Cyclic Codes via the General Two-Prime Generalized Cyclotomic Sequence of Order Two

Xia Zhou

School of Economics and Management, Nanjing Institute of Technology, Nanjing 211167, China

Received 6 November 2020; Revised 23 November 2020; Accepted 4 December 2020; Published 23 December 2020

1. Introduction

Throughout this paper, assume that \( l \) is a power of a prime number \( r \). A linear \([n,k,d]\) code \( C \) over \( \mathbb{F}_l \) is defined as a \( k \)-dimensional subspace of \( \mathbb{F}_l^n \) with minimum distance \( d \), where \( \mathbb{F}_l \) is a finite field with order \( l \). The ring \( \mathbb{F}_l \) is called to be the generator polynomial of \( C \), respectively. Please refer to [1] for more details on cyclic codes.

Let \( s^n = (s_i)_{i=0}^{n-1} \) be a sequence with period \( n \) over \( \mathbb{F}_l \) and \( S(x) = \sum_{i=0}^{n-1} s_i x^i \in \mathbb{F}_l[x] \). At present, the methods of constructing cyclic codes are substantial. One of the important methods is to employ

\[
h(x) = \frac{x^n - 1}{\gcd(x^n - 1, S(x))},
\]

where \( h(x) \) is named as the generator polynomial of \( s^n \).

As is known to all, there are a good deal of results on cyclic codes in a series of papers [2–11]. Let \( p \) and \( q \) be two distinct prime numbers. In order to search for more residue difference sets, Whiteman [12] introduced a generalized cyclotomy regarding \( pq \). In 1997, Ding [13] introduced the Whiteman’s generalized cyclotomic sequence (WGCS) and studied its coding properties in [6, 7, 9, 11]. To be more specific, Ding [6] constructed three families of cyclic codes, some of which are optimal with regard to the minimum distance. In addition, Ding [7] presented many cyclic codes and their lower bounds about the minimum weight. Furthermore, based on a number of WGCSs of order 4 and order 6, some classes of cyclic codes were produced by Sun et al. [9] and Kewat and Kumari [11], respectively, whose lower bounds on the nonzero minimum weight were also provided.

As an important measure of the quality of a sequence, its linear complexity is defined as the length of the shortest linear feedback shift register which can produce this sequence. Nowadays, pseudorandom sequences with higher
linear complexity are widely used in communication systems and cryptography.

The main contributions of this article are as follows: firstly, we proved that there are only three classes of general-ized cyclotomic sequences with order two over \( \mathbb{Z}_{pq} \), see Lemmas 4 and 5. Specifically, the generalized cyclotomic sequences with order two in [12] and in [14, 15] are special cases of the first class and the second class, respectively. In essence, the generalized cyclotomic sequences with order two over \( \mathbb{Z}_{pq} \) in [7, 16] are exactly the first type and the second type, respectively. Secondely, by means of this general generalization of cyclotomic sequences, we constructed a class of the general two-prime GCSs of order two (see Definition 2) with period \( n \) over \( \mathbb{F}_q \), where \( n = pq \) and \( \gcd(l, n) = 1 \), and computed their minimal polynomials and linear complexities. The result shows that their linear complexities are high. Compared with the previous constructions of sequences with high linear complexity, our construction not only includes the aforementioned constructions in [14, 15] as special cases but also gives more parameters with high linear complexity due to the free choice of \( p \) and \( q \), see Remark 4. Particularly, if \( \gcd(p - 1, q - 1) \neq 2 \), these sequences are new. Thirdly, we employed these sequences to produce some families of cyclic codes. The idea of constructing cyclic codes employing special sequences in this paper is enlightened by [7]. Let us say it again, more optimal cyclic codes with new parameters can be generated by our construction compared to the cyclic codes obtained by [7], see Remark 3 for details.

2. Preliminaries

2.1. Minimal Polynomial and Linear Complexity. Suppose that the sequence \( s^l = s_0 s_1 s_2 \ldots s_{n-1} \), where \( s_i \in \mathbb{F}_q \) and \( \gcd(l, n) = 1 \). The sequence \( s^l \) is called to be linear feedback sequence, if there are \( L + 1 \) constants \( c_0 = 1, c_1, \ldots, c_L \in \mathbb{F}_q \), satisfying

\[
-c_0 s_i = c_1 s_{i-1} + c_2 s_{i-2} + \cdots + c_L s_{i-L}, \quad L \leq i \leq n - 1. \quad (2)
\]

It is widely known that such a positive integer \( L \) for any finite sequence always exists. Here, the linear complexity of the sequence \( s^l \) is defined as the minimal positive integer \( L \) and the feedback polynomial (or characteristic polynomial) of \( s^l \) is defined as the polynomial \( c(x) = c_0 + c_1 x + \cdots + c_L x^L \). Furthermore, the minimal polynomial of \( s^l \) is defined as the characteristic polynomial with the minimal length. It is demonstrated that the degree of its minimal polynomial of a periodic sequence is equal to its linear complexity. So far, there are many ways to calculate the minimal polynomial and linear complexity of a periodic sequence, one of which is stated as follows.

Lemma 1 (see [1]). Define

\[
S(x) = s_0 + s_1 x + \cdots + s_{n-1} x^{n-1} \in \mathbb{F}_q[x]. \quad (3)
\]

For the sequence \( s^l \), its minimal polynomial \( m(x) \) is given by

\[
m(x) = \frac{x^n - 1}{\gcd(x^n - 1, S(x))}. \quad (4)
\]

and its linear complexity \( L_s \) is determined by

\[
L_s = n - \deg(\gcd(x^n - 1, S(x))). \quad (5)
\]

2.2. Classical Cyclotomy with Order Two. Suppose that \( f \) is an integer and \( q = 2f + 1 \) is an odd prime number. Then, there exists a finite field \( G = \mathbb{F}_q \) with order \( q \). Furthermore, one can always find an element \( g \in G \) such that \( G^* = \langle g \rangle \), where \( G^* = G \setminus \{0\} \) is the set of nonzero elements of \( G \). Define the cyclotomic classes \( D_i^{(q)} \) with order two in \( G \):

\[
D_i^{(q)} = \{ g^2 \cdot i : s = 0, 1, \ldots, f - 1 \}, \quad i = 0, 1. \quad (6)
\]

For given integers \( i \) and \( j \), \( 0 \leq i, j \leq 1 \), the cyclotomic number \( (i, j)^{(q)} \) with order two regarding \( q \) is defined as

\[
(i, j)^{(q)} = (D_i^{(q)} + 1) \cap D_j^{(q)}. \quad (7)
\]

Now, we will recall the properties of the classical cyclotomy with order two in [17] as follows.

Lemma 2. Suppose that \( q = 2f + 1 \) is an odd prime number. Then,

\[
(0, 0)^{(q)} = \frac{q - (-1)^f}{4} - 1, \quad (0, 1)^{(q)} = \frac{q - (-1)^f}{4}, \quad (1, 0)^{(q)} = \frac{q - 2 - (-1)^f}{4}.
\]

Let \( \gcd(q, l) = 1 \) and \( \Omega_l \) denote an algebraic closure of a finite field \( \mathbb{F}_q \). Define \( \eta_0 \) and \( \eta_1 \) as

\[
\eta_0 = \sum_{i \in D_0^{(q)}} \zeta_i, \quad \eta_1 = \sum_{i \in D_1^{(q)}} \zeta_i \quad (9)
\]

where \( \zeta_i \in \Omega_l \) is a \( q \)-th primitive root of unity; \( D_0^{(q)} \) and \( D_1^{(q)} \) are the cyclotomic classes with order two regarding \( q \).

When \( 2 \nmid l \), \( \eta_i (i = 0, 1) \) over \( \Omega_l \) are identified by the following lemma.

Lemma 3 (see [18]). Let the symbols be the same as before. Then,

\[
[\eta_0, \eta_1] = \left\{ \frac{1}{2} \left( -1 \pm \sqrt{-1/\left( q \right)^{-1}} \right) \right\}, \quad (10)
\]

where \( (\cdot) \) is the Legendre symbol.

2.3. The General Two-Prime Generalized Cyclotomic Sequence of Order Two. Suppose that \( \mathbb{Z}_n \) is the residue class ring modulo \( n \) and \( \mathbb{Z}_n^* = \{ x : \gcd(x, n) = 1, 1 \leq x \leq n - 1 \} \), where \( n \)
is a positive integer. Let \( \phi(n) \) denote the Euler function. For \( \gcd(a, n) = 1 \), if the multiplicative order of \( a \) modulo \( n \) is \( \phi(n) \), then \( a \) is named as a primitive root modulo \( n \).

**Definition 1.** A partition \( \{W_0, W_1, \ldots, W_{h-1}\} \) of \( \mathbb{Z}_n^* \) is a family of sets, satisfying

\[
W_i \cap W_j = \emptyset, \text{ for all } i \neq j, \quad i = 0, \ldots, h-1.
\]

If there exist a subgroup \( W_0 \) of \( \mathbb{Z}_n^* \), for any \( i \leq h-1 \), then \( W_i \) are called to be classical cyclotomic classes with order \( h \) if \( n \) is a prime number, and generalized cyclotomic classes with order \( h \) if \( n \) is a composite number. The (generalized) cyclotomic numbers with order \( h \) are defined as

\[
(i, j) = [(W_i + 1) \cap W_j], \quad 0 \leq i, j \leq h-1.
\]

**Lemma 4.** There are only three classes of generalized cyclotomies with order two regarding \( pq \).

**Proof.** Let \( D_0 \) be a fixed multiplicative subgroup of \( \mathbb{Z}_n^* \) with order \( \phi(n)/2 \). So, there exists \( a \in \mathbb{Z}_n^* \) such that

\[
\mathbb{Z}_n^* = D_0 \cup aD_0.
\]

Obviously, \( a \neq D_0 \) and \( a^2 \in D_0 \). Let

\[
H = (\mathbb{Z}_n^*)^2 = \{u^2 : u \in \mathbb{Z}_n^*\}.
\]

We next show that \( H \) is a multiplicative subgroup of \( D_0 \). It is straightforward to prove that \( H \) is a multiplicative subgroup of \( \mathbb{Z}_n^* \). We only need to show that \( H \subseteq D_0 \). For any \( h \in H \), there exists \( u \in \mathbb{Z}_n^* \) such that \( u^2 = h \). If \( u \in D_0 \), then \( h = D_0 \). If \( u \notin D_0 \), then there exists \( v \in D_0 \) such that \( u = av \) and \( h = u^2 = a^2v^2 \in D_0 \). Hence, \( H \) is a multiplicative subgroup of \( D_0 \) with order \( \phi(n)/2 \) and there exists \( \beta \in \mathbb{Z}_n^* \) such that \( D_0 = H \cup \beta H \). Finally, \( \mathbb{Z}_n^* = H \cup \beta H \cup aH \cup \beta aH \).

Therefore, \( W_0 = H \cup \beta H \cup H \cup \beta aH \) and the corresponding \( W_1 = aH \cup \beta aH \cup \beta H \cup aH \cup \beta H \). This finishes the proof of Lemma 4.

Suppose that \( g \) is a common primitive root modulo \( p \) and \( q \). Let \( x \) be a positive integer satisfying

\[
x \equiv 1 \pmod{q},
\]

\[
x \equiv g \pmod{p}.
\]

Assume that \( e = (p - 1)(q - 1)/d \), where \( d = \gcd(p - 1, q - 1) \). Therefore, the multiplicative group of \( \mathbb{Z}_n^* \) is as follows [12]:

\[
\mathbb{Z}_n^* = \{g^s x^t : 0 \leq s \leq e - 1; 0 \leq t \leq d - 1\}.
\]

According to Lemma 4, we easily verify the assertion as the following:

**Lemma 5.** There are only three classes of generalized cyclotomies with order two over \( \mathbb{Z}_{pq} \) as follows. The first generalized cyclotomic classes \( H_i^{(n)} (0 \leq i \leq 1) \) with order two are defined as

\[
H_i^{(n)} = \left\{ g^s x^{2i+1} : s = 0, 1, \ldots, e - 1; t = 0, 1, \ldots, d - 1 \right\}.
\]

The second generalized cyclotomic classes \( D_i^{(n)} (0 \leq i \leq 1) \) with order two are defined as

\[
D_i^{(n)} = \left\{ g^{2i+1} x^t : s = 0, 1, \ldots, e - 1; t = 0, 1, \ldots, d - 1 \right\},
\]

and the third generalized cyclotomic classes \( W_i^{(n)} (0 \leq i \leq 1) \) with order two are defined as

\[
W_i^{(n)} = \left\{ g^{2i+1} x^t : s = 0, 1, \ldots, e - 1; t = 0, 1, \ldots, d - 1 \right\},
\]

where the multiplications are operated modulo \( n \).

**Remark 1.** By definition, when \( \gcd(p - 1, q - 1) = 1 \), the first generalized cyclotomy with order two over \( \mathbb{Z}_{pq} \) is exactly Whitman’s generalized cyclotomy [12]. In essence, it is in accord with the one introduced by Ding [7]. When \( \gcd(p - 1, q - 1) = 2 \), the second generalized cyclotomy with order two over \( \mathbb{Z}_{pq} \) is identical to Ding-Helleseth’s generalized cyclotomy [2] in the case of \( v = pq \). Furthermore, this cyclotomy is the same as the extended generalized cyclotomy with order two presented by Wang and Lin [16]. For fixed \( p, q \), and \( x \) defined by (14), the third generalized cyclotomy is new. In [7], the linear complexity and minimal polynomial of generalized cyclotomic sequence with period \( n \) over \( \mathbb{F}_q \) based on the first generalized cyclotomy of order two have been determined. In addition, cyclic codes defined by this sequence were analyzed. Here, we only study the second generalized cyclotomy with order two in this paper.

The generalized cyclotomies with order two are defined by

\[
(i, j)^{(n)} = \left| \{D_i^{(n)} \cap D_j^{(n)}\} \right|, \quad 0 \leq i, j \leq 1.
\]

Define

\[
P = \{p, 2p, \ldots, (q - 1)p\},
\]

\[
Q = \{q, 2q, \ldots, (p - 1)q\},
\]

\[
C_1^{(n)} = P \cup D_1^{(n)},
\]

\[
C_0^{(n)} = \emptyset \cup Q \cup D_0^{(n)}.
\]

Then,

\[
\mathbb{Z}_n^* = C_0^{(n)} \cup C_1^{(n)},
\]

\[
C_0^{(n)} \cap C_1^{(n)} = \emptyset.
\]

**Definition 2.** The two-prime general generalized cyclotomic sequences (GGCS) of order two are defined by
where 0 and 1 are the zero element and identity element, respectively, in \( F_q \).

Remark 2. In [16], 0 and 1 in equation (22) are both in \( F_2 \). Hence, our sequence and the sequence defined by Wang and Lin are totally different.

### 3. A Family of New Cyclic Codes Defined by Our Sequences

#### 3.1. The Properties on the Generalized Cyclotomy with Order Two Over \( \mathbb{Z}_n \)

In this subsection, the following lemmas follow from [16].

**Lemma 6.** When \( q \equiv 1 \pmod{4} \), \(-1 \in D_0^{(n)} \). When \( q \equiv 3 \pmod{4} \), \(-1 \in D_1^{(n)} \).

**Lemma 7.** If \( q \equiv 1 \pmod{4} \), then
\[
(0,0)_2^{(n)} = \frac{(p-2)(q-5)}{4},
\]
\[
(0,1)_2^{(n)} = (1,0)_2^{(n)} = (1,1)_2^{(n)} = \frac{(p-2)(q-1)}{4}.
\]

If \( q \equiv 3 \pmod{4} \), then
\[
(0,1)_2^{(n)} = \frac{(p-2)(q+1)}{4},
\]
\[
(0,0)_2^{(n)} = (1,0)_2^{(n)} = (1,1)_2^{(n)} = \frac{(p-2)(q-3)}{4}.
\]

**Lemma 8**
\[
\left| D_0^{(n)} + \omega \right| \cap D_1^{(n)} = \begin{cases} 
(0,1)_2^{(n)}, & \text{if } \omega \in D_0^{(n)}, \\
(1,0)_2^{(n)}, & \text{if } \omega \in D_1^{(n)}.
\end{cases}
\]
\[
\left| D_1^{(n)} + \omega \right| \cap D_1^{(n)} = \begin{cases} 
(1,1)_2^{(n)}, & \text{if } \omega \in D_0^{(n)}, \\
(0,0)_2^{(n)}, & \text{if } \omega \in D_1^{(n)}.
\end{cases}
\]

**Lemma 9.** When \( \omega \in P \),
\[
\left| D_i^{(n)} + \omega \right| \cap D_j^{(n)} = \begin{cases} 
(p-1)(i,j)_2^{(q)}, & \text{if } \frac{\omega}{q} = 1, \\
(p-1)(i+1,j)_2^{(q)}, & \text{if } \frac{\omega}{q} = -1.
\end{cases}
\]

When \( \omega \in Q \),
\[
\left| D_i^{(n)} + \omega \right| \cap D_j^{(n)} = \begin{cases} 
\frac{(p-2)(q-1)}{2}, & \text{if } i = j, \\
0, & \text{if } i \neq j.
\end{cases}
\]

#### 3.2. The Parameters of the Code \( C_r \), Minimal Polynomial, and Linear Complexity of the Sequence \( s^n \)

Let \( p \) and \( q \) be two different odd prime numbers with \( n = pq \) and \( l \) be a power of a prime number \( r \). We always assume that \( \gcd(n,l) = 1 \) and \( m \) is the order of \( l \) modulo \( n \). Define
\[
S(x) = \sum_{i \in C_1^{(n)}} x^i = \left( \sum_{i \in D_1^{(n)}} + \sum_{i \in P} \right) x^i \in F_q[x].
\]

Our main objective in this section is to compute the generator polynomial
\[
g(x) = \frac{x^n - 1}{\gcd(x^n - 1, S(x))}
\]
of the cyclic code \( C_r \) defined by the sequence \( s^n \), where \( S(x) \) is defined as equation (28). With this purpose, we need to seek out the \( a (0 \leq a \leq n - 1) \), satisfying \( S(C_a^{(n)}) = 0 \), where \( z_n \) is a fixed \( n \)-th primitive root of unity of the finite field \( F_p \). The following auxiliary results are important for our calculation. Obviously, we have
\[
\sum_{i \in P} z_i^{S} = \sum_{i \in Q} z_i^{S} = -1,
\]
\[
\sum_{i \in Z_n} z_i^{S} = 1.
\]

**Lemma 10**
\[
\sum_{i \in D_1^{(n)}} z_i^{S} = \frac{(p-1)\eta_l}{(p-1)\eta_0},
\]
\[
\text{if } a \in P \text{ and } \left( \frac{al/p}{q} \right) = 1,
\]
\[
\text{if } a \in P \text{ and } \left( \frac{al/p}{q} \right) = -1.
\]

**Proof.** Obviously, \( D_1^{(n)} \pmod{p} = \{1,2,\ldots,p-1\} \), since \( g \) is a common primitive root modulo \( p \) and \( q \), and \( x \equiv g \pmod{p} \). Furthermore, one has
\[ D_{1}^{(n)} \pmod{p} = \left\{ g^{2r+1}x' \pmod{p} : s = 0, 1, \ldots, \frac{e}{2} - 1; t = 0, 1, \ldots, d - 1 \right\} \]
\[ = \left\{ g^{2r+1} \pmod{p} : s = 0, 1, \ldots, \frac{e}{2} - 1; t = 0, 1, \ldots, d - 1 \right\} \]  
\[ = \left( \frac{q-1}{2} \right) \ast \{ 1, 2, \ldots, p-1 \}. \]  

Hence, \( g^{2r+1}x'(\pmod{p}) \) takes on every element of \( \{1, 2, \ldots, p-1\} \) exactly \( (q-1)/2 \) times, when \( t \) ranges among \( \{0, 1, \ldots, d-1\} \) and \( s \) ranges among \( \{0, 1, \ldots, e/2 - 1\} \). If \( a \in \mathbb{Q} \), it follows from equations (30) and (32) that

\[ \sum_{\mathbb{Q} \setminus D_i^{(q)}} \zeta_n^{ci} = \left( \frac{q-1}{2} \right) \sum_{\mathbb{Q} \setminus D_i^{(q)}} \zeta_q^{ci} = \left( \frac{q-1}{2} \right) (\pmod{r}). \]  

Similarly, we have

\[ D_{1}^{(n)} \pmod{q} = \left\{ g^{2r+1}x' \pmod{q} : 0 \leq s \leq \frac{e}{2} - 1; 0 \leq t \leq d - 1 \right\} \]
\[ = d \ast \left\{ g^{2r+1} \pmod{q} : 0 \leq s \leq \frac{e}{2} - 1 \right\} \]
\[ = (p - 1) \ast D_{1}^{(q)}. \]

If \( a \in \mathbb{P} \), it follows that

\[ \sum_{a \in D_i^{(n)}} \zeta_n^{ci} = (p - 1) \sum_{a \in D_i^{(q)}} \zeta_q^{ci}. \]

and for \( a \in \mathbb{P} \) and \( (a/p)/q = -1 \),

\[ \sum_{a \in D_i^{(q)}} \zeta_q^{ci} = \sum_{j \in D_i^{(q)}} \zeta_{\{a(p)\}j} = \sum_{i \in D_i^{(q)}} \zeta_{\eta_i} = \eta_0. \]

Hence, we get the conclusions that, for \( a \in \mathbb{P} \) and \( (a/p)/q = 1 \),

\[ \sum_{j \in D_i^{(q)}} \zeta_q^{ci} = \sum_{j \in D_i^{(q)}} \zeta_{\{a(p)\}j} = \sum_{i \in D_i^{(q)}} \zeta_{\eta_i} = \eta_1, \]

Lemma 11

\[ S(\zeta_n) = \begin{cases} 
\frac{(p + 1)(q - 1)}{2} (\pmod{r}), & \text{if } a = 0, \\
-S(\zeta_n) - 1, & \text{if } a \in D_i^{(n)}, \\
S(\zeta_n), & \text{if } a \in D_i^{(n)}, \\
\left( \frac{q-1}{2} \right) (\pmod{r}), & \text{if } a \in \mathbb{Q}, \\
-1 + (p - 1)\eta_0, & \text{if } a \in \mathbb{P} \text{ and } \left( \frac{a/p}{q} \right) = -1, \\
-1 + (p - 1)\eta_1, & \text{if } a \in \mathbb{P} \text{ and } \left( \frac{a/p}{q} \right) = 1.
\end{cases} \]
Proof. If \( a = 0 \), then the conclusion is straightforward.

If \( a \in D_1^{(n)} \), then \( aD_1^{(n)} = D_0^{(n)} \) and \( aP(\text{mod} \, n) = P \). By equation (30), we get

\[
S(\zeta_n^a) = \left( \sum_{i \in P} \sum_{i \in D_1^{(n)}} \zeta_n^i \right) = \sum_{j \in P} \zeta_n^j + \sum_{j \in D_1^{(n)}} \zeta_n^j = \sum_{j \in P} \zeta_n^j + \left[ 1 - \sum_{j \in D_1^{(n)}} \zeta_n^j \right] = -S(\zeta_n) - 1. \tag{39}
\]

If \( a \in D_0^{(n)} \), we have \( aD_1^{(n)} = D_1^{(n)} \) and \( aP(\text{mod} \, n) = P \), since \( \gcd(a, q) = 1 \). So, we have

\[
S(\zeta_n^a) = \left( \sum_{i \in P} \sum_{i \in D_1^{(n)}} \zeta_n^i \right) = \sum_{j \in P} \zeta_n^j + \sum_{j \in D_1^{(n)}} \zeta_n^j = S(\zeta_n). \tag{40}
\]

If \( a \in D_0^{(n)} \), then \( aP(\text{mod} \, n) = 0 \). So by Lemma 10,

\[
S(\zeta_n^a) = \left( \sum_{i \in P} \sum_{i \in D_1^{(n)}} \zeta_n^i \right) = (q - 1) + \sum_{i \in D_1^{(n)}} \zeta_n^i = \frac{q - 1}{2} \, (\text{mod} \, r). \tag{41}
\]

If \( a \in P \), then \( aP(\text{mod} \, n) = P \). By equation (30) and Lemma 10, one has

\[
S(\zeta_n^a) = \sum_{j \in P} \zeta_n^j + \sum_{i \in D_1^{(n)}} \zeta_n^i = \begin{cases} 
-1 + (p - 1)n_1, & \text{if } a \in P \text{ and } \left( \frac{a/p}{q} \right) = 1, \\
-1 + (p - 1)n_0, & \text{if } a \in P \text{ and } \left( \frac{a/p}{q} \right) = -1.
\end{cases} \tag{42}
\]

**Lemma 12.** (1) If \( l(\text{mod} \, n) \in D_0^{(n)} \), then \( S(\zeta_n) \in \mathbb{F}_l \) and thus \( S(\zeta_n) + 1 \in \mathbb{F}_l \); (2) if \( l(\text{mod} \, n) \in D_1^{(n)} \), then \( S(\zeta_n) \neq -S(\zeta_n) - 1 \).

Proof

(1) If \( l(\text{mod} \, n) \in D_0^{(n)} \), then by Lemma 11, we have

\[
(S(\zeta_n)^l)^i = S(\zeta_n^i) = S(\zeta_n). \tag{43}
\]

Hence, \( S(\zeta_n) \in \mathbb{F}_l \).

(2) If \( l(\text{mod} \, n) \in D_1^{(n)} \), then by Lemma 11, we have similarly

\[
(S(\zeta_n)^l)^i = S(\zeta_n^i) = -S(\zeta_n) - 1. \tag{44}
\]

Under this assumption, \( S(\zeta_n) \notin \mathbb{F}_l \) if \( l \) is even, and \( S(\zeta_n) \) may be in \( \mathbb{F}_l \) if \( l \) is odd.

**Lemma 13.** When \( q \equiv 1 \, (\text{mod} \, 4) \), we have

\[
S(\zeta_n)[S(\zeta_n) + 1] = \left( \frac{q - 1}{4} \right) \, (\text{mod} \, r). \tag{45}
\]

When \( q \equiv 3 \, (\text{mod} \, 4) \), we have

\[
S(\zeta_n)[S(\zeta_n) + 1] = \left( \frac{q + 1}{4} \right) \, (\text{mod} \, r). \tag{46}
\]

Proof. According to equation (30) and the definition of \( S(x) \), one has

\[
S(\zeta_n) = -1 + \sum_{i \in D_0^{(n)}} \zeta_n^i = -\sum_{i \in D_0^{(n)}} \zeta_n^i. \tag{47}
\]

Then, we get

\[
S(\zeta_n)[S(\zeta_n) + 1] = -\sum_{i \in D_0^{(n)}} \sum_{j \in D_1^{(n)}} \zeta_n^{i+j}. \tag{48}
\]

Suppose that \( q \equiv 1 \, (\text{mod} \, 4) \). According to Lemma 6, \( -1 \in D_0^{(n)} \) and \( -D_1^{(n)} = D_0^{(n)} \). It follows from Lemmas 2, 7, 8, and 9 that
\[
\sum_{i \in D_1^{(n)}} \sum_{j \in D_2^{(n)}} \zeta_n^{i+j} = \sum_{i \in D_1^{(n)}} \sum_{j \in D_2^{(n)}} \zeta_n^{i-j}
\]
\[
= (p-1)(0,1)_2^{(q)} \sum_{i \in p, (i|q)=1} \zeta_n^i + (0,1)_2^{(n)} \sum_{i \in D_2^{(n)}} \zeta_n^i
\]
\[
+ (p-1)(0,1)_2^{(q)} \sum_{i \in D_1^{(n)}} \zeta_n^i + (0,1)_2^{(n)} \sum_{i \in D_2^{(n)}} \zeta_n^i.
\]
\[
(49)
\]
Combining equations (48) and (49), one can get the first conclusion of this lemma.

\[
\sum_{i \in D_1^{(n)}} \sum_{j \in D_2^{(n)}} \zeta_n^{i+j} = \sum_{i \in D_1^{(n)}} \sum_{j \in D_2^{(n)}} \zeta_n^{i-j}
\]
\[
= (p-1)(1,1)_2^{(q)} \sum_{i \in p, (i|q)=1} \zeta_n^i + (p-1)(0,0)_2^{(q)} \sum_{i \in p, (i|q)=1} \zeta_n^i + \frac{(p-1)(q-1)}{2}
\]
\[
+ (0,0)_2^{(n)} \sum_{i \in D_2^{(n)}} \zeta_n^i + (1,1)_2^{(n)} \sum_{i \in D_1^{(n)}} \zeta_n^i + \frac{(p-2)(q-1)}{2} \sum_{i \in Q} \zeta_n^i
\]
\[
= \left( q + \frac{1}{4} \right) \left( \text{mod } r \right).
\]
\[
(50)
\]
Combining equations (48) and (50), we can arrive at the second conclusion of this lemma.

**Lemma 14.** (1) \( l \pmod {n} \in D_0^{(n)} \) and \( r \in D_1^{(n)} \) if \( q \equiv 1 \pmod {4r} \) with \( q \equiv 1 \pmod {4} \); (2) \( l \pmod {n} \in D_0^{(n)} \) and \( r \in D_1^{(n)} \), if \( q \equiv -1 \pmod {4r} \) with \( q \equiv 3 \pmod {4} \).

**Proof.** Obviously, \( l \pmod {n} \in D_0^{(n)} \) if \( r \in D_0^{(n)} \). Now, we only give the proof of the first conclusion since the proof of the second part is similar to it. Let \( q \equiv 1 \pmod {4r} \) with \( q \equiv 1 \pmod {4} \).

Firstly, we consider the case that \( r = 2 \). Therefore, \( q \equiv 1 \pmod {8} \) and \( (2|q) = 1 \). Suppose that \( 2 \in D_0^{(n)} \) on the contrary. Then, 2 can be written as 2 = \( g^{2^s+1} x^t \) for \( 0 \leq s < e/2 - 1 \) and \( 0 \leq t < d - 1 \). According to the definition of \( g \) and \( x \), it follows that \( 2 \equiv g^{2^s+1} \pmod {q} \). Therefore, 2 is not a quadratic residue modulo \( q \). The contradiction proves the conclusion for the case \( r = 2 \).

Secondly, when \( r \) is an odd prime number, we prove this lemma. Since \( q \equiv 1 \pmod {4r} \), \( q \equiv 1 \pmod {r} \). Hence, \( (q|r) = 1 \). Now, one has

\[
\left( \frac{r}{q} \right) = (-1)^{\frac{(r-1)(q-1)}{4}} = 1.
\]
\[
(51)
\]
Suppose that \( r \in D_1^{(n)} \) on the contrary. By definition of \( D_1^{(n)} \), \( r = g^{2^s+1} x^t \) for \( 0 \leq s < e/2 - 1 \) and \( 0 \leq t < d - 1 \). Then, we have \( r \equiv g^{2^s+1} \pmod {q} \). Therefore, \( r \) is not a quadratic residue modulo \( q \). This is contrary to equation (69). So, we arrive at the conclusion.

In order to calculate the minimal polynomial and linear complexity of \( s^n \), we need to study the factorization of \( x^n - 1 \) over \( \mathbb{F}_q \). It can be checked that the \( \zeta_n^i (i \in P \cup \{0\}) \) are \( q \)-th roots of unity and \( \zeta_n^i (i \in Q \cup \{0\}) \) are \( p \)-th roots of unity. Therefore,

\[
\prod_{i \in \{0\} \cup P} (x - \zeta_n^i),
\]
\[
\prod_{i \in \{0\} \cup Q} (x - \zeta_n^i).
\]
\[
(52)
\]
For any \( i \in \{0,1\} \), define
\[ d_i(x) = \prod_{j \in D^{(n)}_i} (x - \zeta^n_j), \]  
(53)

where \( D^{(n)}_i \) denotes the general generalized cyclotomic classes with order two. If \( I \mod n \in D^{(n)}_0 \), then it is obvious that \( d_i(x) \in \mathbb{F}_q[x] \) for any \( i \).

Let \( d(x) = d_0(x)d_1(x) \in \mathbb{F}_q[x] \). After the above preparations, one has

\[ x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta_i^n) = d(x) \left( \frac{x^p - 1}{x - 1}, \frac{x^q - 1}{x - 1} \right) \]  
(54)

**Theorem 1.** Assume that \( r = 2 \). We have the assertions as follows:

1. When \( q \equiv 5 \mod(8) \), the linear complexity of \( s^n \) is \( L_s = n - p \), and the cyclic code \( C_s \) defined by \( s^n \) has the parameters \( \{n, p, q\} \), whose generator polynomial is \( m(x) = (x^n - 1)/x^p - 1 \).

2. When \( q \equiv 3 \mod(8) \), the linear complexity of \( s^n \) is \( L_s = n - 1 \), and the cyclic code \( C_s \) defined by \( s^n \) has the parameters \( \{n, 1, n\} \), whose generator polynomial is \( m(x) = (x^n - 1/x) - 1 \).

3. When \( q \equiv 1 \mod(8) \), the linear complexity of \( s^n \) is \( L_s = ((p + 1)(q - 1)/2) - 2 \), and the cyclic code \( C_s \) defined by \( s^n \) has the parameters \( \{n, (p + 1)(q - 1)/2 + 1, d\} \), whose generator polynomial is

\[ m(x) = \begin{cases} 
\frac{x^n - 1}{x - 1} d_1(x), & \text{if } S(\zeta^n_i) = 0, \\
\frac{x^n - 1}{x - 1} d_0(x), & \text{if } S(\zeta^n_i) = 1. 
\end{cases} \]  
(55)

4. When \( q \equiv 7 \mod(8) \), the linear complexity of \( s^n \) is \( L_s = ((p + 1)(q + 1)/2) - 2 \), and the cyclic code \( C_s \) defined by \( s^n \) has the parameters \( \{n, (p + 1)(q - 1)/2 + 1, d\} \), whose generator polynomial is

\[ m(x) = \begin{cases} 
\frac{x^n - 1}{d_0(x)(x - 1)} d_1(x), & \text{if } S(\zeta^n_i) = 0, \\
\frac{x^n - 1}{d_1(x)(x - 1)} d_0(x), & \text{if } S(\zeta^n_i) = 1. 
\end{cases} \]  
(56)

**Proof.** From \( r = 2 \), we get \( p \equiv 1 \mod(r) \). According to Lemma 11, one has

\[ \{a \in P: S(\zeta^n_i) = 0\} = \emptyset, \]  
(57)

Now, we only prove Case 1, since the others are similar. For Case 1, by Lemma 11,

\[ S(\zeta^n_i) = \begin{cases} 
0, & \text{if } a = 0, \\
\neq 0, & \text{if } a \in \mathbb{Z}_n^\times \text{(by Lemma 13)}, \\
0, & \text{if } a \in Q, \\
\neq 0, & \text{if } a \in P. 
\end{cases} \]  
(58)

Therefore, \( \gcd(x^n - 1, S(x)) = x^p - 1 \) and \( m(x) = (x^n - 1/x^p - 1) \). Then, the linear complexity of the sequence \( s^n \) is \( L_s = \deg(m(x)) = n - p \), Furthermore, the definition of the code can lead to the parameters of the code \( C_s \).

**Example 1.** Assume that \( (l, p, q) = (2, 3, 5) \). Then, \( n = 15, q \equiv 5 \mod(8) \), the minimal polynomial is \( x^{12} + x^9 + x^6 + x^3 + 1 \), and the linear complexity of \( s^n \) is 12. The cyclic code \( C_s \) defined by \( s^n \) is a \([15, 3, 5]\) cyclic code over \( \mathbb{F}_2 \). According to the database [19], the best linear code known with the parameters \([15, 3, d]\) has minimum distance 8.

**Example 2.** Assume that \( (l, p, q) = (2, 3, 7) \). In this case, \( n = 21, q \equiv 7 \mod(8) \), the minimal polynomial is \( x^{14} + x^{13} + x^9 + x^8 + x^7 + x^5 + x^3 + x^1 \), and the linear complexity of \( s^n \) is 14. The cyclic code \( C_s \) defined by \( s^n \) is a \([21, 7, 8]\) cyclic code over \( \mathbb{F}_2 \), which is an optimal linear code according to the database [19].

**Remark 3.** In [7], Example 3.20 presents a \([21, 7, 3]\) cyclic code over \( \mathbb{F}_2 \), whose generator polynomial is \( x^{14} + x^7 + 1 \). This is bad because of its poor minimum distance. Obviously, our cyclic code is more optimal.

**Example 3.** Assume that \( (l, p, q) = (2, 5, 13) \). Then, \( n = 65, q \equiv 5 \mod(8) \), the minimal polynomial is \( x^{60} + x^{55} + x^{50} + x^{45} + x^{40} + x^{35} + x^{30} + x^{25} + x^{20} + x^{15} + x^{10} + x^5 + 1 \), and the linear complexity of \( s^n \) is 60. The cyclic code \( C_s \) defined by \( s^n \) is a \([65, 5, 13]\) cyclic code over \( \mathbb{F}_2 \).

**Theorem 2.** Assume that \( p \equiv 1 \mod(r) \) and \( r \neq 2 \).

1. When \( q \equiv \pm 1 \mod(r) \) and \( q \equiv 3 \mod(4) \), or \( q \equiv 1 \mod(r) \) and \( q \equiv 1 \mod(4) \), the linear complexity of \( s^n \) is \( L_s = n \), and \( s^n \) has the minimal polynomial \( m(x) = x^n - 1 \).

2. When \( q \equiv 1 \mod(r) \) and \( q \equiv 3 \mod(4) \), the linear complexity of \( s^n \) is \( L_s = n - p \), and \( s^n \) has the minimal polynomial \( m(x) = (x^n - 1)/x^p - 1 \). The cyclic code \( C_s \) defined by \( s^n \) has the parameters \( \{n, p, q\} \).

3. When \( q \equiv 1 \mod(r) \) and \( q \equiv 1 \mod(4) \), \( l \mod(n) \in D^{(n)}_0 \) and \( d_i(x) \in \mathbb{F}_q[x] \) for \( i = 0,1 \) by Lemma 14. Hence, \( S(\zeta^n_i) \in [0, -1] \). The linear complexity of \( s^n \) is \( L_s = ((p + 1)(q - 1)/2) \), and the minimal polynomial
The cyclic code $C_s$ defined by $s^a$ has the parameters $[n, (p-1)(q+1)/2, d]$.  

(4) When $q = 1 (\mod r)$ and $q = 3 (\mod 4)$, $l(\mod n) \in D_0^{(n)}$ and $d_i(x) \in F[x]$ for $i = 0, 1$ by Lemma 14. Hence, $S(\zeta_n) \in \{0, -1\}$. The linear complexity of $s^a$ is $L_s = ((p+1)(q+1)/2) - 1$, and $s^a$ has the minimal polynomial

$$m(x) = \begin{cases} 
\frac{x^n - 1}{d_0(x)} & \text{if } S(\zeta_n) = 0, \\
\frac{x^n - 1}{d_1(x)} & \text{if } S(\zeta_n) = -1.
\end{cases}$$

The cyclic code $C_s$ defined by $s^a$ has the parameters $[n, (p-1)(q+1)/2, d]$.  

**Proof.** According to Lemma 11 and $p = 1 (\mod r)$, one has $\{a \in P: S(\zeta_n) = 0\} = \emptyset$. Now, we only prove Case 3, since the others are similar.

For Case 3, if $S(\zeta_n) = 0$, by Lemma 11,

$$S(\zeta_n^a) = \begin{cases} 
0, & \text{if } a = 0, \\
\# & \text{if } a = D_1^{(n)}, \\
0, & \text{if } a = D_0^{(n)}, \\
\# & \text{if } a = P, \\
0, & \text{if } a = Q.
\end{cases}$$

Therefore,

$$m(x) = (x^n - 1/d_0(x)(x^p - 1)) = (x^n - 1/x - 1)d_1(x).$$

If $S(\zeta_n) = -1$, by Lemma 11,

$$S(\zeta_n^a) = \begin{cases} 
0, & \text{if } a = 0, \\
\# & \text{if } a = D_1^{(n)}, \\
0, & \text{if } a = D_0^{(n)}, \\
\# & \text{if } a = P, \\
0, & \text{if } a = Q.
\end{cases}$$

Therefore,

$$m(x) = (x^n - 1/d_1(x)(x^p - 1)) = (x^n - 1/x - 1)d_0(x).$$

Then, the linear complexity of $s^a$ is $L_s = \deg(m(x))$. Moreover, the definition of the cyclic code can lead to the parameters of $C_s$.

**Example 4.** Assume that $(l, p, q) = (3, 7, 11)$. Then, $n = 77$, $q = -1 (\mod 3)$ and $q = 3 (\mod 4)$, the minimal polynomial is $x^{47} + 2x^{45} + x^{44} + 2x^{43} + 2x^{42} + 2x^{40} + x^{38} + 2x^{37} + x^{36} + x^{35} + 2x^{31} + x^{31} + 2x^{30} + x^{29} + 2x^{28} + 2x^{26} + 2x^{24} + 2x^{23} + x^{22} + x^{21} + x^{19} + 2x^{17} + x^{16} + 2x^{15} + 2x^{14} + 2x^{13} + x^{12} + 2x^{12} + x^2 + 2x + 2$, and the linear complexity of $s^a$ is 47. The cyclic code $C_s$ defined by $s^a$ is a $[77, 30, 12]$ cyclic code over $F_3$.

**Lemma 15** (see [15]). Let $A = (-1/q)\alpha - (p + 1/p - 1)^2$. If $A = 0$ and $p = 1 (\mod r)$, then $l(\mod q) \in D_0^{(q)}$. Define

$$d_0(x) = \prod_{\substack{i \in P \cap \{1, 2, \ldots, q\} \mid |(i/p)/q| = 0}} (x - \zeta_n^i),$$

$$d'_1(x) = \prod_{\substack{i \in P \cap \{1, 2, \ldots, q\} \mid |(i/p)/q| = -1}} (x - \zeta_n^i).$$

If $l(\mod q) \in D_0^{(q)}$, then it is straightforward to prove that $d_i(x) \in F[x]$ for $i = 0, 1$. Therefore, when $A = 0$ and $p = 1 (\mod r)$, one has $d_0(x), d'_1(x) \in F[x]$ by Lemma 15.

**Theorem 3.** Assume that $p = 1 (\mod r)$.

(1) When $q = 1 (\mod r)$, $q = 1 (\mod 4)$, and $p = 1 (\mod r)$ or $q = 1 (\mod r)$, $q = 3 (\mod 4)$, and $p = 1 (\mod r)$, the linear complexity of $s^a$ is $L_s = n - 1$, and $s^a$ has the minimal polynomial

$$m(x) = \begin{cases} 
x^n - 1, & \text{if } A \neq 0, \\
0, & \text{if } A = 0,
\end{cases}$$

and $s^a$ has the minimal polynomial

$$m(x) = \begin{cases} 
x^n - 1, & \text{if } A \neq 0, \\
\frac{x^n - 1}{d'_1(x)} & \text{if } \eta_0 = \frac{1}{p - 1}.
\end{cases}$$

The cyclic code $C_s$ defined by $s^a$ has the parameters $[n, n - \deg(m(x)), d]$.  

(3) When $q = 1 (\mod r)$ and $q = 3 (\mod 4)$, the linear complexity of $s^a$ is
and $s^n$ has the minimal polynomial

$$m(x) = \begin{cases} \frac{x^n - 1}{d_0(x)(x^p - 1)}, & \text{if } A \neq 0, \\ \frac{x^n - 1}{d_0(x)}(x^p - 1), & \text{if } A = 0, \end{cases}$$

(66)

The cyclic code $C_s$ defined by $s^n$ has the parameters $[n, n - \deg(m(x)), d]$. 

(4) When $q \equiv 1 \pmod{r}$ and $q \equiv 1 \pmod{4}$, the linear complexity of $s^n$ is $L_s = (\frac{p + 1}{2}(q - 1)/2)$, and $s^n$ has the minimal polynomial

$$m(x) = \begin{cases} \frac{x^n - 1}{d_1(x)(x^p - 1)}, & \text{if } A \neq 0, \\ \frac{x^n - 1}{d_1(x)}(x^p - 1), & \text{if } A = 0, \end{cases}$$

(67)

The cyclic code $C_s$ defined by $s^n$ has the parameters $[n, n - \deg(m(x)), d]$, where the minimum weight $d$ follows from Theorem 5.

(5) When $q \equiv -1 \pmod{r}$, $q \equiv 3 \pmod{4}$, and $p \equiv -1 \pmod{r}$, the linear complexity of $s^n$ is $L_s = (\frac{p + 1}{2}(q + 1)/2) - 2$, and $s^n$ has the minimal polynomial

$$m(x) = \begin{cases} \frac{x^n - 1}{d_0(x)}(x^p - 1), & \text{if } S(\zeta_n) = 0, \\ \frac{x^n - 1}{d_1(x)}(x^p - 1), & \text{if } S(\zeta_n) = -1. \end{cases}$$

(68)

The cyclic code $C_s$ defined by $s^n$ has the parameters $[n, ((p - 1)/2)(q - 1)/3 + 1, d]$, where the minimum weight $d$ follows from Theorem 5.

(6) When $q \equiv -1 \pmod{r}$, $q \equiv 3 \pmod{4}$, and $p \equiv -1 \pmod{r}$, the linear complexity of $s^n$ is $L_s = (\frac{p + 1}{2}(q + 1)/2) - 1$, and $s^n$ has the minimal polynomial

$$m(x) = \begin{cases} \frac{x^n - 1}{d_1(x)(x^p - 1)}, & \text{if } S(\zeta_n) = 0, \\ \frac{x^n - 1}{d_0(x)}(x^p - 1), & \text{if } S(\zeta_n) = -1. \end{cases}$$

(69)

The cyclic code $C_s$ defined by $s^n$ has the parameters $[n, n - \deg(m(x)), d]$. 

Proof. From $p \equiv 1 \pmod{r}$, we get that $r$ is an odd prime. Define

$$\Delta = \frac{q - 1}{2} \pmod{r},$$

(70)

$$\Delta' = \frac{(p + 1)(q - 1)}{2} \pmod{r}.$$

We will use the following property, which is easily seen to hold.

Property 1. $q \equiv 1 \pmod{r}$ if and only if $\Delta = 0$; $p \equiv -1 \pmod{r}$ or $q \equiv 1 \pmod{r}$ if and only if $\Delta' = 0$. If $\Delta = 0$, then $\Delta' = 0$.

Property 2. $(p - 1)\eta_0 = 1$ and $(p - 1)\eta_1 = 1$ cannot exist simultaneously, since $\gcd(n, l) = 1$ and $p \equiv 1 \pmod{r}$.

Property 3. $(p - 1)\eta_0 = 1$ if and only if $A = 0$.

Property 4. $\Delta' \neq 0$, if $A = 0$ and $q \equiv 1 \pmod{r}$.

Property 5. $A \neq 0$, if $q \equiv 1 \pmod{r}$ and $q \equiv 1 \pmod{4}$, or $q \equiv -1 \pmod{r}$ and $q \equiv 3 \pmod{4}$.

Now, we only prove Case 3, since the others are similar. One has $(q + 1)(q + 1/4) \neq 0$ and $\Delta = \Delta' = 0$, since $q \equiv 3 \pmod{4}$ and $q \equiv 1 \pmod{r}$. Hence, $\{a \in Q \cup \{0\}: S(\zeta^n_0) = 0\} = Q \cup \{0\}$ and $\{a \in \mathbb{Z}_n^*: S(\zeta^n_0) = 0\} = \emptyset$. According to Properties 1–5, if $A \neq 0$, by Lemma 11,

$$S(\zeta_0^n) = \begin{cases} 0, & \text{if } a = 0, \\ \neq 0, & \text{if } a \in \mathbb{Z}_n^*, \\ 0, & \text{if } a \in Q, \\ \neq 0, & \text{if } a \in P. \end{cases}$$

(71)

Therefore, $m(x) = (x^n - 1/x^p - 1)$. If $\eta_0 = (1/p - 1)$, by Lemma 11,
4. The Minimum Distance of the Cycle Codes Obtained in This Paper

Theorem 4 (see [7]). If the generator polynomial of \( C_s \) over \( \mathbb{F}_2 \) is \( g(x) = (x^n - 1)/(x^p - 1) \), then \( C_s \) has parameters \([n, p, q]\). Also, if the generator polynomial of \( C_s \) over \( \mathbb{F}_2 \) is \( g(x) = (x^n - 1)/(x^q - 1) \), then \( C_s \) has parameters \([n, q, p]\).

Theorem 5. Let \( l \equiv (\mod n) \in D_{l(n)} \). Let \( C_{l(n)}^{\omega} \) be the cyclic code over \( \mathbb{F}_2 \) generated by the polynomial

\[
g^{\omega}(x) = d_1(x) \frac{x^l - 1}{x - 1}.
\]

Assume that \( d_{i(p,q,l)}^{(\omega)} (i = 0, 1) \) is the minimum distance of this code. The parameters of the cycle code \( C_{l(n)}^{\omega} \) are

\[
\left[ n, \frac{(p - 1)(q + 1)}{2} + 1, d_{i(p,q,l)}^{(l(n))}, \sqrt{q} \right].
\]

If \(-1 \in D_{l(n)}^{(n)}\), we have

\[
\left( d_{i(p,q,l)}^{(l(n))} \right)^2 - d_{i(p,q,l)}^{(l(n))} + 1 \geq q.
\]

Proof. Assume that \( c(x) \in C_{l(n)}^{\omega} \), whose Hamming weight is \( \omega \). Take any \( k \in D_{l(n)}^{(n)} \). Then, \( c(x^k) \) is a code word in \( C_{l(n)}^{\omega} \), whose Hamming weight is also \( \omega \). Therefore, we have \( d_{i(p,q,l)}^{(l(n))} = d_{i(p,q,l)}^{(l(n))} \).

Suppose that \( c(x) \in C_{l(n)}^{\omega} \), whose Hamming weight is minimum. Then, \( c(x^k) \) is a code word in \( C_{l(n)}^{\omega} \), whose Hamming weight is also minimum. Furthermore, for any \( k \in D_{l(n)}^{(n)} \), \( c(x)c(x^k) \) is a code word in the cyclic code

\[
C_{l(n)}^{\omega} \cap \bigcap_{l \in D_{l(n)}^{(n)}} C_{l(n)}^{(l+1 \mod 2)},
\]

whose generator polynomial is \( (x^n - 1/x^p - 1) \) and minimum distance is \( q \) (see Theorem 4). Hence, we have that

\[
\left( d_{i(p,q,l)}^{(l(n))} \right)^2 - d_{i(p,q,l)}^{(l(n))} + 1 \geq q.
\]

Remark 4. Theorems 1, 2, and 3 show that the linear complexity of the two-prime GGCSs defined by equation (22) is very high. Without the limit of gcd \((p - 1, q - 1) = 2\), this paper can obtain some binary sequences with new parameters and higher linear complexity. Furthermore, when gcd \((p - 1, q - 1) = 2\), Theorem 1 in our paper is the same with Theorem 1 in [14]. When gcd \((p - 1, q - 1) = 2\), Theorem 2 in our paper is in accord with Theorems 13 and 16 in [15], and Theorem 3 in our paper is exactly identical with Theorems 14 and 18 in [15]. However, if gcd \((p - 1, q - 1) \) is not equal to 2, the conclusions in Theorems 1, 2, and 3 of our paper are new, which can be seen from Example 3. Therefore, the sequences defined by equation (22) will be more attractive than those in [14, 15] in some cryptographic applications.

Example 5. Assume that \((l, p, q) = (3, 5, 7)\). Then, \( n = 35, q \equiv 1 \pmod{3}, p \equiv 2 \pmod{3}, q \equiv 3 \pmod{4}, A \neq 0\), the minimal polynomial is \( x^{30} + x^{25} + x^{20} + x^{15} + x^{10} + x^5 + 1\), and the linear complexity of \( s^a \) is 30. The code cycle \( C_s \) defined by \( s^a \) is a \([35, 5, 7]\) cyclic code over \( \mathbb{F}_3 \).

Example 6. Assume that \((l, p, q) = (2, 3, 17)\). In this case, \( 2 \in D_{l(n)}^{(n)} \), the cyclic code \( C_s \) generated by the polynomial \( g(x) = (x^4 - 1/x - 1)d_1(x) \) has parameters \([51, 19, 10]\). The actual minimum distance is 10, but the lower bound of (77) is 2.
sequences in our paper have high linear complexity. Notably, our construction can generate more sequences with new parameters and high linear complexity. Furthermore, inspired by the idea of [7], we constructed some cyclic codes by virtue of special classes of sequences. Our results show that several cyclic codes are optimal, such as Example 2.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The author declares no conflicts of interest.

Acknowledgments

This work was supported by the Foundation of Nanjing Institute of Technology (no. QKJ201804).

References

[1] L. Lidl and H. Niederreiter, 
*Finite Fields*, Cambridge University Press, Cambridge, UK, 1997.

[2] C. Ding and T. Helleseth, “New generalized cyclotomy and its applications,” 
*Finite Fields and their Applications*, vol. 4, no. 2, pp. 140–166, 1998.

[3] C. Ding and V. Pless, “Cyclotomy and duadic codes of prime lengths,” 
*IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 453–466, 1999.

[4] C. Ding and T. Helleseth, “Generalized cyclotomic codes of length $p_1^{e_1} \cdots p_t^{e_t}$,” 
*IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 467–474, 1999.

[5] E. Betti and M. Sala, “A new bound for the minimum distance of a cyclic code from its defining set,” 
*IEEE Transactions on Information Theory*, vol. 52, no. 8, pp. 3700–3706, 2006.

[6] C. Ding, “Cyclotomic constructions of cyclic codes with length being the product of two primes,” 
*IEEE Transactions on Information Theory*, vol. 58, no. 4, pp. 2231–2236, 2012.

[7] C. Ding, “Cyclic codes from the two-prime sequences,” 
*IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3881–3891, 2012.

[8] C. Ding, “Cyclic codes from cyclotomic sequences of order four,” 
*Finite Fields and Their Applications*, vol. 23, pp. 8–34, 2013.

[9] Y. Sun, T. Yan, and H. Li, “Cyclic code from the first class Whiteman’s generalized cyclotomic sequence with order 4,” 2013, http://arxiv.org/abs/1303.6378.

[10] C. Ding, X. Du, and Z. Zhou, “The bose and minimum distance of a class of BCH codes,” 
*IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2351–2356, 2015.

[11] P. Kewat and P. Kumari, “Cyclic codes from the first class two-prime Whiteman’s generalized cyclotomic sequence with order 6,” 2015, http://arxiv.org/abs/1509.07714.

[12] A. L. Whiteman, “A family of difference sets,” 
*Illinois Journal of Mathematics*, vol. 6, no. 6, pp. 107–121, 1962.

[13] C. Ding, “Linear complexity of generalized cyclotomic binary sequences of order 2,” 
*Finite Fields and Their Applications*, vol. 3, no. 2, pp. 159–174, 1997.

[14] S. Li, Z. Chen, R. Sun, and G. Xiao, “On the randomness of generalized cyclotomic sequences of order two and length $pq$,” 
*IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E90-A, no. 9, pp. 2037–2041, 2007.

[15] Q. Wang, Y. Jiang, and D. Lin, “Linear complexity of Ding-Helleseth sequences of order 2 over $GF(l)$,” 
*Cryptography and Communications*, vol. 8, no. 1, pp. 33–49, 2016.

[16] Q. Wang and D. Lin, “Generalized cyclotomic numbers of order two and their applications,” 
*Cryptography and Communications*, vol. 8, no. 4, pp. 605–616, 2016.

[17] T. Storer, *Cyclotomy and Difference Sets*, Markham Publishing Company, Markham, Canada, 1967.

[18] 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.

[19] M. Grassl, “Bounds on the minimum distance of linear codes,” 
http://www.codetables.de.