$

In any case, by Lemma 2 (ii) $S_b^{(p^n)}(\beta^j)+S_b^{(p^n)}(\beta^{jq^m})$ is equal to 0 or 1 for all $j\in p^{n-k_0}q^{m-1}\mathbb{Z}_{p^{k_0}q}$ and $j\not\equiv 0 \pmod{q^m}$.

Then, according to (7) we obtain $S_c^{(q^m)}(\gamma^{jp^n})=S_c^{(q)}(\gamma_1^{j_0p^n})\in\{0,1\}$ where $j=q^{m-1}j_0$, $\gcd(j_0,q)=1$. In this case, by Lemma 2 (v) we have

$$|\{j|\ S_b^{(p)}(\beta_1^{j_0})=0,\ (\text{ or } 1), j_0=1,2,\dots,p-1\}|=r_p\cdot\mathrm{ord}_p(2).$$

For fixed j_0 we have p^{k_0} numbers from $\mathbb{Z}_{p^{k_0}q}$ with the same residue modulo q. Thus, we get

$$|\{j\ \mid\ S(\alpha^j)=0,\ \ j=1,2,\dots,N,\ \ j\not\equiv 0 \pmod{q^m}\}|=p^{k_0}r_q\cdot\mathrm{ord}_q(2),$$

where $0\le r_q\le\frac{q-1}{2\,\mathrm{ord}_q(2)}$.

Finally, we get $|\{j\mid S(\alpha^j)=0,\ j=1,2,\dots,N,\}|=r_p\cdot\mathrm{ord}_p(2)+p^{k_0}r_q\cdot\mathrm{ord}_q(2)$.

□

We consider a few examples with different values r_p, r_q and $k_0=1$.

Example 1. (i) $p = 19, q = 7, e = 3$, in this case $7 \in D^{(19)}$ and $r_p = 0, r_q \cdot \mathrm{ord}_7(2) = 3$. Hence $LC(s^\infty) = N - 19 \cdot 3$ for $n = 1,2; m = 1,2$.

(ii) $p = 7, q = 43, e = 3$, here $43 \in D^{(7)}$, but $r_p = 1, r_q = 0$. Hence $LC(s^\infty) = 301 - 1 \cdot 3 = 298$.

(iii) $p = 43, q = 7, e = 3$, here $f = 14$, $7 \in \eta^7 D^{(43)}$ and $r_p = 0, r_q \cdot \mathrm{ord}_7(2) = 3$. Hence $LC(s^\infty) = 301 - 43 \cdot 3 = 172$. Similarly, for $n = 1,2; m = 1,2$.

(iv) $p = 41, q = 31, e = 5, f = 8$, $31 \in \eta^4 D^{(41)}$, $r_p = 0, r_q \cdot \mathrm{ord}_3\, 1(2) = 15$. Finally, $LC(s^\infty) = 1271 - 41 \cdot 15 - 1 = 655$.

(v) $p = 7, q = 73, e = 3$, here $f = 2$, $73 \in \eta D^{(7)}$ and $r_p = 1, r_q \cdot \mathrm{ord}_{73}(2) = 7 \cdot 18$. Hence $LC(s^\infty) = 511 - 7 \cdot 18 - 3 - 1 = 381$.

Lemma 10. *Let notation be as above and $k_0 = 0$. Let $2^{p-1} \not\equiv 1 \pmod{p^2}$, $2^{q-1} \not\equiv 1 \pmod{q^2}$, $\gcd(p, q-1) = \gcd(p-1, q) = 1$ and let s^∞ be defined by (5). Then*

$$\mathrm{LC}(s^\infty) = N - r_N \cdot \mathrm{ord}_{pq}(2) - r_p \cdot \mathrm{ord}_p(2) - r_q \cdot \mathrm{ord}_q(2) - \delta,$$

where $0 \le r_N \le \frac{(p-1)(q-1)}{2\,\mathrm{ord}_{pq}(2)}$ and

$$\delta = \begin{cases} 1, & \text{if } (p^n q^m + 1)/2 \text{ is even}, \\ 0, & \text{if } (p^n q^m + 1)/2 \text{ is odd}. \end{cases}$$

Proof. Let $S(\alpha^j) = 0, j \ne 0$. As in Lemma 9 we obtain that $|\{j \mid S(\alpha^j) = 0,\ j = q^m, \ldots, (p^n - 1)q^m\}| = r_p \cdot \mathrm{ord}_p(2)$ and if $j \not\equiv 0 \pmod{q^m}$ then $S_c^{(q^m)}(\gamma^{jp^n}) \in \mathbb{K}$ and $S_b^{(p^n)}(\beta^j) + S_b^{(p^n)}(\beta^{jq^m}) \in \mathbb{K}$.

In the last case, according to Lemma 7 and 8 we get that $j \equiv 0 \pmod{q^{m-1}}$ and $j \equiv 0 \pmod{p^{n-1}}$. Further, if $j \equiv 0 \pmod{p^n}$ then by Lemma 5 we have $S(\alpha^j) = S_c^{(q)}(\gamma^{jp^n}) + 1$ and in this case we observe that $|\{j \mid S(\alpha^j) = 0,\ j = p^n, \ldots, (q^m - 1)p^n\}| = r_q \cdot \mathrm{ord}_q(2)$ by Lemma 2 (v).

Suppose $j = p^{n-1} q^{m-1} t$ and $\gcd(t, pq) = 1$. Then by Lemma 7 and Lemma 2 (i)

$$S(\alpha^j) = S_b^{(p)}(\beta_1^{tq^{m-1}}) + S_b^{(p)}(\beta_1^{tq^{2m-1}}) + S_c^{(q)}(\gamma_1^{tp^{2n-1}}) + 1.$$

It is clear that if $S(\alpha^j) = 0$ then $S(\alpha^j)^{2^u} = 0$ for $u = 0, 1, \ldots, \mathrm{ord}_{pq}(2)$. Hence, $|\{j : S(\alpha^j) = 0,\ j \in \mathbb{Z}_{pq}| = r_N \cdot \mathrm{ord}_{pq}(2)$ for the some r_N.

Let $w = \zeta_p^{f/2} \zeta_q^{h/2}$. Then $w \equiv \eta^{f/2} \pmod{p}$ and $w \equiv \xi^{h/2} \pmod{q}$. So, by Lemma 2 (i) we obtain

$$S(\alpha^{wj}) = S_{b+f/2}^{(p)}(\beta_1^{tq^{m-1}}) + S_{b+f/2}^{(p)}(\beta_1^{tq^{2m-1}}) + S_{c+h/2}^{(q)}(\gamma_1^{tp^{2n-1}}) + 1.$$

Hence, by Lemma 2 (ii) we see that $S(\alpha^{wj}) = S(\alpha^j) + 1$. Thus, $0 \le r_N \le \frac{(p-1)(q-1)}{2\,\mathrm{ord}_{pq}(2)}$. This completes the proof of this lemma. □

The statement of Theorem 1 follows from Lemmas 9 and 10.

The following examples show that in this case the value r depends on N, so we are using a denotation r_N.

Example 2. (i) Let $p = 73, q = 7, e = 3, b = 0, c = 0$. Here $7 \in \eta^9 D^{(73)}$, $r_p \cdot \mathrm{ord}_p(2) = 18, r_q \cdot \mathrm{ord}_q(2) = 3$ and $\mathrm{ord}_{511}(2) = 9$.

For $n = m = 1$ we get $LC(s^\infty) = 435 = 511 - 76$, in this case $r_N = 5$.

For $n = 1, m = 2$ we have $LC(s^\infty) = 3577 - 18 - 3 = 3556$, i.e., $r_N = 0$.

(ii) Let $p = 41, q = 11, e = 5, n = 2, m = 1, b = 0, c = 0$.

Here $\mathrm{ord}_{pq}(2) = 20$. For $n = 1, 2; m = 1, 3$ we get $LC(s^\infty) = N - 101$ ($r_N = 5$), and $LC(s^\infty) = N - 200$ ($r_N = 10$) if $n = 1, 2; m = 2$.

5 Conclusions

Pseudorandom sequences are widely used in communication, radar navigation, cryptography and some other scenarios. By using the new generalized cyclotomy presented by Zeng et al., we constructed a new kind of generalized cyclotomic sequences with period $p^n q^m$ where p, q are odd distinct primes and n, m are natural numbers. Thus, we generalized the results obtained in [15–17].

Our results show that such sequences have high linear complexity and are suitable for applications. To illustrate the results, some examples are presented. For further study, the k-error linear complexity, autocorrelation, 2-adic complexity and some other cryptographic properties of these sequences may be interesting topics.

References

1. Golomb, S.W.: Shift Register Sequences. Holden-Day, San Francisco (1967)
2. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and Its Applications, vol. 20. Addison-Wesley (1983)
3. Ding, C., Helleseth, T.: New generalized cyclotomy and its applications. Finite Fields Their Appl. **4**(2), 140–166 (1998)
4. Whiteman, A.L.: A family of difference sets. Illinois J. Math. **6**, 107–121 (1962)
5. Ding, C., Helleseth, T.: Generalized cyclotomic codes of length $p_1^{e_1} \cdots p_t^{e_t}$. IEEE Trans. Inf. Theory **45**(2), 467–474 (1999)
6. Fan, C., Ge, G.: A unified approach to Whiteman's and Ding-Helleseth's generalized cyclotomy over residue class rings. IEEE Trans. Inf. Theory **60**(2), 1326–1336 (2014)
7. Du, X., Chen, Z.: A generalization of the Hall's sextic residue sequences. Inf. Sci. **222**, 784–794 (2013)
8. Yan, T., Li, S., Xiao, G.: On the linear complexity of generalized cyclotomic sequences with the period p^m. Appl. Math. Lett. **21**(2), 187–193 (2008)
9. Chen, X., Chen, Z., Liu, H.: A family of pseudorandom binary sequences derived from generalized cyclotomic classes modulo $p^{m+1}q^{n+1}$. Int. J. Netw. Secur. **22**(4), 610–620 (2020)
10. Hu, L., Yue, Q., Wang, M.H.: The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$. IEEE Trans. Inf. Theory **58**(8), 5533–5543 (2012)
11. Kim, Y.J., Song, H.Y.: Linear complexity of prime n-square sequences. In: 2008 IEEE International Symposium on Information Theory, pp. 2405–2408 (2008)
12. Ke, P., Zhang, J., Zhang, S.: On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^m$. Des. Codes Cryptogr. **67**(3), 325–339 (2013)
13. Zeng, X., Cai, H., Tang, X., Yang, Y.: Optimal frequency hopping sequences of odd length. IEEE Trans. Inf. Theory **59**(5), 3237–3248 (2013)

14. Xu, S., Cao, X., Mi, J., Tang, C.: More cyclotomic constructions of optimal frequency-hopping sequences. Adv. Math. Commun. **13**(3), 373–391 (2019)
15. Xiao, Z., Zeng, X., Li, C., Helleseth, T.: New generalized cyclotomic binary sequences of period p^2. Des. Codes Cryptogr. **86**(7), 1483–1497 (2018)
16. Edemskiy, V., Li, C., Zeng, X., Helleseth, T.: The linear complexity of generalized cyclotomic binary sequences of period p^n. Des. Codes Cryptogr. **87**(5), 1183–1197 (2019)
17. Ye, Z., Ke, P., Wu, C.: A further study of the linear complexity of new binary cyclotomic sequence of length p^n. Appl. Algebra Eng. Commun. Comput. **30**(3), 217–231 (2019)
18. Ouyang, Y., Xie, X.: Linear complexity of generalized cyclotomic sequences of period $2p^m$. Des. Codes Cryptogr. **87**(5), 1–12 (2019)
19. Edemskiy, V., Wu, C.: On the linear complexity of binary sequences derived from generalized cyclotomic classes modulo $2^n p^m$. WSEAS Trans. Math. **18**, 197–202 (2019)
20. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory. Graduate Texts in Mathematics. Springer, New York (1990). https://doi.org/10.1007/978-1-4757-2103-4
21. Cusick, T., Ding, C., Renvall, A.: Stream Ciphers and Number Theory. Elsevier, North-Holland mathematical library (2004)