Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 7, pp. 2769–2796
DOI : 10.47974/JDMSC-2116

Idempotent generators of cyclic codes, cyclic self-dual codes and cyclic LCD codes of length $p^t q$ over $\mathbb{Z}_4$

Kapil Kumar *
Sudhir Batra †
Department of Mathematics
Deenbandhu Chhotu Ram University of Science and Technology
Murthal
Sonipat 131039
Haryana
India

Abstract

Cyclic codes having length $p^t q$ have been studied using the primitive binary idempotent generators when $O_{p^t}(2) = \frac{\phi(p^t)}{2}$ and $O_q(2) = q-1$ with $\left(\frac{\phi(p^t)}{2}, q-1\right) = 1$. Using the expressions of these idempotent generators and the theory of cyclotomy, expressions of idempotent generators of $\mathbb{Z}_4$ – cyclic codes are obtained. In this case, all the self-dual codes and LCD codes of length $p^t q$ over $\mathbb{Z}_4$ are defined in terms of the idempotent generators. Clearly, these self-dual cyclic codes of length $p^t q$ are Type-I codes. Also, the permutational equivalence of these cyclic codes has been discussed.

Subject Classification: *94B15, 11T71, 16S34.*

Keywords: *Cyclic codes, Idempotent generators, LCD codes, Self-dual codes, Codes over $\mathbb{Z}_4$.*

1. Introduction

Hammons et al. presented construction techniques for interesting non-linear codes, including Kerdock and Delsarte-Goethals codes, as the gray images of linear $\mathbb{Z}_4$-codes [9]. The weight enumerators of many non-linear binary codes were found to satisfy MacWilliam's identity, which posed another significant challenge in coding theory. Hammons et al. also addressed this problem in [9]. These findings, along with Nechaeve's related work [20], spark a lot of interest in $\mathbb{Z}_4$-linear codes.

* *E-mail:* kapil.kumar1810@gmail.com (Corresponding Author)
† *E-mail:* batrasudhir@rediffmail.com

Furthermore,using gray map, a number of binary non-linear codes that perform better than comparable binary linear codes of the same length have been found as the images of $\mathbb{Z}_4$-linear codes.

Encoding and decoding are accomplished with efficiency via cyclic codes. Cyclic codes are a class of linear codes. So, several authors have investigated them. In [22] Pless and Qian described the structure of cyclic codes and their duals over $\mathbb{Z}_4$. They also defined $\mathbb{Z}_4$–quadratic residue codes, using their idempotent generators. They demonstrated that these codes possess multiple features that are analogous to those of quadratic residue codes over fields in various respects.

Self-dual codes over $\mathbb{Z}_4$ are classified in [5] up to length 9, whereas in [7] these are classified up to length 15. Unlike the situation of self dual codes over $\mathbb{F}_2$, there exist cyclic self dual codes of odd length over $\mathbb{Z}_4$. In [21], an existence condition for self dual codes of odd length over $\mathbb{Z}_4$ is given. It is worth noting that, as we can see in [21], in some particular cases, it is possible to directly determine the generator polynomial of a cyclic self dual code over $\mathbb{Z}_4$. In this case, we may readily determine if a certain code its extended version is categorized as type I or type II with the help of the Euclidean weight of the generating polynomial. Nonetheless, finding the explicit formulations of the generating polynomials for cyclic self-dual codes over $\mathbb{Z}_4$ is generally challenging. However, under certain general conditions, we can study cyclic self-dual codes over $\mathbb{Z}_4$ using their idempotent generators. Batra and Jain [1] obtained the explicit expressions for primitive idempotents in the ring $\frac{\mathbb{Z}_4[x]}{\langle x^{p^n}-1\rangle}$. They also discussed the conditions for $\mathbb{Z}_4$–cyclic codes to be orthogonal and self-dual Additionally, a procedure to develop self and iso dual codes over $\mathbb{Z}_4$ of length p^n was provided. In [11] Jain and Batra obtained explicit expressions of idempotent generators of $\mathbb{Z}_4$–cyclic codes of length pq and hence discussed the self dual codes(which are cyclic) of length pq over $\mathbb{Z}_4$ with the help of these idempotent generators.

The family of linear codes known as linearly complementary dual codes, or LCD codes, is another fascinating class. An LCD code is defined as a linear code $\mathcal{C}$ satisfying $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$. Due to their numerous uses LCD codes have recently received a lot of attention[2, 3]. Li et. al. [15], created numerous families of LCD cyclic codes, while Jin [12] demonstrated that some Reed-Solomon codes are similar to LCD codes. Research is also being carried out on LCD codes examined over finite Frobenius rings. Liu et. al.[16] examined linearly complementary dual codes over chain rings. A necessary and sufficient condition was provided by Liu et al. [17] for a

cyclic code over chain ring to be an LCD code. Using idempotent generators, we obtain all the LCD code over $\mathbb{Z}_4$ of length p^tq.

In the present paper, we present a method for finding all cyclic codes over $\mathbb{Z}_4$ of length p^tq. We gave these expressions in terms of the idempotent generators. Also, we describe all the self-dual codes having length p^tq which are cyclic when $O_{p^t}(2)=\frac{\phi(p^t)}{2}$ and $O_q(2)=\phi(q)$. In the study of cyclic codes over finite fields and the modular rings of integers, cyclotomy is an important tool. We apply the results on cyclotomy of [14] to obtain the expressions of the idempotent-generators of $\mathbb{Z}_4$–cyclic codes of length p^tq over when $O_{p^t}(2)=\frac{\phi(p^t)}{2}$ and $O_q(2)=q-1$. This method is more elementary to find idempotent generators. Using our construction method,we observe that there are 9^t self-dual cyclic codes over the ring of integers modulo 4 having length p^tq, when $O_{p^t}(2)=\frac{\phi(p^t)}{2}$ and 2 is a primitive root modulo q. Using the enumeration formula of corollary 3.5 of [4], we can also see that there are 9^t total $\mathbb{Z}_4$–cyclic codes which are self dual for this case. However, Chen et. al. just commented on the number of these codes in [4], and we have given the explicit expressions of idempotent generators for all of these codes for the case $n=p^tq$ over $\mathbb{Z}_4$. We also observed that out of these 9^t self-dual codes, $\frac{9^t+1}{2}$ are permutational non-equivalent. Also, since for type-II codes of length n we have $n=8k$ for some positive integer k, so these self-dual codes and their extensions are Type-I codes. Additionally, our results with $t=1$ gives the results obtained by Jain and Batra in [11] as particular case.

We also gave examples of cyclic codes over the ring of integers modulo 4 of length 21 and the symmetrized weight enumerator of these codes. In fact, the expressions of Idempotent generators obtained by us, enable us to compute the weight enumerator of these codes using a program in Wolfram Mathematica. It has been observed that the torsion codes of some of these codes are constant weight and two-weight codes. Also, examples of the extremal Type-I code of length 21 have been given.

In [23], some kind of topological indices of the idempotent graph of $\mathbb{Z}_n$ are computed. Topological indices of a graph may be applied in studying quantitative structure-activity relationships. For instance, in [6], the stability of alkanes and the strain energy of cycloalkanes were studied using a topological measure called the atom bond connectivity (ABC) index.

It will be interesting to obtain the idempotent graphs of various codes studied in our paper, which are themselves subrings of $\mathcal{R}_{p^tq}=\frac{\mathbb{F}_2[x]}{\langle x^{p^tq}-1\rangle}$ and $\mathcal{R}'_{p^tq}=\frac{\mathbb{Z}_4[x]}{\langle x^{p^tq}-1\rangle}$, and in general of the rings $\mathcal{R}_{p^tq}$ and $\mathcal{R}'_{p^tq}$, and explore some

kind of applications in the area discussed in previous paragraph, by computing various topological indices.

The notations and assumptions of the present paper are identical to those in [14]. Supplementary notations and terminologies are provided below:

(i) p and q are distinct primes. Further, $p \equiv -1 (mod\ 8)$ and $q \equiv \pm 3 (mod\ 8)$.

(ii) If A is a finite set then the cardinality of A is denoted by $|A|$.

(iii) $\mathcal{R}_{p^t q} = \frac{\mathbb{F}_2[x]}{\langle x^{p^t q} - 1 \rangle}$ and $\mathcal{R}'_{p^t q} = \frac{\mathbb{Z}_4[x]}{\langle x^{p^t q} - 1 \rangle}$

(iv) $\mathcal{S} = \{0, 1, 2, \ldots, t-1\}$.

Unless otherwise stated, all other assumptions and terminologies throughout this paper are the same as in [14]. The rest of this paper is arranged as follows:

- In section 2, we obtain the expressions of binary idempotent by obtaining the Gaussian sums with the help of the forms of cyclotomic cosets obtained in [14].
- In section 3, expressions for primitive idempotents in the ring $\frac{\mathbb{Z}_4[x]}{\langle x^{p^t q} - 1 \rangle}$ have been obtained using the results of [14] and the binary idempotents obtained in Section 2. Orthogonal properties and permutational equivalence of these codes have also been discussed. Also, some examples of cyclic codes of length 21 with their symmetrized weight enumerator have been given.
- In Section 4, all the cyclic self-dual codes and cyclic LCD codes having length $p^t q$ over $\mathbb{Z}_4$ are defined in terms of the idempotent generators. These self-dual codes are Type-I codes. We also give the examples of a Type-I extremal self-dual codes having length 21.

2. Idempotents in the ring $\mathcal{R}_{p^t q} = \frac{\mathbb{F}_2[x]}{\langle x^{p^t q} - 1 \rangle}$

The expressions of the generating idempotent of minimal ideals of the ring $\mathcal{R}_{p^t q} = \frac{\mathbb{F}_2[x]}{\langle x^{p^t q} - 1 \rangle}$ will be obtained in this section. In order to acquire these formulations, we must first recollect the following theorem on cyclotomic cosets that was established in [14].

Theorem 2.1: *[14][Theorem 2.4] "The 2-cyclotomic cosets modulo $n = p^t q$ can be represented as follow:*

1. If $q \,(mod\ p^t) \in N_0$, then

$$\Omega_0 = \{0\}$$

$$\Omega_{p^i} = \{p^i qx + p^t y \mid x \in N_i, 1 \le y \le q-1\}, 0 \le i \le t-1;$$

$$\Omega_{p^t} = \{p^t x \mid 1 \le x \le q-1\};$$

$$\Omega_{p^i q} = \{p^i qx \mid x \in R_i\}, 0 \le i \le t-1;$$

$$\Omega_{p^i g} = \{p^i qx + p^t y \mid x \in R_i, 1 \le y \le q-1\}, 0 \le i \le t-1;$$

$$\Omega_{p^i qg} = \{p^i qx \mid \ x \in N_i\}, 0 \le i \le t-1;$$

2. If $q \,(mod\ p^t) \in R_0$, then

$$\Omega_0 = \{0\}$$

$$\Omega_{p^i} = \{p^i qx + p^t y \mid x \in R_i, 1 \le y \le q-1\}, 0 \le i \le t-1;$$

$$\Omega_{p^t} = \{p^t x \mid \ 1 \le x \le q-1\};$$

$$\Omega_{p^i q} = \{p^i qx \mid x \in R_i\}, 0 \le i \le t-1;$$

$$\Omega_{p^i g} = \{p^i qx + p^t y \mid x \in N_i, 1 \le y \le q-1\}, 0 \le i \le t-1;$$

$$\Omega_{p^i qg} = \{p^i qx \mid x \in N_i\}, 0 \le i \le t-1."$$

Lemma 2.1: *Let p be an odd prime and let δ_i be an element in some extension of $\mathbb{F}_2$ such that*

$$\delta_i^{p^i} = 1 \text{ and } \delta^k \ne 1 \text{ for any } 1 \le k \le p^i - 1.$$

For each $i \in \{1, 2, 3, \ldots, t\}$, let R_i represent the set of quadratic residues modulo p^i, and let N_i represent the set of non-residues modulo p^i.

1. $\sum_{s \in R_j} \delta_i^s = \sum_{s \in N_j} \delta_i^s = 0$ for $2 \le i \le j$.
2. For $i = 1$ there always exists δ_1 such that $\sum_{s \in R_k} \delta_1^s = 1$ and $\sum_{s \in N_k} \delta_1^s = 0$ for every natural number k.

Proof: The reader is left to do the proof, which is rather simple.

Let $k \in \{0, p^i, p^t, p^i q, p^i g, p^i qg : i \in \mathcal{S}\}$, then define $X_k(x) = \sum_{s \in \Omega_k} x^s$. For the sake of convenience, we shall denote $X_k(x)$ as X_k. Let α be an element in some extension of $\mathbb{F}_2$, such that

$$\alpha^{p^t q} = 1 \text{ and } \alpha^k \neq 1 \text{ for any } 1 \leq k \leq p^t q - 1.$$

Let $\alpha^{p^i} = \gamma_i$ and $\alpha^{p^i q} = \beta_i$, for $0 \leq i \leq t$, then it is clear that for any i

$$\gamma_i^{p^{t-i} q} = 1 \text{ and } \gamma_i^k \neq 1 \text{ for any } 1 \leq k \leq p^{t-i} q - 1$$

and

$$\beta_i^{p^{t-i}} = 1 \text{ and } \beta_i^k \neq 1 \text{ for any } 1 \leq k \leq p^{t-i} - 1.$$

Also, using Lemma 2.1, with no loss of generality, it is permissible to presume that $\sum_{s \in R} \beta_{t-1}^s = 1$ and $\sum_{s \in N} \beta_{t-1}^s = 0$. Subsequently, using the forms of the cyclotomic cosets as laid out in the Theorem 2.1 and Lemma 2.1, we have the subsequent theorems.

Theorem 2.2: *If* $q \,(mod\, p^t) \in N_0$ *and* $1 \leq i \leq t-1$. *then*

1. $X_1(\alpha^j) = \begin{cases} 1; & \text{if } j \in \Omega_{p^t} \cup \Omega_{p^{t-1} g} \\ 0; & \text{otherwise} \end{cases}$

2. $X_g(\alpha^j) = \begin{cases} 1; & \text{if } j \in \Omega_{p^t} \cup \Omega_{p^{t-1}} \\ 0; & \text{otherwise} \end{cases}$

3. $X_q(\alpha^j) = \begin{cases} 1; & \text{if } j \in \Omega_0 \cup \Omega_{p^{t-1}} \cup \Omega_{p^t} \cup \Omega_{p^{t-1} qg} \\ 0; & \text{otherwise} \end{cases}$

4. $X_{qg}(\alpha^j) = \begin{cases} 1; & \text{if } j \in \Omega_0 \cup \Omega_{p^{t-1} g} \cup \Omega_{p^t} \cup \Omega_{p^{t-1} q} \\ 0; & \text{otherwise} \end{cases}$

5. $X_{p^i}(\alpha^j) = \begin{cases} 1; & \text{if } j \in \bigcup_{k=t-i}^{t-1} (\Omega_{p^k} \cup \Omega_{p^k g}) \cup \Omega_{p^{t-i-1} g} \cup \Omega_{p^t} \\ 0; & \text{otherwise} \end{cases}$

6. $X_{p^i g}(\alpha^j) = \begin{cases} 1; & \text{if } j \in \bigcup_{k=t-i}^{t-1} (\Omega_{p^k} \cup \Omega_{p^k g}) \cup \Omega_{p^{t-i-1}} \cup \Omega_{p^t} \\ 0; & \text{otherwise} \end{cases}$

7. $X_{p^i q}(\alpha^j) = \begin{cases} 1; & \text{if } j \in \bigcup_{k=t-i}^{t-1} (\Omega_{p^k} \cup \Omega_{p^k g} \cup \Omega_{p^k q} \cup \Omega_{p^k qg}) \cup \Omega_0 \cup \Omega_{p^{t-i-1}} \cup \Omega_{p^t} \cup \Omega_{p^{t-i-1} qg} \\ 0; & \text{otherwise} \end{cases}$

8. $$X_{p^i qg}(\alpha^j) = \begin{cases} 1; & \text{if } j \in \bigcup_{k=t-i}^{t-1} (\Omega_{p^k} \cup \Omega_{p^k g} \cup \Omega_{p^k q} \cup \Omega_{p^k qg}) \cup \Omega_0 \cup \Omega_{p^{t-i-1} g} \cup \Omega_{p^t} \cup \Omega_{p^{t-i-1} q} \\ 0; & \text{otherwise} \end{cases}$$

9. $$X_{p^t}(\alpha^j) = \begin{cases} 1; & \text{if } j \in \bigcup_{k=0}^{t-1} (\Omega_{p^k} \cup \Omega_{p^k g}) \cup \Omega_{p^t} \\ 0; & \text{otherwise} \end{cases}$$

Proof: We are going to prove only part 1 of the theorem, the remaining parts can be proved using similar arguments.

Now by definition, it is clear that,

$$X_1(\alpha^j) = \sum_{s \in \Omega_1} \alpha^{js} = \sum_{x \in N_0} \sum_{y=1}^{q-1} \alpha^{j(qx + p^t y)} \tag{1}$$

Now if $j \in \Omega_0$, then $j = 0$. So, by (1), $X_1(\alpha^j) = (q-1)\,|N_0| = 0$. Now if $j \in \Omega_{p^k}$, then $j = p^k q x_0 + p^t y_0$ for some $x_0 \in N_k$ and $1 \le y_0 \le q-1$. So, by (1),

$$X_1(\alpha^j) = \sum_{x \in N_0} \sum_{y=1}^{q-1} \alpha^{(p^k q x_0 + p^t y_0)(qx + p^t y)}$$

$$= \sum_{x \in N0} \alpha^{(p^k q^2 x x_0)} \sum_{y=1}^{q-1} \alpha^{(p^t)^2 y y_0} = \sum_{x \in N_0} \beta_k^{qxx_0} = 0$$

Similarlly, if $j \in \Omega_{p^k g}$, then $j = p^k q x_0 + p^t y_0$ for some $x_0 \in R_k$ and $1 \le y_0 \le q-1$. So, by (1) and Lemma 2.1

$$X_1(\alpha^j) = \sum_{x \in N_0} \beta_k^{qxx_0} = \begin{cases} 1 \text{ if } k = t-1 \\ 0 \text{ otherwise} \end{cases}$$

Now if $j \in \Omega_{p^t}$, then $j = p^t y_0$ for some $1 \le y_0 \le q-1$. So, again by (1) we have

$$X_1(\alpha^j) = \sum_{x \in N_0} \beta_k^{qxx_0} = \sum_{x \in N_0} \sum_{y=1}^{q-1} \alpha^{(p^t y_0)(qx + p^t y)} = |N_0| = 1$$

Similarly, we can show that for any k with $0 \le k \le t-1$, $X_1(\alpha^j) = 0$ if $j \in \Omega_{p^k q}$ or $j \in \Omega_{p^k qg}$ so we can say that $X_1(\alpha^j) = \begin{cases} 1; & \text{if } j \in \Omega_{p^t} \cup \Omega_{p^{t-1} g} \\ 0; & \text{otherwise} \end{cases}$

Similar arguments can be used to prove all remaining parts of the theorem.

Theorem 2.3: *If* $q \,(mod\, p^t) \in R_0$ *and* $1 \le i \le t-1$. *then*

1. $X_1(\alpha^j) = \begin{cases} 1; & \text{if } j \in \Omega_{p^t} \cup \Omega_{p^{t-1}} \\ 0; & \text{otherwise} \end{cases}$

2. $X_g(\alpha^j) = \begin{cases} 1; & \text{if } j \in \Omega_{p^t} \cup \Omega_{p^{t-1}g} \\ 0; & \text{otherwise} \end{cases}$

3. $X_q(\alpha^j) = \begin{cases} 1; & \text{if } j \in \Omega_0 \cup \Omega_{p^{t-1}} \cup \Omega_{p^t} \cup \Omega_{p^{t-1}q} \\ 0; & \text{otherwise} \end{cases}$

4. $X_{qg}(\alpha^j) = \begin{cases} 1; & \text{if } j \in \Omega_0 \cup \Omega_{p^{t-1}g} \cup \Omega_{p^t} \cup \Omega_{p^{t-1}qg} \\ 0; & \text{otherwise} \end{cases}$

5. $X_{p^i}(\alpha^j) = \begin{cases} 1; & \text{if } j \in \bigcup_{k=t-i}^{t-1} (\Omega_{p^k} \cup \Omega_{p^k g}) \cup \Omega_{p^{t-i-1}} \cup \Omega_{p^t} \\ 0; & \text{otherwise} \end{cases}$

6. $X_{p^i g}(\alpha^j) = \begin{cases} 1; & \text{if } j \in \bigcup_{k=t-i}^{t-1} (\Omega_{p^k} \cup \Omega_{p^k g}) \cup \Omega_{p^{t-i-1}g} \cup \Omega_{p^t} \\ 0; & \text{otherwise} \end{cases}$

7. $X_{p^i q}(\alpha^j) = \begin{cases} 1; & \text{if } j \in \bigcup_{k=t-i}^{t-1} (\Omega_{p^k} \cup \Omega_{p^k g} \cup \Omega_{p^k q} \cup \Omega_{p^k qg}) \cup \Omega_0 \cup \Omega_{p^{t-i-1}} \cup \Omega_{p^t} \cup \Omega_{p^t - i - 1_q} \\ 0; & \text{otherwise} \end{cases}$

8. $X_{p^i qg}(\alpha^j) = \begin{cases} 1; & \text{if } j \in \bigcup_{k=t-i}^{t-1} (\Omega_{p^k} \cup \Omega_{p^k g} \cup \Omega_{p^k q} \cup \Omega_{p^k qg}) \cup \Omega_0 \cup \Omega_{p^{t-i-1}g} \cup \Omega_{p^t} \cup \Omega_{p^{t-i-1}qg} \\ 0; & \text{otherwise} \end{cases}$

9. $X_{p^t}(\alpha^j) = \begin{cases} 1; & \text{if } j \in \bigcup_{k=0}^{t-1} (\Omega_{p^k} \cup \Omega_{p^k g}) \cup \Omega_{p^t} \\ 0; & \text{otherwise} \end{cases}$

Proof: The proof for this theorem is identical to that of Theorem 2.2.

Prior to determining the primitive idempotent expressions in the ring $\mathcal{R}_{p^t q}$, we must first establish the subsequent Lemma.

Lemma 2.2: *Let* $i \in \mathcal{S}$ *and* $j \neq 0$, *then we have*

1. $j \in \Omega_{p^i}$ *if and only if* $-j \in \Omega_{p^i g}$.
2. $j \in \Omega_{p^i q}$ *if and only if* $-j \in \Omega_{p^i qg}$.
3. $j \in \Omega_{p^t}$ *if and only if* $-j \in \Omega_{p^t}$.

Proof: As $p \equiv -1 \pmod 8$ is a prime. So, $-1 \in N$, indicating that -1 is a non-residue modulo p^t. Therefore, Theorem 2.1 makes it simple to establish the results.

We know that the primitive idempotents of the ring $\mathcal{R}_m = \frac{\mathbb{F}_q[x]}{\langle x^m - 1 \rangle}$ are the idempotent generators of the minimal cyclic codes of over $\mathbb{F}_q$ having block length m (or minimal ideals of $\mathcal{R}_m$), where $(q, m) = 1$. Now we can easily derive the primitive idempotent expressions in the ring $\mathcal{R}_{p^t q} = \frac{\mathbb{F}_2[x]}{\langle x^{p^t q} - 1 \rangle}$.

Theorem 2.4: *"[18][Theorem 6, p.220] The primitive idempotent θ_s in $\mathcal{R}_m = \frac{\mathbb{F}_q[x]}{\langle x^m - 1 \rangle}$, corresponding to $q-$cyclotomic coset C_s is given by*

$$\theta_s(x) = \sum_{i=0}^{m-1} \varepsilon_i^{(s)} x^i, \text{ where } \varepsilon_i^{(s)} = \frac{1}{m} \sum_{j \in C_s} \lambda^{-ij},$$

where λ is a primitive m^{th} root of unity in some extension of $\mathbb{F}_q$."

For the sake of convenience, for $0 \le i \le t-1$, let us define following:

- $\mathcal{A}_i = X_{p^i} + X_{p^i g} + X_{p^i q} + X_{p^i qg}$
- $\mathcal{B}_i = X_{p^i} + X_{p^i g}$
- $\mathcal{C}_i = X_{p^i q} + X_{p^i qg}$

Let θ_k denote the primitive idempotent in the ring $\mathcal{R}_{p^t q}$ corresponding to the $2-$cyclotomic coset Ω_k, where $k \in \{0, p^i, p^t, p^i q, p^i g, p^i qg \mid 0 \le i \le t-1\}$, Then using Theorem 2.2, Theorem 2.3, Theorem 2.4, Lemma 2.2, and the classical approach to obtain primitive idempotents in $\mathcal{R}_m$ as used by Mathur and Batra in [19], we can obtain the expressions of primitive idempotents in the ring $\mathcal{R}_{p^t q}$, which are given below in Theorem 2.5 and Theorem 2.6

Theorem 2.5: *If $q (mod\ p^t) \in N_0$, then for any $i \in \mathcal{S}$, we have*

1. $\theta_0 = 1 + X_{p^t} + \sum_{k=0}^{t-1} \mathcal{A}_k$
2. $\theta_1 = X_{p^{t-1}} + X_{p^t}$
3. $\theta_g = X_{p^{t-1} g} + X_{p^t}$

4. $\theta_q = 1 + X_{p^{t-1}g} + X_{p^{t-1}q} + X_{p^t}$

5. $\theta_{qg} = 1 + X_{p^{t-1}} + X_{p^{t-1}qg} + X_{p^t}$

6. $\theta_{p^i} = X_{p^t} + X_{p^{t-i-1}} + \sum_{k=t-i}^{t-1} \mathcal{B}_k$

7. $\theta_{p^i g} = X_{p^t} + X_{p^{t-i-1}g} + \sum_{k=t-i}^{t-1} \mathcal{B}_k$

8. $\theta_{p^i q} = 1 + X_{p^t} + X_{p^{t-i-1}g} + X_{p^{t-i-1}q} + \sum_{k=t-i}^{t-1} \mathcal{A}_k$

9. $\theta_{p^i qg} = 1 + X_{p^t} + X_{p^{t-i-1}} + X_{p^{t-i-1}qg} + \sum_{k=t-i}^{t-1} \mathcal{A}_k$

10. $\theta_{p^t} = X_{p^t} + \sum_{k=0}^{t-1} \mathcal{B}_k$

Theorem 2.6: *If* $q(mod\ p^t) \in R_0$, *then for any* $i \in \mathcal{S}$, *we have*

1. $\theta_0 = 1 + X_{p^t} + \sum_{k=0}^{t-1} \mathcal{A}_k$

2. $\theta_1 = X_{p^{t-1}g} + X_{p^t}$

3. $\theta_g = X_{p^{t-1}} + X_{p^t}$

4. $\theta_q = 1 + X_{p^{t-1}g} + X_{p^{t-1}qg} + X_{p^t}$

5. $\theta_{qg} = 1 + X_{p^{t-1}} + X_{p^{t-1}q} + X_{p^t}$

6. $\theta_{p^i} = X_{p^t} + X_{p^{t-i-1}g} + \sum_{k=t-i}^{t-1} \mathcal{B}_k$

7. $\theta_{p^i g} = X_{p^t} + X_{p^{t-i-1}} + \sum_{k=t-i}^{t-1} \mathcal{B}_k$

8. $\theta_{p^i q} = 1 + X_{p^t} + X_{p^{t-i-1}g} + X_{p^{t-i-1}qg} + \sum_{k=t-i}^{t-1} \mathcal{A}_k$

9. $\theta_{p^iqg} = 1 + X_{p^t} + X_{p^{t-i-1}} + X_{p^{t-i-1}q} + \sum_{k=t-i}^{t-1} \mathcal{A}_k$

10. $\theta_{p^t} = X_{p^t} + \sum_{k=0}^{t-1} \mathcal{B}_k$

3. Idempotent Generators of $\mathbb{Z}_4$–cyclic codes of length p^tq

Now following the notations of [14], for $0 \le i \le t-1$ let us define the following

- $\chi_i = X_{p^i}$ and $\chi_i^* = X_{p^ig}$
- $\tau_i = \begin{cases} X_{p^iq}; & \text{if } q(mod\ p) \in N \\ X_{p^iqg}; & \text{if } q(mod\ p) \in R \end{cases}$
- $\tau_i^* = \begin{cases} X_{p^iqg}; & \text{if } q(mod\ p) \in N \\ X_{p^iq}; & \text{if } q(mod\ p) \in R \end{cases}$

Now by the above notations and the definitions of $\mathcal{A}_i, \mathcal{B}_i, \mathcal{C}_i$, as in the previous section, we can easily observe that for $0 \le i \le t-1$, we have

- $\mathcal{A}_i = \chi_i + \chi_i^* + \tau_i + \tau_i^*$
- $\mathcal{B}_i = \chi_i + \chi_i^*$
- $\mathcal{C}_i = \tau_i + \tau_i^*$

Now, we will obtain the expressions of all the primitive idempotents in the ring $\mathcal{R}'_{p^tq} = \frac{\mathbb{Z}_4[x]}{\langle x^{p^tq}-1\rangle}$. The expressions of binary idempotents found in the preceding section can be used to obtain these expressions. Theorems 3.1 – 3.5 can be obtained by reducing the coefficients *modulo* 4 in the expressions of X_iX_j's in $\frac{\mathbb{Z}[x]}{\langle x^{p^tq}-1\rangle}$ obtained in Theorems 4.1-4.5 of [14].

Theorem 3.1: *For any* $i \in \mathcal{S}$, *we have:*

1. If $q \equiv -3(mod\ 8)$, then
   (a) $\chi_i^2 = (2u + (-1)^{t-i-1})\chi_i + 2u\chi_i^*$
   (b) $\chi_i^{*2} = 2u\chi_i + (2u + (-1)^{t-i-1})\chi_i^*$
   (c) $\tau_i^2 = (2u - (-1)^{t-i-1})\tau_i + 2u\tau_i^*$

(c) $\tau_i^2 = (2u-(-1)^{t-i-1})\tau_i + 2u\tau_i^*$

(d) $\tau_i^{*2} = 2u\tau_i + (2u-(-1)^{t-i-1})\tau_i^*$

(e) $X_{p^t}^2 = 3X_{p^t}$

2. If $q \equiv 3(mod\ 8)$, then

(a) $\chi_i^2 = (2u-(-1)^{t-i-1})\chi_i + 2u\chi_i^* + 2\tau_i^*$

(b) $\chi_i^{*2} = 2u\chi_i + (2u-(-1)^{t-i-1})\chi_i^* + 2\tau_i$

(c) $\tau_i^2 = (2u-(-1)^{t-i-1})\tau_i + 2u\tau_i^*$

(d) $\tau_i^{*2} = 2u\tau_i + (2u-(-1)^{t-i-1})\tau_i^*$

(e) $X_{p^t}^2 = X_{p^t} + 2$

Theorem 3.2: *Let* $i \in \mathcal{S}$. *Then, we have:*

1. If $q \equiv -3(mod\ 8)$, then

(a) $\chi_i.\tau_i = \chi_i^*.\tau_i^* = (2u-(-1)^{t-i-1})\mathcal{B}_i + (-1)^{t-i}\sum_{k=1}^{t-i-1}\mathcal{B}_{i+k} + (-1)^{t-i}X_{p^t}$

(b) $\chi_i.\chi_i^* = (2u+(-1)^{t-i-1})\mathcal{B}_i + (-1)^{t-i-1}\sum_{k=1}^{t-i-1}\mathcal{B}_{i+k} + (-1)^{t-i-1}X_{p^t}$

(c) $\chi_i.\tau_i^* = (2u-(-1)^{t-i-1})\chi_i + 2u\chi_i^*$

(d) $\tau_i.\tau_i^* = (2u-(-1)^{t-i-1})\mathcal{C}_i + (-1)^{t-i}\sum_{k=1}^{t-i-1}\mathcal{C}_{i+k} + (-1)^{t-i}$

(e) $\chi_i^*.\tau_i = 2u\chi_i + (2u-(-1)^{t-i-1})\chi_i^*$

2. If $q \equiv 3(mod\ 8)$, then

(a) $\chi_i.\tau_i = \chi_i^*.\tau_i^* = (2u-(-1)^{t-i-1})\mathcal{B}_i + (-1)^{t-i}\sum_{k=1}^{t-i-1}\mathcal{B}_{i+k} + (-1)^{t-i}X_{p^t}$

(b) $\chi_i.\chi_i^* = (2u-(-1)^{t-i-1})\mathcal{B}_i + 2\mathcal{C}_i + (-1)^{t-i}\sum_{k=1}^{t-i-1}\mathcal{B}_{i+k} + 2\sum_{k=1}^{t-i-1}\mathcal{C}_{i+k} + (-1)^{t-i}X_{p^t} + 2$

(c) $\chi_i.\tau_i^* = (2u-(-1)^{t-i-1})\chi_i + 2u\chi_i^*$

(d) $\tau_i.\tau_i^* = (2u-(-1)^{t-i-1})\mathcal{C}_i + (-1)^{t-i}\sum_{k=1}^{t-i-1}\mathcal{C}_{i+k} + (-1)^{t-i}$

(e) $\chi_i^*.\tau_i = 2u\chi_i + (2u-(-1)^{t-i-1})\chi_i^*$

Theorem 3.3: *Let* $i \in \mathcal{S}$, *we have:*

1. If $q \equiv -3(mod\ 8)$, then

(a) $\chi_i . X_{p^t} = 3\chi_i$

(b) $\chi_i^* . X_{p^t} = 3\chi_i^*$

(c) $\tau_i . X_{p^t} = \chi_i^*$

(d) $\tau_i^* . X_{p^t} = \chi_i$

2. If $q \equiv 3 (mod\ 8)$, then

(a) $\chi_i . X_{p^t} = \chi_i + 2\tau_i^*$

(b) $\chi_i^* . X_{p^t} = \chi_i^* + 2\tau_i$

(c) $\tau_i . X_{p^t} = \chi_i^*$

(d) $\tau_i^* . X_{p^t} = \chi_i$

Theorem 3.4: *If* $i, j \in \mathcal{S}$, *with* $i < j$, *then*

1. If $q \equiv -3 (mod\ 8)$, then

(a) $\chi_i \chi_j = \chi_i \chi_j^* = (-1)^{t-j} \chi_i + 2\tau_i^*$

(b) $\chi_i^* \chi_j^* = (-1)^{t-j} \chi_i^* + 2\tau_i$

(c) $\chi_i \tau_j = \chi_i \tau_j^* = (-1)^{t-j} \chi_i$

(d) $\chi_i^* \tau_j^* = \tau_i \chi_j^* = (-1)^{t-j} \chi_i^*$

(e) $\tau_i \tau_j = \tau_i \tau_j^* = (-1)^{t-j} \tau_i$

(f) $\tau_i^* \tau_j^* = (-1)^{t-j} \tau_i^*$

2. If $q \equiv 3 (mod\ 8)$, then

(a) $\chi_i \chi_j = \chi_i \chi_j^* = (-1)^{t-j-1} \chi_i$

(b) $\chi_i^* \chi_j^* = (-1)^{t-j-1} \chi_i^*$

(c) $\chi_i \tau_j = \chi_i \tau_j^* = (-1)^{t-j} \chi_i$

(d) $\chi_i^* \tau_j^* = \tau_i \chi_j^* = (-1)^{t-j} \chi_i^*$

(e) $\tau_i \tau_j = \tau_i \tau_j^* = (-1)^{t-j} \tau_i$

(f) $\tau_i^* \tau_j^* = (-1)^{t-j} \tau_i^*$

Theorem 3.5: *If* $i, j \in \mathcal{S}$, *with* $j < i$, *then*

1. If $q \equiv -3 (mod\ 8)$, then
   (a) $\chi_i \tau_j = \tau_i \chi_j^* = (-1)^{t-i} \chi_j^*$
   (b) $\chi_i \tau_j^* = \chi_i^* \tau_j^* = (-1)^{t-i} \chi_j$
   (c) $\chi_i \chi_j^* = (-1)^{t-i-1} \chi_j^*$
   (d) $\tau_i \tau_j^* = (-1)^{t-i} \tau_j^*$

2. If $q \equiv 3 (mod\ 8)$, then
   (a) $\chi_i \tau_j = \tau_i \chi_j^* = (-1)^{t-i} \chi_j^*$
   (b) $\chi_i \tau_j^* = \chi_i^* \tau_j^* = (-1)^{t-i} \chi_j$
   (c) $\chi_i \chi_j^* = (-1)^{t-i} \chi_j^* + 2\tau_j$
   (d) $\tau_i \tau_j^* = (-1)^{t-i} \tau_j^*$

Theorems 3.7-3.8 provide an expression for primitive idempotents in $\mathcal{R}'_{p^t q}$. To derive these expressions, we require specific results from the subsequent theorem.

Theorem 3.6: *[13] "Suppose p is a prime not dividing n and suppose* $x^n - 1 = f_1 f_2 \cdots f_r$ *is the representation of* $x^n - 1$ *as a product of basic irreducible, pairwise-coprime polynomials in* $\mathbb{Z}_{p^m}[x]$. *Suppose* $e_1, e_2 \ldots, e_r \in \frac{\mathbb{Z}_p[x]}{\langle x^n - 1 \rangle}$ *are primitive idempotents with* $(\mu \hat{f}_i) = (e_i)$. *For* $1 \le i \le r$, *let* $\theta_i = e_i^{p^{m-1}}$ *viewed as elements of* $\frac{\mathbb{Z}p^m[x]}{\langle x^n - 1 \rangle}$. *Then*

1. for each i with $1 \le i \le r$, θ_i is an idempotent generator of the cyclic $\mathbb{Z}_{p^m}$-code $\hat{f}_i$,
2. $\sum_{i=1}^{r} \theta_i \equiv 1$ and for $1 \le i, j \le r$ with $i \ne j$, $\theta_i \theta_j \equiv 0$,
3. Each idempotent in $\frac{\mathbb{Z}p^m[x]}{\langle x^n - 1 \rangle}$ is a sum of θ_i*s."*

Finally, note that *p* is a prime and 8 divides $p+1$, hence let $p = 8u - 1$, leading to $u = \frac{p+1}{8}$.

Theorems 3.7-3.8, which provide the expressions for primitive idempotents in $\mathcal{R}'_{p^t q}$, are now presented. The proofs of these theorems

can be obtained by combining the results of the previous section with Theorem 3.6 and the relevant findings in Theorems 3.1-3.5.

Let us denote the primtive idempotents in the ring $\mathcal{R}'_{p^tq}$ as θ'_k, for $k \in \{0,\ p^i, p^t,\ p^iq, p^ig,\ p^iqg\ :\ i \in \mathcal{S}\}$.

Theorem 3.7: *If* $q(mod\ p^t) \in N_0$ *and* $i \in \mathcal{S}$, *then*

1. If $q \equiv -3(mod\ 8)$, then

   (a) $\theta'_0 = (-1)^t(\sum_{k=0}^{t-1}\mathcal{A}_k + X_{p^t} + 1)$

   (b) $\theta'_1 = (2u+3)X_{p^{t-1}} + 2uX_{p^{t-1}g} + 3X_{p^t}$

   (c) $\theta'_g = 2uX_{p^{t-1}} + (2u+3)X_{p^{t-1}g} + 3X_{p^t}$

   (d) $\theta'_q = 2u(X_{p^{t-1}} + X_{p^{t-1}qg}) + (2u+1)(X_{p^{t-1}g} + X_{p^{t-1}q}) + X_{p^t} + 1$

   (e) $\theta'_{qg} = (2u+1)(X_{p^{t-1}} + X_{p^{t-1}qg}) + 2u(X_{p^{t-1}g} + X_{p^{t-1}q}) + X_{p^t} + 1$

   (f) $\theta'_{p^i} = (-1)^i[3\sum_{k=t-i}^{t-1}\mathcal{B}_k + 3X_{p^t} + (2u+3)X_{p^{t-i-1}} + 2uX_{p^{t-i-1}g}]$

   (g) $\theta'_{p^ig} = (-1)^i[3\sum_{k=t-i}^{t-1}\mathcal{B}_k + 3X_{p^t} + 2uX_{p^{t-i-1}} + (2u+3)X_{p^{t-i-1}g}]$

   (h) $\theta'_{p^iq} = (-1)^i[\sum_{k=t-i}^{t-1}\mathcal{A}_k + 2u(X_{p^{t-i-1}} + X_{p^{t-i-1}qg}) +$
   $(2u+1)(X_{p^{t-i-1}g} + X_{p^{t-i-1}q}) + X_{p^t} + 1]$

   (i) $\theta'_{p^iqg} = (-1)^i[\sum_{k=t-i}^{t-1}\mathcal{A}_k + (2u+1)(X_{p^{t-i-1}} + X_{p^{t-i-1}qg}) +$
   $2u(X_{p^{t-i-1}g} + X_{p^{t-i-1}q}) + X_{p^t} + 1]$

   (j) $\theta'_{p^t} = (-1)^{t-1}[\sum_{k=0}^{t-1}\mathcal{B}_k + X_{p^t}]$

2. If $q \equiv 3(mod\ 8)$, then

   (a) $\theta'_0 = (-1)^t(3\sum_{k=0}^{t-1}\mathcal{A}_k + 3X_{p^t} + 3)$

   (b) $\theta'_1 = (2u+1)X_{p^{t-1}} + 2uX_{p^{t-1}g} + 2X_{p^{t-1}qg} + X_{p^t} + 2$

   (c) $\theta'_g = 2uX_{p^{t-1}} + (2u+1)X_{p^{t-1}g} + 2X_{p^{t-1}q} + X_{p^t} + 2$

   (d) $\theta'_q = 2u(X_{p^{t-1}} + X_{p^{t-1}qg}) + (2u+3)(X_{p^{t-1}g} + X_{p^{t-1}q}) + 3X_{p^t} + 3$

   (e) $\theta'_{qg} = (2u+3)(X_{p^{t-1}} + X_{p^{t-1}qg}) + 2u(X_{p^{t-1}g} + X_{p^{t-1}q}) + 3X_{p^t} + 3$

   (f) $\theta'_{p^i} = (-1)^i[\sum_{k=t-i}^{t-1}(\mathcal{B}_k + 2\mathcal{C}_k) + X_{p^t} + 2 + (2u+1)X_{p^{t-i-1}}$

$$+2uX_{p^{t-i-1}g}+2X_{p^{t-i-1}qg}]$$

(g) $\theta'_{p^ig}=(-1)^i[\sum_{k=t-i}^{t-1}(\mathcal{B}_k+2\mathcal{C}_k)+X_{p^t}+2+2uX_{p^{t-i-1}}$
$+(2u+1)X_{p^{t-i-1}g}+2X_{p^{t-i-1}q}]$

(h) $\theta'_{p^iq}=(-1)^i[3\sum_{k=t-i}^{t-1}\mathcal{A}_k+2u(X_{p^{t-i-1}}+X_{p^{t-i-1}qg})$
$+(2u+3)(X_{p^{t-i-1}g}+X_{p^{t-i-1}q})+3X_{p^t}+3]$

(i) $\theta'_{p^iqg}=(-1)^i[3\sum_{k=t-i}^{t-1}\mathcal{A}_k+(2u+3)(X_{p^{t-i-1}}+X_{p^{t-i-1}qg})$
$+2u(X_{p^{t-i-1}g}+X_{p^{t-i-1}q})+3X_{p^t}+3]$

(j) $\theta'_{p^t}=(-1)^t[\sum_{k=0}^{t-1}(\mathcal{B}_k+2\mathcal{C}_k)+X_{p^t}+2]$

Proof: We'll only prove 1(a). Obtaining the rest of the expressions is as easy as following the same steps. In point of view of Theorem 3.6, for any $k\in\{0,\ p^i,p^t,\ p^iq,p^ig,\ p^iqg\ \mid\ 0\le i\le t-1\}$, $\theta'_k=\theta_k^2$, viewed as element of $\mathcal{R}'_{p^tq}=\frac{\mathbb{Z}_4[x]}{\langle x^{p^tq}-1\rangle}$.

Since $\theta_0=1+X_{p^t}+\sum_{k=0}^{t-1}\mathcal{A}_k$, so

$$\begin{aligned}\theta'_0&=(1+X_{p^t}+\sum_{k=0}^{t-1}\mathcal{A}_k)^2\\&=1+X_{p^t}^2+(\sum_{k=0}^{t-1}\mathcal{A}_k)^2+2X_{p^t}+2X_{p^t}\sum_{k=0}^{t-1}\mathcal{A}_k+2\sum_{k=0}^{t-1}\mathcal{A}_k\end{aligned}\tag{2}$$

Now, since $q=8m-3$, so using Theorems 3.1-3.5, we can obtain that for any $0\le i\le t-1$,

$$X_{p^t}\mathcal{A}_i=0 \text{ in } \mathcal{R}'_{p^tq}\tag{3}$$

So using (2),(3) and Theorems 3.1-3.5, we get

$$\theta'_0=1+3X_{p^t}+\sum_{k=0}^{t-1}\mathcal{A}_k{}^2+2\sum_{k=0}^{t-2}\sum_{j=1}^{t-k-1}\mathcal{A}_k\mathcal{A}_{k+j}+2X_{p^t}+2\sum_{k=0}^{t-1}\mathcal{A}_k\tag{4}$$

Now again as $q=8m-3$, so for any $i\in\mathcal{S}$, and $1\le j\le t-i-1$, using Theorems 3.1-3.5, we obtain that

$$\mathcal{A}_i\mathcal{A}_{i+j}=2\mathcal{A}_i \text{ and hence } 2\mathcal{A}_i\mathcal{A}_{i+j}=0$$

and $\mathcal{A}_i^2=(-1)^{t-i-1}\mathcal{A}_i+2\sum_{s=1}^{t-i-1}\mathcal{A}_{i+s}+2X_{p^t}+2$

in $\mathcal{R}'_{p^tq}$. So, by (4), we get

$$\begin{aligned}\theta'_0 &= 1 + X_{p^t} + \sum_{k=0}^{t-1}((-1)^{t-k-1}\mathcal{A}_k + 2\sum_{s=1}^{t-k-1}\mathcal{A}_{k+s} + 2X_{p^t} + 2) + 2\sum_{k=0}^{t-1}\mathcal{A}_k \\ &= \sum_{k=0}^{t-1}(2 + (-1)^{t-k-1})\mathcal{A}_k + 2\sum_{k=0}^{t-1}\sum_{s=1}^{t-k-1}\mathcal{A}_{k+s} + (2t+1)(X_{p^t} + 1) \\ &= \begin{cases} 3(\sum_{k=0}^{t-1}\mathcal{A}_k + X_{p^t} + 1) \text{ if t is odd} \\ \sum_{k=0}^{t-1}\mathcal{A}_k + X_{p^t} + 1) \text{ if t is even} \end{cases}\end{aligned}$$

Hence, $\theta'_0 = (-1)^t[\sum_{k=0}^{t-1}\mathcal{A}_k + X_{p^t} + 1]$

A similar argument can be used to prove the other parts.

Theorem 3.8: *If* $q(mod\ p^t) \in R_0$ *and* $1 \le i \le t-1$, *then*

1. If $q \equiv -3(mod\ 8)$, then
   (a) $\theta'_0 = (-1)^t(\sum_{k=0}^{t-1}\mathcal{A}_k + X_{p^t} + 1)$
   (b) $\theta'_1 = 2uX_{p^{t-1}} + (2u+3)X_{p^{t-1}g} + 3X_{p^t}$
   (c) $\theta'_g = (2u+3)X_{p^{t-1}} + 2uX_{p^{t-1}g} + 3X_{p^t}$
   (d) $\theta'_q = 2u(X_{p^{t-1}} + X_{p^{t-1}q}) + (2u+1)(X_{p^{t-1}g} + X_{p^{t-1}qg}) + X_{p^t} + 1$
   (e) $\theta'_{qg} = (2u+1)(X_{p^{t-1}} + X_{p^{t-1}q}) + 2u(X_{p^{t-1}g} + X_{p^{t-1}qg}) + X_{p^t} + 1$
   (f) $\theta'_{p^i} = (-1)^i[3\sum_{k=t-i}^{t-1}\mathcal{B}_k + 3X_{p^t} + 2uX_{p^{t-i-1}} + (2u+3)X_{p^{t-i-1}g}]$
   (g) $\theta'_{p^ig} = (-1)^i[3\sum_{k=t-i}^{t-1}\mathcal{B}_k + 3X_{p^t} + (2u+3)X_{p^{t-i-1}} + 2uX_{p^{t-i-1}g}]$
   (h) $\theta'_{p^iq} = (-1)^i[\sum_{k=t-i}^{t-1}\mathcal{A}_k + 2u(X_{p^{t-i-1}} + X_{p^{t-i-1}q}) + (2u+1)(X_{p^{t-i-1}g} + X_{p^{t-i-1}qg}) + X_{p^t} + 1]$
   (i) $\theta'_{p^iqg} = (-1)^i[\sum_{k=t-i}^{t-1}\mathcal{A}_k + (2u+1)(X_{p^{t-i-1}} + X_{p^{t-i-1}q}) + 2u(X_{p^{t-i-1}g} + X_{p^{t-i-1}qg}) + X_{p^t} + 1]$
   (j) $\theta'_{p^t} = (-1)^{t-1}[\sum_{k=0}^{t-1}\mathcal{B}_k + X_{p^t}]$

2. If $q \equiv 3(mod\ 8)$, then

(a) $\theta'_0 = (-1)^t (3\sum_{k=0}^{t-1} \mathcal{A}_k + 3X_{p^t} + 3)$

(b) $\theta'_1 = 2uX_{p^{t-1}} + (2u+1)X_{p^{t-1}g} + 2X_{p^{t-1}qg} + X_{p^t} + 2$

(c) $\theta'_g = (2u+1)X_{p^{t-1}} + 2uX_{p^{t-1}g} + 2X_{p^{t-1}q} + X_{p^t} + 2$

(d) $\theta'_q = 2u(X_{p^{t-1}} + X_{p^{t-1}q}) + (2u+3)(X_{p^{t-1}g} + X_{p^{t-1}qg}) + 3X_{p^t} + 3$

(e) $\theta'_{qg} = (2u+3)(X_{p^{t-1}} + X_{p^{t-1}q}) + 2u(X_{p^{t-1}g} + X_{p^{t-1}qg}) + 3X_{p^t} + 3$

(f) $\theta'_{p^i} = (-1)^i [\sum_{k=t-i}^{t-1} (\mathcal{B}_k + 2\mathcal{C}_k) + X_{p^t} + 2 + 2uX_{p^{t-i-1}} +$
$(2u+1)X_{p^{t-i-1}g} + 2X_{p^{t-i-1}qg}]$

(g) $\theta'_{p^i g} = (-1)^i [\sum_{k=t-i}^{t-1} (\mathcal{B}_k + 2\mathcal{C}_k) + X_{p^t} + 2 + (2u+1)X_{p^{t-i-1}} +$
$2uX_{p^{t-i-1}g} + 2X_{p^{t-i-1}q}]$

(h) $\theta'_{p^i q} = (-1)^i [3\sum_{k=t-i}^{t-1} \mathcal{A}_k + 2u(X_{p^{t-i-1}} + X_{p^{t-i-1}q}) +$
$(2u+3)(X_{p^{t-i-1}g} + X_{p^{t-i-1}qg}) + 3X_{p^t} + 3]$

(i) $\theta'_{p^i qg} = (-1)^i [3\sum_{k=t-i}^{t-1} \mathcal{A}_k + (2u+3)(X_{p^{t-i-1}} + X_{p^{t-i-1}q}) +$
$2u(X_{p^{t-i-1}g} + X_{p^{t-i-1}qg}) + 3X_{p^t} + 3]$

(j) $\theta'_{p^t} = (-1)^t [\sum_{k=0}^{t-1} (\mathcal{B}_k + 2\mathcal{C}_k) + X_{p^t} + 2]$

Proof: Proof of this theorem can be accomplished in a manner analogous to that of Theorem 3.7.

Remark 3.1: For any $k \in \{0, p^i, p^t, p^i q, p^i g, p^i qg \mid 0 \le i \le t-1\}$, let $C_k = \langle \theta'_k \rangle$, then using Theorem 3.7 and Theorem 3.8, we can see that under the permutation which interchange the co-ordinates of every codeword corresponding to the elements of Ω_{p^i} with the co-ordinates corresponding to elements of $\Omega_{p^i g}$ and interchange the co-ordinates corresponding to the elements of $\Omega_{p^i q}$ with the co-ordinates corresponding to the elements of $\Omega_{p^i qg}$ for any $0 \le i \le t-1$, C_{p^i} are permutational equivalent to $C_{p^i g}$ and $C_{p^i q}$ are permutational equivalent to $C_{p^i qg}$ for any $0 \le i \le t-1$.

We are now going to talk about the orthogonal properties of some cyclic codes. Let $\mathcal{I} = \{0, p^i, p^t, p^i q, p^i g, p^i qg : i \in \mathcal{S}\}$ be the set of all coset representatives. For $k \in \{p^i, p^i q : i \in \mathcal{S}\}$, let $k^{\#} = kg$, $kg^{\#} = k$, $0^{\#} = 0$ and

$p^{t\#} = p^t$. The reciprocal polynomial denoted by $f^*(x)$ of a polynomial $f(x)$ having degree k is defined to be

$$f^*(x) = x^k g(x^{-1}).$$

Now we have a theorem which discusses the Dual of cyclic codes of the type $C_k = \langle \theta'_k \rangle$, for any $k \in \{0, p^i, p^t, p^iq, p^ig, p^iqg \mid 0 \le i \le t-1\}$.

Theorem 3.9: *Let for any* $k \in \{0, p^i, p^t, p^iq, p^ig, p^iqg \mid 0 \le i \le t-1\}$, $C_k = \langle \theta'_k \rangle$ *be the cyclic code then* $C_k^{\perp} = \langle \sum_{i \in \mathcal{I},\, i \neq k^{\#}} \theta'_i \rangle$. *Hence the codes* $C_k = \langle \theta'_k \rangle$, *where* $k \in \{p^i, p^iq, p^ig, p^iqg \mid 0 \le i \le t-1\}$ *are self orthogonal.*

Proof: Let $x^n - 1 = f_0(x) f_{p^t}(x) \prod_{i=0}^{t-1} f_{p^i}(x) f_{p^ig}(x) f_{p^iq}(x) f_{p^iqg}(x)$ be the factorization of $x^n - 1$ into basic irreducible factors over $\mathbb{Z}_4$. Let $\hat{f}_k(x) = \frac{x^n-1}{f_k(x)}$, then we know that $C_k = \langle \theta'_k \rangle = \langle \hat{f}_k \rangle$ for any $k \in \{0, p^i, p^t, p^iq, p^ig, p^iqg \mid 0 \le i \le t-1\}$. We can easily prove that for any $0 \le i \le t-1$, $f^*_{p^i}(x) = \pm f_{p^ig}(x)$, $f^*_{p^iq}(x) = \pm f_{p^iqg}(x)$, $f^*_0(x) = \pm f_0(x)$, $f^*_{p^i}(x) = \pm f_{p^t}(x)$ and vise-versa, with the help of the expressions of cyclotomic cosets obtained in Theorem 2.1. Also, If $C = \langle f \rangle$, where $f.g = x^n - 1$, then $C_k^{\perp} = \langle g^* \rangle$. So, we can say that for any $k \in \{0, p^i, p^t, p^iq, p^ig, p^iqg : i \in \mathcal{S}\}$, if $C_k = \langle \theta'_k \rangle$ then $C_k^{\perp} = \langle \sum_{i \in \mathcal{I},\, i \neq k^{\#}} \theta'_i \rangle$. Hence for any $k \in \{p^i, p^iq, p^ig, p^iqg : i \in \mathcal{S}\}$, $C_k \subseteq C^{\perp}$. So, C_k is self-orthogonal for any $k \in \{p^i, p^iq, p^ig, p^iqg : i \in \mathcal{S}\}$.

Example 3.1: Now, we will give expressions of all the primitive idempotents in $\frac{\mathbb{Z}_4[x]}{\langle x^{21}-1 \rangle}$, with $p = 7, t = 1$ and $q = 3$. It is easy to find that $g = 17$. Also, as $t = 1$ so, there are six cyclotomic cosets which are given below:

$$\Omega_0 = \{0\},$$

$$\Omega_{p^0} = \Omega_1 = \{1, 2, 4, 8, 11, 16\},$$

$$\Omega_{p^0 g} = \Omega_{17} = \{5, 10, 13, 17, 19, 20\},$$

$$\Omega_{p^0 q} = \Omega_3 = \{3, 12, 6\},$$

$$\Omega_{p^0 qg} = \Omega_9 = \{9, 15, 18\},$$

$$\Omega_p = \Omega_7 = \{7, 14\}.$$

Hence, we can say that $X_0 = 1$, $X_{p^0} = X_1 = x + x^2 + x^4 + x^8 + x^{11} + x^{16}$, $X_{p^0g} = X_{17} = x^5 + x^{10} + x^{13} + x^{17} + x^{19} + x^{20}$, $X_{p^0q} = X_3 = x^3 + x^6 + x^{12}$, $X_{p^0qg} = X_9 = x^9 + x^{15} + x^{18}$, $X_p = X_7 = x^7 + x^{14}$.

Now since $q = 3$ and $p = 8u - 1 = 7$ which imply that $u = 1$, So, Using Theorem 3.7(2) the six primitive Idempotents in $\frac{\mathbb{Z}_4[x]}{\langle x^{21}-1\rangle}$ are given as below:

$$\theta_0' = \sum_{i=0}^{20} x^i$$

$$\theta_1' = 2 + 3x + 3x^2 + 3x^4 + 2x^5 + x^7 + 3x^8 + 2x^9 + 2x^{10} + 3x^{11} + 2x^{13} + x^{14} + 2x^{15} + 3x^{16} + 2x^{17} + 2x^{18} + 2x^{19} + 2x^{20}$$

$$\theta_g' = \theta_{17}' = 2 + 2x + 2x^2 + 2x^3 + 2x^4 + 3x^5 + 2x^6 + x^7 + 2x^8 + 3x^{10} + 2x^{11} + 2x^{12} + 3x^{13} + x^{14} + 2x^{16} + 3x^{17} + 3x^{19} + 3x^{20}$$

$$\theta_q' = \theta_3' = 3 + 2x + 2x^2 + x^3 + 2x^4 + x^5 + x^6 + 3x^7 + 2x^8 + 2x^9 + x^{10} + 2x^{11} + x^{12} + x^{13} + 3x^{14} + 2x^{15} + 2x^{16} + x^{17} + 2x^{18} + x^{19} + x^{20}$$

$$\theta_{qg}' = \theta_9' = 3 + x + x^2 + 2x^3 + x^4 + 2x^5 + 2x^6 + 3x^7 + x^8 + x^9 + 2x^{10} + x^{11} + 2x^{12} + 2x^{13} + 3x^{14} + x^{15} + x^{16} + 2x^{17} + x^{18} + 2x^{19} + 2x^{20}$$

$$\theta_p' = \theta_7' = 2\sum_{j=0}^{6} x^{3j} + 3\sum_{\substack{j=1 \\ 3 \nmid j}}^{20} x^j, \text{where } 3 \nmid j \text{ means that 3 does not devide j.}$$

"If $n_i(x)$ is represent the number of components equal to i in the code-word x, then symmetrized weight enumerator [10] the code C is defined as

$$\sum_{x \in C} a^{n_0(x)} b^{n_1(x)+n_3(x)} c^{n_2(x)}"$$

Therefore, it is straightforward to determine the minimum Hamming weight, Lee weight, and Euclidean weight of a code C by finding the symmetrized weight enumerator. The number of code-words having a specific weight in the code C can also be found using the symmetrized weight enumerator C.

Now as we know that the codes $\langle \theta_1' \rangle$ and $\langle \theta_q' \rangle$ are permutational equivalent to the codes $\langle \theta_g' \rangle$ and $\langle \theta_{qg}' \rangle$ respectively, so in the Table 1 we give the parameters of the Five codes generated by θ_k', $k \in \{1, g, q, qg, p\}$. From Table 1 it is clear that the torsion codes $Tor(C_1)$ and $Tor(C_g)$ are Two-weight Codes with parameters $[21, 6, \{8, 12\}]$ and the torsion codes $Tor(C_q)$ and $Tor(C_{qg})$ are constant weight codes with parameters $[21, 3, 12]$, where $C_k = \langle \theta_k' \rangle$. Also, The Residue Codes $Res(C_1)$ and $Res(C_g)$ are binary cyclic codes with parameters $[21, 6, 8]$ and the residue codes $Res(C_q)$ and $Res(C_{qg})$ are binary cyclic codes with parameters $[21, 3, 12]$. These codes attain their bounds for the dimensions 6 and 3 respectively as per [8].

Table 1

Symmetrized Weight Enumerators of Cyclic Codes of Length 21

Code	Type	Symmetrized Weight Enumerator	Hamming Weight	Lee Weight	Euclidean Weight
$\langle \theta_1' \rangle$ and $\langle \theta_g' \rangle$	4^6	$a^{21} + 126a^{11}b^8c^2 + 1176a^6b^{12}c^3 + 1008a^4b^{12}c^5 + 672a^7b^8c^6 + 504a^2b^{12}c^7 + 21a^{13}c^8 + 504a^5b^8c^8 + 42a^3b^8c^{10} + 42a^9c^{12}$	8	12	16
$\langle \theta_p' \rangle$ and $\langle \theta_{qg}' \rangle$	4^3	$a^{21} + 42a^6b^{12}c^3 + 14b^{12}c^9 + 7a^9c^{12}$	12	18	24
$\langle \theta_p' \rangle$	4^2	$a^{21} + 6a^7b^{14} + 6b^{14}c^7 + 3a^7c^{14}$	14	14	14

4. $\mathbb{Z}_4$ – Cyclic self-dual and $\mathbb{Z}_4$ – cyclic LCD codes having length $p^t q$

The $\mathbb{Z}_4$ – cyclic self-dual and $\mathbb{Z}_4$ – cyclic LCD codes having length $p^t q$ will be discussed in this section using the idempotent generators. Let $m_k(x)$ be the minimal polynomial of α^k over $\mathbb{F}_2$, where $k \in \{0, p^i, p^t, p^i q, p^i g, p^i qg : i \in \mathcal{S}\}$. Then the factorization of $x^n - 1$ over $\mathbb{F}_2$ is given as

$$x^n - 1 = m_0(x) m_{p^t}(x) \prod_{i=0}^{t-1} m_{p^i}(x) m_{p^i g}(x) m_{p^i q}(x) m_{p^i qg}(x)$$

Now, we need the following presumptions and definitions.

- For $k \in \{0, p^i, p^t, p^i q, p^i g, p^i qg : i \in \mathcal{S}\}$, let $f_k(x)$ be the Hensel lift of $m_k(x)$, i.e., $h^{m_k(x)} = f_k(x)$.
- The reciprocal polynomial denoted by $f^*(x)$ of a polynomial $f(x)$ having degree *k* is defined to be

$$f^*(x) = \pm x^k f\left(\frac{1}{x}\right).$$

  where the choice of + or – ensures that $f^*(x)$ is monic.
- $\mu : \mathbb{Z}_4[x] \to \mathbb{Z}_2[x]$ is the map that maps *x* to *x*, 1, 3 to 1, and 0, 2 to 0.

Theorem 4.5 is our key result on self duality, and its proof requires Theorems 4.1–4.4.

Theorem 4.1: [22] *"Let C be a* Z_4 *-cyclic code of odd length n.*

1. If $C = (f)$, where $fgh = x^n - 1$ for some *g*, then *C* has an idempotent generator in Z_4.
2. If $C = (2f)$ and *f* divides $x^n - 1$, then *C* = (2*e*), where e is an binary idempotent generator of (μf).
3. If *C* = $(fh, 2fg)$, where $fgh = x^n - 1$, then *C* = (e, 2*v*), where *e* is an idempotent in Z_4, v is an idempotent in Z_2. "

Theorem 4.2: [22] *"Let* $C = (fh, 2fg)$ *be a* Z_4 *-cyclic code of odd length n, where f, g and h are monic polynomials such that* $fgh = x^n - 1$ *and* $|C| = 4^{degg} 2^{degh}$. *Then* $C^{\perp} = (g^* h^*, 2g^* f^*)$ and $|C^{\perp}| = 4^{degf} 2^{degh}$

If $h = 1$, then $C = (f)$ and $C^{\perp} = (g^*)$

If $g = 1$, then $C = (2f)$ and $C^{\perp} = (h^*, 2f^*)$ "

A code *C* over $\mathbb{Z}_4$ is considered self-dual if it equals its dual. Using the following result, we can say that the $\mathbb{Z}_4$ – cyclic self-dual codes having length $p^t q$ exist. These codes will be addressed in Theorem 4.5.

Theorem 4.3: [21] *"For a nontrivial odd length n, cyclic self-dual codes exist over* Z_4 *if and only if n is an odd integer either divisible by*

1. a prime $r \equiv -1 (mod 8)$ or
2. a prime $r \equiv 1 (mod 8)$, where $O_r(2)$ is odd, or
3. a prime *p* and *a* prime *q*, where *p* and *q* are two different odd primes and let $O_p(2) = 2^l i$ and $O_q(2) = 2^l j$ with i odd and j even and $l \geq 1$ ".

Theorem 4.4: *[1] "Let $f(x)$ be a polynomial of degree k over F_2. Then*

$$(h^f)^*(x) = \begin{cases} -h^{f^*}(x); & \text{if } k \text{ is odd,} \\ h^{f^*}(x); & \text{if } k \text{ is even.} \end{cases}$$

We will now present a Lemma that can be proven through the use of basic combinatorics.

Lemma 4.1: *If A is a set with m elements, then the total no. of ordered pairs (B_1, B_2), such that, $B_1, B_2 \subseteq A$ with $B_1 \cap B_2 = \phi$, is 3^m.*

Now for any set $B \subseteq \mathcal{S}$, let B^c denote the relative complement of B with respect to $\mathcal{S}$. Now, using Theorems 4.1-4.4 together with Lemma 4.1, we see that there are 9^t $\mathbb{Z}_4$ – self-dual cyclic codes having length p^tq, which are given in terms of idempotent generators in the following Theorem.

Theorem 4.5: *For $S_1, S_2, S_3, S_4 \subseteq \mathcal{S}$ with $S_1 \cap S_2 = \phi$ and $S_3 \cap S_4 = \phi$ and at least one of the sets S_1, S_2, S_3, S_4 is non-empty, the self-dual codes having length p^tq are provided as*

$$\langle f_0 f_{p^t} \prod_{i \in S_2^c} f_{p^i} \prod_{i \in S_1^c} f_{p^i g} \prod_{i \in S_4^c} f_{p^i q} \prod_{i \in S_3^c} f_{p^i qg} \rangle + 2\langle \prod_{i \in S_1 \cup S_2} f_{p^i} f_{p^i g} \prod_{i \in S_3 \cup S_4} f_{p^i q} f_{p^i qg} \rangle$$

and corresponding to $S_1 = S_2 = S_3 = S_4 = \phi$, the self-dual code is $\langle 2 \rangle$. In terms of the idempotent generator, the above codes can be written as

$$\langle \sum_{i \in S_2} \theta'_{p^i} + \sum_{i \in S_1} \theta'_{p^i g} + \sum_{i \in S_4} \theta'_{p^i q} + \sum_{i \in S_3} \theta'_{p^i qg} \rangle + 2\langle \theta'_0 + \theta'_{p^t} + \sum_{i \in S_1^c \cap S_2^c} (\theta'_{p^i} + \theta'_{p^i g}) + \sum_{i \in S_3^c \cap S_4^c} (\theta'_{p^i q} + \theta'_{p^i qg}) \rangle.$$

Out of these 9^t codes, $\frac{9^t+1}{2}$ codes are permutational non-equivalent.

Proof: In view of Theorem 3.6 in $\mathcal{R}'_{p^tq}$, we have

$$x^{p^tq} - 1 = f_0(x) f_{p^t}(x) \prod_{i=0}^{t-1} f_{p^i}(x) f_{p^i g}(x) f_{p^i q}(x) f_{p^i qg}(x)$$

where $\mu(f_k(x)) = m_k(x)$, and for $k \in \{0, p^i, p^t, p^iq, p^ig, p^iqg \mid 0 \le i \le t-1\}$, $m_k(x)$ denote the minimal polynomial of α^k over $\mathbb{F}_2$. We also know that $(\hat{m}_k(x)) = (\theta_k(x))$, for $k \in \{0, p^i, p^t, p^iq, p^ig, p^iqg \mid 0 \le i \le t-1\}$, where $\hat{m}_k(x) = \frac{x^{p^tq}-1}{m_k(x)}$. Also since $p \equiv -1 (mod\ 8)$, so -1 is a quadratic non-residue modulo p and hence in view of Theorem 2.1, for any $0 \le i \le t-1$, $m^*_{p^i}(x) = m_{p^ig}(x)$, $m^*_{p^iq}(x) = m_{p^iqg}(x)$, $m^*_{p^t}(x) = m_{p^t}(x)$, $m^*_0(x) = m_0(x)$ and vise-versa.

And hence in view of Theorem 4.4, for any $0 \le i \le t-1$, $f^*_{p^i}(x) = \pm f_{p^i g}(x)$, $f^*_{p^i q}(x) = \pm f_{p^i qg}(x)$, $f^*_{p^i}(x) = \pm f_{p^t}(x)$, $f^*_0(x) = \pm f_0(x)$ and vise-versa. This proves that all the cyclic codes given above are self-dual. Hence in point of view of Lemma 4.1, there are 9^t self dual codes of length $p^t q$ over $\mathbb{Z}_4$ which are cyclic.

Now, as the code corresponding to oredered pairs (S_1, S_2) and (S_3, S_4) is permutational equivalent to the code corresponding to ordered pairs (S_2, S_1) and (S_4, S_3). So out of these 9^t self-dual codes, there is $\frac{9^t+1}{2}$ permutational non-equivalent codes.

Now, in Example 3.1, we obtained the expressions of all the idempotent of the minimal cyclic codes having length 21. The expressions of all non-trivial self-dual codes having length 21 in terms of generating idempotent are provided in the example below.

Example 4.1: There are 9 self dual codes of length 21 over $\mathbb{Z}_4$, with 5 of them being permutationally non-equivalent. In Table 2, we give the weights of the $\mathbb{Z}_4$ – cyclic self-dual codes having length 21.

Table 2

$\mathbb{Z}_4$ – Cyclic Self-Dual Codes of Length 21

S_1	S_2	S_3	S_4	Code	Type	Hamming Weight	Lee Weight	Euclidean Weight
ϕ	{0}	ϕ	{0}	$\langle \theta_{1'} + \theta_{q'} \rangle + 2\langle \theta_{0'} + \theta_{p'} \rangle$	$4^9 2^3$	5	8	8
ϕ	{0}	{0}	ϕ	$\langle \theta_{1'} + \theta_{qg}' \rangle + 2\langle \theta_{0'} + \theta_{p'} \rangle$	$4^9 2^3$	4	4	4
ϕ	ϕ	ϕ	{0}	$\langle \theta_{q'} \rangle + 2\langle \theta_{0'} + \theta_{1'} + \theta_{g'} + \theta_{p'} \rangle$	$4^3 2^{15}$	2	4	8
ϕ	{0}	ϕ	ϕ	$\langle \theta_{1'} \rangle + 2\langle \theta_{0'} + \theta_{q'} + \theta_{qg}' + \theta_{p'} \rangle$	$4^6 2^9$	3	6	8

Now we give the expressions of all the $\mathbb{Z}_4$ – cyclic LCD codes having length $p^t q$ using the generating idempotent. Using Theorem 25 of [17], we can easily see that a cyclic code $C = \langle f(x) \rangle$ over $\mathbb{Z}_4$ is LCD if and only if the generating polynomial of C is self-reciprocal polynomial, i.e., $f^*(x) = f(x)$.

So to find LCD codes over $\mathbb{Z}_4$, we just have to find all the self-reciprocal polynomials which are divisiors of x^n-1.

Theorem 4.6: *For* $S_1, S_2 \subseteq \mathcal{S}$ *and* $\varepsilon_1, \varepsilon_2 = \pm 1$, *the LCD codes of length* p^tq *over* $\mathbb{Z}_4$ *are given as*

$$\langle f_0^{\varepsilon_1} f_{p^t}^{\varepsilon_2} \prod_{i\in S_1} f_{p^i} f_{p^ig} \prod_{i\in S_2} f_{p^iq} f_{p^iqg} \rangle$$

In terms of idempotent generators, the above codes may also be written as

$$\langle (1-\varepsilon_1)\theta_{0'} + (1-\varepsilon_2)\theta_{p^t}' + \sum_{i\in S_1^c} (\theta_{p^i}' + \theta_{p^ig}') + \sum_{i\in S_2^c} (\theta_{p^iq}' + \theta_{p^iqg}') \rangle$$

Proof: Since we know that for any $0 \le i \le t-1$, $f_{p^i}^*(x) = \pm f_{p^ig}(x)$, $f_{p^iq}^*(x) = \pm f_{p^iqg}(x)$, $f_{p^t}^*(x) = \pm f_{p^t}(x)$, $f_0^*(x) = \pm f_0(x)$ and vise-versa. So we can easily see that any self-reciprocal polynomial which is a divisor of x^n-1 can be written as $f_0^{\varepsilon_1} f_{p^t}^{\varepsilon_2} \prod_{i\in S_1} f_{p^i} f_{p^ig} \prod_{i\in S_2} f_{p^iq} f_{p^iqg}$ and hence all the cyclic codes given above are LCD. Hence there are 4^{t+1} number of LCD codes of length p^tq over $\mathbb{Z}_4$.

5. Conclusions

1. We have obtained the expressions of all the primitive idempotent generators of cyclic codes having length p^tq over the ring of integers modulo 4, therefore, any $\mathbb{Z}_4$ – cyclic codes having length p^tq may be represented using idempotent generators. Also, the permutational equivalence and dual of some of these codes have been discussed. It has been observed that all the cyclic codes generated by primitive idempotents are self-orthogonal (except generated by $\theta_{0'}$ and θ_{p^t}').
2. All the $\mathbb{Z}_4$ – cyclic self-dual codes having length p^tq have been described in terms of idempotent generators and the permutational equivalence of these codes has been discussed. There are 9^t $\mathbb{Z}_4$ – cyclic self-dual codes having length p^tq, with $\frac{9^t+1}{2}$ being non-equivalent.
3. In terms of idempotent generators, each and every LCD code with a length of p^tq over $\mathbb{Z}_4$ has been described. Furthermore, it is worth noting that the total number of cyclic LCD codes with a length of p^tq with respect to $\mathbb{Z}_4$ is 4^{t+1}.

4. Examples of cyclic codes of length 21 have been given with their symmetrized weight enumerator. Using the symmetrized weight enumerator of these codes it has been found that torsion codes of some cyclic codes of length 21 are constant weight and two weight binary codes. Binary constant-weight codes have several applications, including frequency hopping in GSM networks and barcodes while Two-weight linear codes have many applications in authentication codes, association schemes and secret sharing schemes.
5. In view of Theorem 12.5.1 of [10], The self-dual codes of length 21 are Type-I codes whose Minimum Euclidean Weight can be almost 8. So, in view of Table 2 three non-equivalent $\mathbb{Z}_4$ – cyclic self-dual codes having length 21 are Euclidean-Extremal.
6. When $t=1$ is used, the results that Jain and Batra found in their paper [11] are a special example of our own findings. Also, as Jain and Batra proved that the $\mathbb{Z}_4$ – cyclic self-dual codes having length pq and their extensions are Type-I codes, it is observed that the codes of length $p^t q$ and their extensions are also Type-I codes. But if we study the codes of length $p^t q$, when $O_{p^t}(2)=\phi(p^t)$ and $O_q(2)=\frac{\phi(q)}{2}$ then the extension codes can be Type-II codes, as the length of extensions of these codes in this case will be multiple of eight. The results of [11] that were provided by Jain and Batra will therefore be interesting to generalize in this way.

Acknowledgement

This research has been funded by the Council of Scientific and Industrial Research (C.S.I.R.) in New Delhi, India, under File No. 09/1063(0019)/2019-EMR-I.

Furthermore, Wolfram Mathematica's trial version was used to calculate the symmetrized weight enumerators of the different codes in the examples.

Authors are also thankful to the editor and reviewer for their valuable suggestions. Their suggestions and feedbacks helped a lot in improving the quality of this article.

References

[1] S. Batra and S. Jain, "Generalized cyclotomic numbers and cyclic codes of prime power length over $\mathbb{Z}_4$," *Asian-European Journal of Mathematics*, vol. 12, no. 5, pp. 1950085 (2019).

[2] C. Carlet and S. Guilley, "Complementary dual codes for counter-measures to side-channel attacks," *Adv. Math. Commun.*, vol. 10, no. 1, pp. 131–150 (2016).

[3] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan, "Linear codes over Fq are equivalent to LCD codes for q > 3," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 3010–3017 (2018).

[4] B. Chen, S. Ling, and G. Zhang, "Enumeration formulas for self-dual cyclic codes," *Finite Fields Appl.*, vol. 42, pp. 1–22 (2016).

[5] J. H. Conway and N. J. Sloane, "Self-dual codes over the integers modulo 4," *J. Combin. Theory Ser. A*, vol. 62, no. 1, pp. 30–45 (1993).

[6] E. Estrada, L. Torres, L. Rodriguez, and I. Gutman, "An atom-bond connectivity index: modelling the enthalpy of formation of alkanes," *Indian J. Chem. Sect. A*, vol. 37, pp. 849–855 (1998).

[7] J. Fields, P. Gaborit, J. Leon, and V. Pless, "All self-dual $\mathbb{Z}_4$ codes of length 15 or less are known," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 311–322 (1998).

[8] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," online available at http://www.codetables.de, 2007. Accessed on 2023-08-20.

[9] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory,* vol. 40, no. 2, pp. 301–319 (1994).

[10] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, UK (2010).

[11] S. Jain and S. Batra, "Cyclic self-dual codes of length pq over $\mathbb{Z}_4$," *J. Discrete Math. Sci. Cryptogr.,* vol. 25, no. 8, pp. 2305–2319 (2022).

[12] L. Jin, "Construction of MDS codes with complementary duals," *IEEE Trans. Inf. Theory,* vol. 63, no. 5, pp. 2843–2847 (2016).

[13] P. Kanwar and S. R. Lopez-Permouth, "Cyclic codes over the integers modulo pm," *Finite Fields Appl.*, vol. 3, no. 4, pp. 334–352 (1997).

[14] K. Kumar and S. Batra, "Cyclotomy, cyclotomic cosets and arithmetic properties of some families in 1 ptq Fl x ⟨x − ⟩," *Asian-European J. Math.*, vol. 16, no. 2, p. 2350023 (2023).

[15] C. Li, C. Ding, and S. Li, "LCD cyclic codes over finite fields," *IEEE Trans. Inf. Theory,* vol. 63, no. 7, pp. 4344–4356 (2017).

[16] X. Liu and H. Liu, "LCD codes over finite chain rings," *Finite Fields Their Appl.,* vol. 34, pp. 1–19 (2015).

[17] Z. Liu and J. Wang, "Linear complementary dual codes over rings," *Designs, Codes, and Cryptography,* vol. 87, pp. 3077–3086 (2019).

[18] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland Publishing Company, New York (1977).

[19] R. Mathur and S. Batra, "Primitive idempotents of cyclic codes of length p and 2p," *J. Appl. Math. Comput.,* vol. 58, pp. 693–719 (2018).

[20] A. A. Nechaev, "Kerdock code in a cyclic form," vol. 1, no. 4, pp. 365–384 (1991).

[21] V. Pless, P. Solé, and Z. Qian, "Cyclic self-dual $\mathbb{Z}_4$-codes," Finite Fields Appl., vol. 3, no. 1, pp. 48–69 (1997).

[22] V. S. Pless and Z. Qian, "Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$," *IEEE Trans. Inf. Theory,* vol. 42, no. 5, pp. 1594–1600 (1996).

[23] S. Razaghi and S. Sahebi, "Calculating different indices of idempotent graph of ring Zn," *J. Inf. Optim. Sci.,* vol. 44, no. 5, pp. 835–843 (2023).

Received December, 2023