Journal of Rajasthan Academy of Physical Sciences
ISSN : 0972-6306; URL : http://raops.org.in
Vol.15, No.3, September, 2016, 155-182

CYCLIC CODES FROM WHITEMAN'S GENERALIZED CYCLOTOMIC SEQUENCES OF ORDER 8

Pankaj and Manju Pruthi
Department of Mathematics, Indira Gandhi University, Meerpur (Rewari)-122502, Haryana, India
Email: pankajarora1242@yahoo.com, manju.pruthi@yahoo.com

Abstract: Cyclic Codes are a subclass of linear codes and have important applications in data storage systems and communication systems because of their efficient encoding and decoding algorithms. In this paper, we construct several classes of cyclic codes over the finite field $GF(q)$ and give their generator polynomials by employing two-prime Whiteman's generalized cyclotomic sequences of order 8. And we also calculate the minimum distance of some cyclic codes and give lower bounds of the minimum distance for some other cyclic codes.

Keywords: Cyclotomic Sequence, Generator Polynomial, Minimum Distance.
2010 Mathematics Subject Classification: 11Txx, 11T22, 11T71, 68P30, 94Bxx, 94B15.

1. Introduction

Cyclic Codes are a small but highly structured subclass of linear codes. Because of their efficient encoding and decoding algorithms, cyclic codes have wide applications in data storage systems and communication systems. Cyclic codes have been studied for decades and a lot of progress has been made and many important results in the field of cyclic codes have been found (for example, see [1], [10-14]). Recently, several classes of cyclic codes using two-prime Whiteman's generalized cyclotomic sequences and cyclotomic sequences of order 4 have been presented by Ding in [5] and [4] respectively and lower bounds on the nonzero minimum hamming weight of some cyclic codes were developed at the same time. In [15], and [17], several classes of cyclic codes have been constructed by employing Whiteman's generalized cyclotomic sequences of order 4 and 6 respectively. In this paper, employing two-prime Whiteman's generalized cyclotomic sequences of order 8, we construct several cyclic codes over the finite field $GF(q)$ and give their generator polynomials. And we also calculate the minimum distance of some cyclic codes and give lower bounds of the minimum distance for some other cyclic codes.

Let q be a power of any primep, n a positive integer satisfying$\gcd(n, q) = 1$. A linear $[n, k, d]$ code over $GF(q)$ is a k-dimensional subspace of $GF(q)^n$with minimum

(Hamming) nonzero weight$d$. A linear $[n,k]$ code C over the finite field $GF(q)$ is called a cyclic if $(c_0,c_1,\cdots,c_{n-1})\in C$ implies $(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C$[6]. For any vector $(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in GF(q)^n$, we identify it with the polynomial $c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}\in GF(q)[x]/(x^n-1)$. Then any code C of length n over $GF(q)$ is equivalent to a subset of $GF(q)[x]/(x^n-1)$. It is well known that $GF(q)[x]/(x^n-1)$ is a principal ideal ring, i.e., any one of ideals of $GF(q)[x]/(x^n-1)$ is principle. Let $C=\langle g(x)\rangle$ be a cyclic code and $h(x)=\frac{x^n-1}{g(x)}$. Then we call $g(x)$ the generator polynomial and $h(x)$ the perity-check polynomial of C [6].

Let $s^n=(s_i)_{i=0}^{n-1}$ be a sequence of period n over $GF(q)$. We call

$$S^n(x)=\sum_{i=0}^{n-1}s_i\,x^i\in \mathrm{GF(q)[x]},\ (1)$$

the generator polynomial of the sequence s^n. It is well known that the minimal polynomial of $s^n$is given by $(x^n-1)/\gcd\left(x^n-1,S^n(x)\right)$. Then the cyclic code C_s generated by the minimal polynomial of s^n is given by

$$g(x)=\frac{x^n-1}{\gcd\left(x^n-1,S^n(x)\right)}. \qquad (2)$$

Correspondingly, the sequence s^n is called the defining sequence of the cyclic code C_s [6].

2. **The Whiteman's Generalized Cyclotomic Sequences of order 8 and its Construction**

An integer a is called a primitive root modulo n if the multiplicative order of a modulo n, denoted by $ord_n(a)$, is equal to $\phi(n)$ where ϕ is the Euler phi function and$\gcd(a,n)=1$.

Let n_1,n_2be two distinct odd primes satisfying $\gcd(n_1-1,n_2-1)=8$. Let $e=\frac{(n_1-1)(n_2-1)}{8}$, $n=n_1n_2$ and Z_n^* denotes the multiplicative group of integers modulo n. Suppose that g is a common primitive root of n_1 and n_2 and x an integer satisfying$x\equiv g(\mathrm{mod}n_1)$ and $x\equiv 1(\mathrm{mod}n_2)$.

Whiteman [16] has proved that

$$Z_n^*=\left\{g^sx^i:s=0,1,\cdots,e-1,i=0,1,\cdots,7\right\},$$

where Z_n^* denotes the set of all invertible elements of the residue class ring Z_n and e is the order of g modulo n. The Whiteman's generalized cyclotomic classes W_i of order 8 are defined by

$$W_i=\left\{g^sx^i:s=0,1,\cdots,e-1\right\},i=0,1,\cdots,7.$$

The classes $W_i,\ i=0,1,\cdots,7$ give a partition of Z_n^*, i.e., $Z_n^*=\cup_{i=0}^{7}W_i,\ W_i\cap W_j=\emptyset$ for $i\neq j$.

Let p, q, n, n_1, n_2, g, x be defined as before. Without special notation, n_1, n_2 always satisfy $\gcd(n_1 - 1, n_2 - 1) = 8$. Note that $\gcd(n, q) = 1$. Assume that the order of q modulo n is equal to m. Let α be a primitive element of the finite field $GF(q^m)$. Then $\beta = \alpha^{\frac{q^m-1}{n}}$ is a primitive n-th root of unity.

Let

$$P_1 = n_1, 2n_1, 3n_1, \cdots, (n_2 - 1)n_1, \quad P_2 = n_2, 2n_2, 3n_2, \cdots (n_1 - 1)n_2,$$
$$D_0 = \{0\} \cup P_2 \cup W_0 \cup W_1 \cup W_2 \cup W_3, \quad D_1 = P_1 \cup W_4 \cup W_5 \cup W_6 \cup W_7,$$
$$D_0^* = \{0\} \cup P_2 \cup W_0 \cup W_2 \cup W_4 \cup W_6, \quad D_1^* = P_1 \cup W_1 \cup W_3 \cup W_5 \cup W_7.$$

Then the sequence $s^n = (s_i)_{i=0}^{n-1}$ defined by

$$s_i = \begin{cases} 0, & \text{if } i \in D_0 \\ 1, & \text{if } i \in D_1 \end{cases}$$

is called first class two-prime Whiteman's generalized cyclotomic sequences of order 8.

And the sequence $s_n^* = (s_i^*)_{i=0}^{n-1}$ defined by

$$s_i^* = \begin{cases} 0, & \text{if } i \in D_0^* \\ 1, & \text{if } i \in D_1^* \end{cases}$$

is called second class two-prime Whiteman's generalized cyclotomic sequences of order 8.

Define the polynomials

$$S(\mathrm{x}) = \sum_{i \in D_1} x^i = \left(\sum_{i \in P_1} + \sum_{i \in W_4} + \sum_{i \in W_5} + \sum_{i \in W_6} + \sum_{i \in W_7} \right) x^i \tag{3}$$

$$T(\mathrm{x}) = \left(\sum_{i \in P_1} + \sum_{i \in W_1} + \sum_{i \in W_2} + \sum_{i \in W_3} + \sum_{i \in W_4} \right) x^i \tag{4}$$

$$U(\mathrm{x}) = \left(\sum_{i \in P_1} + \sum_{i \in W_2} + \sum_{i \in W_3} + \sum_{i \in W_4} + \sum_{i \in W_5} \right) x^i \tag{5}$$

$$= \left(\sum_{i \in P_1}^{V(\mathrm{x})} + \sum_{i \in W_3} + \sum_{i \in W_4} + \sum_{i \in W_5} + \sum_{i \in W_6} \right) x^i \tag{6}$$

where $S(\mathrm{x}), T(\mathrm{x}), \mathrm{U}(\mathrm{x}), V(\mathrm{x}) \in \mathrm{GF(q)[x]}$.

3. Generator Polynomials of Cyclic Codes

Our main aim in this section is to find the generator polynomial $g(x) = \frac{x^n - 1}{\gcd\left(x^n - 1, S(x)\right)}$ of the cyclic code C_s defined by the sequence s^n, where $S(x)$ is same as that in Equation (3). Hence we need only to find a's such that $S(\beta^a) = 0$ since β is a primitive n-th root of unity, where $0 \leq a \leq n - 1$. To this end, we need the following lemmas.

Lemma 3.1: For any $r \in W_j$, we have $rW_j = W_{i+j \,(\mathrm{mod}\ 8)}$, where $rW_j = \{rt \mid t \in W_j\}$.

Proof: We have $r \in W_i = \{g^s x^i : s = 0,1,\cdots, e-1\}, i = 0,1,\cdots 7$ and let $r = g^s x^i \in W_i$.

Then
$$rW_j = g^{s_1} x^i \{x^j + g x^j + g^2 x^j + \cdots + g^{e-1} x^j\}$$
$$= \{g^{s_1} x^{i+j} + g^{s_1+1} x^{i+j} + g^{s_1+2} x^{i+j} + \cdots + g^{s_1+e-1} x^{i+j}\}.$$

Since $x \in Z_n^*$, there must exist an integer v with $0 \leq v \leq e-1$ such that $x^8 = g^v$, therefore we must have $rW_j = W_{i+j \,(\mathrm{mod}\ 8)}$.

Lemma 3.2: Let the symbols be defined as above. Then we have

(I) $\sum_{i \in P_1} \beta^i = \sum_{i \in P_2} \beta^i = -1$

(II) $\sum_{i \in Z_n^*} \beta^i = \sum_{i \in \bigcup_{i=0}^{7} W_i} \beta^i = 1$

(III) $S(\beta^0) = S(1) = \frac{(n_1 + 1)(n_2 - 1)}{2} (\mathrm{mod}\ p)$.

Proof: It is easy to obtain the conclusions in (I) and (III). Now, we will explain the result in (II). Since

$$\beta^n - 1 = (\beta - 1)\left(\sum_{i=0}^{n-1} \beta^i\right) = 0$$

and $\beta - 1 \neq 0$. We know that

$$\sum_{i=0}^{n-1} \beta^i = 1 + \sum_{i \in P_1} \beta^i + \sum_{i \in P_2} \beta^i + \sum_{i \in Z_n^*} \beta^i.$$

By (I), we get

$$\sum_{i\in Z_n^*}\beta^i=\sum_{i\in\bigcup_{i=0}^{7}W_i}\beta^i=1+1-1=1.$$

Lemma 3.3: For $0\le j\le 7$, we have

$$\sum_{i\in W_j}\beta^{ti}=\begin{cases}-\dfrac{n_1-1}{8}(\mathrm{mod}\,p), & \text{if } t\in P_1,\\ -\dfrac{n_2-1}{8}(\mathrm{mod}\,p), & \text{if } t\in P_2.\end{cases}$$

Proof: Note that for $0\le j\le 7$, we have

$$W_j(\mathrm{mod}\,n_1)=\left\{g^s x^j : s=0,1,\cdots,\frac{(n_1-1)(n_2-1)}{8}-1\right\}$$

$$=\left\{g^{s+j} : s=0,1,\cdots,\frac{(n_1-1)(n_2-1)}{8}-1\right\}$$

$$=\frac{n_2-1}{8}\{1,2,\cdots,(n_1-1)\},$$

where $\frac{n_2-1}{8}$ is the multiplicity of each element in the set $\{1,2,\cdots,(n_1-1)\}$. Similarly, we have

$$W_j(\mathrm{mod}\,n_2)=\frac{n_1-1}{8}\{1,2,\cdots,(n_2-1)\}.$$

Suppose that $t\in P_1$. From Lemma 3.2(I), we get

$$\sum_{i\in W_j}\beta^{ti}=\left(\frac{n_1-1}{8}\right)\sum_{i\in P_1}\beta^i=-\frac{n_1-1}{8}(\mathrm{mod}\,p).$$

For $t\in P_2$, we can get the result by similar argument.

Lemma 3.4: For all $t\in Z_n$, we have

$$S(\beta^t)=T(\beta^t)=U(\beta^t)=V(\beta^t)=\begin{cases}-\dfrac{n_1+1}{2}(\mathrm{mod}\,p), & \text{if } t\in P_1,\\ \dfrac{n_2-1}{2}(\mathrm{mod}\,p), & \text{if } t\in P_2,\end{cases}$$

$$S(\beta^t)=\begin{cases} S(\beta), & \text{if } t\in W_0,\\ -(T(\beta)+1), & \text{if } t\in W_1,\\ -(U(\beta)+1), & \text{if } t\in W_2,\\ -(V(\beta)+1), & \text{if } t\in W_3,\\ -(S(\beta)+1), & \text{if } t\in W_4,\\ T(\beta), & \text{if } t\in W_5,\\ U(\beta), & \text{if } t\in W_6,\\ V(\beta), & \text{if } t\in W_7. \end{cases} T(\beta^t)=\begin{cases} T(\beta), & \text{if } t\in W_0,\\ U(\beta), & \text{if } t\in W_1,\\ V(\beta), & \text{if } t\in W_2,\\ S(\beta), & \text{if } t\in W_3,\\ -(T(\beta)+1), & \text{if } t\in W_4,\\ -(U(\beta)+1), & \text{if } t\in W_5,\\ -(V(\beta)+1), & \text{if } t\in W_6,\\ -(S(\beta)+1), & \text{if } t\in W_7. \end{cases}$$

$$U(\beta^t)=\begin{cases} U(\beta), & \text{if } t\in W_0,\\ V(\beta), & \text{if } t\in W_1,\\ S(\beta), & \text{if } t\in W_2,\\ -(T(\beta)+1), & \text{if } t\in W_3,\\ -(U(\beta)+1), & \text{if } t\in W_4,\\ -(V(\beta)+1), & \text{if } t\in W_5,\\ -(S(\beta)+1), & \text{if } t\in W_6,\\ T(\beta), & \text{if } t\in W_7. \end{cases} V(\beta^t)=\begin{cases} V(\beta), & \text{if } t\in W_0,\\ S(\beta), & \text{if } t\in W_1,\\ -(T(\beta)+1), & \text{if } t\in W_2,\\ -(U(\beta)+1), & \text{if } t\in W_3,\\ -(V(\beta)+1), & \text{if } t\in W_4,\\ -(S(\beta)+1), & \text{if } t\in W_5,\\ T(\beta), & \text{if } t\in W_6,\\ U(\beta), & \text{if } t\in W_7. \end{cases}$$

Proof: Since $\gcd(n_1,n_2)=1$, if $t\in P_1$, then $tP_1=P_1$.Then by Lemma 3.2 and 3.3, we get

$$S(\beta^t)=\sum_{i\in D_1}\beta^{ti}=\left(\sum_{i\in P_1}+\sum_{i\in W_4}+\sum_{i\in W_5}+\sum_{i\in W_6}+\sum_{i\in W_7}\right)\beta^{ti}$$

$$=(-1 \bmod p)-\left(\frac{n_1-1}{8} \bmod p\right)-\left(\frac{n_1-1}{8} \bmod p\right)-\left(\frac{n_1-1}{8} \bmod p\right)$$
$$-\left(\frac{n_1-1}{8} \bmod p\right)$$

$$=-\frac{n_1+1}{2}(\bmod p).$$

Similarly, $T(\beta^t)=U(\beta^t)=V(\beta^t)=-\frac{n_1+1}{2}(\bmod p)$, when $t\in P_1$.

If $t\in P_2$, then $tP_1=0$. Then by Lemma 3.2 and 3.3, we get

$$S(\beta^t)=\sum_{i\in D_1}\beta^{ti}=\left(\sum_{i\in P_1}+\sum_{i\in W_4}+\sum_{i\in W_5}+\sum_{i\in W_6}+\sum_{i\in W_7}\right)\beta^{ti}$$

$$=(n_2-1 \bmod p)-\left(\frac{n_2-1}{8} \bmod p\right)-\left(\frac{n_2-1}{8} \bmod p\right)-\left(\frac{n_2-1}{8} \bmod p\right)$$
$$-\left(\frac{n_2-1}{8} \bmod p\right)$$

$$= \frac{n_2 - 1}{2} (\text{mod } p).$$

Similarly, $T(\beta^t) = U(\beta^t) = V(\beta^t) = \frac{n_2-1}{2} (\text{mod } p)$, when $t \in P_2$.

For the case $t \in W_0$, we have $tW_j = W_{j\,(\text{mod } 8)}$ and $tP_1 = P_1$, since $\gcd(t, n_2) = 1$. Hence

$$S(\beta^t) = \sum_{i \in D_1} \beta^{ti} = \left(\sum_{i \in P_1} + \sum_{i \in W_4} + \sum_{i \in W_5} + \sum_{i \in W_6} + \sum_{i \in W_7} \right) \beta^{ti}$$

$$= \left(\sum_{i \in P_1} + \sum_{i \in W_4} + \sum_{i \in W_5} + \sum_{i \in W_6} + \sum_{i \in W_7} \right) \beta^{i}$$

$$= S(\beta).$$

Similarly, we can obtain $T(\beta^t) = T(\beta),\ U(\beta^t) = U(\beta),\ V(\beta^t) = V(\beta)$, when $t \in W_0$.

For the case $t \in W_1$, we have $tW_i = W_{i+1(\text{mod } 8)}$ for $1 \le i \le 7$. And since $\gcd\ (t, n_2) = 1$, if $t \in W_1$, then $tP_1 = P_1$. We have

$$\beta^n - 1 = (\beta - 1)\left(\sum_{i=0}^{n-1} \beta^i \right) = 0$$

and $\beta - 1 \neq 0$, this gives $\sum_{i=0}^{n-1} \beta^i = 0$. Therefore

$$\sum_{i=0}^{n-1} \beta^i = 1 + \sum_{i \in P_1} \beta^i + \sum_{i \in P_2} \beta^i + \sum_{i \in \bigcup_{i=0}^{7} W_i} \beta^i = 0.$$

From Lemma 3.2, we get

$$\sum_{i \in \bigcup_{i=0}^{7} W_i} \beta^i = 1.$$

Hence

$$S(\beta^t) = \sum_{i \in D_1} \beta^{ti} = \left(\sum_{i \in P_1} + \sum_{i \in W_4} + \sum_{i \in W_5} + \sum_{i \in W_6} + \sum_{i \in W_7} \right) \beta^{ti}$$

$$= \left(\sum_{i \in P_1} + \sum_{i \in W_5} + \sum_{i \in W_6} + \sum_{i \in W_7} + \sum_{i \in W_0} \right) \beta^{i}$$

$$= \left(\sum_{i \in P_1} - \sum_{i \in W_1} - \sum_{i \in W_2} - \sum_{i \in W_3} - \sum_{i \in W_4} \right) \beta^i + 1$$

$$= \left(- \sum_{i \in P_1} - \sum_{i \in W_1} - \sum_{i \in W_2} - \sum_{i \in W_3} - \sum_{i \in W_4} \right) \beta^i + 2 \sum_{i \in P_1} \beta^i + 1$$

$$= -(T(\beta) + 1).$$

Similarly, we can get the results when $t \in W_j, 2 \leq j \leq 7$.

In a similar fashion, we can get the results for $T(\beta^t)$, $U(\beta^t)$ and $V(\beta^t)$.This completes the proof of the lemma.

Corollary 3.5: Let the symbols be defined as before. We have the following conclusions.

(I) If $q \notin W_0$, we have $S(\beta) \neq 0, -1$, $T(\beta) \neq 0, -1$, $U(\beta) \neq 0, -1$, $V(\beta) \neq 0, -1$.
(II) If $q \in W_0$, we have $S^q(\beta) = S(\beta), T^q(\beta) = T(\beta), U^q(\beta) = U(\beta)$ and $V^q(\beta) = V(\beta)$.

Proof: (I) Note that $\gcd(n, q) = 1$, i.e., $q \in Z_n^*$, then $q \in \bigcup_{i=0}^{7} W_i$. If $q \notin W_0$, without loss of generality, assume that $q \in W_1$. By Lemma 3.4, we have

$$\begin{aligned} S^{q^4}(\beta) = S^{q^3}(\beta^q) &= (-T(\beta) - 1)^{q^3} \\ &= (-T(\beta^q) - 1)^{q^2} \\ &= (-U(\beta) - 1)^{q^2} \\ &= (-U(\beta^q) - 1)^q \\ &= (-V(\beta) - 1)^q \\ &= (-V(\beta^q) - 1) \\ &= -S(\beta) - 1, \end{aligned}$$

i.e.,

$$S^{q^4}(\beta) + S(\beta) + 1 = 0. \tag{7}$$

It is easy to chack that 0 and -1 is not a solution of Eq. (7). Similarly, we have

$$T^{q^4}(\beta) + T(\beta) + 1 = 0,$$

$$U^{q^4}(\beta) + U(\beta) + 1 = 0,$$

and

$$V^{q^4}(\beta) + V(\beta) + 1 = 0,$$

i.e., $T(\beta) \neq 0, -1,\ U(\beta) \neq 0, -1,\ V(\beta) \neq 0, -1$. If $q \in W_i, 2 \leq i \leq 7$, the results can be proved by similar argument.

(II) If $q \in W_0$, the conclusion is obvious.

We need to discuss the factorization of $x^n - 1$ over GF(q). Letβ be the same as before. Define for each $i,\ 0 \leq i \leq 7$,

$$d_i(x) = \prod_{j \in W_i} (x - \beta^j),$$

where W_i denote the Whiteman's cyclotomic classes of order 8. Among the n-th roots of unity β^i, where $0 \leq i \leq n-1$, the n_2 elements $\beta^i, i \in P_1 \cup \{0\}$, are the n_2-th roots of unity, the n_1 elements $\beta^i, i \in P_2 \cup \{0\}$, are the n_1-th roots of unity. Hence

$$x^{n_2} - 1 = \prod_{i \in P_1 \cup \{0\}} (x - \beta^i)$$

and

$$x^{n_1} - 1 = \prod_{i \in P_2 \cup \{0\}} (x - \beta^i).$$

Then we have

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \beta^i) = \frac{(x^{n_1} - 1)(x^{n_2} - 1)}{x - 1} d(x) \tag{8}$$

where $d(x) = \prod_{i=0}^{7} d_i(x)$.

It is straightforward to prove that if $q \in W_0$, then $d_i(x) \in$ GF(q) for all i.

Let $\Omega_1 = \frac{n_1+1}{2} (\mathrm{mod}\ p), \Omega_2 = \frac{n_2-1}{2} (\mathrm{mod}\ p)$ and $\Omega = \frac{(n_1+1)(n_2-1)}{2} (\mathrm{mod}\ p)$.

Then from Corollary 3.5, we have the following theorems.

Theorem 3.6: Let the symbols be defined as before and assume that $q \notin W_0$. Then

$$g(x) = \begin{cases} x^n - 1, & \Omega_1 \neq 0, \Omega_2 \neq 0, \Omega \neq 0, \\ \dfrac{x^n - 1}{x^{n_2} - 1}, & \Omega_1 = 0, \Omega_2 \neq 0, \Omega = 0, \\ \dfrac{x^n - 1}{x^{n_1} - 1}, & \Omega_1 \neq 0, \Omega_2 = 0, \Omega = 0, \\ d(x), & \Omega_1 = \Omega_2 = \Omega = 0. \end{cases}$$

In this case, the cyclic code C_s over $GF(q)$ defined by Whiteman's generalized cyclotomic sequence s^n of the order 8 has generator polynomial $g(x)$ as above.

Proof: Note that for $i = 1, 2, \Omega_i = 0$ results in $\Omega = 0$ and that both $\Omega_1 = 0$ and $\Omega_2 = 0$ lead to $\Omega = 0$. By Corollary 3.5, we know that if $q \notin W_0$, then $S(\beta) \notin \{0, -1\}$.

Case 1: $\Omega_1 \neq 0, \Omega_2 \neq 0, \Omega \neq 0$. By Lemma 3.4, we can obtain

$$\gcd(S(x), x^n - 1) = 1,$$

then by equation (2),

$$g(x) = \frac{x^n - 1}{\gcd(S(x), x^n - 1)} = x^n - 1.$$

Case 2: $\Omega_1 = 0, \Omega_2 \neq 0, \Omega = 0$. By Lemma 3.4, we can obtain

$$\gcd(S(x), x^n - 1) = x^{n_2} - 1,$$

then by equation (2),

$$g(x) = \frac{x^n - 1}{\gcd(S(x), x^n - 1)} = \frac{x^n - 1}{x^{n_2} - 1}.$$

Case 3: $\Omega_1 \neq 0, \Omega_2 = 0, \Omega = 0$. By Lemma 3.4, we can obtain

$$\gcd(S(x), x^n - 1) = x^{n_1} - 1,$$

then by equation (2),

$$g(x) = \frac{x^n - 1}{\gcd(S(x), x^n - 1)} = \frac{x^n - 1}{x^{n_1} - 1}.$$

Case 4: $\Omega_1 = \Omega_2 = \Omega = 0$. By Lemma 3.4, we can obtain

$$\gcd(S(x), x^n - 1) = \frac{(x^{n_1} - 1)(x^{n_2} - 1)}{x - 1},$$

then by equation (2),

$$g(x) = \frac{x^n - 1}{\gcd(S(x), x^n - 1)} = \frac{(x^n - 1)(x - 1)}{(x^{n_1} - 1)(x^{n_2} - 1)} = d(x).$$

This completes the proof of the theorem.

Theorem 3.7: Let the symbols be defined as before and assume that $q \in W_0$.

(I) If one of $S(\beta),\ T(\beta),\ U(\beta),\ V(\beta)$ is in $\{0, -1\}$, then

$$g(x)=\begin{cases}\dfrac{x^n-1}{d_m(x)}, & \Omega_1\neq 0,\Omega_2\neq 0,\Omega\neq 0,\\ \dfrac{x^n-1}{(x^{n_2}-1)d_m(x)}, & \Omega_1=0,\Omega_2\neq 0,\Omega=0,\\ \dfrac{x^n-1}{(x^{n_1}-1)d_m(x)}, & \Omega_1\neq 0,\Omega_2=0,\Omega=0,\\ \dfrac{d(x)}{d_m(x)}, & \Omega_1=\Omega_2=\Omega=0,\end{cases}$$

where

$$m=\begin{cases}0, & S(\beta)=0,\\ 4, & S(\beta)=-1,\end{cases} m=\begin{cases}5, & T(\beta)=0,\\ 1, & T(\beta)=-1,\end{cases}$$

$$m=\begin{cases}6, & U(\beta)=0,\\ 2, & U(\beta)=-1,\end{cases} m=\begin{cases}7, & V(\beta)=0,\\ 3, & V(\beta)=-1.\end{cases}$$

(II) If two of $S(\beta)$, $T(\beta)$, $U(\beta)$, $V(\beta)$ are in $\{0,-1\}$, then the specific generator polynomials are listed as follows.

(i) If $S(\beta),\ T(\beta)\in\{0,-1\}$, then

$$g(x)=\begin{cases}\dfrac{x^n-1}{d_s(x)d_t(x)}, & \Omega_1\neq 0,\Omega_2\neq 0,\Omega\neq 0,\\ \dfrac{x^n-1}{(x^{n_2}-1)d_s(x)d_t(x)}, & \Omega_1=0,\Omega_2\neq 0,\Omega=0,\\ \dfrac{x^n-1}{(x^{n_1}-1)d_s(x)d_t(x)}, & \Omega_1\neq 0,\Omega_2=0,\Omega=0,\\ \dfrac{d(x)}{d_s(x)d_t(x)}, & \Omega_1=\Omega_2=\Omega=0,\end{cases}$$

where

$$s=\begin{cases}0, & S(\beta)=0,\\ 4, & S(\beta)=-1,\end{cases} t=\begin{cases}5, & T(\beta)=0,\\ 1, & T(\beta)=-1.\end{cases}$$

(ii) If $S(\beta),\ U(\beta)\in\{0,-1\}$, then

$$g(x)=\begin{cases}\dfrac{x^n-1}{d_s(x)d_u(x)}, & \Omega_1\neq 0,\Omega_2\neq 0,\Omega\neq 0,\\ \dfrac{x^n-1}{(x^{n_2}-1)d_s(x)d_u(x)}, & \Omega_1=0,\Omega_2\neq 0,\Omega=0,\\ \dfrac{x^n-1}{(x^{n_1}-1)d_s(x)d_u(x)}, & \Omega_1\neq 0,\Omega_2=0,\Omega=0,\\ \dfrac{d(x)}{d_s(x)d_u(x)}, & \Omega_1=\Omega_2=\Omega=0,\end{cases}$$

where

$$s=\begin{cases}0, & S(\beta)=0,\\ 4, & S(\beta)=-1,\end{cases}\quad u=\begin{cases}6, & U(\beta)=0,\\ 2, & U(\beta)=-1.\end{cases}$$

(iii) If $S(\beta),\ V(\beta)\in\{0,-1\}$, then

$$g(x)=\begin{cases}\dfrac{x^n-1}{d_s(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2\neq 0,\Omega\neq 0,\\ \dfrac{x^n-1}{(x^{n_2}-1)d_s(x)d_v(x)}, & \Omega_1=0,\Omega_2\neq 0,\Omega=0,\\ \dfrac{x^n-1}{(x^{n_1}-1)d_s(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2=0,\Omega=0,\\ \dfrac{d(x)}{d_s(x)d_v(x)}, & \Omega_1=\Omega_2=\Omega=0,\end{cases}$$

where

$$s=\begin{cases}0, & S(\beta)=0,\\ 4, & S(\beta)=-1,\end{cases}\quad v=\begin{cases}7, & V(\beta)=0,\\ 3, & V(\beta)=-1.\end{cases}$$

(iv) If $T(\beta),\ U(\beta)\in\{0,-1\}$, then

$$g(x)=\begin{cases}\dfrac{x^n-1}{d_t(x)d_u(x)}, & \Omega_1\neq 0,\Omega_2\neq 0,\Omega\neq 0,\\ \dfrac{x^n-1}{(x^{n_2}-1)d_t(x)d_u(x)}, & \Omega_1=0,\Omega_2\neq 0,\Omega=0,\\ \dfrac{x^n-1}{(x^{n_1}-1)d_t(x)d_u(x)}, & \Omega_1\neq 0,\Omega_2=0,\Omega=0,\\ \dfrac{d(x)}{d_t(x)d_u(x)}, & \Omega_1=\Omega_2=\Omega=0,\end{cases}$$

where

$$t=\begin{cases}5, & T(\beta)=0,\\ 1, & T(\beta)=-1,\end{cases}\quad u=\begin{cases}6, & U(\beta)=0,\\ 2, & U(\beta)=-1.\end{cases}$$

(v) If $T(\beta),\ V(\beta) \in \{0,-1\}$, then

$$g(x)=\begin{cases} \dfrac{x^n-1}{d_t(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2\neq 0,\Omega\neq 0,\\ \dfrac{x^n-1}{(x^{n_2}-1)d_t(x)d_v(x)}, & \Omega_1=0,\Omega_2\neq 0,\Omega=0,\\ \dfrac{x^n-1}{(x^{n_1}-1)d_t(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2=0,\Omega=0,\\ \dfrac{d(x)}{d_t(x)d_v(x)}, & \Omega_1=\Omega_2=\ \Omega=0, \end{cases}$$

where

$$t=\begin{cases} 5, & T(\beta)=0,\\ 1, & T(\beta)=-1, \end{cases} \quad v=\begin{cases} 7, & V(\beta)=0,\\ 3, & V(\beta)=-1. \end{cases}$$

(vi) If $U(\beta),\ V(\beta) \in \{0,-1\}$, then

$$g(x)=\begin{cases} \dfrac{x^n-1}{d_u(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2\neq 0,\Omega\neq 0,\\ \dfrac{x^n-1}{(x^{n_2}-1)d_u(x)d_v(x)}, & \Omega_1=0,\Omega_2\neq 0,\Omega=0,\\ \dfrac{x^n-1}{(x^{n_1}-1)d_u(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2=0,\Omega=0,\\ \dfrac{d(x)}{d_u(x)d_v(x)}, & \Omega_1=\Omega_2=\ \Omega=0, \end{cases}$$

where

$$u=\begin{cases} 6, & U(\beta)=0,\\ 2, & U(\beta)=-1, \end{cases} \quad v=\begin{cases} 7, & V(\beta)=0,\\ 3, & V(\beta)=-1. \end{cases}$$

(III) If three of $S(\beta),\ T(\beta),\ U(\beta),\ V(\beta)$ are in $\{0,-1\}$, then the specific generator polynomials are listed as follows

(i) If $S(\beta),\ T(\beta), U(\beta) \in \{0,-1\}$, then

$$g(x)=\begin{cases} \dfrac{x^n-1}{d_s(x)d_t(x)d_u(x)}, & \Omega_1\neq 0,\Omega_2\neq 0,\Omega\neq 0,\\ \dfrac{x^n-1}{(x^{n_2}-1)d_s(x)d_t(x)d_u(x)}, & \Omega_1=0,\Omega_2\neq 0,\Omega=0,\\ \dfrac{x^n-1}{(x^{n_1}-1)d_s(x)d_t(x)d_u(x)}, & \Omega_1\neq 0,\Omega_2=0,\Omega=0,\\ \dfrac{d(x)}{d_s(x)d_t(x)d_u(x)}, & \Omega_1=\Omega_2=\ \Omega=0, \end{cases}$$

where

$$s=\begin{cases} 0, & S(\beta)=0,\\ 4, & S(\beta)=-1,\end{cases} t=\begin{cases} 5, & T(\beta)=0,\\ 1, & T(\beta)=-1,\end{cases} u=\begin{cases} 6, & U(\beta)=0,\\ 2, & U(\beta)=-1.\end{cases}$$

(ii) If $S(\beta),\ T(\beta), V(\beta)\in\{0,-1\}$, then

$$g(x)=\begin{cases} \dfrac{x^n-1}{d_s(x)d_t(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2\neq 0,\Omega\neq 0,\\ \dfrac{x^n-1}{(x^{n_2}-1)d_s(x)d_t(x)d_v(x)}, & \Omega_1=0,\Omega_2\neq 0,\Omega=0,\\ \dfrac{x^n-1}{(x^{n_1}-1)d_s(x)d_t(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2=0,\Omega=0,\\ \dfrac{d(x)}{d_s(x)d_t(x)d_v(x)}, & \Omega_1=\Omega_2=\ \Omega=0,\end{cases}$$

where

$$s=\begin{cases} 0, & S(\beta)=0,\\ 4, & S(\beta)=-1,\end{cases} t=\begin{cases} 5, & T(\beta)=0,\\ 1, & T(\beta)=-1,\end{cases} v=\begin{cases} 7, & V(\beta)=0,\\ 3, & V(\beta)=-1.\end{cases}$$

(iii) If $S(\beta), U(\beta), V(\beta)\in\{0,-1\}$, then

$$g(x)=\begin{cases} \dfrac{x^n-1}{d_s(x)d_u(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2\neq 0,\Omega\neq 0,\\ \dfrac{x^n-1}{(x^{n_2}-1)d_s(x)d_u(x)d_v(x)}, & \Omega_1=0,\Omega_2\neq 0,\Omega=0,\\ \dfrac{x^n-1}{(x^{n_1}-1)d_s(x)d_u(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2=0,\Omega=0,\\ \dfrac{d(x)}{d_s(x)d_u(x)d_v(x)}, & \Omega_1=\Omega_2=\ \Omega=0,\end{cases}$$

where

$$s=\begin{cases} 0, & S(\beta)=0,\\ 4, & S(\beta)=-1,\end{cases} u=\begin{cases} 6, & U(\beta)=0,\\ 2, & U(\beta)=-1,\end{cases} v=\begin{cases} 7, & V(\beta)=0,\\ 3, & V(\beta)=-1.\end{cases}$$

(iv) If $T(\beta), U(\beta), V(\beta)\in\{0,-1\}$, then

$$g(x)=\begin{cases}\dfrac{x^n-1}{d_t(x)d_u(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2\neq 0,\Omega\neq 0,\\ \dfrac{x^n-1}{(x^{n_2}-1)d_t(x)d_u(x)d_v(x)}, & \Omega_1=0,\Omega_2\neq 0,\Omega=0,\\ \dfrac{x^n-1}{(x^{n_1}-1)d_t(x)d_u(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2=0,\Omega=0,\\ \dfrac{d(x)}{d_t(x)d_u(x)d_v(x)}, & \Omega_1=\Omega_2=\Omega=0,\end{cases}$$

where

$$t=\begin{cases}5, & T(\beta)=0,\\ 1, & T(\beta)=-1,\end{cases}\ u=\begin{cases}6, & U(\beta)=0,\\ 2, & U(\beta)=-1,\end{cases}\ v=\begin{cases}7, & V(\beta)=0,\\ 3, & V(\beta)=-1.\end{cases}$$

(IV) If $S(\beta),T(\beta),U(\beta),V(\beta)\in\{0,-1\}$, then

$$g(x)=\begin{cases}\dfrac{x^n-1}{d_s(x)d_t(x)d_u(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2\neq 0,\Omega\neq 0,\\ \dfrac{x^n-1}{(x^{n_2}-1)d_s(x)d_t(x)d_u(x)d_v(x)}, & \Omega_1=0,\Omega_2\neq 0,\Omega=0,\\ \dfrac{x^n-1}{(x^{n_1}-1)d_s(x)d_t(x)d_u(x)d_v(x)}, & \Omega_1\neq 0,\Omega_2=0,\Omega=0,\\ \dfrac{d(x)}{d_s(x)d_t(x)d_u(x)d_v(x)}, & \Omega_1=\Omega_2=\Omega=0,\end{cases}$$

where

$$s=\begin{cases}0, & S(\beta)=0,\\ 4, & S(\beta)=-1,\end{cases}\ t=\begin{cases}5, & T(\beta)=0,\\ 1, & T(\beta)=-1,\end{cases}$$

$$u=\begin{cases}6, & U(\beta)=0,\\ 2, & U(\beta)=-1,\end{cases}\ v=\begin{cases}7, & V(\beta)=0,\\ 3, & V(\beta)=-1.\end{cases}$$

In the cases above, the cyclic code C_s over $GF(q)$ defined by Whiteman's generalized cyclotomic sequence s^n of the order 8 has generator polynomial $g(x)$ as above correspondingly.

Proof: Note that for $i=1,2,\Omega_i=0$ results in $\Omega=0$ and that both $\Omega_1=0$ and $\Omega_2=0$ lead to $\Omega=0$. By Corollary 3.5, we know that if $q\in W_0$, then it is possible that$S(\beta)\in\{0,-1\},T(\beta)\in\{0,-1\},U(\beta)\in\{0,-1\}$ and $V(\beta)\in\{0,-1\}$.

In the following we only give the proof of the case that $S(\beta)\in\{0,-1\}$ and the other cases can be proved similarly.

Case 1: $\Omega_1\neq 0,\Omega_2\neq 0,\Omega\neq 0,S(\beta)=0$. By Lemma 3.4, we can obtain

$$\gcd(S(x),x^n-1)=d_0(x),$$

then by equations (2) and (8), the corresponding generator polynomial is

$$g(x) = \frac{x^n - 1}{\gcd(S(x), x^n - 1)} = \frac{x^n - 1}{d_0(x)},$$

which means that $m = 0$.

Case 2: $\Omega_1 \neq 0, \Omega_2 \neq 0, \Omega \neq 0, S(\beta) = -1$. By Lemma 3.4, we can obtain

$$\gcd(S(x), x^n - 1) = d_4(x),$$

then by equations (2) and (8), the corresponding generator polynomial is

$$g(x) = \frac{x^n - 1}{\gcd(S(x), x^n - 1)} = \frac{x^n - 1}{d_4(x)},$$

which means that $m = 4$.

Case 3: $\Omega_1 = 0, \Omega_2 \neq 0, \Omega = 0, S(\beta) = 0$. By Lemma 3.4, we can obtain

$$\gcd(S(x), x^n - 1) = (x^{n_2} - 1)d_0(x),$$

then by equations (2) and (8), the corresponding generator polynomial is

$$g(x) = \frac{x^n - 1}{\gcd(S(x), x^n - 1)} = \frac{x^n - 1}{(x^{n_2} - 1)d_0(x)},$$

which means that $m = 0$.

Case 4: $\Omega_1 = 0, \Omega_2 \neq 0, \Omega = 0, S(\beta) = -1$. By Lemma 3.4, we can obtain

$$\gcd(S(x), x^n - 1) = (x^{n_2} - 1)d_4(x),$$

then by equations (2) and (8), the corresponding generator polynomial is

$$g(x) = \frac{x^n - 1}{\gcd(S(x), x^n - 1)} = \frac{x^n - 1}{(x^{n_2} - 1)d_4(x)},$$

which means that $m = 4$.

Case 5: $\Omega_1 \neq 0, \Omega_2 = 0, \Omega = 0, S(\beta) = 0$. By Lemma 3.4, we can obtain

$$\gcd(S(x), x^n - 1) = (x^{n_1} - 1)d_0(x),$$

then by equations (2) and (8), the corresponding generator polynomial is

$$g(x) = \frac{x^n - 1}{\gcd(S(x), x^n - 1)} = \frac{x^n - 1}{(x^{n_1} - 1)d_0(x)},$$

which means that $m = 0$.

Case 6: $\Omega_1 \neq 0, \Omega_2 = 0, \Omega = 0, S(\beta) = -1$. By Lemma 3.4, we can obtain

$$\gcd(S(x), x^n - 1) = (x^{n_1} - 1)d_4(x),$$

then by equations (2) and (8), the corresponding generator polynomial is

$$g(x) = \frac{x^n - 1}{\gcd(S(x), x^n - 1)} = \frac{x^n - 1}{(x^{n_1} - 1)d_4(x)},$$

which means that $m = 4$.

Case 7: $\Omega_1 = \Omega_2 = \ \Omega = 0, S(\beta) = 0$. By Lemma 3.4, we can obtain

$$\gcd(S(x), x^n - 1) = \frac{(x^{n_1} - 1)(x^{n_2} - 1)}{x - 1} d_0(x),$$

then by equations (2) and (8), the corresponding generator polynomial is

$$g(x) = \frac{x^n - 1}{\gcd(S(x), x^n - 1)} = \frac{(x^n - 1)(x - 1)}{(x^{n_1} - 1)(x^{n_2} - 1)d_0(x)} = \frac{d(x)}{d_0(x)},$$

which means that $m = 0$.

Case 8: $\Omega_1 = \Omega_2 = \ \Omega = 0, S(\beta) = -1$. By Lemma 3.4, we can obtain

$$\gcd(S(x), x^n - 1) = \frac{(x^{n_1} - 1)(x^{n_2} - 1)}{x - 1} d_4(x),$$

then by equations (2) and (8), the corresponding generator polynomial is

$$g(x) = \frac{x^n - 1}{\gcd(S(x), x^n - 1)} = \frac{(x^n - 1)(x - 1)}{(x^{n_1} - 1)(x^{n_2} - 1)d_4(x)} = \frac{d(x)}{d_4(x)},$$

which means that $m = 4$.

The rest results of this theorem can be proved similarly.

4. The Minimum Distance of the Cyclic Codes

In this section, we determine the minimum distance of some cyclic codes and give lower bounds of the minimum distance of some other cyclic codes constructed in section 3. By the same argument as that in [5], we get the following two results immediately.

Theorem 4.1: Let C_i denote the cyclic code over $GF(q)$ with the generator polynomial $g_i(x) = \frac{x^n - 1}{x^{n_i} - 1}$. The cyclic code C_i has paramenters $[n, n_i, d_i]$, where $d_i = n_{i-(-1)^i}$ and $i = 1,2$.

Example 4.2: Let $q = 2, n_1 = 17$ and $n_2 = 73$.Then the cyclic code C_1 over $GF(q)$ with thegenerator polynomial $g_1(x) = \frac{x^n - 1}{x^{n_1} - 1}$ has parameters [1241,17,73] and the cyclic code C_2 over $GF(q)$ with the generator polynomial $g_2(x) = \frac{x^n - 1}{x^{n_2} - 1}$ has parameters [1241,73,17].

Theorem 4.3: Let C_{n_1,n_2} denote the cyclic code over $GF(q)$ with the generator polynomial $g(x) = \frac{(x^n - 1)(x - 1)}{(x^{n_1} - 1)(x^{n_2} - 1)}$. The cyclic code C_{n_1,n_2} has paramenters $[n, n_1 + n_2 - 1, d_{n_1,n_2}]$, where $d_{n_1,n_2} = \min(n_1, n_2)$.

Example 4.4: Let $q = 2, n_1 = 17$ and $n_2 = 73$. Then the cyclic code C_1 over $GF(q)$ with thegenerator polynomial $g(x) = \frac{(x^n-1)(x-1)}{(x^{n_1}-1)(x^{n_2}-1)}$ has parameters [1241,89,17].

We also derive the following lower bounds of the minimum distances of other cyclic codes.

Theorem 4.5: Suppose that $q \in W_0$. Let C_i and $d_i$be defined as in Theorem 4.1. Let $C_{i,j}$denotethe cyclic code over $GF(q)$ with the generator polynomial $g_{i,j}(x) = \frac{x^n-1}{(x^{n_i}-1)d_j(x)}$. Then the cyclic code $C_{i,j}$ has parameters $\left[n, n_i + \frac{(n_1-1)(n_2-1)}{8}, d_{i,j}\right]$, where $d_{i,j} \geq \left\lceil\sqrt{n_{i-(-1)^i}}\right\rceil, i = 1,2$ and $0 \leq j \leq 7$.

Proof: Note that for $0 \leq j \leq 7$ and for any $r \in W_j$, we have $r^{-1}(\mathrm{mod} n) \in W_{(8-j)\mathrm{mod}\ 8}$. Let $i = 1$ and $j = 0$ and $c(x) \in GF(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{1,0}$. Take $r \in W_1$, we have $r^{-1}(\mathrm{mod} n) \in W_7$ and $c(x^r)$ is a codeword of Hamming weight ω in $C_{1,7}$ which implies that $d_{1,0} = d_{1,7}$. By taking $r \in W_j$, we can get $d_{1,0} = d_{1,8-j}$, where $2 \leq j \leq 7$. Further, for any $j \in \{1,2,3,4,5,6,7\}, r \in W_j$, we have that $c(x)c(x^r)$ is a codeword of C_1. Hence from Theorem 4.1,$d_{1,j}^2 \geq d_1 = n_2$, i.e., $d_{1,j} \geq \lceil\sqrt{n_2}\rceil$. By similar argument, we get $d_{2,j} \geq \lceil\sqrt{n_1}\rceil$, where $0 \leq j \leq 7$.

Example 4.6: Let $q = 2, n_1 = 17$ and $n_2 = 73$. Then the cyclic code C_1 over $GF(q)$ with thegenerator polynomial $g(x) = \frac{x^n-1}{(x^{n_1}-1)d_0(x)}$ has parameters [1241,161,73]. In this case $d \geq \lceil\sqrt{n_2}\rceil = 9$, the lower bound of d is 9 while the actual minimum distance is 73.

Theorem 4.7: Suppose that $q \in W_0$. Let C_{n_1,n_2} and d_{n_1,n_2}be defined as in Theorem 4.3. Let$C_{n_1,n_2,j}$ denotethe cyclic code over $GF(q)$ with the generator polynomial

$$g_{n_1,n_2,j}(x) = \frac{(x^n - 1)(x - 1)}{(x^{n_1} - 1)(x^{n_2} - 1)d_j(x)}.$$

Then the cyclic code $C_{n_1,n_2,j}$ has parameters $\left[n, n_1 + n_2 - 1 + \frac{(n_1-1)(n_2-1)}{8}, d_{n_1,n_2,j}\right]$, where $d_{n_1,n_2,j} \geq \left\lceil\sqrt{\min(n_1, n_2)}\right\rceil$ and $0 \leq j \leq 7$.

Proof: Let $j = 0$ and $c(x) \in GF(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{n_1,n_2,0}$. Take $r \in W_1$, we have $r^{-1}(\mathrm{mod} n) \in W_7$ and $c(x^r)$ is a codeword of Hamming weight ω in $C_{n_1,n_2,7}$ which implies that $d_{n_1,n_2,0} = d_{n_1,n_2,7}$. Take $r \in W_2$, we have $r^{-1}(\mathrm{mod} n) \in W_6$ and $c(x^r)$ is a codeword of Hamming weight ω in $C_{n_1,n_2,6}$ which implies that $d_{n_1,n_2,0} = d_{n_1,n_2,6}$.

By taking $r \in W_3, r \in 4, r \in W_5, r \in W_6$ and $r \in W_7$, we can get $d_{n_1,n_2,0} = d_{n_1,n_2,5}, d_{n_1,n_2,0} = d_{n_1,n_2,4}, d_{n_1,n_2,0} = d_{n_1,n_2,3}, d_{n_1,n_2,0} = d_{n_1,n_2,2}$ and $d_{n_1,n_2,0} = d_{n_1,n_2,1}$ respectively. Further, for any $j \in \{1,2,3,4,5,6,7\}, r \in W_j$, we have that $c(x)c(x^r)$ is a codeword of C_{n_1,n_2}. Hence from Theorem 4.3,$d_{n_1,n_2,j}^2 \geq \left\lceil\sqrt{\min(n_1, n_2)}\right\rceil$, where $0 \leq j \leq 7$.

Example 4.8: Let $q = 2, n_1 = 17$ and $n_2 = 89$. Then the cyclic code C_1 over $GF(q)$ with thegenerator polynomial $g(x) = \frac{(x^n-1)(x-1)}{(x^{n_1}-1)(x^{n_2}-1)d_1(x)}$ has parameters [1513,281,17]. In this case $d \geq \left\lceil \sqrt{\min(n_1, n_2)} \right\rceil = 4$, the lower bound of d is 4 while the actual minimum distance is 17.

Theorem 4.9: Suppose that $q \in W_0$. Let C_i and d_i be defined as in Theorem 4.1. Let $C_{i,j,h}$ denotethe cyclic code over $GF(q)$ with the generator polynomial

$$g_{i,j,h}(x) = \frac{x^n - 1}{(x^{n_i} - 1)d_j(x)d_h(x)},$$

where $i = 1,2$ and

$$(j,h) \in \{(0,1),(0,2),(0,3),(1,2),(1,3),(1,4),(2,3),(2,4),(2,5),(3,4),(3,5),(3,6)$$
$$(4,5),(4,6),(4,7),(5,6),(5,7),(5,0),(6,7),(6,0),(6,1)(7,0),(7,1),(7,2)\}.$$

Then the cyclic code $C_{i,j,h}$ has parameters $\left[n, n_i + \frac{(n_1-1)(n_2-1)}{4}, d_{i,j,h}\right]$, where $d_{i,j,h} \geq \left\lceil \sqrt{n_{i-(-1)^i}} \right\rceil$.

Proof: Let $j = 0, h = 1$ and $c(x) \in GF(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{i,0,1}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{i,(0-k) \bmod 8,(1-k) \bmod 8}$. It then follows that

$$d_{i,0,1} = d_{i,(0-k) \bmod 8,(1-k) \bmod 8}.$$

Therefore, we have

$$d_{i,0,1} = d_{i,7,0} = d_{i,6,7} = d_{i,5,6} = d_{i,4,5} = d_{i,3,4} = d_{i,2,3} = d_{i,1,2}. \quad (9)$$

Let $j = 0, h = 2$ and $c(x) \in GF(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{i,0,2}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{i,(0-k) \bmod 8,(2-k) \bmod 8}$. It then follows that

$$d_{i,0,2} = d_{i,(0-k) \bmod 8,(2-k) \bmod 8}.$$

Therefore, we have

$$d_{i,0,2} = d_{i,7,1} = d_{i,6,0} = d_{i,5,7} = d_{i,4,6} = d_{i,3,5} = d_{i,2,4} = d_{i,1,3}. \quad (10)$$

Let $j = 0, h = 3$ and $c(x) \in GF(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{i,0,3}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{i,(0-k) \bmod 8,(3-k) \bmod 8}$. It then follows that

$$d_{i,0,3} = d_{i,(0-k) \bmod 8,(3-k) \bmod 8}.$$

Therefore, we have

$$d_{i,0,3} = d_{i,7,2} = d_{i,6,1} = d_{i,5,0} = d_{i,4,7} = d_{i,3,6} = d_{i,2,5} = d_{i,1,4}. \quad (11)$$

From (9), (10) and (11), for any $r \in W_4$, we have that $c(x)c(x^r)$ is a codeword of C_i, where C_i denote the cyclic code over $GF(q)$ with the generator polynomial $g_i(x) = \frac{x^n-1}{x^{n_i}-1}$ and the minimum distance $d_i = n_{i-(-1)^i}$.Hence from theorem 4.1,$d^2_{i,j,h} \geq d_i = n_{i-(-1)^i}$, i.e., $d_{i,j,h} \geq \left\lceil \sqrt{n_{i-(-1)^i}} \right\rceil$, where

$(j,h) \in \{(0,1),(0,2),(0,3),(1,2),(1,3),(1,4),(2,3),(2,4),(2,5),(3,4),(3,5),(3,6)$
$(4,5),(4,6),(4,7),(5,6),(5,7),(5,0),(6,7),(6,0),(6,1)(7,0),(7,1),(7,2)\}.$

Theorem 4.10: Suppose that $q \in W_0$. Let C_{n_1,n_2} and d_{n_1,n_2}be defined as in Theorem 4.3. Let $C_{n_1,n_2,j,h}$ denotethe cyclic code over $GF(q)$ with the generator polynomial

$$g_{n_1,n_2,j,h}(x) = \frac{(x^n-1)(x-1)}{(x^{n_1}-1)(x^{n_2}-1)d_j(x)d_h(x)}.$$

Then the cyclic code $C_{n_1,n_2,j,h}$ has parameters $\left[n, n_1+n_2-1+\frac{(n_1-1)(n_2-1)}{4},\ d_{n_1,n_2,j,h}\right]$, where $d_{n_1,n_2,j,h} \geq \left\lceil \sqrt{\min(n_1,n_2)} \right\rceil$ and

$(j,h) \in \{(0,1),(0,2),(0,3),(1,2),(1,3),(1,4),(2,3),(2,4),(2,5),(3,4),(3,5),(3,6)$
$(4,5),(4,6),(4,7),(5,6),(5,7),(5,0),(6,7),(6,0),(6,1)(7,0),(7,1),(7,2)\}.$

Proof: Let $j = 0, h = 1$ and $c(x) \in GF(q)[x]/(x^n-1)$ be a codeword of Hamming weight ω in $C_{n_1,n_2,0,1}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{n_1,n_2,(0-k)\bmod 8,(1-k)\bmod 8}$. It then follows that

$$d_{n_1,n_2,0,1} = d_{n_1,n_2,(0-k)\bmod 8,(1-k)\bmod 8}.$$

Therefore, we have

$$d_{n_1,n_2,0,1} = d_{n_1,n_2,7,0} = d_{n_1,n_2,6,7} = d_{n_1,n_2,5,6}$$
$$= d_{n_1,n_2,4,5} = d_{n_1,n_2,3,4} = d_{n_1,n_2,2,3} = d_{n_1,n_2,1,2}. \quad (12)$$

Let $j = 0, h = 2$ and $c(x) \in GF(q)[x]/(x^n-1)$ be a codeword of Hamming weight ω in $C_{n_1,n_2,0,2}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{n_1,n_2,(0-k)\bmod 8,(2-k)\bmod 8}$. It then follows that

$$d_{n_1,n_2,0,2} = d_{n_1,n_2,(0-k)\bmod 8,(2-k)\bmod 8}.$$

Therefore, we have

$$d_{n_1,n_2,0,2} = d_{n_1,n_2,7,1} = d_{n_1,n_2,6,0} = d_{n_1,n_2,5,7}$$
$$= d_{n_1,n_2,4,6} = d_{n_1,n_2,3,5} = d_{n_1,n_2,2,4} = d_{n_1,n_2,1,3}. \quad (13)$$

Let $j = 0, h = 3$ and $c(x) \in GF(q)[x]/(x^n-1)$ be a codeword of Hamming weight ω in $C_{n_1,n_2,0,3}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{n_1,n_2,(0-k)\bmod 8,(3-k)\bmod 8}$. It then follows that

$$d_{n_1,n_2,0,3} = d_{n_1,n_2,(0-k)\bmod 8,(3-k)\bmod 8}.$$

Therefore, we have

$$d_{n_1,n_2,0,3} = d_{n_1,n_2,7,2} = d_{n_1,n_2,6,1} = d_{n_1,n_2,5,0}$$
$$= d_{n_1,n_2,4,7} = d_{n_1,n_2,3,6} = d_{n_1,n_2,2,5} = d_{n_1,n_2,1,4}. \quad (14)$$

From (12), (13) and (14), for any $r \in W_4$, we have that $c(x)c(x^r)$ is a codeword of C_{n_1,n_2}, where C_{n_1,n_2} and d_{n_1,n_2} be defined as Theorem 4.3.Hence from theorem 4.3,$d^2_{n_1,n_2,j,h} \geq d_{n_1,n_2} = \min(n_1,n_2)$, i.e., $d_{n_1,n_2,j,h} \geq \left\lceil\sqrt{\min(n_1,n_2)}\right\rceil$, where

$$(j,h) \in \{(0,1),(0,2),(0,3),(1,2),(1,3),(1,4),(2,3),(2,4),(2,5),(3,4),(3,5),(3,6)$$
$$(4,5),(4,6),(4,7),(5,6),(5,7),(5,0),(6,7),(6,0),(6,1)(7,0),(7,1),(7,2)\}.$$

Theorem 4.11: Suppose that $q \in W_0$. Let C_i and d_i be defined as in Theorem 4.1. Let $C_{i,j,h,l}$ denote the cyclic code over $GF(q)$ with the generator polynomial

$$g_{i,j,h,l}(x) = \frac{x^n - 1}{(x^{n_i} - 1)d_j(x)d_h(x)d_l(x)},$$

where $i = 1,2$ and

$$(j,h,l) \in \{(0,1,2),(0,1,3),(0,2,3),(0,2,5),(1,2,3),(1,2,4),(1,3,4),(1,3,6),$$
$$(2,3,4),(2,3,5),(2,4,5),(2,4,7),(3,4,5),(3,4,6),(3,5,6),(3,5,0),$$
$$(4,5,6),(4,5,7),(4,6,7),(4,6,1),(5,6,7),(5,6,0),(5,7,0),(5,7,2),$$
$$(6,7,0),(6,7,1),(6,0,1),(6,0,3),(7,0,1),(7,0,2),(7,1,2),(7,1,4)\}.$$

Then the cyclic code $C_{i,j,h,l}$ has parameters $\left[n, n_i + \frac{3(n_1-1)(n_2-1)}{8}, d_{i,j,h,l}\right]$, where $d_{i,j,h,l} \geq \left\lceil\sqrt{n_{i-(-1)^i}}\right\rceil$.

Proof: Let $j = 0, h = 1, l = 2$ and $c(x) \in GF(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{i,0,1,2}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{i,(0-k)\bmod 8,(1-k)\bmod 8,(2-k)\bmod 8}$. It then follows that

$$d_{i,0,1,2} = d_{i,(0-k)\bmod 8,(1-k)\bmod 8,(2-k)\bmod 8}.$$

Therefore, we have

$$d_{i,0,1,2} = d_{i,7,0,1} = d_{i,6,7,0} = d_{i,5,6,7} = d_{i,4,5,6} = d_{i,3,4,5} = d_{i,2,3,4} = d_{i,1,2,3}. \quad (15)$$

Let $j = 0, h = 1, l = 3$ and $c(x) \in GF(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{i,0,1,3}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{i,(0-k)\bmod 8,(1-k)\bmod 8,(3-k)\bmod 8}$. It then follows that

$$d_{i,0,1,3} = d_{i,(0-k)\bmod 8,(1-k)\bmod 8,(3-k)\bmod 8}.$$

Therefore, we have

$$d_{i,0,1,3} = d_{i,7,0,2} = d_{i,6,7,1} = d_{i,5,6,0} = d_{i,4,5,7} = d_{i,3,4,6} = d_{i,2,3,5} = d_{i,1,2,4}. \quad (16)$$

Let $j = 0, h = 2, l = 3$ and $c(x) \in GF(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{i,0,2,3}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{i,(0-k)\bmod 8,(2-k)\bmod 8,(3-k)\bmod 8}$. It then follows that

$$d_{i,0,2,3} = d_{i,(0-k)\bmod 8,(2-k)\bmod 8,(3-k)\bmod 8}.$$

Therefore, we have

$$d_{i,0,2,3} = d_{i,7,1,2} = d_{i,6,0,1} = d_{i,5,7,0} = d_{i,4,6,7} = d_{i,3,5,6} = d_{i,2,4,5} = d_{i,1,3,4}. \quad (17)$$

Let $j = 0, h = 2, l = 5$ and $c(x) \in GF(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{i,0,2,5}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{i,(0-k)\bmod 8,(2-k)\bmod 8,(5-k)\bmod 8}$. It then follows that

$$d_{i,0,2,5} = d_{i,(0-k)\bmod 8,(2-k)\bmod 8,(5-k)\bmod 8}.$$

Therefore, we have

$$d_{i,0,2,5} = d_{i,7,1,4} = d_{i,6,0,3} = d_{i,5,7,2} = d_{i,4,6,1} = d_{i,3,5,0} = d_{i,2,4,7} = d_{i,1,3,6}. \quad (18)$$

From (15), (16), (17) and (18), for any $r \in W_4$, we have that $c(x)c(x^r)$ is a codeword of C_i, where C_i denote the cyclic code over $GF(q)$ with the generator polynomial $g_i(x) = \frac{x^n-1}{x^{n_i}-1}$ and the minimum distance $d_i = n_{i-(-1)^i}$.Hence from theorem 4.1,$d^2_{i,j,h,l} \geq d_i = n_{i-(-1)^i}$, i.e., $d_{i,j,h,l} \geq \left\lceil \sqrt{n_{i-(-1)^i}} \right\rceil$, where

$$(j,h,l) \in \{(0,1,2),(0,1,3),(0,2,3),(0,2,5),(1,2,3),(1,2,4),(1,3,4),(1,3,6),$$
$$(2,3,4),(2,3,5),(2,4,5),(2,4,7),(3,4,5),(3,4,6),(3,5,6),(3,5,0),$$
$$(4,5,6),(4,5,7),(4,6,7),(4,6,1),(5,6,7),(5,6,0),(5,7,0),(5,7,2),$$
$$(6,7,0),(6,7,1),(6,0,1),(6,0,3),(7,0,1),(7,0,2),(7,1,2),(7,1,4)\}.$$

Theorem 4.12: Suppose that $q \in W_0$. Let C_{n_1,n_2} and d_{n_1,n_2}be defined as in Theorem 4.3. Let $C_{n_1,n_2,j,h,l}$ denotethe cyclic code over $GF(q)$ with the generator polynomial

$$g_{n_1,n_2,j,h,l}(x) = \frac{(x^n - 1)(x - 1)}{(x^{n_1} - 1)(x^{n_2} - 1)d_j(x)d_h(x)d_l(x)}.$$

Then the cyclic code $C_{n_1,n_2,j,h,l}$ has parameters $\left[n, n_1 + n_2 - 1 + \frac{3(n_1-1)(n_2-1)}{8}, d_{n_1,n_2,j,h,l}\right]$, where $d_{n_1,n_2,j,h,l} \geq \left\lceil \sqrt{\min(n_1,n_2)} \right\rceil$ and

$$(j,h,l) \in \{(0,1,2),(0,1,3),(0,2,3),(0,2,5),(1,2,3),(1,2,4),(1,3,4),(1,3,6),$$
$$(2,3,4),(2,3,5),(2,4,5),(2,4,7),(3,4,5),(3,4,6),(3,5,6),(3,5,0),$$

$$(4,5,6),(4,5,7),(4,6,7),(4,6,1),(5,6,7),(5,6,0),(5,7,0),(5,7,2),$$
$$(6,7,0),(6,7,1),(6,0,1),(6,0,3),(7,0,1),(7,0,2),(7,1,2),(7,1,4)\}.$$

Proof: Let $j=0,h=1,l=2$ and $c(x)\in GF(q)[x]/(x^n-1)$ be a codeword of Hamming weight ω in $C_{n_1,n_2,0,1,2}$. Take any $r\in W_k$, for $1\le k\le 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{n_1,n_2,(0-k)\bmod 8,(1-k)\bmod 8,(2-k)\bmod 8}$. It then follows that

$$d_{n_1,n_2,0,1,2}=d_{n_1,n_2,(0-k)\bmod 8,(1-k)\bmod 8,(2-k)\bmod 8}.$$

Therefore, we have

$$d_{n_1,n_2,0,1,2}=d_{n_1,n_2,7,0,1}=d_{n_1,n_2,6,7,0}=d_{n_1,n_2,5,6,7}$$
$$=d_{n_1,n_2,4,5,6}=d_{n_1,n_2,3,4,5}=d_{n_1,n_2,2,3,4}=d_{n_1,n_2,1,2,3}. \quad (19)$$

Let $j=0,h=1,l=3$ and $c(x)\in GF(q)[x]/(x^n-1)$ be a codeword of Hamming weight ω in $C_{n_1,n_2,0,1,3}$. Take any $r\in W_k$, for $1\le k\le 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{n_1,n_2,(0-k)\bmod 8,(1-k)\bmod 8,(3-k)\bmod 8}$. It then follows that

$$d_{n_1,n_2,0,1,3}=d_{n_1,n_2,(0-k)\bmod 8,(1-k)\bmod 8,(3-k)\bmod 8}.$$

Therefore, we have

$$d_{n_1,n_2,0,1,3}=d_{n_1,n_2,7,0,2}=d_{n_1,n_2,6,7,1}=d_{n_1,n_2,5,6,0}$$
$$=d_{n_1,n_2,4,5,7}=d_{n_1,n_2,3,4,6}=d_{n_1,n_2,2,3,5}=d_{n_1,n_2,1,2,4}. \quad (20)$$

Let $j=0,h=2,l=3$ and $c(x)\in GF(q)[x]/(x^n-1)$ be a codeword of Hamming weight ω in $C_{n_1,n_2,0,2,3}$. Take any $r\in W_k$, for $1\le k\le 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{n_1,n_2,(0-k)\bmod 8,(2-k)\bmod 8,(3-k)\bmod 8}$. It then follows that

$$d_{n_1,n_2,0,2,3}=d_{n_1,n_2,(0-k)\bmod 8,(2-k)\bmod 8,(3-k)\bmod 8}.$$

Therefore, we have

$$d_{n_1,n_2,0,2,3}=d_{n_1,n_2,7,1,2}=d_{n_1,n_2,6,0,1}=d_{n_1,n_2,5,7,0}$$
$$=d_{n_1,n_2,4,6,7}=d_{n_1,n_2,3,5,6}=d_{n_1,n_2,2,4,5}=d_{n_1,n_2,1,3,4}. \quad (21)$$

Let $j=0,h=2,l=5$ and $c(x)\in GF(q)[x]/(x^n-1)$ be a codeword of Hamming weight ω in $C_{n_1,n_2,0,2,5}$. Take any $r\in W_k$, for $1\le k\le 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{n_1,n_2,(0-k)\bmod 8,(2-k)\bmod 8,(5-k)\bmod 8}$. It then follows that

$$d_{n_1,n_2,0,2,5}=d_{n_1,n_2,(0-k)\bmod 8,(2-k)\bmod 8,(5-k)\bmod 8}.$$

Therefore, we have

$$d_{n_1,n_2,0,2,5}=d_{n_1,n_2,7,1,4}=d_{n_1,n_2,6,0,3}=d_{n_1,n_2,5,7,2}$$
$$=d_{n_1,n_2,4,6,1}=d_{n_1,n_2,3,5,0}=d_{n_1,n_2,2,4,7}=d_{n_1,n_2,1,3,6}. \quad (22)$$

From (19), (20), (21) and (22), for any $r \in W_4$, we have that $c(x)c(x^r)$ is a codeword of C_{n_1,n_2}, where C_{n_1,n_2} and d_{n_1,n_2} be defined as Theorem 4.3. Hence from theorem 4.3,$d^2_{n_1,n_2,j,h,l} \geq d_{n_1,n_2} = \min(n_1, n_2)$, i.e., $d_{n_1,n_2,j,h,l} \geq \left\lceil \sqrt{\min(n_1, n_2)} \right\rceil$, where

$$(j,h,l) \in \{(0,1,2),(0,1,3),(0,2,3),(0,2,5),(1,2,3),(1,2,4),(1,3,4),(1,3,6),$$
$$(2,3,4),(2,3,5),(2,4,5),(2,4,7),(3,4,5),(3,4,6),(3,5,6),(3,5,0),$$
$$(4,5,6),(4,5,7),(4,6,7),(4,6,1),(5,6,7),(5,6,0),(5,7,0),(5,7,2),$$
$$(6,7,0),(6,7,1),(6,0,1),(6,0,3),(7,0,1),(7,0,2),(7,1,2),(7,1,4)\}.$$

Theorem 4.13: Suppose that $q \in W_0$. Let C_i and d_i be defined as in Theorem 4.1. Let $C_{i,j,h,l,t}$ denote the cyclic code over $GF(q)$ with the generator polynomial

$$g_{i,j,h,l,t}(x) = \frac{x^n - 1}{(x^{n_i} - 1)d_j(x)d_h(x)d_l(x)d_t(x)},$$

where $i = 1,2$ and

$$(j,h,l,t) \in \{(0,1,2,3),(0,2,3,5),(1,2,3,4),(1,3,4,6),(2,3,4,5),(2,4,5,7),(3,4,5,6),(3,5,6,0),$$
$$(4,5,6,7),(4,6,7,1),(5,6,7,0),(5,7,0,2),(6,7,0,1),(6,0,1,3),(7,0,1,2),(7,1,2,4)\}.$$

Then the cyclic code $C_{i,j,h,l,t}$ has parameters $\left[n, n_i + \frac{(n_1-1)(n_2-1)}{2}, d_{i,j,h,l,t}\right]$, where $d_{i,j,h,l,t} \geq \left\lceil \sqrt{n_{i-(-1)^i}} \right\rceil$.

Proof: Let $j = 0, h = 1, l = 2, t = 3$ and $c(x) \in GF(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{i,0,1,2,3}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{i,(0-k)\bmod 8,(1-k)\bmod 8,(2-k)\bmod 8,(3-k)\bmod 8}$. It then follows that

$$d_{i,0,1,2,3} = d_{i,(0-k)\bmod 8,(1-k)\bmod 8,(2-k)\bmod 8,(3-k)\bmod 8}.$$

Therefore, we have

$$d_{i,0,1,2,3} = d_{i,7,0,1,2} = d_{i,6,7,0,1} = d_{i,5,6,7,0} = d_{i,4,5,6,7} = d_{i,3,4,5,6} = d_{i,2,3,4,5} = d_{i,1,2,3,4}. \quad (23)$$

Let $j = 0, h = 2, l = 3, t = 5$ and $c(x) \in GF(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{i,0,2,3,5}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{i,(0-k)\bmod 8,(2-k)\bmod 8,(3-k)\bmod 8,(5-k)\bmod 8}$. It then follows that

$$d_{i,0,2,3,5} = d_{i,(0-k)\bmod 8,(2-k)\bmod 8,(3-k)\bmod 8,(5-k)\bmod 8}.$$

Therefore, we have

$$d_{i,0,2,3,5} = d_{i,7,1,2,4} = d_{i,6,0,1,3} = d_{i,5,7,0,2} = d_{i,4,6,7,1} = d_{i,3,5,6,0} = d_{i,2,4,5,7} = d_{i,1,3,4,6}. \tag{24}$$

From (23) and (24), for any $r \in W_4$, we have that $c(x)c(x^r)$ is a codeword of C_i, where C_i denote the cyclic code over $GF(q)$ with the generator polynomial $g_i(x) = \frac{x^n-1}{x^{n_i}-1}$ and the minimum distance $d_i = n_{i-(-1)^i}$.Hence from theorem 4.1,$d_{i,j,h,l,t}^2 \geq d_i = n_{i-(-1)^i}$, i.e., $d_{i,j,h,l,t} \geq \left\lceil \sqrt{n_{i-(-1)^i}} \right\rceil$, where

(j,h,l,t)
$\in \{(0,1,2,3),(0,2,3,5),(1,2,3,4),(1,3,4,6),(2,3,4,5),(2,4,5,7),(3,4,5,6),(3,5,6,0),$
$(4,5,6,7),(4,6,7,1),(5,6,7,0),(5,7,0,2),(6,7,0,1),(6,0,1,3),(7,0,1,2),(7,1,2,4)\}.$

Theorem 4.14: Suppose that $q \in W_0$. Let C_{n_1,n_2} and d_{n_1,n_2}be defined as in Theorem 4.3. Let $C_{n_1,n_2,j,h,l,t}$ denotethe cyclic code over $GF(q)$ with the generator polynomial

$$g_{n_1,n_2,j,h,l,t}(x) = \frac{(x^n-1)(x-1)}{(x^{n_1}-1)(x^{n_2}-1)d_j(x)d_h(x)d_l(x)d_t(x)}.$$

Then the cyclic code $C_{n_1,n_2,j,h,l,t}$ has parameters $\left[n, n_1+n_2-1+\frac{(n_1-1)(n_2-1)}{2}, d_{n_1,n_2,j,h,l,t}\right]$, where $d_{n_1,n_2,j,h,l,t} \geq \left\lceil \sqrt{\min(n_1,n_2)} \right\rceil$ and

(j,h,l,t)
$\in \{(0,1,2,3),(0,2,3,5),(1,2,3,4),(1,3,4,6),(2,3,4,5),(2,4,5,7),(3,4,5,6),(3,5,6,0),$
$(4,5,6,7),(4,6,7,1),(5,6,7,0),(5,7,0,2),(6,7,0,1),(6,0,1,3),(7,0,1,2),(7,1,2,4)\}.$

Proof: Let $j=0, h=1, l=2, t=3$ and $c(x) \in GF(q)[x]/(x^n-1)$ be a codeword of Hamming weight ω in $C_{n_1,n_2,0,1,2,3}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{n_1,n_2,(0-k)\bmod 8,(1-k)\bmod 8,(2-k)\bmod 8,(3-k)\bmod 8}$. It then follows that

$$d_{n_1,n_2,0,1,2,3} = d_{n_1,n_2,(0-k)\bmod 8,(1-k)\bmod 8,(2-k)\bmod 8,(3-k)\bmod 8}.$$

Therefore, we have

$$d_{n_1,n_2,0,1,2,3} = d_{n_1,n_2,7,0,1,2} = d_{n_1,n_2,6,7,0,1} = d_{n_1,n_2,5,6,7,0}$$
$$= d_{n_1,n_2,4,5,6,7} = d_{n_1,n_2,3,4,5,6} = d_{n_1,n_2,2,3,4,5} = d_{n_1,n_2,1,2,3,4}. \tag{25}$$

Let $j=0, h=2, l=3, t=5$ and $c(x) \in GF(q)[x]/(x^n-1)$ be a codeword of Hamming weight ω in $C_{n_1,n_2,0,2,3,5}$. Take any $r \in W_k$, for $1 \leq k \leq 7$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{n_1,n_2,(0-k)\bmod 8,(2-k)\bmod 8,(3-k)\bmod 8,(5-k)\bmod 8}$. It then follows that

$$d_{n_1,n_2,0,2,3,5} = d_{n_1,n_2,(0-k)\bmod 8,(2-k)\bmod 8,(3-k)\bmod 8,(5-k)\bmod 8}.$$

Therefore, we have

$$d_{n_1,n_2,0,2,3,5} = d_{n_1,n_2,7,1,2,4} = d_{n_1,n_2,6,0,1,3} = d_{n_1,n_2,5,7,0,2}$$
$$= d_{n_1,n_2,4,6,7,1} = d_{n_1,n_2,3,5,6,0} = d_{n_1,n_2,2,4,5,7} = d_{n_1,n_2,1,3,4,6}. \quad (26)$$

From (25) and (26), for any $r \in W_4$, we have that $c(x)c(x^r)$ is a codeword of C_{n_1,n_2}, where C_{n_1,n_2} and d_{n_1,n_2} be defined as Theorem 4.3.Hence from theorem 4.3,$d^2_{n_1,n_2,j,h,l,t} \geq d_{n_1,n_2} = \min(n_1, n_2)$, i.e., $d_{n_1,n_2,j,h,l,t} \geq \left\lceil \sqrt{\min(n_1, n_2)} \right\rceil$, where

(j, h, l, t)
$\in \{(0,1,2,3), (0,2,3,5), (1,2,3,4), (1,3,4,6), (2,3,4,5), (2,4,5,7), (3,4,5,6), (3,5,6,0),$
$(4,5,6,7), (4,6,7,1), (5,6,7,0), (5,7,0,2), (6,7,0,1), (6,0,1,3), (7,0,1,2), (7,1,2,4)\}.$

Acknowledgment

The authors are thankful to the Referee for valuable comments and suggestions.

References

[1] Bakshi, G. K. and Raka, M. (2003).Minimal cyclic codes of length $p^n q$,*Finite Fields and Their Applications* 9, 432-448.

[2] Betti, E. and Sala,M. (2006). A new bound for the minimum distance of a cyclic code from its defining set, *IEEE Transactions on Information Theory* 52(8), 3700-3706.

[3] Cusik, T., Ding, C. and Renvall, A. (2003),*Stream Ciphers and Number Theory*, North-Holland Mathematical Lib., North-Holland.

[4] Ding, C. (2012). Cyclic codes from cyclotomic sequence of order four, *Finite Fields and Their Applications* 23, 8-34.

[5] Ding, C. (2012). Cyclic codes from the two-prime sequences, *IEEE Transactions on Information Theory* 58(6), 3881-3891.

[6] Ding, C. (2012). Cyclotomic constructions of cyclic codes with length being the product of two primes, *IEEE Transactions on Information Theory* 58(4), 2231-2236.

[7] Ding, C., Du, X. and Zhou, Z. (2015). The bose and minimum distance of a class of BCH codes, *IEEE Transactions on Information Theory* 61(5), 2351-2356.

[8] Eupen, M. and Lint, J. van (1993).On the minimum distance of ternary cyclic codes, *IEEE Transactions on Information Theory* 39(2), 409-416.

[9] Kewat, P. K. and Kumari, P. (2015). Cyclic codes from the second class two-prime whiteman's genrealized cyclotomic sequence with order 6, *CoRR* arxiv:1507.05506.

[10] Lidl, R. and Niederreiter, H.(1997),*Finite fields*, Cambridge Univ. Press.

[11] Lint, J. van and Wilson, R. (1986).On the minimum distance of cyclic codes, *IEEE Transactions on Information Theory* 32(1), 23-40.

[12] Macwilliams, F. and Sloane, N. (1997), *The theory of error correcting codes,* North-Holland Mathematical Lib., North-Holland.

[13] Pruthi, M.and Arora, S. K. (1999). Minimal Codes of Length $2p^n$ *Finite Fields and Their Applications* 5, 177-187,

[14] Pruthi, M. and Arora, S. K. (1997). Minimal Codes of Prime-Power Length, *Finite Fields and Their Applications* 3, 99-113.

[15] Sun, Y., Yan, T. and Li, H. (2013). Cyclic codes from the two-prime whiteman's genrealizedcyclotomic sequences with order 4, *CoRR* arxiv:1303.6378.

[16] Whiteman, A. L. (1962). A family of difference sets, *Illionois J. Math* 6, 107-121.

[17] Yan, T., Lui, Y. and Sun, Y. (2015). Cyclic codes from generalized cyclotomic sequences of order 6, *CoRR* arxiv:1510.01022.