Some Cyclic Codes of length $4p^n$ and their Minimum Distance Bounds

Jagbir Singh  
Department of Mathematics, M.D. University, Rohtak 124001, India.

Sonika Ahlawat  
Department of Mathematics, M.D. University, Rohtak 124001, India.

Abstract

The idempotents generating the minimal ideal in the semi-simple group algebra $FC_{4p^n}$ of the cyclic group $C_{4p^n}$ of order $4p^n$ over finite field $F$ are obtained. Generating polynomials and minimum distance bounds for the corresponding cyclic codes of length $4p^n$ are also calculated.

Key Words: Group algebra, cyclotomic cosets, primitive idempotents, generating polynomials.

AMS Subject Classification: 11T71, 11T55, 22D20.

1. Introduction

Let $F$ be a Galois field of order $q$ where $q$ is some prime power of the form $4k + 3$ and $C_m$ be a cyclic group of order $m$ such that $g.c.d.(q, m) = 1$. Then the group algebra $FC_m$ is semi-simple having finite cardinality of collection of primitive idempotents which equals the cardinality of collection of $q$-cyclotomic cosets modulo $m$. Let $t$ be the multiplicative order of $q$ modulo $p^n$, then $1 \leq t \leq \phi(p^n)$ [6]. Pruthi and Arora ([12, 8]) computed the primitive idempotents of minimal cyclic codes of length $m$ in case, when $t = \phi(m)$ and $m = 2, 4, p^n, 2p^n$. The primitive idempotents of length $p^n$ with order of $q$ modulo $p^n$ is $\phi(p^n)\over 2$ were obtained by Arora et.al. [1] and minimal quadratic residue codes of length $p^n$ by Batra and Arora [4]. Cyclic codes of length $2p^n$ over $F$, where order of $q$ modulo $2p^n$ is $\phi(2p^n)\over 2$ were obtained by Batra and Arora [5]. Minimal cyclic codes of length $p^nq$, where $p$ and $q$ are distinct odd primes were obtained by Sahni and Sehgal [9]. The minimal cyclic codes of length $p^nq$ were obtained by Bakshi and Raka [3]. Further, for $t = \phi(p^n)$ the minimal cyclic codes of length $8p^n$, were discussed by Singh and Arora [10]. F. Li et.al. obtained irreducible cyclic codes of length $4p^n$ and $8p^n$, where $q \equiv 3(\text{mod } 8)$ and $p/(q - 1)$ [7].

In present paper, we obtained cyclic codes of length $4p^n$ over $F$ where order of $q$ modulo $p^n$ is $\phi(p^n)\over 2$. The $q$-cyclotomic cosets modulo $4p^n$ are obtained in Section 2 and corresponding primitive idempotents in Section 3. In Section 4, we discussed generating polynomials and dimensions for the corresponding cyclic codes of length $4p^n$. The minimum distance or the bounds for minimum distance of these codes are obtained in Section 5.

2. Cyclotomic Cosets

Lemma 2.1 Suppose $\phi(p^n)\over 2$ be the order of $q$ modulo $p^n$. Then the order of $q$ modulo $p^{n-i}$ is $\phi(p^{n-i})\over 2$ for all $i, \ 0 \leq i \leq n - 1$.

Proof. Proof is on similar lines as that of ([5], Theorem 2.5).

Lemma 2.2 If $\phi(p^n)\over 2$ is the order of $q$ modulo $p^n$ then for $0 \leq i \leq n - 1$,

(i) order of $q$ modulo $2p^{n-i}$ is $\phi(p^{n-i})\over 2$.

(ii) For $p \equiv 1(\text{mod } 4)$, order of $q$ modulo $4p^{n-i}$ is $\phi(p^{n-i})\over 2$.

(iii) For $p \equiv 3(\text{mod } 4)$, order of $q$ modulo $4p^{n-i}$ is $\phi(p^{n-i})$. Proof. (i) Since $\phi(p^n)\over 2$ is the order of $q$ modulo $p^n$ therefore by lemma 2.1 order of $q$ modulo $p^{n-i}$ is $\phi(p^{n-i})\over 2, 1 \leq i \leq n - 1$. Hence

$q^{\phi(p^{n-i})\over 2} \equiv 1(\text{mod } p^{n-i}) \ (1)$

Since $q$ is of the form $4k + 1$ therefore $q \equiv 1(\text{mod } 2)$. Hence, $q^{\phi(p^{n-i})\over 2} \equiv 1(\text{mod } 2)$. As $\text{gcd}(2, p^{n-i}) = 1$, so
Lemma 2.3 For \(0 \leq i \leq n - 1\), and \(0 \leq k \leq \frac{\phi(p^n - 1)}{2} - 1\), \(1 + 2p^n \not\equiv q^k (mod 4p^n - 1)\).

**Proof.** Proof can be obtained by using lemma 2.1 and lemma 2.2. □

Lemma 2.4 Let \(p\) be an odd prime. Then there exists an integer \(g\), \(1 < g < 4p\) such that \(g\) is primitive root modulo \(p\), order of \(g\) modulo \(4\) is 2. Further, if \(q\) is any prime power and \(g.c.d.(q, p) = 1\), then \(g \not\equiv \{1, q, q^2, \ldots, q^{\frac{\phi(p^n - 1)}{2} - 1}\}\).

**Proof.** Consider the complete residue system, \(S_p = \{0, 1, 2, \ldots, p - 1\}\) modulo \(p\), \(S_{2p} = \{0, 1, 2, \ldots, 2p - 1\}\) modulo \(2p\). Since \(g.c.d.(2, p) = 1\), there exists an integer \(v \in S_p\) such that \(2v - p = 1\). Let \(a\) be any primitive root mod \(p\) in \(S_p\). For \(p \equiv 1(mod 4)\), let \(g \equiv 2av + 3p + 2ap(mod 4p)\). Then, \(g \equiv a(mod p)\). Hence, \(g\) is primitive root modulo \(p\). Now, \(g \equiv 2av + 3p + 2ap(mod 4p)\), \(g \equiv 3(mod 4)\), as \(p\) is of the form \(4k + 1\). Hence, order of \(g\) modulo \(4\) is 2. Further, for \(p \equiv 3(mod 4)\), \(g \equiv 2av + p(mod 4p)\). Then, as for the case of \(p \equiv 1(mod 4)\), \(g\) is primitive root modulo \(p\) and 4 both. Let \(g \in \{1, q, q^2, \ldots, q^{\frac{\phi(p^n - 1)}{2} - 1}\}\). So \(g = q^i\) for some \(1 \leq i \leq \frac{\phi(p^n - 1)}{2} - 1\). This implies \(o(g) = o(q^i)\). Here, order of \(g\) modulo \(4p\) is \(\frac{\phi(p^n - 1)}{2}\). So \(o(q^i) \leq \frac{\phi(p^n - 1)}{2}\) modulo \(4p\). This implies \(o(g) \leq \frac{\phi(p^n - 1)}{2}\) modulo \(4p\). But order of \(g\) modulo \(4p\) is \(\phi(p)\). Hence \(g \not\equiv \{1, q, q^2, \ldots, q^{\frac{\phi(p^n - 1)}{2} - 1}\}\). □

Lemma 2.5 If \(p \equiv 1(mod 4)\), there exist a fixed integer \(g\) satisfying \(\gcd(g, 2pq) = 1, 1 < g < 4p, g \not\equiv q^k (mod 4p)\) where \(0 \leq k \leq \frac{\phi(p^n - 1)}{2} - 1\), such that for \(0 \leq j \leq n - 1\), the set \(\{1, q, q^2, \ldots, q^{\frac{\phi(p^n - 1)}{2} - 1}\}, g, gq, gq^2, \ldots, gq^{\frac{\phi(p^n - 1)}{2} - 1}\}\) forms a reduced residue system modulo \(p^n - j\) and the set \(\{1, q, q^2, \ldots, q^{\frac{\phi(p^n - 1)}{2} - 1}\}, g, gq, gq^2, \ldots, gq^{\frac{\phi(p^n - 1)}{2} - 1}\}\) forms a reduced residue system modulo \(4p^n - j\), where \(\lambda = 1 + 2p^n\).

**Proof.** By lemma 2.1, order of \(g\) modulo \(p\) is \(\phi(p)\). Therefore the numbers \(1, q, q^2, \ldots, q^{\frac{\phi(p^n - 1)}{2} - 1}\) are incongruent modulo \(p\). But there are exactly \(\phi(p)\) numbers in the reduced residue system modulo \(p\). Therefore there exist a number \(g\) satisfying \(\gcd(g, 2pq) = 1, 1 < g < 4p, g \not\equiv q^k (mod 4p)\) for \(0 \leq k \leq \frac{\phi(p^n - 1)}{2} - 1\). Then the set \(\{1, q, q^2, \ldots, q^{\frac{\phi(p^n - 1)}{2} - 1}\}, g, gq, gq^2, \ldots, gq^{\frac{\phi(p^n - 1)}{2} - 1}\}\) forms a reduced residue system modulo \(p^n - j\). Since for \(0 \leq k \leq \frac{\phi(p^n - 1)}{2} - 1\), \(g \not\equiv q^k (mod 4p^n - j)\); for \(0 \leq k \leq \frac{\phi(p^n - 1)}{2} - 1\). Hence the set \(\{1, q, q^2, \ldots, q^{\frac{\phi(p^n - 1)}{2} - 1}, g, gq, gq^2, \ldots, gq^{\frac{\phi(p^n - 1)}{2} - 1}\}\) forms a reduced residue system modulo \(p^n - j\), \(0 \leq j \leq n - 1\). Similar result holds to show that the set \(\{1, q, q^2, \ldots, q^{\frac{\phi(p^n - 1)}{2} - 1}, g, gq, gq^2, \ldots, gq^{\frac{\phi(p^n - 1)}{2} - 1}, \lambda, \lambda q, q^{\lambda^2}, \ldots, \lambda q^{\frac{\phi(p^n - 1)}{2} - 1}, \lambda g, qg^{\lambda^2}, \ldots, \lambda gq^{\frac{\phi(p^n - 1)}{2} - 1}\}\) forms a reduced residue system modulo \(4p^n - j\). □

Lemma 2.6 If \(p \equiv 3(mod 4)\), there exist a fixed integer \(g\) satisfying \(\gcd(g, 2pq) = 1, 1 < g < 2p, g \not\equiv q^k (mod 4p)\) where \(0 \leq k \leq \frac{\phi(p^n - 1)}{2} - 1\), such that for \(0 \leq j \leq n - 1\), the set \(\{1, q, q^2, \ldots, q^{\frac{\phi(p^n - 1)}{2} - 1}\}, g, gq, gq^2, \ldots, gq^{\frac{\phi(p^n - 1)}{2} - 1}\}\) forms a reduced residue system modulo \(p^n - j\) and the set \(\{1, q, q^2, \ldots, q^{\frac{\phi(p^n - 1)}{2} - 1}, g, gq, gq^2, \ldots, gq^{\frac{\phi(p^n - 1)}{2} - 1}\}\) forms a reduced residue system modulo \(4p^n - j\), where \(\lambda = 1 + 2p^n\).

**Proof.** Proof is similar to that of lemma 2.5. □
Theorem 2.1 If \( p \equiv 1 (\mod 4) \), then the \((8n + 3)\) \( q\)-cyclotomic cosets modulo \( 4p^n \) are given by:

\[
\Omega_0 = \{0\}, \ \Omega_{p^n} = \{p^n, p^n q\}, \ \Omega_{2p^n} = \{2p^n\}
\]

and for \( 0 \leq i \leq n - 1 \),

\[
\Omega_{sp^i} = \{sp^i, sp^i q, sp^i q^2, ..., sp^i q^{\phi(p^n - 1)}\} \text{ for } s = 1, 2, \lambda, g, 2g, 4g, \lambda g.
\]

Proof. \( \Omega_0 = \{0\} \) is trivial.

Since \( q \) is of the form \( 4k + 3 \), so \( p^n q^2 \equiv p^n (\mod 4p^n) \) and hence \( \Omega_{p^n} = \{p^n, p^n q\} \), \( \Omega_{2p^n} = \{2p^n\} \).

By lemma 2.2; \( q^\frac{4(p^n - 1)}{2} \equiv 1 (\mod 4p^n) \). Equivalently, \( p^n q^{\frac{4(p^n - 1)}{2}} \equiv p^n (\mod 4p^n) \). Therefore,

\[
\Omega_{sp^i} = \{p^i, p^i q, p^i q^2, ..., p^i q^{\phi(p^n - 1)}\}.
\]

Similarly, \( \Omega_{2sp^i} = \{sp^i, sp^i q, sp^i q^2, ..., sp^i q^{\phi(p^n - 1)}\} \) for \( s = 2, 4, \lambda, g, 2g, 4g, \lambda g \).

Obviously, \( |\Omega_0| = 1 \). Also, \( |\Omega_{p^n}| = 2 \), \( |\Omega_{2p^n}| = 1 \), and

\[
|\Omega_{p^n}| = |\Omega_{2p^n}| = |\Omega_{4p^n}| = |\Omega_{8p^n}| = |\Omega_{16p^n}| = \frac{\phi(p^n - 1)}{2}.
\]

Therefore,

\[
\sum_{i=0}^{n-1} |\Omega_{p^n} - I| = \sum_{i=0}^{n-1} \frac{\phi(p^n - 1)}{2} = \frac{\phi(p^n)}{2} + \frac{\phi(p^{n-2})}{2} + \cdots + \frac{\phi(p)}{2} = p^n - 1.
\]

Hence, \( |\Omega_0| + |\Omega_{p^n}| + |\Omega_{2p^n}| + \sum_{i=1}^{n-1} \sum_{t=1,2,4,\lambda,g,2g,4g,\lambda g} |\Omega_{sp^i}| = 4p^n \). \( \square \)

Theorem 2.2 If \( p \equiv 3 (\mod 4) \), there are \((6n + 3)\) \( q\)-cyclotomic cosets modulo \( 4p^n \) given by:

\[
\Omega_0 = \{0\}, \ \Omega_{p^n} = \{p^n, p^n q\}, \ \Omega_{2p^n} = \{2p^n\}
\]

and for \( 0 \leq i \leq n - 1 \),

\[
\Omega_{sp^i} = \{sp^i, sp^i q, sp^i q^2, ..., sp^i q^{\phi(p^n - 1)}\} \text{ for } s = 1, 2, 4, g, 2g, 4g.
\]

3. Primitive Idempotents

Throughout this paper, we consider that \( \alpha \) is \( 4p^n \)th root of unity in some extension field of \( F \). Let \( M_s \) be the minimal ideal in \( R_{4p^n} = \frac{F[x]}{x^{4p^n} - 1} \equiv FC_{4p^n} \), generated by \( \frac{x^{4p^n - 1}}{m_s(x)} \), where \( m_s(x) \) is the minimal polynomial for \( \alpha^s \), \( s \in \Omega_s \). We denote \( \theta_s(x) \), the primitive idempotent in \( R_{4p^n} \), corresponding to the minimal ideal \( M_s \), given by \( \theta_s(x) = \frac{1}{4p^n} \sum_{t=0}^{4p^n - 1} \varepsilon_t^s x^t \)

where \( \varepsilon_t^s = \sum_{s \in \Omega_s} \alpha^{-is} \) and \( \varepsilon_t = \sum_{s \in \Omega_t} x^s \).

Lemma 3.1 For any odd prime \( p \) and a positive integer \( k \), if \( \beta \) is primitive \( p^k \)th root of unity in some extension field of \( F \), then the following holds:

(i) If \( q \) is quadratic residue \( p \) and a positive integer \( k \), then \( \beta^{\phi(k)} \equiv \beta^{-1} (\mod p^k) \),

\[
\sum_{t=0}^{\phi(k)-1} (\beta^t + \beta^{qk}) = \begin{cases} 
-1, & k = 1 \\
0, & k \geq 2 
\end{cases}
\]

(ii) If \( q \) is quadratic non-residue \( p \),

\[
\sum_{t=0}^{\phi(k)-1} \beta^t = \begin{cases} 
-1, & k = 1 \\
0, & k \geq 2 
\end{cases}
\]
Proof. By lemma 2.5, the set \( \{1, q, q^2, ..., q^{\frac{\phi(n)}{2}} - 1, g, gg, gg^2, ..., gg^{\frac{\phi(n)}{2}} - 1\} \) is a reduced residue system \((mod p)\). Then:
\[
\sum_{t=0}^{\frac{\phi(n)}{2} - 1} (\beta^{gt} + \beta^{gt}) = \sum_{t=0}^{\phi(n)} \beta^t - \sum_{t=1, p/t}^{\phi(n)} \beta^t = - \sum_{t=1}^{p-1} \beta^{pt}
\]
If \( k = 1 \), then \(-\beta^p = -1\).
If \( k \geq 2 \), then \( \beta^p \neq 1 \), therefore
\[
\sum_{t=1}^{p-1} \beta^{pt} = \beta^p(1 + \beta^p + ... + \beta^{p-1}) = \beta^p \left( \frac{\beta^p}{1} - 1 \right) = 0.
\]
For the remaining part see [3, lemma 4]. 

\[\square\]

Lemma 3.2 For cyclotomic cosets \( \Omega_{p^i}, 0 \leq i \leq n - 1 \), \( \lambda^2 \Omega_{p^i} = \Omega_{p^j} = \lambda \Omega_{p^i} \).

Proof. Since \( \lambda^2 \equiv 1 (mod 4p^n) \), so the required result holds.

\[\square\]

Lemma 3.3 (i) If \( p \equiv 1 (mod 4) \), then \( \Omega_1 = -\Omega_1 \) or \( \Omega_\lambda = -\Omega_1 \) according as \( \frac{\phi(p^n)}{4} \) is odd or even. (ii) If \( p \equiv 3 (mod 4) \), then \( \Omega_2 = -\Omega_1 \).

Proof. Since \( p \) is an odd prime, so \( \frac{\phi(p^n)}{4} \) is odd if and only if \( p \equiv 3 (mod 4) \).

(i) If \( p \equiv 1 (mod 4) \) and \( q \equiv 3 (mod 4) \)
Clearly, \( \lambda = 1 + 2p^n \equiv -1 (mod 4) \) and \( q \equiv -1 (mod 4) \)
If \( \frac{\phi(p^n)}{4} \) is odd, then \( q^{\frac{\phi(p^n)}{4}} \equiv -1 (mod 4) \). Also, \( q^{\frac{\phi(p^n)}{4}} \equiv -1 (mod p^n) \)

Since, \( \Omega_1 = -\Omega_1 \) and \( \lambda = -\Omega_1 \)

If \( q^{\frac{\phi(p^n)}{4}} \) is even, then \( q^{\frac{\phi(p^n)}{4}} \equiv 1 (mod 4) \) and \( \lambda \equiv -1 (mod 4) \). So, \( \lambda q^{\frac{\phi(p^n)}{4}} \equiv -1 (mod 4) \). Further, \( q^{\frac{\phi(p^n)}{4}} \equiv -1 (mod p^n) \). Thus, \( \lambda q^{\frac{\phi(p^n)}{4}} \equiv -1 (mod p^n) \).

Since, \( \lambda = -\Omega_1 \) and \( \lambda q^{\frac{\phi(p^n)}{4}} \equiv -1 (mod 4p^n) \). Hence, \( \Omega_1 = -\Omega_1 \)

(ii) If \( p \equiv 3 (mod 4) \), then \( q \equiv -1 (mod 4) \) and for even \( k \), \( q^{4k} \equiv 1 (mod 4) \). So, \( gg^{k} \equiv -1 (mod 4) \).

Now, \( q^{\frac{\phi(p^n)}{4}} \equiv 1 (mod p^n) \). Here, \( \frac{\phi(p^n)}{4} \) is odd. So, \( q^{k} \equiv -1 (mod p^n) \) for \( 0 \leq k \leq \frac{\phi(p^n)}{4} - 1 \).

Also the set \( \{1, q, q^2, ..., q^{\frac{\phi(p^n)}{4}} - 1, g, gg, gg^2, ..., gg^{\frac{\phi(p^n)}{4}} - 1\} \), forms a reduced residue system modulo \( p^n \), so \( gg^{k} \equiv -1 (mod p^n) \).

Since \( \lambda = -\Omega_1 \) is true, therefore
\[
q^{\frac{\phi(p^n)}{4}} \equiv -1 (mod 4p^n) . \text{ Hence } \Omega_2 = -\Omega_1
\]

\[\square\]

Notations: For \( 0 \leq j \leq n - 1 \), define:
\[
A_j = p^j \sum_{s \in \Omega_{p^j}} \alpha^s , \quad B_j = p^j \sum_{s \in \Omega_{p^{2j}}} \alpha^s , \quad C_j = p^j \sum_{s \in \Omega_{p^{2j}}} \alpha^s , \quad D_j = p^j \sum_{s \in \Omega_{p^{2j}}} \alpha^s , \quad E_j = p^j \sum_{s \in \Omega_{p^{2j}}} \alpha^s , \quad F_j = p^j \sum_{s \in \Omega_{p^{2j}}} \alpha^s .
\]
Here, \( A_j = A_j \), so \( A_j \in F \). Similarly, \( B_j, C_j, D_j, E_j \) and \( F_j \) are all in \( F \).

Lemma 3.4 For \( p \equiv 3 (mod 4) \). \( A_j + B_j = 0 \) for all \( j \). Proof. By definition, \( A_j + B_j = \sum_{t=0}^{\phi(p^n)-1} (\alpha^{gp^j}q^t + \alpha^{gp^j}q^t) = \sum_{t=0}^{\phi(p^n)-1} (\beta^{gp^j} + \beta^t) \), where \( \beta = \alpha^{gp^j} \).

Since, \( p^j q^t \equiv p^j q^{t^2} (mod 4p^n) \) if and only if \( t \equiv q^t (mod 4p^{n-j}) \)
if and only if \( t \equiv s (mod \phi(p^{n-j})) \).

Thus,
\[
\sum_{t=0}^{\phi(p^n)-1} (\beta^{gp^j} + \beta^t) = \phi(p^n-1) \sum_{t=0}^{\phi(p^n)-1} (\beta^{gp^j} + \beta^t) = \phi(p^n-1) \sum_{t=0}^{\phi(p^n)-1} (\beta^{gp^j} + \beta^t) .
\]
As the set \( \{1, q, q^2, ..., q^{\phi(p^n)-1}, g, gg, gg^2, ..., gg^{\phi(p^n)-1}\} \) forms a reduced residue system modulo \( 4p^{n-j} \), therefore the above sum is:

\[16711\]
\[ \sum_{t=0}^{\phi(p^n)-1} (\beta^{q^t} + \beta^t) = \sum_{t=1}^{4p^{n-j}} \beta^{-t} - \sum_{t=1+p/2}^{4p^{n-j}} \beta^{-t} - \sum_{t=1+2/p}^{4p^{n-j}} \beta^{-t} + \sum_{t=1,2/p}^{4p^{n-j}} \beta^t. \]

Further, \( \beta \) is 4\( p^{n-j} \)th root of unity, so \( \beta \neq 1, \beta^p \neq 1, \beta^2 \neq 1, \beta^{2p} \neq 1 \). Thus,
\[ \sum_{t=1}^{4p^{n-j}} \beta^t = \sum_{t=1+p/2}^{4p^{n-j}} \beta^t = \sum_{t=1+2/p}^{4p^{n-j}} \beta^t = 0. \]

Hence: \( A_j + B_j = 0 \) for all \( j \).

**Lemma 3.5** (i) \( C_j + D_j = \begin{cases} p^{n-1}, & j = n-1 \\ 0, & \text{otherwise.} \end{cases} \)

(ii) \( E_j + F_j = \begin{cases} -p^{n-1}, & j = n-1 \\ 0, & \text{otherwise.} \end{cases} \)

**Proof.** Proof can be derived directly as of lemma 3.4 and using the facts that
\( \{1, q, q^2, \ldots, q^{\frac{\phi(p^n)-1}{4}}, \beta, gq, gq^2, \ldots, gq^{\frac{\phi(p^n)-1}{4}}\} \) is a reduced residue system modulo \( (2p^n) \)
and modulo \( (p^n) \) and using lemma 3.1

**Lemma 3.6** For \( 0 \leq i \leq n \), \( 0 \leq j \leq n-1 \)
\[ \sum_{s \in \Omega_{p,l}} \alpha^{gp^i} = \sum_{s \in \Omega_{2p,l}} \alpha^{lp^i} = - \sum_{s \in \Omega_{p,l}} \alpha^{gp^i} = \begin{cases} 0, & \text{if } i + j \geq n, \\ \frac{1}{p^l} A_{i+j}, & \text{if } i + j \leq n-1. \end{cases} \]

**Proof.** Here
\[ \sum_{s \in \Omega_{p,l}} \alpha^{gp^i} = \sum_{t=0}^{\phi(p^n)-1} \alpha^{(1+2p^n)^2 gp^{i+j} q^t} = \sum_{t=0}^{\phi(p^n)-1} \alpha^{gp^{i+j} q^t} = \sum_{s \in \Omega_{p,l}} \alpha^{gp^i}. \]

Let \( \beta = \alpha^{gp^i+j} \). Then, \( \sum_{s \in \Omega_{p,l}} \alpha^{gp^i} = \sum_{t=0}^{\phi(p^n)-1} \beta^{q^t} \).

If \( i+j \geq n \), then \( \beta \) is 4th root of unity, then
\[ \sum_{s \in \Omega_{p,l}} \alpha^{gp^i} = \sum_{t=0}^{\phi(p^n)-1} \beta^{q^t} = 0. \]

If \( i+j \leq n-1 \), then \( \beta \) is 4\( p^{n-i-j} \)th root of unity, then \( \beta^{q^t} \equiv \beta^{p^l q^t} \) if and only if \( q^t \equiv q^t (\text{mod } 4p^{n-i-j}) \)
and if and only if \( l \equiv r (\text{mod } \frac{\phi(p^n)}{4p^{n-i-j}}) \).

Therefore
\[ \sum_{s \in \Omega_{p,l}} \alpha^{gp^i} = \sum_{t=0}^{\phi(p^n)-1} \beta^{q^t} = \frac{p^{i+j}}{p^l} \sum_{t=0}^{\phi(p^n)-1} \beta^{p^l q^t} = \frac{1}{p^l} A_{i+j}. \]

**Proof of following lemmas can be obtained on similar lines as of lemma 3.6 and using lemma 3.2.**

**Lemma 3.7** For \( 0 \leq i \leq n \), \( 0 \leq j \leq n-1 \)
\[ \sum_{s \in \Omega_{p,l}} \alpha^{gp^i} = \sum_{s \in \Omega_{2p,l}} \alpha^{lp^i} = \sum_{s \in \Omega_{p,l}} \alpha^{lp^i} = \sum_{s \in \Omega_{p,l}} \alpha^{gp^i} = \begin{cases} 0, & \text{if } i + j \geq n, \\ \frac{1}{p^l} C_{i+j}, & \text{if } i + j \leq n-1. \end{cases} \]

**Lemma 3.8** For \( 0 \leq i \leq n \), \( 0 \leq j \leq n-1 \)
If \( p \equiv 1 \) (mod 4) then,
\[ (i) \sum_{s \in \Omega_{p,l}} \alpha^{2gp^i} = \sum_{s \in \Omega_{2p,l}} \alpha^{2lp^i} = \begin{cases} -\frac{\phi(p^n)}{2}, & \text{if } i + j \geq n, \\ \frac{1}{p^l} C_{i+j}, & \text{if } i + j \leq n-1. \end{cases} \]
\( \sum_{s \in \Omega_{p^i}} \alpha^{2p^i} = \sum_{s \in \Omega_{2p^i}} \alpha^{2p^i} = \sum_{s \in \Omega_{2p^i}} \alpha^{4p^i} = \sum_{s \in \Omega_{4p^i}} \alpha^{4p^i} = \sum_{s \in \Omega_{4p^i}} \alpha^{4p^i} = \sum_{s \in \Omega_{4p^i}} \alpha^{4p^i} = \left\{ \begin{array}{ll}
\frac{-\phi(p^{n-j})}{p}, & i + j \geq n \\
\frac{\phi(p^{n-j})}{p^2}, & i + j \leq n - 1.
\end{array} \right. \)

\( \sum_{s \in \Omega_{p^i}} \alpha^{4p^i} = \sum_{s \in \Omega_{2p^i}} \alpha^{4p^i} = \sum_{s \in \Omega_{4p^i}} \alpha^{4p^i} = \sum_{s \in \Omega_{4p^i}} \alpha^{4p^i} = \sum_{s \in \Omega_{4p^i}} \alpha^{4p^i} = \sum_{s \in \Omega_{4p^i}} \alpha^{4p^i} = \left\{ \begin{array}{ll}
\frac{-\phi(p^{n-j})}{p}, & i + j \geq n \\
\frac{\phi(p^{n-j})}{p^2}, & i + j \leq n - 1.
\end{array} \right. \)

**Lemma 3.9** For \( 0 \leq i \leq n, \ 0 \leq j \leq n - 1 \)

If \( p \equiv 3 \mod 4 \), then

\( \sum_{s \in \Omega_{p^i}} \alpha^{2p^i} = \sum_{s \in \Omega_{2p^i}} \alpha^{2p^i} = \sum_{s \in \Omega_{2p^i}} \alpha^{2p^i} = \sum_{s \in \Omega_{4p^i}} \alpha^{2p^i} = \sum_{s \in \Omega_{4p^i}} \alpha^{2p^i} = \sum_{s \in \Omega_{4p^i}} \alpha^{2p^i} = \left\{ \begin{array}{ll}
\frac{-\phi(p^{n-j})}{p}, & i + j \geq n \\
\frac{\phi(p^{n-j})}{p^2}, & i + j \leq n - 1.
\end{array} \right. \)

\( \sum_{s \in \Omega_{p^i}} \alpha^{4p^i} = \sum_{s \in \Omega_{2p^i}} \alpha^{4p^i} = \sum_{s \in \Omega_{2p^i}} \alpha^{4p^i} = \sum_{s \in \Omega_{4p^i}} \alpha^{4p^i} = \sum_{s \in \Omega_{4p^i}} \alpha^{4p^i} = \sum_{s \in \Omega_{4p^i}} \alpha^{4p^i} = \left\{ \begin{array}{ll}
\frac{-\phi(p^{n-j})}{p}, & i + j \geq n \\
\frac{\phi(p^{n-j})}{p^2}, & i + j \leq n - 1.
\end{array} \right. \)

**Theorem 3.1** For \( p \equiv 1 \mod 4 \), the explicit expression for the \((8n + 3)\) primitive idempotents in \( R_{4p^n} \) are given by

\[
\theta_0(x) = \frac{1}{4p} \left[ \mathcal{C}_0 + \mathcal{C}_{p^n} + \mathcal{C}_{2p^n} + \sum_{i=1}^{n-1} \left( \mathcal{C}_{p^i} - \mathcal{C}_{2p^i} + \mathcal{C}_{4p^i} + \mathcal{C}_{2p^i} + \mathcal{C}_{4p^i} + \mathcal{C}_{8p^i} + \mathcal{C}_{8p^i} + \mathcal{C}_{8p^i} \right) \right]
\]

\[
\theta_{p^n}(x) = \frac{1}{4p} \left[ 2\mathcal{C}_0 - 2\mathcal{C}_{2p^n} - \sum_{i=-n}^{n-1} \left( 2\mathcal{C}_{2p^i} - 2\mathcal{C}_{4p^i} + 2\mathcal{C}_{2p^i} - 2\mathcal{C}_{4p^i} \right) \right]
\]

\[
\theta_{2p^n}(x) = \frac{1}{4p^2} \left[ \mathcal{C}_0 - \mathcal{C}_{p^n} + \mathcal{C}_{2p^n} - \sum_{i=0}^{n-1} \left( \mathcal{C}_{p^i} - \mathcal{C}_{2p^i} - \mathcal{C}_{4p^i} + \mathcal{C}_{p^i} + \mathcal{C}_{2p^i} - \mathcal{C}_{4p^i} - \mathcal{C}_{8p^i} \right) \right]
\]

\[
\theta_{2p^n}(x) = \frac{1}{4p^2} \left[ \frac{-\phi(p^{n-j})}{p}, \mathcal{C}_0 - \mathcal{C}_{p^n} + \mathcal{C}_{2p^n} - \sum_{i=-n}^{n-1} \left( \mathcal{C}_{p^i} - \mathcal{C}_{2p^i} - \mathcal{C}_{4p^i} + \mathcal{C}_{p^i} + \mathcal{C}_{2p^i} - \mathcal{C}_{4p^i} + \mathcal{C}_{8p^i} \right) \right] + \frac{1}{p^2} \sum_{i=0}^{n-1} \left\{ D_{i+j} \mathcal{C}_{p^i} + F_{i+j} \mathcal{C}_{2p^i} + F_{i+j} \mathcal{C}_{4p^i} + D_{i+j} \mathcal{C}_{p^i} + C_{i+j} \mathcal{C}_{8p^i} + E_{i+j} \mathcal{C}_{8p^i} + E_{i+j} \mathcal{C}_{8p^i} + C_{i+j} \mathcal{C}_{8p^i} \right\}
\]
\[
\theta_{4p'}(x) = \frac{1}{4p'} \left( \frac{\phi(p^n - j)}{2} \{ C_0 + C_{2p'} + C_{22p'} \} + \frac{\phi(p^n - j)}{2} \sum_{i=j}^{n-1} \{ C_{p'} + C_{2p'} + C_{4p'} + C_{2p'} + C_{42p'} + C_{44p'} \} + \frac{1}{p'} \sum_{i=0}^{n-j-1} \{ F_{i+j} C_{p'} + F_{i+j} C_{2p'} + F_{i+j} C_{4p'} + E_{i+j} C_{2p'} + E_{i+j} C_{22p'} + E_{i+j} C_{42p'} + E_{i+j} C_{44p'} \} \right)
\]

\[
\theta_{2gp'}(x) = \frac{1}{4p'} \left( \frac{\phi(p^n - j)}{2} \{ C_0 - C_{2p'} + C_{22p'} \} - \frac{\phi(p^n - j)}{2} \sum_{i=n-j}^{n-1} \{ C_{p'} - C_{2p'} - C_{4p'} + C_{p'} + C_{2p'} - C_{42p'} + C_{44p'} \} + \frac{1}{p'} \sum_{i=0}^{n-j-1} \{ C_{i+j} C_{p'} + E_{i+j} C_{2p'} + C_{i+j} C_{4p'} + D_{i+j} C_{2p'} + F_{i+j} C_{22p'} + D_{i+j} C_{42p'} \} \right)
\]

\[
\theta_{4gp'}(x) = \frac{1}{4p'} \left( \frac{\phi(p^n - j)}{2} \{ C_0 + C_{2p'} + C_{22p'} \} + \frac{\phi(p^n - j)}{2} \sum_{i=n-j}^{n-1} \{ C_{p'} + C_{2p'} + C_{4p'} + C_{2p'} + C_{42p'} + C_{44p'} \} + \frac{1}{p'} \sum_{i=0}^{n-j-1} \{ E_{i+j} C_{p'} + E_{i+j} C_{2p'} + E_{i+j} C_{4p'} + F_{i+j} C_{2p'} + F_{i+j} C_{22p'} + F_{i+j} C_{42p'} \} \right)
\]

for \(-\Omega_{p'} = \Omega_{p'}
\]

\[
\theta_{p'}(x) = \frac{1}{4p'} \left( \frac{\phi(p^n - j)}{2} \{ C_0 - C_{2p'} \} - \frac{\phi(p^n - j)}{2} \sum_{i=n-j}^{n-1} \{ C_{2p'} - C_{4p'} + C_{2p'} - C_{42p'} \} + \frac{1}{p'} \sum_{i=0}^{n-j-1} \{ B_{i+j} C_{p'} + D_{i+j} C_{2p'} + F_{i+j} C_{4p'} - B_{i+j} C_{22p'} + A_{i+j} C_{42p'} + E_{i+j} C_{44p'} - A_{i+j} C_{24p'} \} \right)
\]

\[
\theta_{\lambda p'}(x) = \frac{1}{4p'} \left( \frac{\phi(p^n - j)}{2} \{ C_0 - C_{2p'} \} + \frac{\phi(p^n - j)}{2} \sum_{i=n-j}^{n-1} \{ C_{2p'} - C_{4p'} + C_{2p'} - C_{42p'} \} - \frac{1}{p'} \sum_{i=0}^{n-j-1} \{ B_{i+j} C_{p'} + D_{i+j} C_{2p'} + F_{i+j} C_{4p'} - B_{i+j} C_{22p'} + A_{i+j} C_{42p'} + E_{i+j} C_{44p'} - A_{i+j} C_{24p'} \} \right)
\]

\[
\theta_{gp'}(x) = \frac{1}{4p'} \left( \frac{\phi(p^n - j)}{2} \{ C_0 - C_{2p'} \} + \frac{\phi(p^n - j)}{2} \sum_{i=n-j}^{n-1} \{ C_{2p'} - C_{4p'} + C_{2p'} - C_{42p'} \} + \frac{1}{p'} \sum_{i=0}^{n-j-1} \{ A_{i+j} C_{p'} + C_{i+j} C_{2p'} + E_{i+j} C_{4p'} - A_{i+j} C_{22p'} + B_{i+j} C_{42p'} + D_{i+j} C_{44p'} \} \right)
\]

\[
\theta_{\lambda gp'}(x) = \frac{1}{4p'} \left( \frac{\phi(p^n - j)}{2} \{ C_0 - C_{2p'} \} + \frac{\phi(p^n - j)}{2} \sum_{i=n-j}^{n-1} \{ C_{2p'} - C_{4p'} + C_{2p'} - C_{42p'} \} - \frac{1}{p'} \sum_{i=0}^{n-j-1} \{ A_{i+j} C_{p'} + C_{i+j} C_{2p'} + E_{i+j} C_{4p'} - A_{i+j} C_{22p'} + B_{i+j} C_{42p'} + D_{i+j} C_{44p'} \} \right)
\]

and for \(-\Omega_{p'} = \Omega_{\lambda p'}
\]

\[
\theta_{p'}(x) = \frac{1}{4p'} \left( \frac{\phi(p^n - j)}{2} \{ C_0 - C_{2p'} \} - \frac{\phi(p^n - j)}{2} \sum_{i=n-j}^{n-1} \{ C_{2p'} - C_{4p'} + C_{2p'} - C_{42p'} \} - \frac{1}{p'} \sum_{i=0}^{n-j-1} \{ B_{i+j} C_{p'} + D_{i+j} C_{2p'} + F_{i+j} C_{4p'} - B_{i+j} C_{22p'} + A_{i+j} C_{42p'} + E_{i+j} C_{44p'} - A_{i+j} C_{24p'} \} \right)
\]

\[
\theta_{\lambda p'}(x) = \frac{1}{4p'} \left( \frac{\phi(p^n - j)}{2} \{ C_0 - C_{2p'} \} + \frac{\phi(p^n - j)}{2} \sum_{i=n-j}^{n-1} \{ C_{2p'} - C_{4p'} + C_{2p'} - C_{42p'} \} + \frac{1}{p'} \sum_{i=0}^{n-j-1} \{ B_{i+j} C_{p'} + D_{i+j} C_{2p'} + F_{i+j} C_{4p'} - B_{i+j} C_{22p'} + A_{i+j} C_{42p'} + E_{i+j} C_{44p'} - A_{i+j} C_{24p'} \} \right)
\]

\[
\theta_{gp'}(x) = \frac{1}{4p'} \left( \frac{\phi(p^n - j)}{2} \{ C_0 - C_{2p'} \} + \frac{\phi(p^n - j)}{2} \sum_{i=n-j}^{n-1} \{ C_{2p'} - C_{4p'} + C_{2p'} - C_{42p'} \} + \frac{1}{p'} \sum_{i=0}^{n-j-1} \{ A_{i+j} C_{p'} + C_{i+j} C_{2p'} + E_{i+j} C_{4p'} - B_{i+j} C_{22p'} - A_{i+j} C_{42p'} + C_{i+j} C_{44p'} \} \right)
\]

\[
\theta_{\lambda gp'}(x) = \frac{1}{4p'} \left( \frac{\phi(p^n - j)}{2} \{ C_0 - C_{2p'} \} - \frac{\phi(p^n - j)}{2} \sum_{i=n-j}^{n-1} \{ C_{2p'} - C_{4p'} + C_{2p'} - C_{42p'} \} + \frac{1}{p'} \sum_{i=0}^{n-j-1} \{ A_{i+j} C_{p'} + C_{i+j} C_{2p'} + E_{i+j} C_{4p'} - B_{i+j} C_{22p'} + A_{i+j} C_{42p'} + C_{i+j} C_{44p'} \} \right)
\]
where $A_{i+j}$, $B_{i+j}$, $C_{i+j}$, $D_{i+j}$, $E_{i+j}$ and $F_{i+j}$ are given by:

$$C_{n-1} = \frac{1}{2} p^{n-1} (\sqrt{p} + 1), \quad D_{n-1} = \frac{1}{2} p^{n-1} (1 - \sqrt{p}).$$

$$E_{n-1} = \frac{1}{2} p^{n-1} (\sqrt{p} - 1), \quad F_{n-1} = \frac{1}{2} p^{n-1} (-\sqrt{p} - 1).$$

For $-\Omega_{p^i} = \Omega_{p^i}$.

$$A_{n-1} = \sqrt{p^{2n-1}}, \quad B_{n-1} = 0$$

for $-\Omega_{p^i} = \Omega_{\lambda p^i}$.

$$A_{n-1} = [\sqrt{-3p^{2n-1}}], \quad B_{n-1} = 0$$

and for all $j \leq n - 2$,

$$A_j = B_j = C_j = D_j = E_j = F_j = 0.$$

**Proof.** By definition,

$$\theta_k(x) = \frac{1}{4p} \left[ \varepsilon_0 \bar{C}_0 + \varepsilon_{p^n} \bar{C}_{p^n} + \varepsilon_{2p^n} \bar{C}_{2p^n} + \sum_{i=0}^{n-1} \left\{ \varepsilon_{p^i} \bar{C}_{p^i} + \varepsilon_{2p^i} \bar{C}_{2p^i} + \varepsilon_{4p^i} \bar{C}_{4p^i} + \varepsilon_{\lambda p^i} \bar{C}_{\lambda p^i} + \varepsilon_{\lambda^2 p^i} \bar{C}_{\lambda^2 p^i} + \varepsilon_{\lambda^3 p^i} \bar{C}_{\lambda^3 p^i} \right\} \right].$$

To evaluate $\theta_0(x)$, take $s = 0$, then $\varepsilon_0 = \sum_{s \in \Omega} \alpha^0 = 1$ for all $0 \leq k \leq 4p^n - 1$. Therefore,

$$\theta_0(x) = \frac{1}{4p} \left[ \bar{C}_0 + \bar{C}_{p^n} + \bar{C}_{2p^n} + \sum_{i=0}^{n-1} \left\{ \bar{C}_{p^i} + \bar{C}_{2p^i} + \bar{C}_{4p^i} + \bar{C}_{\lambda p^i} + \bar{C}_{\lambda^2 p^i} + \bar{C}_{\lambda^3 p^i} \right\} \right].$$

For the evaluation of $\theta_{p^n}(x)$, take $s = p^n$, so we have to compute $\varepsilon_{p^n}^n$ for $k = 0, p^n, 2p^n, 3p^n, p^i, 2p^i, 4p^i, \lambda p^i, gp^i, 2gp^i, 4gp^i, \lambda gp^i$. Here,

$$\varepsilon_{p^n}^n = \sum_{s \in \Omega^{p^n}} \alpha^{-sk} \equiv \alpha^{p^n k}.$$

Therefore, $\varepsilon_{p^n}^n = \sum_{s \in \Omega^{p^n}} \alpha^{-sk} \equiv \alpha^{p^n k}$. Therefore,

$$\varepsilon_0 = -\varepsilon_{p^n}^n = -\varepsilon_{2p^n}^n = -\varepsilon_{4p^n}^n = \varepsilon_{\lambda p^n}^n = \varepsilon_{\lambda^2 p^n}^n = \varepsilon_{\lambda^3 p^n}^n = 2.$$

$$\varepsilon_p = \varepsilon_{4p} = -\varepsilon_{4p} = \varepsilon_{\lambda 4p} = \varepsilon_{\lambda^2 4p} = \varepsilon_{\lambda^3 4p} = 0.$$

$$\theta_{p^n}(x) = \frac{1}{2p^n} (\bar{C}_0 - \bar{C}_{2p^n} - \frac{\varepsilon_0^{p^n}}{2} \sum_{i=0}^{n-1} \left\{ \bar{C}_{2p^i} + \bar{C}_{4p^i} + \bar{C}_{\lambda p^i} + \bar{C}_{\lambda^2 p^i} + \bar{C}_{\lambda^3 p^i} \right\}).$$

Similarly $\theta_{p^i}(x)$ can be obtained.

Further to evaluate $\theta_{p^i}(x)$, take $s = p^i$ so we have to compute $\varepsilon_{p^i}^i$ for $k = 0, p^n, 2p^n, 3p^n, p^i, 2p^i, 4p^i, \lambda p^i, gp^i, 2gp^i, 4gp^i, \lambda gp^i$.

$$\varepsilon_{p^i}^i = \sum_{s \in \Omega^{p^i}} \alpha^{-sk} \equiv \sum_{s \in \Omega^{p^i}} \alpha^{p^i k}.$$ 

Therefore, using lemma 3.6 - 3.8.

$$\varepsilon_0 = -\varepsilon_{2p^n} = \frac{\varepsilon_0^{p^n}}{2}.$$

$$\varepsilon_{p^i} = 0.$$ 

$$\sum_{s \in \Omega^{p^i} \cap p^n} \alpha^{p^i s} = \sum_{s \in \Omega^{p^i} \cap 2p^n} \alpha^{p^i s} = \left\{ \begin{array}{ll} 0, & \text{if } i + j \geq n, \\ \frac{1}{p^n} A_{i+j}, & \text{if } i + j \leq n - 1. \end{array} \right.$$

$$\sum_{s \in \Omega^{p^i} \cap \lambda p^n} \alpha^{p^i s} = \sum_{s \in \Omega^{p^i} \cap \lambda^2 p^n} \alpha^{p^i s} = \left\{ \begin{array}{ll} 0, & \text{if } i + j \geq n, \\ \frac{1}{p^n} B_{i+j}, & \text{if } i + j \leq n - 1. \end{array} \right.$$

$$\sum_{s \in \Omega^{p^i} \cap \lambda^3 p^n} \alpha^{p^i s} = \left\{ \begin{array}{ll} \frac{\varepsilon_0^{p^n}}{2}, & \text{if } i + j \geq n \\ \frac{1}{p^n} C_{i+j}, & \text{if } i + j \leq n - 1. \end{array} \right.$$

16715
\[
\sum_{s \in \Omega_{2p^\ell}} \alpha^{p^\ell}_s = \begin{cases} 
-\frac{\phi(p^{n-j})}{p^j}, & if\ i + j \geq n \\
\frac{1}{p^j}D_{i+j}, & if\ i + j \leq n - 1.
\end{cases}
\]

\[
\sum_{s \in \Omega_{4p^\ell}} \alpha^{p^\ell}_s = \begin{cases} 
\phi(p^{n-j}), & if\ i + j \geq n \\
\frac{1}{p^j}F_{i+j}, & if\ i + j \leq n - 1.
\end{cases}
\]

\[
\sum_{s \in \Omega_{4p}} \alpha^{p}_s = \begin{cases} 
\phi(p^{n-j}), & if\ i + j \geq n \\
\frac{1}{p^j}F_{i+j}, & if\ i + j \leq n - 1.
\end{cases}
\]

So, \( \theta_{p^\ell}(x) = \frac{1}{4p^\ell}[\phi(p^{n-j})\{C_0 - C_{2p^\ell}\} - \phi(p^{n-j}) \sum_{i=n-j}^{n-1} \{C_{2p^\ell} - C_{4p^\ell} + C_{2gp^\ell} - C_{4gp^\ell}\} +
\]

\[
\frac{1}{p^j} \sum_{i=0}^{n-j-1} \{C_{i+j}C_{p^\ell} + F_{i+j}C_{2p^\ell} + H_{i+j}C_{4p^\ell} - C_{i+j}C_{4gp^\ell} + A_{i+j}C_{gp^\ell} + E_{i+j}C_{2gp^\ell} + G_{i+j}C_{4gp^\ell} - A_{i+j}C_{4gp^\ell}\}
\]

Similarly using lemma 3.6-3.8, we can evaluate \( \theta_{2p^\ell}(x), \theta_{4p^\ell}(x), \theta_{gp^\ell}(x), \theta_{2gp^\ell}(x), \theta_{4gp^\ell}(x) \) and \( \theta_{gp^\ell}(x) \).

Further, the relations for \( A_j, B_j, C_j, D_j, E_j \) and \( F_j \) can be obtained by using the relation \( \theta_{p^\ell}(\alpha^{p^\ell}) = 1, \theta_{p^\ell}(\alpha^{gp^\ell}) = 0, \theta_{gp^\ell}(\alpha^{2p^\ell}) = 1 \) and \( \theta_{4p^\ell}(\alpha^{4p^\ell}) = 1 \) and lemma 3.4-3.9.

Similarly we can find \( \Omega_{p^\ell}(x) \) when \( \Omega_{p^\ell} = -\Omega_{\lambda_{p^\ell}}. \)

Expressions in the following theorem 3.11–3.12 can be obtained on similar lines as in theorem 3.10 and using lemma 3.4–3.9.

**Theorem 3.2** For \( p \equiv 3(\text{mod} \ 4) \) the explicit expression for the \((6n + 3)\) primitive idempotents in \( R_{4p^n} \) are given by

\[
\theta_0(x) = \frac{1}{4p^\ell}[C_0 + C_{p^\ell} + C_{2p^\ell} + \sum_{i=0}^{n-1} \{C_{2p^\ell} + C_{4p^\ell} + C_{2gp^\ell} + C_{4gp^\ell}\}]
\]

\[
\theta_{p^\ell}(x) = \frac{1}{4p^\ell}[2C_0 - 2C_{2p^\ell} - \sum_{i=0}^{n-1} \{2C_{2p^\ell} - 2C_{4p^\ell} + 2C_{2gp^\ell} - 2C_{4gp^\ell}\}]
\]

\[
\theta_{2p^\ell}(x) = \frac{1}{4p^\ell}[C_0 - C_{p^\ell} + C_{2p^\ell} - \sum_{i=0}^{n-1} \{C_{2p^\ell} - 2C_{4p^\ell} + 2C_{4gp^\ell} - 2C_{4gp^\ell}\}]
\]

\[
\theta_{2p^\ell}(x) = \frac{1}{4p^\ell}[C_0 - C_{p^\ell} + C_{2p^\ell} - \sum_{i=0}^{n-1} \{C_{2p^\ell} - C_{4p^\ell} + C_{2gp^\ell} - C_{4gp^\ell}\}]
\]

\[
\theta_{4p^\ell}(x) = \frac{1}{4p^\ell}[\phi(p^{n-j})\{C_0 - C_{2p^n} - \phi(p^{n-j}) \sum_{i=n-j}^{n-1} \{C_{2p^\ell} - C_{4p^\ell} + C_{2gp^\ell} - C_{4gp^\ell}\} + \frac{1}{p^j} \sum_{i=0}^{n-j-1} \{C_{i+j}C_{p^\ell} + E_{i+j}C_{2p^\ell} + E_{i+j}C_{4p^\ell} + F_{i+j}C_{2gp^\ell} + F_{i+j}C_{4gp^\ell}\}]
\]

\[
\theta_{4p^\ell}(x) = \frac{1}{4p^\ell}[\phi(p^{n-j})\{C_0 + C_{p^\ell} - C_{2p^\ell} \sum_{i=n-j}^{n-1} \{C_{p^\ell} - C_{2p^\ell} - C_{4p^\ell} + C_{2gp^\ell} - C_{4gp^\ell}\} + \frac{1}{p^j} \sum_{i=0}^{n-j-1} \{E_{i+j}C_{p^\ell} + E_{i+j}C_{2p^\ell} + E_{i+j}C_{4p^\ell} + F_{i+j}C_{2gp^\ell} + F_{i+j}C_{4gp^\ell}\}]
\]

\[
\theta_{2gp^\ell}(x) = \frac{1}{4p^\ell}[\phi(p^{n-j})\{C_0 - C_{p^\ell} + C_{2p^\ell} - \phi(p^{n-j}) \sum_{i=n-j}^{n-1} \{C_{p^\ell} - C_{2p^\ell} - C_{4p^\ell} + C_{2gp^\ell} - C_{4gp^\ell}\} + \frac{1}{p^j} \sum_{i=0}^{n-j-1} \{B_{i+j}C_{p^\ell} + 2D_{i+j}C_{2p^\ell} + 2E_{i+j}C_{4gp^\ell}\}]
\]

\[
\theta_{2gp^\ell}(x) = \frac{1}{4p^\ell}[\phi(p^{n-j})\{C_0 - C_{p^\ell} + C_{2p^\ell} - \phi(p^{n-j}) \sum_{i=n-j}^{n-1} \{C_{p^\ell} - C_{2p^\ell} - C_{4p^\ell} + C_{2gp^\ell} - C_{4gp^\ell}\} +
\]

©Research India Publications. http://www.ripublication.com
\[
\frac{1}{p^j} \sum_{i=0}^{n-j-1} \left( D_{i+j} C_{p^j} + F_{i+j} C_{2p^j} + F_{i+j} C_{4p^j} + C_{i+j} C_{gp^j} + E_{i+j} C_{2gp^j} + E_{i+j} C_{4gp^j} \right)
\]
\[
\theta_{4gp^j}(x) = \frac{1}{q^j} \left\{ \phi(p^{n-j}) \right\} \left( C_0 + C_{p^n} + C_{2p^n} \right) + \frac{\phi(p^{n-j})}{2} \sum_{i=0}^{n-j} \left( C_{p^i} + C_{2p^i} + C_{4p^i} + C_{gp^i} + C_{2gp^i} + C_{4gp^i} \right)
\]
\[
\frac{1}{p^j} \sum_{i=0}^{n-j-1} \left( F_{i+j} C_{p^j} + F_{i+j} C_{2p^j} + F_{i+j} C_{4p^j} + E_{i+j} C_{2gp^j} + E_{i+j} C_{4gp^j} \right)
\]
\[
A_{n-1} = 0, \quad B_{n-1} = 0, \quad C_{n-1} = \frac{p^n}{2} (1 + \sqrt{-p}), \quad D_{n-1} = \frac{p^n}{2} (1 - \sqrt{-p}),
\]
\[
E_{n-1} = \frac{p^n}{2} (\sqrt{-p} - 1), \quad F_{n-1} = -\frac{p^n}{2} (\sqrt{-p} + 1),
\]
\[
\text{for all } j \leq n - 2, \quad A_j = B_j = C_j = D_j = E_j = F_j = 0.
\]

4. Dimension and Generating Polynomials

If \( \alpha \) is primitive \( 4p^n \)th root of unity in some extension field of \( F \), then \( m_s(x) = \prod_{s \in \Omega_s} (x - \alpha^s) \) denote the minimal polynomial for \( \alpha^s \).

If \( m_s(x) \) denote the minimal polynomial for \( \alpha^s, s \in \Omega_s \), then the generating polynomial for cyclic code \( M_s \) of length \( 4p^n \) corresponding to the cyclotomic coset \( \Omega_s \) is \( \frac{x^{4p^n} - 1}{m_s(x)} \) and the dimension of minimal cyclic code \( M_s \) is equal to the cardinality of the class \( \Omega_s \) [11].

Thus the dimensions of the codes \( M_0, M_{p^n}, M_{2p^n}, M_{p^2}, M_{4p^2}, M_{\lambda p^2}, M_{gp^2}, M_{2gp^2}, M_{4gp^2} \) and \( M_{\lambda gp^2} \) are \( 1, 2, 1, \frac{p^n}{2}, \frac{p^n}{2}, \frac{p^n}{2}, \frac{p^n}{2}, \frac{p^n}{2} \) and \( \frac{p^n}{2} \) respectively.

**Theorem 4.1** (i) The generating polynomial for the codes \( M_0, M_{p^n} \) and \( M_{2p^n} \) are \( (1 + x + x^2 + \ldots + x^{4p^n-1}) \), \((x^2 - 1)(1 + x + \ldots + x^{4(p^n-1)})\) and \((x^2 + 1)(1 + x + \ldots + x^{4p^n-1})\) respectively.

(ii) The generating polynomial for \( M_{2p^2} \oplus M_{2gp^2} \) and \( M_{4p^2} \oplus M_{4gp^2} \) are \( (x^{4p^{n-1}} + 1)(x^{p^{n-1}} - 1)(x^{2p^{n-1}} + 1)(1 + x^{4p^{n-1}} + \ldots + x^{4p^{n-1}(p-1)}) \) respectively.

(iii) For \( p \equiv 1(\mod 4) \), the generating polynomial for \( M_{p^2} \oplus M_{p^2} \oplus M_{p^2} \oplus M_{p^2} \oplus M_{p^2} \oplus M_{p^2} \oplus M_{p^2} \) is \( (x^{2p^{n-1}} + 1)(x^{p^{n-1}} - 1)(1 + x^{4p^{n-1}} + \ldots + x^{4p^{n-1}(p-1)}) \).

(iv) For \( p \equiv 3(\mod 4) \), the generating polynomial for \( M_{p^2} \oplus M_{p^2} \) is \( (x^{2p^{n-1}} + 1)(x^{p^{n-1}} - 1)(1 + x^{4p^{n-1}} + \ldots + x^{4p^{n-1}(p-1)}) \).

**Proof.** (i) The minimal polynomial for \( \alpha^0, \alpha^p \) and \( \alpha^{2p^n} \) are \((x - 1)^2, (x^2 - \mu^2), (x + 1) \) and \((x + \mu) \) respectively. The corresponding generating polynomials are \((1 + x + x^2 + \ldots + x^{4p^n-1})\), \((x^2 - 1)(1 + x + \ldots + x^{4p^n-1})\), \((x^2 + 1)(x^2 + 1 + x^2 + \ldots + x^{4p^n-1})\) and \((x^2 + 1)(x^2 + 1)(1 + x^2 + \ldots + x^{4p^n-1})\).

(ii) The product of minimal polynomial satisfied by \( \alpha^{2p^n} \) and \( \alpha^{2gp^n} \) is \( \frac{x^{4p^{n-1}} + 1}{x^{2p^{n-1}} + 1} \). Therefore, the generating polynomial for \( M_{2p^{n}} \oplus M_{4p^{n}} \) is \((x^{p^{n-1}} + 1)(x^{2p^{n-1}} + 1)(1 + x^{4p^{n-1}} + \ldots + x^{4p^{n-1}(p-1)})\).

(iii) The product of minimal polynomial satisfied by \( \alpha^{4p^n} \) and \( \alpha^{2gp^n} \) is \( \frac{x^{2p^{n-1}} + 1}{x^{2p^{n-1}} + 1} \). Therefore, the generating polynomial for \( M_{4p^{n}} \oplus M_{4gp^{n}} \) is \((x^{p^{n-1}} - 1)(x^{2p^{n-1}} + 1)(1 + x^{4p^{n-1}} + \ldots + x^{4p^{n-1}(p-1)})\). Also the product of minimal polynomial satisfied by \( \alpha^{p^n}, \alpha^{gp^n}, \alpha^{4p^n} \) and \( \alpha^{4gp^n} \) is \( \frac{x^{2p^{n-1}} + 1}{x^{2p^{n-1}} + 1} \). Therefore, the generating polynomial for \( M_{p^{n}} \oplus M_{p^{n}} \oplus M_{p^{n}} \oplus M_{p^{n}} \) is \((x^{2p^{n-1}} + 1)(x^{2p^{n-1}} + 1)(1 + x^{4p^{n-1}} + \ldots + x^{4p^{n-1}(p-1)})\).

5. Minimum Distance Bounds

**Lemma 5.1** If \( l \) is a cyclic code of length \( m \) generated by \( g(x) \) and its minimum distance is \( d \), then the code \( l \) generated by \( g(x)(1 + x^m + x^{2m} + \ldots + x^{(k-1)m}) \) is a repetition code of \( l \) repeated \( k \) times and its minimum distance is \( dk \). [2]
Here, we find the minimum distance of the minimal cyclic code $M_s$, of length $4p^n$, generated by the primitive idempotent $\theta_s$.

**Theorem 5.1** The minimum distance of the codes $M_0, M_{2p}$, and $M_{2p^0}$ are $4p^n, 2p^n, 4p^n$ respectively. For $0 \leq i \leq n-1$, the minimum distance of the cyclic codes $M_2p^i, M_{2gp^i}, M_{4p^i}$ and $M_{4gp^i}$ are greater than equal to $8p^i$, and for the codes $M_{p'}, M_{gp'}, M_{\lambda p'}$ and $M_{\lambda gp'}$ are greater than equal to $4p^i$.

**Proof.** Since generating polynomial for the code $M_0$ is $(1 + x + x^2 + \ldots + x^{4p^n-1})$, which is itself a polynomial of length $4p^n$, hence its minimum distance is $4p^n$.

The minimum distance of the cyclic code $M_{2p}$ with generating polynomial $(x^2 - 1)(1 + x^4 + \ldots + x^{4(p^n-1)})$ is $2p^n$ as it is repetition code of length 4 with generating polynomial $(x^2 - 1)$, whose minimum distance is $2$ repeated $p^n$ times.

The minimum distance of the cyclic code $M_{2p^0}$ with generating polynomial $(x^3 - x^2 + x - 1)(1 + x^4 + \ldots + x^{4(p^n-1)})$ is $4p^n$ as it is repetition of the cyclic code of length 4 with generating polynomial $(x^3 - x^2 + x - 1)$ whose minimum distance is 4, repeated $p^n$ times.

Since the product of generating polynomial for the cyclic codes $M_{2p^i}$ and $M_{2gp^i}$ is $(x^{4p^n-i} + 1)$, then the minimum distance of this code say $C$ is 2. Now consider the cyclic code $C_1$ of length $2p^{n-i}$ generated by the polynomial $(x^{p^{n-i}} + 1)(x^{p^{n-i}} - 1)$, and then minimum distance of this code is 4, as it is 2 time repetition of the code $C$. Further, the minimum distance of the code $C_2$ of length $4p^{n-i}$ generated by the polynomial $(x^{p^{n-i}} - 1)(x^{p^{n-i}} - 1)(x^{2p^{n-i}} + 1)$ is $8$, as it is again 2 time repetition of the code $C_1$. Since the cyclic code of length $4p^n$ generated by the polynomial $(x^{p^{n-i}} + 1)(x^{p^{n-i}} - 1)(x^{2p^{n-i}} + 1)(1 + x^{4p^{n-i}} + \ldots x^{4p^n-i(p^n-1)})$ is a repetition code of the code $C_2$, repeated $p^n$ times. Hence its minimum distance is $8p^n$, by Lemma 5.1. The codes corresponding to $\Omega_{2p^i}$ and $\Omega_{2gp^i}$ are the sub codes of above code so, by [3, 5, 4] their minimum distance are greater than or equal to $8p^i$.

The product of generating polynomial for the cyclic codes $M_{4p^i}$ and $4gp^i$ is $(x^{4p^n-i} - 1)(x^{2p^{n-i}} + 1)(x^{2p^{n-i}} + 1)(1 + x^{4p^{n-i}} + \ldots x^{4p^n-i(p^n-1)})$. Hence, similarly as above minimum distance of cyclic codes $M_{4p^i}$ and $4gp^i$ are greater than or equal to $8p^i$.

Now the product of generating polynomial for the cyclic codes $M_{p'}, M_{gp'}, M_{\lambda p'}$ and $M_{\lambda gp'}$ is $(x^{2p^{n-i}} + 1)(x^{2p^{n-i}} - 1)(1 + x^{4p^{n-i}} + \ldots x^{4p^n-i(p^n-1)})$, therefore, if we take a code $C$ of length $4p^{n-1}$ generated by the polynomial $(x^{2p^{n-1}} + 1)(x^{2p^{n-1}} - 1)$, then the minimum distance of this code $C_1$ of length $4p^n$ generated by the polynomial $(x^{2p^{n-1}} + 1)(x^{2p^{n-1}} - 1)(1 + x^{4p^{n-i}} + \ldots x^{4p^n-i(p^n-1)})$ is a repetition code of the code $C$, repeated $p^i$ times. Hence its minimum distance is $4p^i$. The codes corresponding to $\Omega_{p'}, \Omega_{gp'}, \Omega_{\lambda p'}$ and $\Omega_{\lambda gp'}$ are the sub codes of above codes so, their minimum distances are greater than or equal to $4p^i$.

\[ \square \]

**References**


