Abstract. Assume that $F$ is a finite field of prime power order $q$ (odd) and $q$ is a quadratic residue modulo $2^n$ $(n \geq 3)$. Then $q = 8m + 1 (m = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}, \alpha_i \geq 0)$. If $\alpha_0 = 0$ i.e. $m$ is odd, then the ring $R_{2^n} = F[x]/\langle x^{2^n} - 1 \rangle$ has $4(n - 1)$ primitive idempotents. The explicit expressions for these primitive idempotents are obtained. The minimum distance, the dimension and the generating polynomial of the $4(n - 1)$ minimum cyclic codes of length $2^n$ generated by these primitive idempotents are also obtained.

AMS Mathematics Subject Classification (2000): 94B15, 16S34, 20C05.

Keywords: Cyclotomic cosets, Minimal cyclic codes, Generating polynomials, Primitive idempotents.

1. Introduction

Let $G = C_\theta = \langle g \rangle$ be a finite cyclic group of order $\theta$ and $F(= GF(q))$ be a field of order $q$, a power of its prime (odd) characteristic $\rho$, (say). The cyclic codes of length $2^n$ over $F$ can be viewed as ideals in the semi-simple ring $R_{2^n} = F[x]/\langle x^{2^n} - 1 \rangle$. Here we assume that $q$ is quadratic residue modulo $2^n$. Then by Theorem 9.12 [3, p. 204], $q \equiv 1(\text{mod } 8)$ i.e. $q = 8m + 1 (m = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}, \alpha_i \geq 0)$. By Lemma 1.1, order of $q$ modulo $2^n$ is $\phi(2^n)/2^{\alpha_0 + 2} (n \geq \alpha_0 + 3)$. Let $S$ be the set $\{0, 1, 2, ..., 2^n - 1\}$. For $a, b \in S$, the relation $a \equiv bq^i (\text{mod } 2^n)$, partitions $S$ into $2^{\alpha_0 + 2}(n - \alpha_0 - 1)$ disjoint $q$-cyclotomic cosets modulo $2^n$, denoted by $\Omega_{(i),i}$ and given by Theorem 1.2. In view of Theorem 42 and 53 of [5] and the theory of primitive idempotents developed in section 2 and 3 of Chapter 8 of [4] (generalize to non-binary case), an expression $e_{(i),i}(x)$ is idempotent iff $e_{(i),i}(\alpha\mu) = 0$ or 1, for $0 \leq \mu \leq 2^n - 1$, and the idempotent $e_{(i),i}(x)$ is primitive if and only if

$$e_{(i),i}(\alpha\mu) = \begin{cases} 1 & \text{if } \mu \in \Omega_{(i),i} \\ 0 & \text{otherwise} \end{cases}$$
where \( \alpha \) is a primitive \( 2^n \)-th root of unity in some extension field of \( F \). In this paper we assume that \( \alpha_0 = 0 \) i.e. \( m \) is odd. Then \( R_{2^n} \) has \( 4(n-1) \) primitive idempotents. The expressions for these primitive idempotents are obtained in Theorem 2.4. The codes generated by these primitive idempotents are minimal cyclic codes of length \( 2^n \). These codes are described in section 4. Although we have already given these idempotents in [6] using a different terminology and approach, however in this paper to describe the codes generated, the expressions for these are verified by classical method of [1]. This enabled us to obtain generator polynomials of these codes which do not seem easy to obtain otherwise.

The case when \( m \) is even is interesting in itself and is dealt with a subsequent paper, with the view point that few basic results proved in this paper will frequently be used to prove the results in part - II, wherever and whenever needed.

**Lemma 1.1.** Let \( q = 8m + 1 \) \( (m = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}; \alpha_i \geq 0) \). Then, \( \phi(2^n) \) is the order of \( q \) modulo \( 2^n \) \( (n \geq \alpha_0 + 3) \).

**Proof.** It is easy to see that for \( n \geq \alpha_0 + 3 \),

\[
\frac{\phi(2^n)}{2^{\alpha_0+2}} = 2^{n-\alpha_0-3} = 2^n u + 1 \quad \text{where} \quad u \quad \text{is odd integer}
\]

If \( t \) is the order of \( q \) modulo \( 2^n \), it then follows that

\[
t = 2^r \quad \text{where} \quad r \leq n - \alpha_0 - 3.
\]

If \( r = n - \alpha_0 - 3 \), then Lemma follows.

Now, let \( r < n - \alpha_0 - 3 \). As discussed above, we have

\[
q^{2^r} = 2^{r+\alpha_0+3} u + 1 \quad \text{for some odd integer} \quad u.
\]

But then \( 2^n \) divides \( q^{2^r} - 1 \) implies that \( u \) is even, a contradiction.  

**Theorem 1.2.** Suppose \( q = 8m + 1 \) \( (m = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}; \alpha_i \geq 0) \). Then \( 2^{\alpha_0+2}(n - \alpha_0 - 1) \) \( q \)-cyclotomic cosets modulo \( 2^n \) are given by:

(i) \( \Omega_0 = \{0\} \)

(ii) for \( (n - \alpha_0 - 1) < i < n \) and \( 1 \leq l \leq 2^{n-i} \),

\( \Omega_{(l, i)} = \{l, 2^{i-1}\} \)

(iii) for \( 1 \leq i \leq n - (\alpha_0 + 2) \) and \( 1 \leq l \leq 2^{\alpha_0+2}, \)
\[ \Omega_{(l),i} = \{ 2^{i-1} (2^{a_0+3} \lambda + 2l - 1) : 0 \leq \lambda \leq 2^{n-(a_0+i+2)} - 1 \}. \]

**Proof.** By Lemma 1.1, the order of \( q \) modulo \( 2^i \) is \( \frac{\phi(2^i)}{2^{a_0+2}} \). Therefore, the equivalence classes can easily be computed by the fact that for \( 1 \leq i \leq n-(a_0+2) \),

\[ \frac{\phi(2^{n-i+1})}{q^{2^{a_0+2}}} \equiv 1 \pmod{2^{n-i+1}} \]

and

\[ 2^{i-1} q^{2^{n-i-(a_0+2)}} \equiv 2^{i-1} \pmod{2^n}. \]

**Notation 1.3.** (i) For \( 1 \leq i \leq n \) and \( 1 \leq l \leq 4 \), denote by \( X_{(l),i} \) the elements \( \sum_{t \in \Omega_{(l),i}} x^i \) of \( R_2^n \). For any \( \eta \in F \) or in some extension of \( F \), we put

\[ X_{(l),i}(\eta) = \sum_{t \in \Omega_{(l),i}} \eta^i \]

(ii) For \( 1 \leq i \leq n-2 \) and \( 1 \leq l, m \leq 4 \ (l \neq m) \), we put

(a) \( X_{(l,m),i} = X_{(l),i} - X_{(m),i} \)

(b) \( \delta_{i+3} = \{ X_{(l),i+3} + \ldots + X_{(4),i+3} \ldots + X_{(l),n} \} - \{ X_{(l),i+2} + \ldots X_{(4),i+3} \} \)

(iii) For \( 1 \leq i \leq n \) and \( 1 \leq l \leq 4 \), let

(a) \( S_{(l),i} = S / \Omega_{(l),i} \) (the set of elements of \( S \) not in \( \Omega_{(l),i} \)).

(b) \( E_{(l),i} \) denotes the codes generated by the primitive idempotents \( e_{(l),i} \).

(iv) Throughout in this paper the element \( \alpha \) denotes a primitive \( 2^n \)-th root of unity in some field extension of \( F \) and \( \alpha^{2^{n-3}} = \gamma \) (say).

2. **Primitive Idempotents in \( R_2^n \)**

In this section, first we assume \( n \geq 3 \). As mentioned earlier that \( a_0 = 0 \) i.e. \( q \) is odd number (prime or prime power) of the form \( 8m+1 \) (m - odd), a power of its prime (odd) characteristic \( \rho \). Then \( \rho \) is either of the type \( 8v+1, 8v+3 \) or \( 8v+5 \).

If \( \rho \) is of the form \( 8v+1 \), then \( \gamma^0 = \gamma \). Therefore, \( \gamma \in GF(\rho) \).

If \( \rho \) is of the form \( 8v+3 \) or \( 8v+5 \), then \( \gamma^2 = \gamma \). Therefore, \( \gamma \in GF(\rho^2) \).
Lemma 2.1. If \( q = 8m + 1 \) \((m \text{ odd})\), then for \( 1 \leq i \leq n - 2 \),

\[
\begin{align*}
I. \quad & X_{(1),i}(\alpha^j) = \begin{cases} 
0 & \text{if } 2^{n-i-2} \text{ does not divide } j \\
2^{n-(i+2)} \gamma^\beta & \text{if } j = 2^{n-i-2} \mu \text{ and } \mu \equiv \beta \pmod{8} \text{ and } \beta = 1, 3, 5, 7 \\
-2^{n-(i+2)} & \text{if } j = 2^{n-i} \mu \text{ and } \mu \text{ is odd} \\
2^{n-(i+2)} & \text{if } 2^{n-i+1} | j
\end{cases} \\
(\text{i}) & \\
(\text{ii}) & \\
(\text{iii}) & \\
(\text{iv}) & \\
(\text{v}) &
\end{align*}
\]

II. \( X_{(2),i}(\alpha^j) = \begin{cases} 
0 & \text{if } 2^{n-i-2} \text{ does not divide } j \\
2^{n-(i+2)} \gamma^3\beta & \text{if } j = 2^{n-i-2} \mu \text{ and } \mu \equiv \beta \pmod{8} \text{ and } \beta = 1, 3, 5, 7 \\
-2^{n-(i+2)} & \text{if } j = 2^{n-i} \mu \text{ and } \mu \text{ is odd} \\
2^{n-(i+2)} & \text{if } 2^{n-i+1} | j
\end{cases} \\
(\text{i}) & \\
(\text{ii}) & \\
(\text{iii}) & \\
(\text{iv}) & \\
(\text{v}) &
\]

III. \( X_{(3),i}(\alpha^j) = \begin{cases} 
0 & \text{if } 2^{n-i-2} \text{ does not divide } j \\
2^{n-(i+2)} \gamma^2\mu & \text{if } j = 2^{n-i-2} \mu \text{ and } \mu \equiv \beta \pmod{8} \text{ and } \beta = 1, 3, 5, 7 \\
-2^{n-(i+2)} & \text{if } j = 2^{n-i} \mu \text{ and } \mu \text{ is odd} \\
2^{n-(i+2)} & \text{if } 2^{n-i+1} | j
\end{cases} \\
(\text{i}) & \\
(\text{ii}) & \\
(\text{iii}) & \\
(\text{iv}) & \\
(\text{v}) &
\]

IV. \( X_{(4),i}(\alpha^j) = \begin{cases} 
0 & \text{if } 2^{n-i-2} \text{ does not divide } j \\
2^{n-(i+2)} \gamma^1\beta & \text{if } j = 2^{n-i-2} \mu \text{ and } \mu \equiv \beta \pmod{8} \text{ and } \beta = 1, 3, 5, 7 \\
-2^{n-(i+2)} & \text{if } j = 2^{n-i} \mu \text{ and } \mu \text{ is odd} \\
2^{n-(i+2)} & \text{if } 2^{n-i+1} | j
\end{cases} \\
(\text{i}) & \\
(\text{ii}) & \\
(\text{iii}) & \\
(\text{iv}) & \\
(\text{v}) &
\]

Proof. I(i) If \( 2^{n-i-2} \) does not divide \( j \), then \( \alpha^{j2^{i+2}} \neq 1 \). By definition of \( \Omega_{(1),i} \), we have

\[
X_{(1),i}(\alpha^j) = \sum_{\lambda=0}^{2^{n-(i+2)}-1} \alpha^{j2^{i-1}(8\lambda+1)} = \alpha^{j2^{i-1}} \left[ \frac{\alpha^{2^n j - 1}}{\alpha^{2^{i+2}} - 1} \right] = 0 .
\]

(ii) Let \( j = 2^{n-i-2} \mu \), where \( \mu \equiv \beta \pmod{8} \). Again by definition of \( \Omega_{(1),i} \), we have

\[
X_{(1),i}(\alpha^j) = \sum_{\lambda=0}^{2^{n-(i+2)}-1} \alpha^{j2^{i-1}(8\lambda+1)} = \sum_{\lambda=0}^{2^{n-(i+2)}-1} \alpha^{2^{n-3} \mu (8\lambda+1)}
\]
\[ 2^{n-(i+2)}_{-1} = \sum_{\lambda=0}^{\gamma^2} \gamma^\beta = 2^{n-i-2} \gamma^\beta. \]

(iii) If \( j = 2^{n-i-1} \mu \), where \( \mu \) is an odd number, then

\[ X_{(1), n}^j(\alpha^j) = \sum_{\lambda=0}^{2^{n-(i+2)}_{-1}} \alpha^{j2^{i-1}(8\lambda+1)} = \sum_{\lambda=0}^{2^{n-(i+2)}_{-1}} \alpha^{2^{n-i-1} \mu 2^{i-1}(8\lambda+1)} = \sum_{\lambda=0}^{2^{n-(i+2)}_{-1}} \gamma^{2\mu} = 2^{n-i-2} \gamma^{2\mu}. \]

(iv) and (v) follows on similar lines as (iii).

II, III and IV follows on similar lines as I.

**Lemma 2.2.** If \( q = 8m + 1 \) (\( m \) – odd), then

I. \( X_{(1), n}^j(\alpha^j) = \begin{cases} 
\gamma^2 & \text{if } j = 4k + 1 \\
-\gamma^2 & \text{if } j = 4k + 3 \\
-1 & \text{if } 2 \mid j \text{ but } 2^2 \nmid j \\
1 & \text{if } 2^2 \mid j
\end{cases} \) (i)

II. \( X_{(2), n}^j(\alpha^j) = \begin{cases} 
-\gamma^2 & \text{if } j = 4k + 1 \\
\gamma^2 & \text{if } j = 4k + 3 \\
-1 & \text{if } 2 \mid j \text{ but } 2^2 \nmid j \\
1 & \text{if } 2^2 \mid j
\end{cases} \) (ii)

III. \( X_{(1), n}^j(\alpha^j) = \begin{cases} 
-1 & \text{if } j \text{ is odd} \\
1 & \text{if } j \text{ is even}
\end{cases} \) (iii)

Proof. Follows trivially by definition of \( \Omega_{(1), n-1}, \Omega_{(2), n-1}, \Omega_{(1), n} \) and by notation 1.3(i).

**Lemma 2.3.** If \( q = 8m + 1 \) (\( m \) – odd), then for \( 0 \leq k \leq n-1 \),

\[ \{1+(X_{(1), k+2} + \ldots + X_{(4), k+2}) + (X_{(1), k+3} + \ldots + X_{(4), k+3}) + \ldots + (X_{(1), n-1} + X_{(2), n-1}) + X_{(1), n}\} - (X_{(1), k+1} + \ldots + X_{(4), k+1}) \}

\[ = \begin{cases} 
2^{n-k} & \text{if } 2^{n-k-1} \mid j \text{ but } 2^{n-k} \nmid j, \\
0 & \text{otherwise.}
\end{cases} \]

Proof. First suppose that \( 0 \leq k \leq n-3 \), and \( 2^{n-k-1} \mid j \text{ but } 2^{n-k} \nmid j \).

By Lemma 2.1 (I(iv), II(iv), III(iv), IV(iv)), we have
\[ X_{(1),k+1}(\alpha^j) = X_{(2),k+1}(\alpha^j) = X_{(3),k+1}(\alpha^j) = X_{(4),k+1}(\alpha^j) = -2^{-n-(k+3)}. \]

As \( 2^{n-k-1} \mid j \) but \( 2^{n-k} \nmid j \), so, for any integer \( t, k + 2 \leq t \leq n - 2 \), \( 2^{n-t+1} \mid j \) and hence, by Lemma 2.1 (I(v), II(v), III(v), IV(v)),
\[
X_{(1),1}(\alpha^j) = X_{(2),1}(\alpha^j) = X_{(3),1}(\alpha^j) = X_{(4),1}(\alpha^j) = 2^{n-(t+2)}.
\]

Since \( 0 \leq k \leq n - 3 \) and \( 2^{n-k-1} \mid j \), therefore by Lemma 2.2 (I(iv), II(iv) and III(ii))
\[
X_{(1),n-1}(\alpha^j) = X_{(2),n-1}(\alpha^j) = 1 \quad \text{and} \quad X_{(1),n}(\alpha^j) = 1.
\]

Thus for \( 0 \leq k \leq n - 3 \), left side of (1) reduces to
\[
\{1 + 4 \left(2^{n-k-4} + 2^{n-k-5} + \ldots + 2^1 + 1\right) + 2 + 1\} - 4\{-2^{n-k-3}\} = 2^{n-k}.
\]

Now suppose that (i) \( 2^{n-k-1} \mid j \) or (ii) \( 2^{n-k} \mid j \).

(i) If \( 2^{n-k-1} \mid j \), then for some integer \( r, 1 \leq r \leq n - k - 1 \), \( 2^{n-k-r-1} \mid j \) but \( 2^{n-k-r} \nmid j \).

First consider that \( r, 1 \leq r \leq n - k - 3 \). Then by repeated application of Lemma 2.1 and Lemma 2.2, for each \( t, 1 \leq t \leq k + r - 2 \),
\[
X_{(1),t}(\alpha^j) = X_{(2),t}(\alpha^j) = X_{(3),t}(\alpha^j) = X_{(4),t}(\alpha^j) = 0 \quad \text{and}
\]
\[
X_{(1),k+r-1}(\alpha^j) + X_{(2),k+r-1}(\alpha^j) + X_{(3),k+r-1}(\alpha^j) + X_{(4),k+r-1}(\alpha^j) = 0
\]
\[
X_{(1),k+r}(\alpha^j) + X_{(2),k+r}(\alpha^j) + X_{(3),k+r}(\alpha^j) + X_{(4),k+r}(\alpha^j) = 0
\]
\[
X_{(1),k+r+1}(\alpha^j) = X_{(2),k+r+1}(\alpha^j) = X_{(3),k+r+1}(\alpha^j) = X_{(4),k+r+1}(\alpha^j) = -2^{n-(k+r+3)}.
\]

Further, for \( k + r + 2 \leq t \leq n - 2 \),
\[
X_{(1),t}(\alpha^j) = X_{(2),t}(\alpha^j) = X_{(3),t}(\alpha^j) = X_{(4),t}(\alpha^j) = 2^{n-t-2} \quad \text{and}
\]
\[
X_{(1),n-1}(\alpha^j) = X_{(2),n-1}(\alpha^j) = 1 \quad \text{and} \quad X_{(1),n}(\alpha^j) = 1.
\]

If \( r = n - k - 2 \), then again by Lemma 2.1 and Lemma 2.2, for each \( t, 1 \leq t \leq n - 4 \),
\[
X_{(1),t}(\alpha^j) = X_{(2),t}(\alpha^j) = X_{(3),t}(\alpha^j) = X_{(4),t}(\alpha^j) = 0 \quad \text{and}
\]
\[
X_{(1),n-3}(\alpha^j) + X_{(2),n-3}(\alpha^j) + X_{(3),n-3}(\alpha^j) + X_{(4),n-3}(\alpha^j) = 0
\]
\[
X_{(1),n-2}(\alpha^j) + X_{(2),n-2}(\alpha^j) + X_{(3),n-2}(\alpha^j) + X_{(4),n-2}(\alpha^j) = 0
\]
\[
X_{(1),n-1}(\alpha^j) = X_{(2),n-1}(\alpha^j) = 1 \quad \text{and} \quad X_{(1),n}(\alpha^j) = 1
\]

If \( r = n - k - 1 \), then once again by Lemmas 2.1 and Lemma 2.2, for each \( t, 1 \leq t \leq n - 3 \),
\[
X_{(1),t}(\alpha^j) = X_{(2),t}(\alpha^j) = X_{(3),t}(\alpha^j) = X_{(4),t}(\alpha^j) = 0 \quad \text{and}
\]
\[
X_{(1),n-2}(\alpha^j) + X_{(2),n-2}(\alpha^j) + X_{(3),n-2}(\alpha^j) + X_{(4),n-2}(\alpha^j) = 0;
\]
\[
X_{(1),n-1}(\alpha^j) + X_{(2),n-1}(\alpha^j) = 0, \quad X_{(1),n}(\alpha^j) = -1.
\]
In all these cases, it can easily be proved that left side of (1) reduces to zero.

(ii) Let \( 2^{n-k} \mid j \). Then, for any integer \( t, k+1 \leq t \leq n-2 \), \( 2^{n-t+1} \mid j \). Therefore, by Lemma 2.1 (I(v), II(v), III(v), IV(v)), we have

\[
X_{(1), t}(\alpha^j) = X_{(2), t}(\alpha^j) = X_{(3), t}(\alpha^j) = X_{(4), t}(\alpha^j) = 2^{n-(t+2)}
\]

By Lemma 2.2 (I(iv), II(iv) and III(ii))

\[
X_{(1), n-1}(\alpha^j) = X_{(2), n-1}(\alpha^j) = 1 \quad \text{and} \quad X_{(1), n}(\alpha^j) = 1
\]

Thus, left side of (1) reduces to

\[
[\{1 + 4(2^{n-k-4} + 2^{n-k-5} + \ldots + 2^1 + 1) + 2 + 1\} - 4(2^{n-k-3})] = 0.
\]

Now if \( k = n-2 \) and \( 2 \mid j \) but \( 4 \nmid j \). Then, by Lemma 2.2 (I(iii), II(iii), III(iii))

\[
X_{(1), n-1}(\alpha^j) = X_{(2), n-1}(\alpha^j) = -1 \quad \text{and} \quad X_{(1), n}(\alpha^j) = 1.
\]

Thus left side of (1) reduces to, \( [(1 + 1) - (-1 - 1)] = 2^2 \).

If \( j \) is odd, then by Lemma 2.2,

\[
X_{(1), n-1}(\alpha^j) + X_{(2), n-1}(\alpha^j) = 0 \quad \text{and} \quad X_{(1), n}(\alpha^j) = -1.
\]

Thus, left side of (1) reduces to zero in this case also.

If \( 4 \mid j \), then again by Lemma 2.2,

\[
X_{(1), n-1}(\alpha^j) = X_{(2), n-1}(\alpha^j) = 1 \quad \text{and} \quad X_{(1), n}(\alpha^j) = 1.
\]

Therefore,

\[
[(1 + X_{(1), n}) - (X_{(1), n-1} + X_{(2), n-1})](\alpha^j) = 0.
\]

Finally, if \( k = n-1 \), then

\[
(1 - X_{(1), n}(\alpha^j)) = \begin{cases} 2 & \text{if } j \text{ is odd} \\ 0 & \text{if } j \text{ is even} \end{cases}
\]

holds trivially from lemma 2.3. III.

\[\Box\]

**Theorem 2.4.** If \( q = 8m + 1 \) (\( m \) – odd), then the \( 4(n-1) \) primitive idempotents in \( R_{2^n} \) are given by:

\[
e_0 = \frac{1}{2^n}[1 + (X_{(1), 1} + \ldots + X_{(4), 1}) + (X_{(1), 2} + \ldots + X_{(4), 2}) + \ldots + (X_{(1), n-1} + X_{(2), n-1}) + X_{(1), n}],
\]

\[
e_{(1), n-1} = \frac{1}{2^n}[1 + (X_{(1), 3} + \ldots + X_{(4), 3}) + (X_{(1), 4} + \ldots + X_{(4), 4}) + \ldots + (X_{(1), n-1} + X_{(2), n-1}) + X_{(1), n} \\
- (X_{(1), 2} + \ldots + X_{(4), 2}) - \gamma^2 [(X_{(1), 1} - X_{(2), 1}) + (X_{(3), 1} - X_{(4), 1})],
\]

\[
e_{(2), n-1} = \frac{1}{2^n}[1 + (X_{(1), 3} + \ldots + X_{(4), 3}) + (X_{(1), 4} + \ldots + X_{(4), 4}) + \ldots + (X_{(1), n-1} + X_{(2), n-1}) + X_{(1), n} \\
- (X_{(1), 2} + \ldots + X_{(4), 2}) + \gamma^2 [(X_{(1), 1} - X_{(2), 1}) + (X_{(3), 1} - X_{(4), 1})],
\]
\[ e_{(1)}, n = \frac{1}{2^n} \left[ 1 + (X_{(1),2} + \ldots + X_{(4),2}) + (X_{(1),3} + \ldots + X_{(4),3}) + \ldots + (X_{(1),n-1} + X_{(2),n-1}) + X_{(1),n} \right] \]

for \( 1 \leq i \leq n-2 \),

\[ e_{(1),i} = \frac{1}{2^{n-i+1}} [\delta_{i+1} - \gamma^2 (X_{(1,2),i+1} + X_{(3,4),i+1}) - \gamma X_{(2,4),i} - \gamma^3 X_{(1,3),i}] \]

\[ e_{(2),i} = \frac{1}{2^{n-i+1}} [\delta_{i+1} + \gamma^2 (X_{(1,2),i+1} + X_{(3,4),i+1}) - \gamma X_{(1,3),i} - \gamma^3 X_{(2,4),i}] \]

\[ e_{(3),i} = \frac{1}{2^{n-i+1}} [\delta_{i+1} - \gamma^2 (X_{(1,2),i+1} + X_{(3,4),i+1}) + \gamma X_{(1,3),i} + \gamma^3 X_{(2,4),i}] \]

\[ e_{(4),i} = \frac{1}{2^{n-i+1}} [\delta_{i+1} + \gamma^2 (X_{(1,2),i+1} + X_{(3,4),i+1}) + \gamma X_{(1,3),i} + \gamma^3 X_{(2,4),i}] \]

**Proof.** It is trivial to see that

\[ e_0(\alpha^j) = \begin{cases} 1 & \text{if } j = 0 \\ 0 & \text{otherwise.} \end{cases} \]

Now, we prove that for \( 1 \leq i \leq n-2 \),

\[ e_{(1),i}(\alpha^j) = \begin{cases} 1 & \text{if } j \in \Omega_{(1),n-i-1} \\ 0 & \text{otherwise.} \end{cases} \]

Let \( j \notin \Omega_{(1),n-i-1} \). Then

(i) if \( j = 0 \), result is trivial.

(ii) if \( j \neq 0 \), then let \( j \in \Omega_{(1),n-k-1} \cup \ldots \cup \Omega_{(4),n-k-1} (k \neq i) \). If \( 0 \leq k \leq i-1 \),

then \( 2^{n-i-1} \mid j \). By Lemma 2.3,

\[ [(1 + (X_{(1),i-3} + \ldots + X_{(4),i+3}) + \ldots + (X_{(1),n-1} + X_{(2),n-1}) + X_{(1),n}) - (X_{(1),i+2} + \ldots + X_{(4),i+2}))](\alpha^j) = 0. \]

Further, for \( 0 \leq k \leq i-3 \), since \( 2^{n-i+1} \mid j \), then by Lemma 2.1 ( I(v), II(v), III(v), IV(v) )

\[ X_{(1),i}(\alpha^j) = X_{(2),i}(\alpha^j) = X_{(3),i}(\alpha^j) = X_{(4),i}(\alpha^j) = 2^{n-(i+2)} \]

\[ X_{(1),i+1}(\alpha^j) = X_{(2),i+1}(\alpha^j) = X_{(3),i+1}(\alpha^j) = X_{(4),i+1}(\alpha^j) = 2^{n-(i+3)} . \]

For \( k = i-2 \), \( 2^{n-i} \mid j \), by Lemma 2.1,

\[ X_{(1),i}(\alpha^j) = X_{(2),i}(\alpha^j) = X_{(3),i}(\alpha^j) = X_{(4),i}(\alpha^j) = -2^{n-(i+2)}, \]

\[ X_{(1),i+1}(\alpha^j) = X_{(2),i+1}(\alpha^j) = X_{(3),i+1}(\alpha^j) = X_{(4),i+1}(\alpha^j) = 2^{n-(i+3)}. \]

For \( k = i-1 \), \( j \) is odd multiple of \( 2^{n-i-1} \). Therefore, by Lemma 2.1 ( I(iii),(iv), II(iii),(iv), III(iii),(iv), IV(iii),(iv) )

\[ X_{(1,3),i}(\alpha^j) = 0, \quad X_{(2,4),i}(\alpha^j) = 0; \]
and

\[ X_{(12), i+1}(\alpha^j) = X_{(3,4), i+1}(\alpha^j) = 0. \]

Hence, if \( 0 \leq k \leq i - 1 \), then

\[ e_{(1), i}(\alpha^j) = 0. \]

Now, if \( i + 2 \leq k \leq n - 2 \), then \( 2^{n-i-3} \nmid j \). By Lemma 2.1 (I(i), II(i), III(i), IV(i)), we have

\[ X_{(1,3), i}(\alpha^j) = X_{(2,4), i}(\alpha^j) = 0 \]

and

\[ X_{(1,2), i+1}(\alpha^j) = X_{(3,4), i+1}(\alpha^j) = 0. \]

and by Lemma 2.3,

\[ \{I + (X_{(1), i+3} + \ldots + X_{(4), i+3}) + \ldots + (X_{(1), n-i} + X_{(2), n-i}) + X_{(1), n} - (X_{(1), i+2} + \ldots + X_{(4), i+2})\}(\alpha^j) = 0. \]

Now, if \( k = i + 1 \), then \( j = 2^{n-i-3} \mu \), where \( \mu \) is odd number. By Lemma 2.1

\[ X_{(1,3), i}(\alpha^j) = X_{(2,4), i}(\alpha^j) = 0. \]

\[ (X_{(1,2), i+1}(\alpha^j) + X_{(3,4), i+1}(\alpha^j)) = 0. \]

and by Lemma 2.3

\[ \{I + (X_{(1), i+3} + \ldots + X_{(4), i+3}) + \ldots + (X_{(1), n-i} + X_{(2), n-i}) + X_{(1), n} - (X_{(1), i+2} + \ldots + X_{(4), i+2})\}(\alpha^j) = 0. \]

Hence, for \( i + 1 \leq k \leq n - 2 \),

\[ e_{(1), i}(\alpha^j) = 0. \]

(iii) Finally let, \( j \in \Omega_{(2), n-i-1} \cup \Omega_{(3), n-i-1} \cup \Omega_{(4), n-i-1} \).

If \( j \in \Omega_{(2), n-i-1} \), then \( j = 2^{n-i-2} \mu \), where \( \mu \equiv 3 \pmod{8} \).

Therefore, by Lemma 2.1, we have

\[ X_{(1,3), i}(\alpha^j) = 2^{n-i-1} \gamma^3, \quad X_{(2,4), i}(\alpha^j) = 2^{n-i-1} \gamma \]

and

\[ X_{(1,2), i+1}(\alpha^j) = 2^{n-i-2} \gamma^2 \mu, \quad X_{(3,4), i+1}(\alpha^j) = 2^{n-i-2} \gamma^2 \mu. \]

Since \( 2^{n-i-2} \nmid j \) but \( 2^{n-i-1} \nmid j \), therefore by Lemma 2.3,

\[ \{I + (X_{(1), i+3} + \ldots + X_{(4), i+3}) + \ldots + (X_{(1), n-i} + X_{(2), n-i}) + X_{(1), n} - (X_{(1), i+2} + \ldots + X_{(4), i+2})\}(\alpha^j) = 2^{n-i-1}. \]

Hence,

\[ e_{(1), i}(\alpha^j) = 0. \]

Similarly, if \( j \in \Omega_{(3), n-i-1} \cup \Omega_{(4), n-i-1} \) then

\[ e_{(1), i}(\alpha^j) = 0. \]

Now if \( j \in \Omega_{(1), n-i-1} \), then \( j = 2^{n-i-2} \mu \), where \( \mu \equiv 1 \pmod{8} \). Therefore, by Lemma 2.1
\[ X_{(1,3),i}(\alpha^j) = 2^{n-i-1}\gamma \quad \text{and} \quad X_{(2,4),i}(\alpha^j) = 2^{n-i-1}\gamma^3 \]

and

\[ X_{(1,2),i+1}(\alpha^j) = 2^{n-i-2}\gamma^2 \mu \quad \text{and} \quad X_{(3,4),i+1}(\alpha^j) = 2^{n-i-2}\gamma^2 \mu \]

and by Lemma 2.3.

\[ \{1 + (X_{(1,i+3} + \ldots + X_{(4,i+3)} + \ldots + (X_{(1),n-1} + X_{(1),n-1}) + X_{(1),n}) \]

\[ - (X_{(1),i+2} + \ldots + X_{(4),i+2})\} \gamma^j = 2^{n-i-1}. \]

Therefore, \( e_{(1),i}(\alpha^j) = 1. \)

Similarly, for \( 1 \leq i \leq n - 2 \) and \( 2 \leq l \leq 4 \)

\[ e_{(l),i}(\alpha^j) = \begin{cases} 1 & \text{if } j \in \Omega_{(l),n-i-1} \\ 0 & \text{otherwise.} \end{cases} \]

Now, we shall prove that

\[ e_{(1),n-1}(\alpha^j) = \begin{cases} 1 & \text{if } j \in \Omega_{n-1}^1 \\ 0 & \text{otherwise.} \end{cases} \]

Let \( j \in \Omega_{(1),n-1}. \) Then, \( j = 2^{n-2} \mu, \) where \( \mu \equiv 1 \pmod{8}. \)

By Lemma 2.3, for \( k = 1, \)

\[ \{1 + (X_{(1),3} + \ldots + X_{(4),3}) + \ldots + X_{(1),n} - (X_{(1),2} + \ldots + X_{(4),2}) \} \gamma^j = 2^{n-1} \]

Also by Lemma 2.1 (I(iii), II(iii), III(iii), IV(iii)),

\[ X_{(1),1}(\alpha^j) = 2^{n-3}\gamma^2 \mu \quad \text{and} \quad X_{(2),1}(\alpha^j) = -2\gamma^2 \mu \quad ; \]

\[ X_{(3),1}(\alpha^j) = 2^{n-3}\gamma^2 \mu \quad \text{and} \quad X_{(4),1}(\alpha^j) = -2\gamma^2 \mu \quad . \]

Therefore,

\[ e_{(1),n-1}(\alpha^j) = 1. \]

If \( j \not\in \Omega_{(1),n-1}. \) Then by Lemma 2.3 (for \( k = 1 \))

\[ \{1 + (X_{(1),3} + \ldots + X_{(4),3}) + \ldots + (X_{(1),n-1} + X_{(2),n-1}) + X_{(1),n} \]

\[ - (X_{(2),1} + \ldots + X_{(4),2}) \} \gamma^j = 0. \]

By Lemma 2.1,

\[ (X_{(1),1}(\alpha^j) - X_{(2),1}(\alpha^j)) + (X_{(3),1}(\alpha^j) - X_{(4),1}(\alpha^j)) = 0. \]

Hence, \( e_{(1),n-1}(\alpha^j) = 0. \)

Therefore,
\[
\begin{align*}
e_{(1),n-1}(\alpha^j) &= 1 \quad \text{if } j \in \Omega_{(1),n-1} \\
&= 0 \quad \text{otherwise.}
\end{align*}
\]

Similarly,
\[
\begin{align*}
e_{(2),n-1}(\alpha^j) &= 1 \quad \text{if } j \in \Omega_{(2),n-1} \\
&= 0 \quad \text{otherwise.}
\end{align*}
\]

The fact that
\[
e_{(1),n}(\alpha^j) = 1 \quad \text{if } j \in \Omega_{(1),n} \\
= 0 \quad \text{otherwise.}
\]
follows immediately by taking \( k = 0 \) in Lemma 2.3.

Hence in view of as remarked in section 1, Theorem follows.

**3. Generating polynomials**

Let \( E_{(l),i} \) denotes the ideals of \( R_{2^n} \) generated by the primitive idempotents \( e_{(l),i} \), given by theorem 2.4. As noted earlier \( E_{(l),i} \) are cyclic codes of length \( 2^n \). In this section, we obtain the explicit expressions for the generating polynomial of these codes.

**Theorem 3.1.** Suppose \( q = 8m + 1 \) (\( m \)- odd). Then

(I) for \( 1 \leq i \leq n-2 \),
\[
\begin{align*}
g_{(1),i}(x) &= \sum_{m=0}^{2^{n-(i+2)}-1} x^{m2^i+2} (x^{2^{i-1}} + \gamma)(x^{2^i} + \gamma^2)(x^{2^{i+1}} - 1) \quad (1) \\
g_{(2),i}(x) &= \sum_{m=0}^{2^{n-(i+2)}-1} x^{m2^i+2} (x^{2^{i-1}} + \gamma^3)(x^{2^i} - \gamma^2)(x^{2^{i+1}} - 1) \quad (2) \\
g_{(3),i}(x) &= \sum_{m=0}^{2^{n-(i+2)}-1} x^{m2^i+2} (x^{2^{i-1}} - \gamma)(x^{2^i} + \gamma^2)(x^{2^{i+1}} - 1) \quad (3) \\
g_{(4),i}(x) &= \sum_{m=0}^{2^{n-(i+2)}-1} x^{m2^i+2} (x^{2^{i-1}} - \gamma^3)(x^{2^i} - \gamma^2)(x^{2^{i+1}} - 1) \quad (4)
\end{align*}
\]

are the generating polynomials of the codes \( E_{(l),i} \) \((1 \leq l \leq 4)\) generated by the primitive idempotents \( e_{(l),i} \) given by Theorem 2.4.

(II) The polynomials
\[
\begin{align*}
g_{(1),n-1}(x) &= \sum_{m=0}^{2^{n-2}-1} x^{2^m}(x + \gamma^2)(x^2 - 1) \quad (5)
\end{align*}
\]
\[ g_{(2), n-1}(x) = \sum_{m=0}^{2^{n-2}-1} x^{2^m} (x - \gamma^2) (x^2 - 1) \] (6)

are the generating polynomials of the code \( E_{(1), n-1} \) and \( E_{(2), n-1} \) respectively generated by the primitive idempotents \( e_{(1), n-1} \) and \( e_{(2), n-1} \) given by Theorem 2.4.

(III) The polynomials

\[ g_0(x) = \sum_{i=0}^{2^n-1} x^i \]

\[ g_{(1), n}(x) = \sum_{i=0}^{2^n-1} (-1)^{i+1} x^i \]

are the generating polynomials of the code \( E_0 \) and \( E_{(1), n} \) generated by the primitive idempotents \( e_0 \) and \( e_{(1), n} \) given by Theorem 2.4.

**Proof.** I. From (1), we can also write

\[ g_{(1), i}(x) = \frac{1 - x^{2^n}}{1 - x^{2^i+2}} (x^{2^i-1} + \gamma) (x^{2^i} + \gamma^2) (x^{2^i+1} - 1) \] (7)

Let \( j \in S_{(1), n-i-1} (1 \leq i \leq n-2) \).

(i) If \( 2^{n-i-1} \mid j \), then \( \alpha_j^{2^i+1} - 1 = 0 \).

Hence, from (1), \( g_{(1), i}(\alpha_j) = 0 \).

(ii) If \( j \in \Omega_{(2), n-i-1} \cup \Omega_{(3), n-i-1} \cup \Omega_{(4), n-i-1} \)

then \( j = 2^{n-i-2} \mu \), where \( \mu \equiv 3 \) or \( 5 \) or \( 7 \pmod{8} \), so

\[ [(x^{2^i-1} + \gamma) (x^{2^i} + \gamma^2)](\alpha_j^i) = (\alpha_j^{2^{n-3}} + \gamma)(\alpha_j^{2^{n-2}} + \gamma^2) \]

becomes zero.

Hence, again from (1)

\[ g_{(1), i}(\alpha_j^i) = 0. \]

(iii) If \( 2^{n-i-2} \nmid j \), then \( \alpha_j^{2^i+2} - 1 \neq 0 \). It then follows from (7) that \( g_{(1), i}(\alpha_j^i) = 0 \).

As \( \deg(g_{(1), i}(x)) = 2^n - 2^{i-1} \mid S_{(1), n-i-1} \) \( \), so the elements of \( S_{(1), n-i-1} \) are the only roots of \( g_{(1), i}(x) \). But then \( e_{(1), i}(\alpha_j^i) = 0 \) (proof of Theorem 2.4) for all \( j \in S_{(1), n-i-1} \) implies that \( g_{(1), i}(x) \) is the generating polynomial of the code \( E_{(1), i} \).

Similarly, \( g_{(2), i}(x) \), \( g_{(3), i}(x) \) and \( g_{(4), i}(x) \) are the generating polynomials of the code \( E_{(2), i} \), \( E_{(3), i} \) and \( E_{(4), i} \) respectively.
II. From (5), we can also write
\[
g_{(1),n-1}(x) = \frac{1-x^{2^n}}{1-x^4}(x + \alpha^{2^{n-2}})(x^2 - 1). \tag{8}
\]

Let \( j \in S_{(1),n-1} = \mathcal{S}/\mathcal{O}_{(1),n-1} \)

(i) If \( 2^{n-1} \mid j \), then \( \alpha^{2^j} - 1 = 0 \).

Hence, from (5)
\[
g_{(1),n-1}(\alpha^j) = 0.
\]

(ii) If \( j \in \mathcal{O}_{(2),n-1} \), then \( j = 3.2^{n-2} \).

Therefore,
\[
[(x + \gamma^2)(x^2 - 1)](\alpha^j) = (\alpha^{3.2^{n-2}} + \gamma^2)(\alpha^{2.3.2^{n-2}} - 1) \text{ becomes zero.}
\]

Hence again from (5),
\[
g_{(1),n-1}(\alpha^j) = 0.
\]

(iii) If \( 2^{n-2} \nmid j \), then \( \alpha^{j.2^{n-2}} - 1 \neq 0 \). It then follows from (8) that
\[
g_{(1),n-1}(\alpha^j) = 0.
\]

As \( \deg g_{(1),n-1}(x) = 2^n - 1 = |S_{(1),n-1}| \), so the elements of \( S_{(1),n-1} \) are the only roots of \( g_{(1),n-1}(x) \). But then \( e_{(1),n-1}(\alpha^j) = 0 \) (proof of Theorem 2.4) for all \( j \in S_{(1),n-1} \) implies that \( g_{(1),n-1}(x) \) is the generating polynomial of the code \( E_{(1),n-1} \).

Similarly, \( g_{(2),n-1}(x) \) is the generating polynomial of the code \( E_{(2),n-1} \).

III. Trivially, \( g_0(x) \) is the generating polynomial of the code \( E_0 \).

By Theorem 2.4,
\[
e_{(1),n}(\alpha^j) = \begin{cases} 1 & \text{if } j \in \mathcal{O}_{(1),n} \\ 0 & \text{otherwise} \end{cases}
\]

Trivially,
\[
g_{(1),n}(\alpha^j) = \begin{cases} -2^n & \text{if } j \in \mathcal{O}_{(1),n} \\ 0 & \text{otherwise} \end{cases}
\]

Therefore, \( g_{(1),n}(x) \) is the generating polynomial of the code \( e_{(1),n} \). \( \blacksquare \)
4. Dimension and minimum distance of the codes $E_{(l),i}$

By Theorem 3.1, for $(1 \leq i \leq n - 2, 1 \leq l \leq 4),$ 
\[
\text{deg.} (g_{(l),i}(x)) = 2^n - 2^{i-1} \quad \text{and} \quad \text{deg.} (g_{(1),n-i}(x)) = \text{deg.} (g_{(2),n-i}(x)) = \text{deg.} (g_{(1),n}(x)) = \text{deg.} (g_0(x)) = 2^n - 1.
\]

By Theorem 7.2 [2, p.42],
\[
\dim. (E_{(l),i}) = 2^n - \text{deg.} (g_{(l),i}(x)) = 2^n - 2^n + 2^{i-1} = 2^{i-1}.
\]

Trivially,
\[
\dim. (E_{(1),n-1}) = \dim. (E_{(2),n-1}) = \dim. (E_{(1),n}) = \dim. (E_0) = 1.
\]

**Theorem 4.1.** If $E_{(l),i}$ denotes the cyclic codes of length $2^n$, generated by the primitive idempotents $e_{(l),i}$, given by theorem 2.4. Then

(i) minimum distance of the codes $E_{(l),i}$ $(1 \leq i \leq n-2$ and $1 \leq l \leq 4)$ are $2^{n-i+1}$.

(ii) minimum distance of the codes $E_{(1),n-1}$, $E_{(2),n-1}$, $E_{(1),n}$ and $E_0$ are $2^n$.

**Proof.** Let $E_{(1),i}$ be the cyclic code of length $2^n$ generated by the polynomial
\[
g_{(1),i}(x) = \sum_{m=0}^{2^{n-i+2}-1} x^m x^{i+2} (x^{2^{i-1}} + \gamma) (x^2 + \gamma^2) (x^{2^{i+1}} - 1).
\]

Here each pair of non-zero entries of generating polynomial are separated by $(2^{i-1} - 1)$ consecutive zero’s. As discussed above
\[
\dim. (E_{(1),i}) = 2^{i-1}
\]

Therefore, any codeword of $E_{(1),i}$ is of the form
\[
\gamma_0 \{ g_{(1),i}(x) \} + \gamma_1 \{ x^2 g_{(1),i}(x) \} + \gamma_2 \{ x^2 g_{(1),i}(x) \} + \ldots + \gamma_{2^{i-1} - 1} \{ x^{2^{i-1}} g_{(1),i}(x) \}, \quad \gamma_i \in F
\]

Since in such a combination the non-zero entries never coincide, therefore weight of generating polynomial is always less than the weight of every codeword. Hence , minimum distance of pol. $(g_{(1),i}(x)) = \text{wt.} (g_{(1),i}(x)) = 8.2^{n-i-2} = 2^{n-i+1}$

minimum distance of codes $(E_{(1),i}) = 2^{n-i+1}$
Similarly, for \((1 \leq i \leq n - 2; \, 2 \leq l \leq 4)\)

minimum distance of codes \((E_{(l,i)}) = 2^{n-i+1}\)

and minimum distance of code \((E_{(1),n-1}) = \text{minimum distance of code } (E_{(2),n-1}) = 2^n\).

Now we find minimum distance of the codes \(E_{(1),n}\) and \(E_0\) generated by the polynomials \(g_{(1),n}(x)\) and \(g_0(x)\) respectively.

Let \(m_{(1),n}(x) \neq 0\) be a minimum code word in \(E_{(1),n}\). Then

\[
m_{(1),n}(x) = a(x)g_{(1),n}(x) \quad \text{for some} \quad a(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{2^{n-1}}x^{2^{n-1}}
\]

or

\[
m_{(2),n}(x) = a_0g_{(1),n}(x) + a_1xg_{(1),n}(x) + a_2x^2g_{(1),n}(x) + \ldots + a_{n-1}x^{2^{n-1}}g_{(1),n}(x)
\]

\[
= a_0g_{(1),n}(x) - a_1g_{(1),n}(x) + a_2g_{(1),n}(x) + \ldots - a_{n-1}g_{(1),n}(x)
\]

\[
= (a_0 - a_1 + a_2 + \ldots - a_{n-1})g_{(1),n}(x)
\]

Hence, \(Wt(m_{(1),n}(x)) = Wt(g_{(1),n}(x)) = 2^n\)

and so \(g_{(1),n}(x)\) is a minimum weight code word in \(E_{(1),n}\).

Trivially \(g_0(x)\) is a minimum weight code word in \(E_0\).  

**Example 4.2.** Let \(q = 41\) and \(n = 4\). Then \(q\)-cyclotomic cosets modulo \(2^4\) are:

\[
\Omega_0 = \{0\} \quad ; \quad \Omega_{(1),4} = \{8\} \quad ; \quad \Omega_{(1),3} = \{4\}, \quad \Omega_{(2),3} = \{12\};
\]

\[
\Omega_{(1),1} = \{1,9\}, \quad \Omega_{(2),1} = \{3,11\}, \quad \Omega_{(3),1} = \{5,13\}, \quad \Omega_{(4),1} = \{7,15\};
\]

\[
\Omega_{(1),2} = \{2\}, \quad \Omega_{(2),2} = \{6\}, \quad \Omega_{(3),2} = \{10\}, \quad \Omega_{(4),2} = \{14\};
\]

By Theorem 2.4 primitive idempotents in \(R_{24}\) are:

\[
e_0 = 18(1 + x + x^2 + \ldots + x^{15})
\]

\[
e_{(1),4} = 18(1 + x^2 + x^4 + \ldots + x^{12} + x^{14}) + 23(x + x^3 + \ldots + x^{13} + x^{15})
\]

\[
e_{(1),3} = 18(1 + x^4 + x^8 + x^{12}) + 23(x^2 + x^6 + x^{10} + x^{14})
\]

\[
+ 2(x + x^5 + x^9 + x^{13}) + 39(x^3 + x^7 + x^{11} + x^{15})
\]

\[
e_{(2),3} = 18(1 + x^4 + x^8 + x^{12}) + 23(x^2 + x^6 + x^{10} + x^{14})
\]

\[
+ 39(x + x^5 + x^9 + x^{13}) + 2(x^3 + x^7 + x^{11} + x^{15})
\]

\[
e_{(1),1} = 18(1 + x^8) + 2(x^2 + x^{10}) + 23(x^4 + x^{12}) + 39(x^6 + x^{14})
\]

\[
+ 6(x + x^9) + 28(x^3 + x^{11}) + 35(x^5 + x^{13}) + 13(x^7 + x^{15})
\]

\[
e_{(2),1} = 18(1 + x^8) + 39(x^2 + x^{10}) + 23(x^4 + x^{12}) + 2(x^6 + x^{14})
\]

\[
+ 28(x + x^9) + 6(x^3 + x^{11}) + 13(x^5 + x^{13}) + 35(x^7 + x^{15})
\]
\[ e_{(3),1} = 18(1 + \alpha^8) + 2(\alpha^2 + \alpha^{10}) + 23(\alpha^4 + \alpha^{12}) + 39(\alpha^6 + \alpha^{14}) + 35(\alpha + \alpha^9) + 13(\alpha^3 + \alpha^{11}) + 6(\alpha^5 + \alpha^{13}) + 28(\alpha^7 + \alpha^{15}) \]

\[ e_{(4),1} = 18(1 + \alpha^8) + 39(\alpha^2 + \alpha^{10}) + 23(\alpha^4 + \alpha^{12}) + 2(\alpha^6 + \alpha^{14}) + 13(\alpha + \alpha^9) + 35(\alpha^3 + \alpha^{11}) + 28(\alpha^5 + \alpha^{13}) + 6(\alpha^7 + \alpha^{15}) \]

\[ e_{(1),2} = 36 + 12\alpha^2 + 4\alpha^4 + 15\alpha^6 + 5\alpha^8 + 29\alpha^{10} + 37\alpha^{12} + 37\alpha^{14} \]

\[ e_{(2),2} = 36 + 15\alpha^2 + 37\alpha^4 + 12\alpha^6 + 5\alpha^8 + 26\alpha^{10} + 4\alpha^{12} + 29\alpha^{14} \]

\[ e_{(3),2} = 36 + 29\alpha^2 + 4\alpha^4 + 26\alpha^6 + 5\alpha^8 + 12\alpha^{10} + 37\alpha^{12} + 15\alpha^{14} \]

\[ e_{(4),2} = 36 + 26\alpha^2 + 37\alpha^4 + 29\alpha^6 + 5\alpha^8 + 15\alpha^{10} + 4\alpha^{12} + 12\alpha^{14} \]

Here \( \alpha(=\sqrt{3}) \) is a primitive 16\textsuperscript{th} root of unity s.t. \( \alpha^2 \in GF(41) \).

The parameter of the codes \( E_{(i),j} \) are:

<table>
<thead>
<tr>
<th>Code</th>
<th>Dimension</th>
<th>Minimum Distance</th>
<th>Generating Polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>( E_0 )</td>
<td>1</td>
<td>16</td>
<td>( 1 + \alpha + \alpha^2 + \alpha^3 + ... + \alpha^{13} + \alpha^{14} + \alpha^{15} )</td>
</tr>
<tr>
<td>( E_{(1),4} )</td>
<td>1</td>
<td>16</td>
<td>( 40(1 + \alpha^2 + \alpha^6 + ... + \alpha^{14}) + (\alpha + \alpha^3 + ... + \alpha^{15}) )</td>
</tr>
<tr>
<td>( E_{(1),3} )</td>
<td>1</td>
<td>16</td>
<td>( 9(1 + \alpha^4 + \alpha^8 + \alpha^{12}) + 40(\alpha + \alpha^5 + \alpha^9 + \alpha^{13}) + 32(\alpha^2 + \alpha^6 + \alpha^{10} + \alpha^{14}) + (\alpha^3 + \alpha^7 + \alpha^{11} + \alpha^{15}) )</td>
</tr>
<tr>
<td>( E_{(2),3} )</td>
<td>1</td>
<td>16</td>
<td>( 32(1 + \alpha^4 + \alpha^8 + \alpha^{12}) + 40(\alpha + \alpha^5 + \alpha^9 + \alpha^{13}) + 9(\alpha^2 + \alpha^6 + \alpha^{10} + \alpha^{14}) + (\alpha^3 + \alpha^7 + \alpha^{11} + \alpha^{15}) )</td>
</tr>
<tr>
<td>( E_{(1),2} )</td>
<td>2</td>
<td>8</td>
<td>( 14 + 32\alpha^2 + 38\alpha^4 + 40\alpha^6 + 27\alpha^8 + 9\alpha^{10} + 3\alpha^{12} + \alpha^{14} )</td>
</tr>
<tr>
<td>( E_{(2),2} )</td>
<td>2</td>
<td>8</td>
<td>( 32 + 9\alpha^2 + 14\alpha^4 + 40\alpha^6 + 3\alpha^8 + 32\alpha^{10} + 9\alpha^{12} + \alpha^{14} )</td>
</tr>
<tr>
<td>( E_{(3),2} )</td>
<td>2</td>
<td>8</td>
<td>( 27 + 32\alpha^2 + 3\alpha^4 + 40\alpha^6 + 14\alpha^8 + 9\alpha^{10} + 32\alpha^{12} + \alpha^{14} )</td>
</tr>
<tr>
<td>( E_{(4),2} )</td>
<td>2</td>
<td>8</td>
<td>( 3 + 9\alpha^2 + 27\alpha^4 + 32\alpha^6 + 38\alpha^8 + 32\alpha^{10} + 32\alpha^{12} + \alpha^{14} )</td>
</tr>
<tr>
<td>( E_{(1),1} )</td>
<td>1</td>
<td>16</td>
<td>( 14 + 32\alpha^2 + 38\alpha^4 + 40\alpha^6 + 27\alpha^8 + 9\alpha^{10} + 3\alpha^{12} + \alpha^{14} )</td>
</tr>
<tr>
<td>( E_{(2),1} )</td>
<td>1</td>
<td>16</td>
<td>( 38 + 9\alpha + 14\alpha^2 + 40\alpha^3 + 3\alpha^4 + 32\alpha^5 + 27\alpha^6 + \alpha^7 + 38\alpha^8 )</td>
</tr>
<tr>
<td>( E_{(3),1} )</td>
<td>1</td>
<td>16</td>
<td>( 9 + 32\alpha + 3\alpha^2 + 40\alpha^3 + 32\alpha^4 + 9\alpha^5 + 38\alpha^6 + \alpha^7 + 9\alpha^8 )</td>
</tr>
</tbody>
</table>
\[ E_{(4),1} \quad 1 \quad 16 \quad 3 + 9x + 27x^2 + 40x^3 + 38x^4 + 32x^5 + 14x^6 + x^7 + 3x^8 \]
\[ \quad + 9x^9 + 27x^{10} + 40x^{11} + 38x^{12} + 32x^{13} + 14x^{14} + x^{15}. \]

References


