Bull. Korean Math. Soc. **56** (2019), No. 2, pp. 285–301
https://doi.org/10.4134/BKMS.b170594
pISSN: 1015-8634 / eISSN: 2234-3016

CYCLIC CODES FROM THE FIRST CLASS TWO-PRIME WHITEMAN'S GENERALIZED CYCLOTOMIC SEQUENCE WITH ORDER 6

Pramod Kumar Kewat and Priti Kumari

Abstract. Let p_1 and p_2 be two distinct odd primes with $\gcd(p_1 - 1, p_2 - 1) = 6$. In this paper, we compute the linear complexity of the first class two-prime Whiteman's generalized cyclotomic sequence (WGCS-I) of order $d = 6$. Our results show that their linear complexity is quite good. So, the sequence can be used in many domains such as cryptography and coding theory. This article enrich a method to construct several classes of cyclic codes over $\mathrm{GF}(q)$ with length $n = p_1p_2$ using the two-prime WGCS-I of order 6. We also obtain the lower bounds on the minimum distance of these cyclic codes.

1. Introduction

Let q be a power of a prime p. An $[n, k, d]$ linear code C over a finite field $\mathrm{GF}(q)$ is a k-dimensional subspace of the vector space $\mathrm{GF}(q)^n$ with minimum distance d. A linear code C is a cyclic code if the cyclic shift of a codeword in C is again a codeword in C, i.e., if $(c_0, \ldots, c_{n-1}) \in C$, then $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. Let $\gcd(n, q) = 1$. We denote by R the ring $\mathrm{GF}(q)[x]/\langle x^n - 1\rangle$. We can consider a cyclic code of length n over $\mathrm{GF}(q)$ as an ideal in R via the following correspondence

$$\mathrm{GF}(q)^n \to R, \qquad (c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1x + \cdots + c_{n-1}x^{n-1}.$$

The total number of cyclic codes over $\mathrm{GF}(q)$ and their construction are closely related to the cyclotomic cosets modulo n. One way to construct cyclic codes over $\mathrm{GF}(q)$ with length n is to use the generator polynomial

$$\frac{x^n - 1}{\gcd(x^n - 1, S(x))}, \tag{1.1}$$

where $S(x) = \sum_{i=0}^{n-1} s_ix^i \in \mathrm{GF}(q)[x]$ and $s^\infty = (s_i)_{i=0}^{\infty}$ is a sequence of period n over $\mathrm{GF}(q)$. The cyclic code C_s generated by the polynomial in (1.1) is called

Received July 6, 2017; Revised February 13, 2018; Accepted September 10, 2018.
2010 *Mathematics Subject Classification.* 94A05, 94A55, 94B15.
Key words and phrases. cyclic codes, finite fields, cyclotomic sequences.

the cyclic code defined by the sequence s^∞, and the sequence s^∞ is called the defining sequence of the cyclic code C_s.

Cyclic codes have been studied in a series of papers due to their efficient coding and decoding properties and a lot of progress have been adapted (see, for example [1], [6], [7], [9] and [10]). The Whiteman's generalized cyclotomy was introduced by Whiteman and its properties were studied in [12], is an important technique to sequence design. Ding defined the two-prime Whiteman's generalized cyclotomic sequence (WGCS) using Whiteman cyclotomic classes in [4] and its coding properties were studied in [5] and [11]. For keystream sequences for additive synchronous stream ciphers there are some common cryptographic measures of their strength such as good autocorrelation property and large linear complexity. In this correspondence, we calculate the exact value of the linear complexity of this sequence. This article enrich a method to construct several classes of cyclic codes over GF(q) using the two-prime WGCS-I with order 6. We also obtain the lower bounds on the minimum distance of these cyclic codes.

Our technique to calculate the linear complexity is same as in [4] and construction of cyclic codes over GF(q) follow from [5]. But we need to remark that in this paper, we investigate the linear complexity of two prime WGCS-I of order six are same as two prime sequence of order two. Therefore, we construct many classes of cyclic codes over GF(q) for large length. In particular, we give the parameters of several classes of cyclic codes for $q = 2$ and $q = 3$.

2. Preliminaries

2.1. Linear complexity and minimal polynomial

The linear span L_s and the minimal polynomial $m_s(x)$ of binary sequence s^∞ of a period n over $GF(q)$ can be calculated by the following equations:

$$\begin{aligned} m_s(x) &= \frac{x^n - 1}{\gcd(x^n - 1, S^n(x))}, \\ L_s &= n - \deg(\gcd(x^n - 1, S^n(x))). \end{aligned}$$

We refer the readers to [8] for detailed informations of the linear complexity and the minimal polynomial.

2.2. The Whiteman's generalized cyclotomic sequences and its construction

Let n be a positive integer. The multiplicative order of an integer a modulo n is equal to $\phi(n)$, then the integer a is known as primitive root of modulo n, where $\phi(n)$ is the Euler phi function and $\gcd(a, n) = 1$. Define $n = p_1 p_2,\ d = \gcd(p_1 - 1, p_2 - 1)$ and $e = (p_1 - 1)(p_2 - 1)/d$, where p_1 and p_2 are two distinct odd primes. From the Chinese Remainder theorem, there are common primitive roots of both p_1 and p_2. Let g be a fixed common primitive root of both p_1

and p_2. Let u be an integer satisfying

$$u \equiv g \pmod{p_1},\ u \equiv 1 \pmod{p_2}. \tag{2.1}$$

The Whiteman's generalized cyclotomic classes D_i of order d are defined by

$$D_i = \{g^s u^i \pmod{n} : s = 0, 1, \ldots, e-1\},\ i = 0, 1, \ldots, d-1.$$

Let

$$P = \{p_1, 2p_1, 3p_1, \ldots, (p_2-1)p_1\},\ Q = \{p_2, 2p_2, 3p_2, \ldots, (p_1-1)p_2\},$$

$$C_0 = \{0\} \cup Q \cup \bigcup_{i=0}^{\frac{d}{2}-1} D_{2i} \quad \text{and} \quad C_1 = P \cup \bigcup_{i=0}^{\frac{d}{2}-1} D_{2i+1},$$

$$C_0^* = \{0\} \cup Q \cup \bigcup_{i=0}^{\frac{d}{2}-1} D_i,\ C_1^* = P \cup \bigcup_{i=\frac{d}{2}}^{d-1} D_i.$$

It is clear that if $d > 2$, then $C_0 \neq C_0^*$ and $C_1 \neq C_1^*$. Now we define two types of Whiteman's generalized cyclotomic sequences of order d (see [2]).

Definition. The first class two-prime Whiteman's generalized cyclotomic sequence (WGCS-I) $\lambda^\infty = (\lambda_i)_{i=0}^{n-1}$ of order d and period n, is defined by

$$\lambda_i = \begin{cases} 0, & \text{if } i \in C_0, \\ 1, & \text{if } i \in C_1. \end{cases} \tag{2.2}$$

The second class two-prime Whiteman's generalized cyclotomic sequence (WGCS-II) $s^\infty = (s_i)_{i=0}^{n-1}$ of order d and period n, is defined by

$$s_i = \begin{cases} 0, & \text{if } i \in C_0^*, \\ 1, & \text{if } i \in C_1^*. \end{cases}$$

The sets C_1 and $C_1^* \subseteq \mathbb{Z}_n$ are known as the characteristic sets of the sequence λ^∞ and s^∞, respectively and the sequences λ_i and s_i are referred to as the characteristic sequences of C_1 and C_1^*, respectively.

The cyclotomic numbers corresponding to these cyclotomic classes are defined as

$$(i,j)_d = |(D_i + 1) \cap D_j|, \quad \text{where} \quad 0 \leq i, j \leq d-1.$$

Additionally, for any $t \in \mathbb{Z}_n$, we define

$$d(i,j;t) = |(D_i + t) \cap D_j|,$$

where $D_i + t = \{w + t \,|\, w \in D_i\}$.

2.3. Properties of Whiteman's cyclotomy of order d

Here, we review some of properties of Whiteman's generalized cyclotomy of order $d = \gcd(p_1 - 1, p_2 - 1)$. The proof of the following lemma follows from Theorem 4.4.6 of [3].

Lemma 1. *Let the notations be defined as above and $t \neq 0$. We have*

$$d(i,j;t) = \begin{cases} \frac{(p_1-1)(p_2-1)}{d^2}, & i \neq j,\ t \in P \cup Q, \\ \frac{(p_1-1)(p_2-1-d)}{d^2}, & i = j,\ t \in P,\ t \notin Q, \\ \frac{(p_1-1-d)(p_2-1)}{d^2}, & i = j,\ t \in Q,\ t \notin P, \\ (i',j')_d \ \text{ for some } (i',j'), & \text{otherwise.} \end{cases}$$

The following two lemmas follow from [8].

Lemma 2. *Let the notations be defined as before. The four statements given below are equivalent*:

(1) $-1 \in D_{\frac{d}{2}}$.

(2) $\frac{(p_1-1)(p_2-1)}{d^2}$ *is even.*

(3) *One of the sets of equations given below are satisfied*:

$$\begin{cases} p_1 \equiv 1 \pmod{2d}, \\ p_2 \equiv d+1 \pmod{2d}, \end{cases} \quad \begin{cases} p_1 \equiv d+1 \pmod{2d}, \\ p_2 \equiv 1 \pmod{2d}. \end{cases}$$

(4) $p_1 p_2 \equiv d+1 \pmod{2d}$.

Lemma 3. *Let the symbols be defined as before. The following four statements are equivalent*:

(1) $-1 \in D_0$.

(2) $\frac{(p_1-1)(p_2-1)}{d^2}$ *is odd.*

(3) *The following set of equation is satisfied*:

$$\begin{cases} p_1 \equiv d+1 \pmod{2d}, \\ p_2 \equiv d+1 \pmod{2d}. \end{cases}$$

(4) $p_1 p_2 \equiv (d+1)^2 \equiv 1 \pmod{2d}$.

Now, we employ the sequence λ^∞ (defined in (2.2)) to construct cyclic codes over $\mathrm{GF}(q)$.

3. A class of cyclic codes over GF(q) defined by two-prime WGCS-I

In this section, we compute the parameters of the cyclic code C_λ defined by the sequence λ^∞ over finite field $\mathrm{GF}(q)$, where q is a power of a prime p. We have $\gcd(n,q) = 1$, where $n = p_1 p_2$ (product of two distinct primes) is the length of the cyclic code. Let r be the order of q modulo n. Then, the field $\mathrm{GF}(q^r)$ has a primitive nth root of unity. Let α be a primitive nth root of unity over the finite field $\mathrm{GF}(q)$. We define

$$\Lambda(x) = \sum_{i \in C_1} x^i = \left(\sum_{i \in P} + \sum_{i \in D_1} + \sum_{i \in D_3} + \sum_{i \in D_5} \right) x^i \in \mathrm{GF}(q)[x]. \tag{3.1}$$

To find the parameters of the cyclic code, for this, first we find the generator polynomial

$$g_\lambda(x) = \frac{x^n - 1}{\gcd(x^n - 1, \Lambda(x))}$$

of the cyclic code C_λ defined by the sequence λ^∞. In the sequel, we need following results. We have

$$0 = \alpha^n - 1 = (\alpha^{p_1})^{p_2} - 1 = (\alpha^{p_1} - 1)(1 + \alpha^{p_1} + \alpha^{2p_1} + \cdots + \alpha^{(p_2-1)p_1}).$$

It follows that

$$\alpha^{p_1} + \alpha^{2p_1} + \cdots + \alpha^{(p_2-1)p_1} = -1, \text{ i.e., } \sum_{i\in P} \alpha^i = -1. \tag{3.2}$$

By symmetry, we get

$$\alpha^{p_2} + \alpha^{2p_2} + \cdots + \alpha^{(p_1-1)p_2} = -1, \text{ i.e., } \sum_{i\in Q} \alpha^i = -1. \tag{3.3}$$

The following two lemmas follow from [8].

Lemma 4. *Let the symbols be same as before. For $0 \le j \le 5$, we have*

$$\sum_{i\in D_j} \alpha^{it} = \begin{cases} -\frac{p_1-1}{6} \pmod p, & \text{if } t \in P, \\ -\frac{p_2-1}{6} \pmod p, & \text{if } t \in Q. \end{cases}$$

Lemma 5. *For any $r \in D_i$, we have $rD_j = D_{(i+j)(\mathrm{mod}\ d)}$, where $rD_j = \{rt \mid t \in D_j\}$.*

Throughout this paper, let $d_0 = D_0 \cup D_2 \cup D_4$ and $d_1 = D_1 \cup D_3 \cup D_5$.

Lemma 6. *Let the symbols be same as before. For all $t \in \mathbb{Z}_n$ we have*

$$\Lambda(\alpha^t) = \begin{cases} -\frac{p_1+1}{2} \pmod p, & \text{if } t \in P, \\ \frac{p_2-1}{2} \pmod p, & \text{if } t \in Q, \\ \Lambda(\alpha), & \text{if } t \in D_0, \\ -(\Lambda(\alpha)+1), & \text{if } t \in D_1. \end{cases}$$

Proof. Since $\gcd(p_1, p_2) = 1$, we have $tP = P$ if $t \in P$. By (3.1), (3.2) and Lemma 4, we get

$$\begin{aligned} \Lambda(\alpha^t) &= \sum_{i\in C_1} \alpha^{ti} = \left(\sum_{i\in P} + \sum_{i\in D_1} + \sum_{i\in D_3} + \sum_{i\in D_5}\right)\alpha^{ti} \\ &= (-1 \bmod p) - \left(\frac{p_1-1}{6} \bmod p\right) - \left(\frac{p_1-1}{6} \bmod p\right) - \left(\frac{p_1-1}{6} \bmod p\right) \\ &= -\frac{p_1+1}{2} \bmod p. \end{aligned}$$

If $t \in Q$, then $tP = 0$. By (3.1), (3.2) and Lemma 4, we get

$$\begin{aligned} \Lambda(\alpha^t) &= \sum_{i\in C_1} \alpha^{ti} = \left(\sum_{i\in P} + \sum_{i\in D_1} + \sum_{i\in D_3} + \sum_{i\in D_5}\right)\alpha^{ti} \\ &= (p_2 - 1 \bmod p) - \left(\frac{p_2-1}{6} \bmod p\right) - \left(\frac{n_2-1}{6} \bmod p\right) - \left(\frac{p_2-1}{6} \bmod p\right) \end{aligned}$$

$$= \frac{p_2 - 1}{2} \bmod p.$$

If $t \in D_0$, we have three cases:
Case I: Let $t \in D_0$, then by Lemma 5, we have $tD_i = D_i$. Since $\gcd(t, p_2) = 1$, we have $tP = P$ if $t \in D_0$. Hence,

$$\begin{aligned}\Lambda(\alpha^t) = \sum_{i \in C_1} \alpha^{ti} &= \left(\sum_{i \in P} + \sum_{i \in D_1} + \sum_{i \in D_3} + \sum_{i \in D_5} \right) \alpha^{ti} \\ &= \left(\sum_{i \in P} + \sum_{i \in D_1} + \sum_{i \in D_3} + \sum_{i \in D_5} \right) \alpha^{i} \\ &= \Lambda(\alpha).\end{aligned}$$

Case II: Let $t \in D_2$, then by similar to the proof of the Case I, we have $\Lambda(\alpha^t) = \Lambda(\alpha)$ and Case III: Let $t \in D_4$, then by similar to the proof of the Case I, we have $\Lambda(\alpha^t) = \Lambda(\alpha)$.

Similarly, if $t \in D_1$, we have three cases:
Case I: Let $t \in D_1$, then by Lemma 5, we have $tD_i = D_{i+1 \pmod 6}$. Since $\gcd(t, p_2) = 1$, we have $tP = P$ if $t \in D_1$. We have $\alpha^n - 1 = (\alpha - 1)(\sum_{i=0}^{n-1} \alpha^i) = 0$ and $\alpha - 1 \neq 0$, this give $\sum_{i=0}^{n-1} \alpha^i = 0$. Therefore,

$$\sum_{i=0}^{n-1} \alpha^i = 1 + \sum_{i \in P} \alpha^i + \sum_{i \in Q} \alpha^i + \sum_{i \in \bigcup_{j=0}^{5} D_j} \alpha^i = 0.$$

From (3.2) and (3.3), we get

$$\sum_{i \in \bigcup_{j=0}^{5} D_j} \alpha^i = 1. \tag{3.4}$$

Hence

$$\Lambda(\alpha^t) = \sum_{i \in C_1} \alpha^{ti} = \left(\sum_{i \in P} + \sum_{i \in D_1} + \sum_{i \in D_3} + \sum_{i \in D_5} \right) \alpha^{ti} = -(\Lambda(\alpha) + 1).$$

Similarly, we can prove other two cases namely, Case II : $t \in D_3$ and Case III : $t \in D_5$. □

Lemma 7. *If $q \in d_0$, we have $\Lambda(\alpha) \in \mathrm{GF}(q)$ and $(\Lambda(\alpha))^q = \Lambda(\alpha)$. If $q \in d_1$, we have $\Lambda(\alpha)^q = -(\Lambda(\alpha) + 1)$.*

Proof. We have $\gcd(n, q) = 1$, i.e., $q \in \mathbb{Z}_n^*$, then $q \in \bigcup_{i=0}^{5} D_i = d_0 \cup d_1$. If $q \in d_0$, by Lemma 6, we have $(\Lambda(\alpha))^q = \Lambda(\alpha^q) = \Lambda(\alpha)$. So, $\Lambda(\alpha) \in \mathrm{GF}(q)$. Similarly, if $q \in d_1$, from Lemma 6, the result follows. □

Lemma 8. *If $p_1 p_2 \equiv 1 \pmod{12}$, we have*

$$\Lambda(\alpha)(\Lambda(\alpha) + 1) = \frac{n-1}{4}.$$

If $p_1p_2 \equiv 7 \pmod{12}$*, we have*

$$\Lambda(\alpha)(\Lambda(\alpha)+1) = -\frac{n+1}{4}.$$

Proof. We have

$$\Lambda(\alpha) = -1 + \sum_{i\in D_1}\alpha^i + \sum_{i\in D_3}\alpha^i + \sum_{i\in D_5}\alpha^i,$$

and

$$\begin{aligned}
\Lambda(\alpha)(\Lambda(\alpha)+1) = \;& -\left(\sum_{i\in D_1}\alpha^i + \sum_{i\in D_3}\alpha^i + \sum_{i\in D_5}\alpha^i\right)\\
&+\sum_{i\in D_1}\sum_{j\in D_1}\alpha^{i+j} + \sum_{i\in D_3}\sum_{j\in D_3}\alpha^{i+j}\\
&+\sum_{i\in D_5}\sum_{j\in D_5}\alpha^{i+j} + 2\sum_{i\in D_1}\sum_{j\in D_3}\alpha^{i+j}\\
&+2\sum_{i\in D_3}\sum_{j\in D_5}\alpha^{i+j} + 2\sum_{i\in D_5}\sum_{j\in D_1}\alpha^{i+j}. \qquad (3.5)
\end{aligned}$$

Let $p_1p_2 \equiv 1 \pmod{12}$ from Lemma 3, $-1 \in D_0$ and from Lemma 5, $-D_j = \{-t : t \in D_j\} = D_j$.

$$\begin{aligned}
\sum_{i\in D_1}\sum_{j\in D_1}\alpha^{i+j} =\;& \sum_{i\in D_1}\sum_{j\in D_1}\alpha^{i-j}\\
=\;& |D_1| + \sum_{r\in P\cup Q} d(1,1;r)\alpha^r + (1,1)_6\sum_{i\in D_0}\alpha^i + (0,0)_6\sum_{i\in D_1}\alpha^i\\
&+(5,5)_6\sum_{i\in D_2}\alpha^i + (4,4)_6\sum_{i\in D_3}\alpha^i\\
&+(3,3)_6\sum_{i\in D_4}\alpha^i + (2,2)_6\sum_{i\in D_5}\alpha^i, \qquad (3.6)
\end{aligned}$$

$$\begin{aligned}
\sum_{i\in D_3}\sum_{j\in D_3}\alpha^{i+j} =\;& \sum_{i\in D_3}\sum_{j\in D_3}\alpha^{i-j}\\
=\;& |D_3| + \sum_{r\in P\cup Q} d(3,3;r)\alpha^r + (3,3)_6\sum_{i\in D_0}\alpha^i + (2,2)_6\sum_{i\in D_1}\alpha^i\\
&+(1,1)_6\sum_{i\in D_2}\alpha^i + (0,0)_6\sum_{i\in D_3}\alpha^i\\
&+(5,5)_6\sum_{i\in D_4}\alpha^i + (4,4)_6\sum_{i\in D_5}\alpha^i, \qquad (3.7)
\end{aligned}$$

$$\sum_{i\in D_5}\sum_{j\in D_5}\alpha^{i+j} = \sum_{i\in D_5}\sum_{j\in D_5}\alpha^{i-j}$$

$$\begin{aligned} &= |D_5| + \sum_{r\in P\cup Q} d(5,5;r)\alpha^r + (5,5)_6 \sum_{i\in D_0}\alpha^i + (4,4)_6 \sum_{i\in D_1}\alpha^i \\ &\quad + (3,3)_6 \sum_{i\in D_2}\alpha^i + (2,2)_6 \sum_{i\in D_3}\alpha^i \\ &\quad + (1,1)_6 \sum_{i\in D_4}\alpha^i + (0,0)_6 \sum_{i\in D_5}\alpha^i, \end{aligned} \tag{3.8}$$

$$\begin{aligned} 2\sum_{i\in D_1}\sum_{j\in D_3}\alpha^{i+j} &= 2\sum_{i\in D_1}\sum_{j\in D_3}\alpha^{i-j} \\ &= 2\Bigg(\sum_{r\in P\cup Q} d(3,1;r)\alpha^r + (3,1)_6 \sum_{i\in D_0}\alpha^i + (2,0)_6 \sum_{i\in D_1}\alpha^i \\ &\quad + (1,5)_6 \sum_{i\in D_2}\alpha^i + (0,4)_6 \sum_{i\in D_3}\alpha^i \\ &\quad + (5,3)_6 \sum_{i\in D_4}\alpha^i + (4,2)_6 \sum_{i\in D_5}\alpha^i\Bigg), \end{aligned} \tag{3.9}$$

$$\begin{aligned} 2\sum_{i\in D_3}\sum_{j\in D_5}\alpha^{i+j} &= 2\sum_{i\in D_3}\sum_{j\in D_5}\alpha^{i-j} \\ &= 2\Bigg(\sum_{r\in P\cup Q} d(5,3;r)\alpha^r + (5,3)_6 \sum_{i\in D_0}\alpha^i + (4,2)_6 \sum_{i\in D_1}\alpha^i \\ &\quad + (3,1)_6 \sum_{i\in D_2}\alpha^i + (2,0)_6 \sum_{i\in D_3}\alpha^i \\ &\quad + (1,5)_6 \sum_{i\in D_4}\alpha^i + (0,4)_6 \sum_{i\in D_5}\alpha^i\Bigg), \end{aligned} \tag{3.10}$$

$$\begin{aligned} 2\sum_{i\in D_5}\sum_{j\in D_1}\alpha^{i+j} &= 2\sum_{i\in D_5}\sum_{j\in D_1}\alpha^{i-j} \\ &= 2\Bigg(\sum_{r\in P\cup Q} d(1,5;r)\alpha^r + (1,5)_6 \sum_{i\in D_0}\alpha^i + (0,4)_6 \sum_{i\in D_1}\alpha^i \\ &\quad + (5,3)_6 \sum_{i\in D_2}\alpha^i + (4,2)_6 \sum_{i\in D_3}\alpha^i \\ &\quad + (3,1)_6 \sum_{i\in D_4}\alpha^i + (2,0)_6 \sum_{i\in D_5}\alpha^i\Bigg). \end{aligned} \tag{3.11}$$

Substituting the values of (3.6)-(3.11) into (3.5) and then from Lemma 1 and (3.4) and [8], we get

$$\begin{aligned}\Lambda(\alpha)(\Lambda(\alpha)+1) = &-\left(\sum_{i\in D_1}\alpha^i+\sum_{i\in D_3}\alpha^i+\sum_{i\in D_5}\alpha^i\right)\\ &+\left(\frac{3M}{2}\right)\sum_{i\in D_0}\alpha^i+\left(\frac{3M}{2}+1\right)\sum_{i\in D_1}\alpha^i\\ &+\left(\frac{3M}{2}\right)\sum_{i\in D_2}\alpha^i+\left(\frac{3M}{2}+1\right)\sum_{i\in D_3}\alpha^i\\ &+\left(\frac{3M}{2}\right)\sum_{i\in D_4}\alpha^i+\left(\frac{3M}{2}+1\right)\sum_{i\in D_5}\alpha^i\\ &-12\frac{(p_1-1)(p_2-1)}{36}-3\frac{(p_1-1)(p_2-7)}{36}\\ &-3\frac{(p_1-7)(p_2-1)}{36}+3\frac{(p_1-1)(p_2-1)}{6}\\ =&\ \frac{n-1}{4}.\end{aligned}$$

Now suppose that $p_1p_2 \equiv 7 \pmod{12}$. By Lemma 2, $-1 \in D_3$ and from Lemma 5, $-D_j = \{-t : t \in D_j\} = D_{(j+3)(\mathrm{mod}\ 6)}$. Similar to the above proof, in this case

$$\Lambda(\alpha)(\Lambda(\alpha)+1) = -\frac{n+1}{4}. \tag{3.12}$$

This completes the proof of the lemma. □

Note that

$$\Lambda(1) = \frac{(p_1+1)(p_2-1)}{2} \pmod{p}. \tag{3.13}$$

It is elementary to prove the following Lemma:

Lemma 9. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p\equiv 1 \pmod{24} \text{ or } p\equiv 7 \pmod{24},\\ -1, & \text{if } p\equiv 13 \pmod{24} \text{ or } p \equiv 19 \pmod{24}.\end{cases}$$

Lemma 10. *If $n \equiv 7 \pmod{12}$ and $\frac{n+1}{4} \equiv 0 \pmod{p}$ or $n \equiv 1 \pmod{12}$ and $\frac{n-1}{4} \equiv 0 \pmod{p}$, then $q \pmod{n} \in d_0$.*

Proof. First, we prove that when $n \equiv 7 \pmod{12}$ and $\frac{n+1}{4} \equiv 0 \pmod{p}$, then $q \pmod{n} \in d_0$. Clearly, d_0 is a multiplicative subgroup of $\mathbb{Z}_n^*$. Since q is a power of p, it is sufficient to prove that $p \in d_0$. Let us assume that $p \in d_1$. We deal with $p = 2$. Let $2 \in d_1$. By the definition of Whiteman's generalized cyclotomic classes, $2 = u^s g^i$, $0 \leqslant i \leqslant e-1$ and s is odd. From (2.1), we have

$$2 \equiv g^{s+i} \pmod{p_1} \quad \text{and} \quad 2 \equiv g^i \pmod{p_2}.$$

Therefore, 2 must be a quadratic residue (non residue, respectively) modulo p_1 if it is a quadratic non residue (residue, respectively) modulo p_2.

For $p = 2$, if $\frac{n+1}{4} \equiv 0 \pmod{p}$, then 8 divides p_1p_2+1. Since $\gcd(p_1-1, p_2-1) = 6$, it is clear that we get only the following four conditions for p_1 and p_2,

$$\begin{cases} p_1 \equiv 1 \pmod{24}, \\ p_2 \equiv 7 \pmod{24}, \end{cases}$$

$$\begin{cases} p_1 \equiv 7 \pmod{24}, \\ p_2 \equiv 1 \pmod{24}, \end{cases}$$

$$\begin{cases} p_1 \equiv 13 \pmod{24}, \\ p_2 \equiv 19 \pmod{24}, \end{cases}$$

$$\begin{cases} p_1 \equiv 19 \pmod{24}, \\ p_2 \equiv 13 \pmod{24}. \end{cases}$$

By Lemma 9, it follows that none of the above four possibilities are possible. This gives a contradiction therefore $2 \in d_0$.

Again suppose that $p \in d_1$. Since $p \in d_1$, then $p = u^s g^i$, $0 \leqslant i \leqslant e-1$ and s is odd. We have

$$p \equiv g^{s+i} \pmod{p_1} \qquad \text{and} \qquad p \equiv g^i \pmod{p_2}.$$

Since s is an odd integer, then we must have

$$\left(\frac{p}{p_1}\right)\left(\frac{p}{p_2}\right) = -1, \tag{3.14}$$

where $(-)$ is the Legendre symbol. If $n \equiv 7 \pmod{12}$, by Lemma 2, $(p_1+p_2)/2$ is even. If $\frac{n+1}{4} \equiv 0 \pmod{p}$, then $n = p_1p_2 \equiv -1 \pmod{p}$. From the Law of Quadratic Reciprocity,

$$\left(\frac{p}{p_i}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{p_i-1}{2}\right)}\left(\frac{p_i}{p}\right) \quad \text{for} \quad i = 1, 2,$$

and

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

It follows that

$$\left(\frac{p}{p_1}\right)\left(\frac{p}{p_2}\right) = 1.$$

This is contrary to (3.14). Thus, $p \in d_0$. Similarly, we prove that if $n \equiv 1 \pmod{12}$ and $\frac{n-1}{4} \equiv 0 \pmod{p}$, then $q \pmod{n} \in d_0$. $\square$

Let the symbols be defined as in Section 2. We explain the factorization of $x^n - 1$ over finite field GF(q). Let $\mu_0(x) = \prod_{i\in d_0}(x-\alpha^i)$ and $\mu_1(x) = \prod_{i\in d_1}(x-\alpha^i)$, where α is the p_1p_2-th primitive root of unity over GF(q). Let $(\alpha^{p_1})^i; 0 \leq i < p_2$ is the p_2-th roots of unity of the splitting field $x^{p_2} - 1$ and

$(\alpha^{p_2})^i; 0 \le i < p_1$ is the p_1-th roots of unity of the splitting field $x^{p_1}-1$. We have,

$$x^{p_2}-1=\prod_{i\in P\cup\{0\}}(x-\alpha^i) \text{ and } x^{p_1}-1=\prod_{i\in Q\cup\{0\}}(x-\alpha^i).$$

Then we have

$$x^n-1=\prod_{i=0}^{n-1}(x-\alpha^i)=\frac{(x^{p_1}-1)(x^{p_2}-1)}{x-1}\mu(x), \tag{3.15}$$

where $\mu(x)=\mu_0(x)\mu_1(x)$. It is straightforward to prove that if $q\in d_0$, then $\mu_i(x)\in \mathrm{GF}(q)$ for $i\in\{0,1\}$.

Now we are ready to compute the generator polynomial and the linear complexity of the sequence λ^∞ (defined in (2.2)). For this, let $\Omega_1=\frac{p_1+1}{2} \pmod p$, $\Omega_2=\frac{p_2-1}{2} \pmod p$ and $\Omega=\frac{(p_1+1)(p_2-1)}{2} \pmod p$. We have the following two theorems.

Theorem 1. (1) *When* $n\equiv 7 \pmod{12}$ *and* $\frac{n+1}{4}\not\equiv 0 \pmod p$ *or* $n\equiv 1 \pmod{12}$ *and* $\frac{n-1}{4}\not\equiv 0 \pmod p$, *then the generator polynomial* $g_\lambda(x)$ *and the linear span* L_λ *of the sequence* λ^∞ (*defined in* (2.2)) *are given by*

$$g_\lambda(x)=\begin{cases} x^n-1, & \text{if } \Omega_1\ne 0,\ \Omega_2\ne 0,\ \Omega\ne 0,\\ \frac{x^n-1}{x-1}, & \text{if } \Omega_1\ne 0,\ \Omega_2\ne 0,\ \Omega= 0,\\ \frac{x^n-1}{x^{p_2}-1}, & \text{if } \Omega_1= 0,\ \Omega_2\ne 0,\\ \frac{x^n-1}{x^{p_1}-1}, & \text{if } \Omega_1\ne 0,\ \Omega_2= 0,\\ \frac{(x^n-1)(x-1)}{(x^{p_1}-1)(x^{p_2}-1)}, & \text{if } \Omega_1=\Omega_2=0.\end{cases}$$

and

$$L_\lambda(x)=\begin{cases} n, & \text{if } \Omega_1\ne 0,\ \Omega_2\ne 0,\ \Omega\ne 0,\\ n-1, & \text{if } \Omega_1\ne 0,\ \Omega_2\ne 0,\ \Omega= 0,\\ n-p_2, & \text{if } \Omega_1= 0,\ \Omega_2\ne 0,\\ n-p_1, & \text{if } \Omega_1\ne 0,\ \Omega_2= 0,\\ n-(p_1+p_2-1), & \text{if } \Omega_1=\Omega_2=0.\end{cases}$$

Thus, C_λ *is the cyclic code with generator polynomial* $g_\lambda(x)$ *as above over* $\mathrm{GF}(q)$ *defined by the two-prime WGCS-I of order* 6 *has parameters* $[n,k,d]$, *where the dimension* $k=n-\deg(g_\lambda(x))$.

(2) *When* $n\equiv 7 \pmod{12}$ *and* $\frac{n+1}{4}\equiv 0 \pmod p$ *or* $n\equiv 1 \pmod{12}$ *and* $\frac{n-1}{4}\equiv 0 \pmod p$, *then the generator polynomial* $g_\lambda(x)$ *and the linear span* L_λ

of the sequence λ^∞ *are given by*

$$g_\lambda(x) = \begin{cases} \frac{x^n-1}{\mu_0(x)}, & \text{if } \Omega_1 \neq 0,\ \Omega_2 \neq 0,\ \Omega \neq 0,\ \Lambda(\alpha) = 0, \\ \frac{x^n-1}{\mu_1(x)}, & \text{if } \Omega_1 \neq 0,\ \Omega_2 \neq 0,\ \Omega \neq 0,\ \Lambda(\alpha) = -1, \\ \frac{x^n-1}{(x-1)\mu_0(x)}, & \text{if } \Omega_1 \neq 0,\ \Omega_2 \neq 0,\ \Omega = 0,\ \Lambda(\alpha) = 0, \\ \frac{x^n-1}{(x-1)\mu_1(x)}, & \text{if } \Omega_1 \neq 0,\ \Omega_2 \neq 0,\ \Omega = 0,\ \Lambda(\alpha) = -1, \\ \frac{x^n-1}{(x^{p_2}-1)\mu_0(x)}, & \text{if } \Omega_1 = 0,\ \Omega_2 \neq 0,\ \Lambda(\alpha) = 0, \\ \frac{x^n-1}{(x^{p_2}-1)\mu_1(x)}, & \text{if } \Omega_1 = 0,\ \Omega_2 \neq 0,\ \Lambda(\alpha) = -1, \\ \frac{x^n-1}{(x^{p_1}-1)\mu_0(x)}, & \text{if } \Omega_1 \neq 0,\ \Omega_2 = 0,\ \Lambda(\alpha) = 0, \\ \frac{x^n-1}{(x^{p_1}-1)\mu_1(x)}, & \text{if } \Omega_1 \neq 0,\ \Omega_2 = 0,\ \Lambda(\alpha) = -1, \\ \frac{(x^n-1)(x-1)}{(x^{p_1}-1)(x^{p_2}-1)\mu_0(x)}, & \text{if } \Omega_1 = \Omega_2 = 0,\ \Lambda(\alpha) = 0, \\ \frac{(x^n-1)(x-1)}{(x^{p_1}-1)(x^{p_2}-1)\mu_1(x)}, & \text{if } \Omega_1 = \Omega_2 = 0,\ \Lambda(\alpha) = -1, \end{cases}$$

and

$$L_\lambda(x) = \begin{cases} n - \frac{(p_1-1)(p_2-1)}{2}, & \text{if } \Omega_1 \neq 0,\ \Omega_2 \neq 0,\ \Omega \neq 0, \\ & \text{one of } \Lambda(\alpha) = \{0,-1\} \text{ but not both}, \\ n - \frac{(p_1-1)(p_2-1)+2}{2}, & \text{if } \Omega_1 \neq 0,\ \Omega_2 \neq 0,\ \Omega = 0, \\ & \text{one of } \Lambda(\alpha) = \{0,-1\} \text{ but not both}, \\ n - \frac{(p_1+1)(p_2-1)+2}{2}, & \text{if } \Omega_1 = 0,\ \Omega_2 \neq 0, \\ & \text{one of } \Lambda(\alpha) = \{0,-1\} \text{ but not both}, \\ n - \frac{(p_1-1)(p_2+1)+2}{2}, & \text{if } \Omega_1 \neq 0,\ \Omega_2 = 0, \\ & \text{one of } \Lambda(\alpha) = \{0,-1\} \text{ but not both}, \\ n - \frac{(p_1+1)(p_2+1)-2}{2}, & \text{if } \Omega_1 = \Omega_2 = 0, \\ & \text{one of } \Lambda(\alpha) = \{0,-1\} \text{ but not both}. \end{cases}$$

Thus, C_λ *is the cyclic code with generator polynomial* $g_\lambda(x)$ *over* $GF(q)$ *defined by the WGCS-I of order* 6 *has parameters* $[n, k, d]$*, where the dimension* $k = n - \deg(g_\lambda(x))$.

Proof. (1) When $n \equiv 7 \pmod{12}$ and $\frac{n+1}{4} \not\equiv 0 \pmod{p}$ or $n \equiv 1 \pmod{12}$ and $\frac{n-1}{4} \not\equiv 0 \pmod{p}$, then by Lemma 8, we have $\Lambda(\alpha) \neq 0, -1$. Therefore, from Lemma 6, $\Lambda(\alpha^t) = 0$ only when t is in P or Q or both. By Lemma 6 and (3.13), we follow that the conclusion on the generator polynomial $g_\lambda(x)$ of cyclic code C_λ over GF(q) defined by the sequence λ^∞. The linear complexity of the sequence λ^∞ is equal to $\deg(g_\lambda(x))$.

(2) When $n \equiv 7 \pmod{12}$ and $\frac{n+1}{4} \equiv 0 \pmod{p}$ or $n \equiv 1 \pmod{12}$ and $\frac{n-1}{4} \equiv 0 \pmod{p}$, then by Lemma 8, we have $\Lambda(\alpha) \in \{0, -1\}$ and $\mu_i(x) \in$ GF$(q)[x]$ for each i if $q \in d_0$. From (3.13), Lemmas 6, 7 and 10, we follow that the conclusion on the generator polynomial $g_\lambda(x)$ of cyclic code C_λ over GF(q) defined by the sequence λ^∞. The linear complexity of the sequence λ^∞ is equal to $\deg(g_\lambda(x))$. □

The following corollaries follow from Theorem 1, Lemmas 8 and 10 and give the parameters of the cyclic codes C_λ with generator polynomial and the linear complexity of the sequence λ^∞ (defined in (2.2)).

Corollary 1. *Let $q = 2$, the generator polynomial and the linear complexity are $g_\lambda(x)$ and L_λ, respectively. We have the following conclusions*:

(1) *If $p_1 \equiv 13 \pmod{24}$ and $p_2 \equiv 7 \pmod{24}$ or $p_1 \equiv 1 \pmod{24}$ and $p_2 \equiv 19 \pmod{24}$, then*

$$g_\lambda(x) = \frac{x^n - 1}{x - 1} \quad \textit{and} \quad L_\lambda = n - 1.$$

Therefore, the parameters of the cyclic code C_λ over $\mathrm{GF}(q)$ are $[n, 1, n-1]$.

(2) *If $p_1 \equiv 7 \pmod{24}$ and $p_2 \equiv 19 \pmod{24}$ or $p_1 \equiv 19 \pmod{24}$ and $p_2 \equiv 7 \pmod{24}$, then*

$$g_\lambda(x) = \frac{x^n - 1}{x^{p_2} - 1} \quad \textit{and} \quad L_\lambda = n - p_2.$$

Therefore, the parameters of the cyclic code C_λ over $\mathrm{GF}(q)$ are $[n, p_2, p_1]$.

(3) *If $p_1 \equiv 7 \pmod{24}$ and $p_2 \equiv 13 \pmod{24}$ or $p_1 \equiv 19 \pmod{24}$ and $p_2 \equiv 1 \pmod{24}$, we have*

$$g_\lambda(x) = \frac{(x^n - 1)(x - 1)}{(x^{p_1} - 1)(x^{p_2} - 1)} \quad \textit{and} \ L_\lambda = n - (p_1 + p_2 - 1).$$

Therefore, the parameters of the cyclic code C_λ over $\mathrm{GF}(q)$ are $[n, p_2, p_1]$.

(4) *If $p_1 \equiv 1 \pmod{24}$ and $p_2 \equiv 7 \pmod{24}$ or $p_1 \equiv 13 \pmod{24}$ and $p_2 \equiv 19 \pmod{24}$, we have*

$$g_\lambda(x) = \begin{cases} \frac{(x^n-1)}{(x-1)\mu_0(x)}, & \textit{if} \ \ \Lambda(\alpha) = 0 \\ \frac{(x^n-1)}{(x-1)\mu_1(x)}, & \textit{if} \ \ \Lambda(\alpha) = 1 \end{cases} \quad \textit{and} \ L_\lambda = n - \frac{(p_1 - 1)(p_2 - 1) + 2}{2}.$$

Therefore, the parameters of the cyclic code C_λ over $\mathrm{GF}(q)$ are

$$[n, \frac{(p_1 - 1)(p_2 - 1) + 2}{2}, d].$$

(5) *If $p_1 \equiv 7 \pmod{24}$ and $p_2 \equiv 7 \pmod{24}$ or $p_1 \equiv 19 \pmod{24}$ and $p_2 \equiv 19 \pmod{24}$, we have*

$$g_\lambda(x) = \begin{cases} \frac{(x^n-1)}{(x^{p_2}-1)\mu_0(x)}, & \textit{if} \ \ \Lambda(\alpha) = 0 \\ \frac{(x^n-1)}{(x^{p_2}-1)\mu_1(x)}, & \textit{if} \ \ \Lambda(\alpha) = 1 \end{cases} \quad \textit{and} \quad L_\lambda = n - \frac{(p_1 + 1)(p_2 - 1) + 2}{2}.$$

In this case, the parameters of the cyclic code C_λ over $\mathrm{GF}(q)$ are

$$[n, \frac{(p_1 + 1)(p_2 - 1) + 2}{2}, d].$$

(6) *If* $p_1 \equiv 7 \pmod{24}$ *and* $p_2 \equiv 1 \pmod{24}$ *or* $p_1 \equiv 19 \pmod{24}$ *and* $p_2 \equiv 13 \pmod{24}$, *we have*

$$g_\lambda(x) = \begin{cases} \frac{(x^n-1)(x-1)}{(x^{p_1}-1)(x^{p_2}-1)\mu_0(x)}, & \text{if } \Lambda(\alpha) = 0 \\ \frac{(x^n-1)(x-1)}{(x^{p_1}-1)(x^{p_2}-1)\mu_1(x)}, & \text{if } \Lambda(\alpha) = 1 \end{cases} \quad \text{and}$$

$$L_\lambda = n - \frac{(p_1+1)(p_2+1)-2}{2}.$$

In this case, the parameters of the cyclic code C_λ *over* $\mathrm{GF}(q)$ *are*

$$[n, \frac{(p_1+1)(p_2+1)-2}{2}, d].$$

If $q = 3$, then we have only one possibility: $p_1 \equiv 7 \pmod{12}$ and $p_2 \equiv 7 \pmod{12}$.

Corollary 2. *Let* $q = 3$ *and* $p_1 \equiv 7 \pmod{12}$ *and* $p_2 \equiv 7 \pmod{12}$. *Then we have*

$$g_\lambda(x) = \begin{cases} \frac{(x^n-1)}{(x^{p_1}-1)\mu_0(x)}, & \text{if } \Lambda(\alpha) = 0 \\ \frac{(x^n-1)}{(x^{p_1}-1)\mu_1(x)}, & \text{if } \Lambda(\alpha) = 1 \end{cases} \quad \text{and } L_\lambda = n - \frac{(p_1-1)(p_2+1)+2}{2}.$$

In this case, the parameters of the cyclic code C_λ *over* $\mathrm{GF}(q)$ *are*

$$[n, \frac{(p_1-1)(p_2+1)+2}{2}, d].$$

4. The minimum distance of the cyclic codes

Here, we determine the lower bounds on the minimum distance of some of the cyclic codes of this paper and the symbols are the same as above.

Theorem 2 ([5])**.** *The cyclic code* C_i *with the generator polynomial* $g_i(x) = \frac{x^n-1}{x^{p_i}-1}$ *has parameters* $[n, p_i, d_i]$ *over* $\mathrm{GF}(q)$, *where* $d_i = p_{i-(-1)^i}$ *and* $i = 1, 2$.

Theorem 3 ([5])**.** *The cyclic code* $C_{(p_1,p_2,q)}$ *with the generator polynomial* $g(x) = \frac{(x^n-1)(x-1)}{(x^{p_1}-1)(x^{p_2}-1)}$ *has parameters* $[n, p_1+p_2-1, d_{(p_1,p_2,q)}]$ *over* $\mathrm{GF}(q)$, *where* $d_{(p_1,p_2,q)} = \min(p_1, p_2)$.

Theorem 4. *Assume that* $q \in d_0$. *Let the cyclic code* $C^{(i,j)}$ *with the generator polynomial* $g^{(i,j)}(x) = \frac{x^n-1}{(x^{p_i}-1)\mu_j(x)}$ *has parameters* $[n, p_i + \frac{(p_1-1)(p_2-1)}{2}, d^{(i,j)}]$ *over* $\mathrm{GF}(q)$, *where* $i \in \{1, 2\}$ *and* $j \in \{0, 1\}$ *and* $d^{(i,j)} \geq \lceil \sqrt{p_{i-(-1)^i}} \rceil$. *If* $-1 \in d_1$, *we have* $(d^{(i,j)})^2 - d^{(i,j)} + 1 \geq p_{i-(-1)^i}$.

Proof. Let the codeword $c(x) \in \mathrm{GF}(q)[x]/(x^n-1)$ with the Hamming weight w in $C^{(i,j)}$. Choose any $r \in d_1$. The codeword $c(x^r)$ with Hamming weight w in $C^{(i,(j+1) \bmod 2)}$. Then, we conclude that $d^{(i,j)} = d^{(i,(j+1) \bmod 2)}$. Thus, $c(x)c(x^r)$ is a codeword of C_i. From Theorem 2, C_i is the cyclic code with minimum distance $d_i = p_{i-(-1)^i}$ and the generator polynomial $g_i(x) = \frac{x^n-1}{x^{p_i}-1}$

over GF(q). Hence, we have $(d^{(i,j)})^2 \geq d_i = p_{i-(-1)^i}$, and $(d^{(i,j)})^2 - d^{(i,j)} + 1 \geq p_{i-(-1)^i}$ if $-1 \in d_1$. $\square$

Theorem 5. *Assume that $q \in d_0$. Let the cyclic code $C^{(j)}_{(p_1,p_2)}$ with the generator polynomial $g^{(j)}_{(p_1,p_2)}(x) = \frac{(x^n-1)(x-1)}{(x^{p_1}-1)(x^{p_2}-1)\mu_j(x)}$ over* GF(q)*, where $i \in \{1,2\}$ and $j \in \{0,1\}$. The cyclic code $C^{(j)}_{(p_1,p_2)}$ has parameters $[n, p_1+p_2-1+\frac{(p_1-1)(p_2-1)}{2}, d^{(j)}_{(p_1,p_2)}]$, where $d^{(j)}_{(p_1,p_2)} \geq \lceil\sqrt{\min(p_1,p_2)}\rceil$. If $-1 \in d_1$, we have $(d^{(j)}_{(p_1,p_2)})^2 - d^{(j)}_{(p_1,p_2)} + 1 \geq \min(p_1,p_2)$.*

Proof. Let the codeword $c(x) \in \mathrm{GF}(q)[x]/(x^n-1)$ with Hamming weight w in $C^{(j)}_{(p_1,p_2)}$. Choose any $r \in d_1$. The codeword $c(x^r)$ with Hamming weight w in $C^{((j+1) \bmod 2)}_{(p_1,p_2)}$. Then, we conclude that $d^{(j)}_{(p_1,p_2)} = d^{((j+1) \bmod 2)}_{(p_1,p_2)}$. Thus, $c(x)c(x^r)$ is a codeword of $C_{(p_1,p_2,q)}$. From Theorem 3, $C_{(p_1,p_2,q)}$ is a cyclic code over GF(q) with the generator polynomial $g(x) = \frac{(x^n-1)(x-1)}{(x^{p_1}-1)(x^{p_2}-1)}$ and minimum distance $d_{(p_1,p_2,q)} = \min(p_1,p_2)$. Hence, we have $(d^{(j)}_{(p_1,p_2)})^2 \geq d_{(p_1,p_2,q)} = \min(p_1,p_2)$, and $(d^{(j)}_{(p_1,p_2)})^2 - d^{(j)}_{(p_1,p_2)} + 1 \geq \min(p_1,p_2)$ if $-1 \in d_1$. $\square$

Example 1. Let $(p,m,p_1,p_2) = (2,1,7,31)$. We have $q = 2$, $n = 217$ and C_λ is a $[217,121]$ cyclic code over GF(q) with generator polynomial $g_\lambda(x) = \frac{x^{217}-1}{(x^{31}-1)d_1(x)} = x^{96}+x^{94}+x^{91}+x^{87}+x^{86}+x^{85}+x^{83}+x^{81}+x^{80}+x^{78}+x^{77}+x^{75}+x^{72}+x^{69}+x^{67}+x^{65}+x^{64}+x^{63}+x^{60}+x^{58}+x^{55}+x^{53}+x^{52}+x^{51}+x^{48}+x^{45}+x^{44}+x^{43}+x^{41}+x^{38}+x^{36}+x^{33}+x^{32}+x^{31}+x^{29}+x^{27}+x^{24}+x^{21}+x^{19}+x^{18}+x^{16}+x^{15}+x^{13}+x^{11}+x^{10}+x^9+x^5+x^2+1$. We did some computation with MAGMA and our computation shows that upper bound on the minimum distance for this binary code is 31.

Example 2. Let $(p,m,p_1,p_2) = (2,1,7,31)$. We have $q = 3$, $n = 217$ and C_λ is a $[217,97]$ cyclic code over GF(q) with generator polynomial $g_\lambda(x) = \frac{x^{217}-1}{(x^7-1)d_1(x)} = x^{120}+2x^{115}+x^{113}+2x^{109}+2x^{108}+x^{106}+x^{105}+x^{104}+2x^{102}+2x^{100}+x^{98}+2x^{96}+x^{95}+x^{92}+x^{90}+x^{88}+2x^{87}+2x^{85}+x^{83}+2x^{81}+x^{79}+x^{78}+2x^{77}+x^{76}+2x^{75}+2x^{74}+2x^{71}+2x^{70}+x^{69}+x^{67}+2x^{66}+2x^{65}+x^{64}+2x^{61}+x^{60}+2x^{59}+x^{56}+2x^{55}+2x^{54}+x^{53}+x^{51}+2x^{50}+2x^{49}+2x^{46}+2x^{45}+x^{44}+2x^{43}+x^{42}+x^{41}+2x^{39}+x^{37}+2x^{35}+2x^{33}+x^{32}+x^{30}+x^{28}+x^{25}+2x^{24}+x^{22}+2x^{20}+2x^{18}+x^{16}+x^{15}+x^{14}+2x^{12}+2x^{11}+x^7+2x^5+1$. We did some computation with MAGMA and our computation shows that upper bound on the minimum distance for this ternary code is 58. From Theorem 4, we have the lower bound on the minimum distance for this binary code is 6.

Example 3. Let $(p,m,p_1,p_2) = (2,1,7,19)$. We have $q = 2$, $n = 133$ and C_λ is a $[133,19,7]$ cyclic code with generator polynomial $g_\lambda(x) = \frac{(x^{133}-1)}{(x^{19}-1)(x^{13}-1)} = x^{114}+x^{95}+x^{76}+x^{57}+x^{38}+x^{19}+1$ over GF(q). From the table of linear codes, this cyclic code has poor minimum distance. The code in this case is bad because $q \notin D_0$.

5. Conclusion

In this manuscript, we have computed the linear complexities of the two-prime WGCS-I of order 6. We have also constructed the cyclic codes of WGCS-I of order 6 over GF(q). If $\Lambda(\alpha) \notin \{0, 1\}$, then the least value of linear complexity is $n-(p_1+p_2-1)$ and if $\Lambda(\alpha) \in \{0, 1\}$, then the least value of linear complexity is $n-\frac{(p_1+1)(p_2+1)-2}{2}$. Therefore, we conclude that these sequence possesses high linear complexity. The cyclic codes employed in this paper depend on p_1, p_2 and q. When $q \in D_0$, we get a good code. We expect that the codes in Examples 1 and 2 give good codes. When $q \notin D_0$, we get a bad code, for example, we get a bad code in Example 3. Hence, we expect that cyclic codes mentioned in this article can be employed to construct the good cyclic codes of large length.

References

[1] E. Betti and M. Sala, *A new bound for the minimum distance of a cyclic code from its defining set*, IEEE Trans. Inform. Theory **52** (2006), no. 8, 3700–3706.

[2] Z.-X. Chen and S.-Q. Li, *Some notes on generalized cyclotomic sequences of length pq*, J. Comput. Sci. Tech. **23** (2008), no. 5, 843–850.

[3] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*, North-Holland Mathematical Library, **55**, North-Holland Publishing Co., Amsterdam, 1998.

[4] C. Ding, *Linear complexity of generalized cyclotomic binary sequences of order* 2, Finite Fields Appl. **3** (1997), no. 2, 159–174.

[5] ———, *Cyclic codes from the two-prime sequences*, IEEE Trans. Inform. Theory **58** (2012), no. 6, 3881–3891.

[6] C. Ding, X. Du, and Z. Zhou, *The Bose and minimum distance of a class of BCH codes*, IEEE Trans. Inform. Theory **61** (2015), no. 5, 2351–2356.

[7] M. van Eupen and J. H. van Lint, *On the minimum distance of ternary cyclic codes*, IEEE Trans. Inform. Theory **39** (1993), no. 2, 409–422.

[8] P. K. Kewat and P. Kumari, *Cyclic codes from the second class two-prime Whiteman's generalized cyclotomic sequence with order* 6, Cryptogr. Commun. **9** (2017), no. 4, 475–499.

[9] J. H. van Lint and R. M. Wilson, *On the minimum distance of cyclic codes*, IEEE Trans. Inform. Theory **32** (1986), no. 1, 23–40.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes. II*, North-Holland Publishing Co., Amsterdam, 1977.

[11] Y. Sun, T. Yan, and H. Li, *Cyclic code from the first class whiteman's generalized cyclotomic sequence with order* 4, CoRR, abs/1303.6378, 2013.

[12] A. L. Whiteman, *A family of difference sets*, Illinois J. Math. **6** (1962), 107–121.

Pramod Kumar Kewat
Department of Applied Mathematics
Indian Institute of Technology (Indian School of Mines)
Dhanbad 826 004, India
Email address: pramodk@iitism.ac.in

Priti Kumari
Department of Applied Mathematics
Indian Institute of Technology (Indian School of Mines)
Dhanbad 826 004, India
Email address: priti.jsr13@gmail.com