Commun. Korean Math. Soc. **39** (2024), No. 1, pp. 31–43
https://doi.org/10.4134/CKMS.c230057
pISSN: 1225-1763 / eISSN: 2234-3024

CYCLIC CODES OF LENGTH p^s OVER $\frac{\mathbb{F}_{p^m}[u]}{\langle u^e \rangle}$

Roghayeh Mohammadi Hesari, Masoumeh Mohebbei, Rashid Rezaei, and Karim Samei

Abstract. Let $R_e = \frac{\mathbb{F}_{p^m}[u]}{\langle u^e \rangle}$, where p is a prime number, e is a positive integer and $u^e = 0$. In this paper, we first characterize the structure of cyclic codes of length p^s over R_e. These codes will be classified into 2^e distinct types. Among other results, in the case that $e = 4$, the torsion codes of cyclic codes of length p^s over R_4 are obtained. Also, we present some examples of cyclic codes of length p^s over R_e.

1. Introduction

Cyclic codes have some additional structural constraints on the codes. They are based on Galois fields and, because of their structural properties, they are very useful for error control. Their structure is strongly related to the Galois field, because of which the encoding and decoding algorithms for cyclic codes are computationally efficient.

In [1], Abualrub and Siap studied cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$. In [8], cyclic codes over $\mathbb{Z}_q + u\mathbb{Z}_q$, where $u^2 = 0$ and q is the power of a prime, were investigated. The structure of negacyclic codes of length 2^s over $\mathbb{Z}_{2^\alpha}$ was obtained in [7].

In recent years, cyclic codes of different lengths over the finite field $\mathbb{F}_{p^m}$ have been intensively studied by many authors. Dinh et al. have done this job of classifying classes of constacyclic codes of certain lengths over certain finite fields or finite chain rings. In 2004, Dinh obtained the structure of negacyclic codes of length 2^s over the Galois ring [3]. Then in 2010, he classified and gave the detailed structure of all constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ [5]. On the basis of the works of Dinh, other researchers have tried the subject, for example, we can refer to the survey of [9]. In [10], some constacyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$ have been studied by X. Liu and X. Xu. The structure and Hamming distances of cyclic codes of length 2^s over the Galois field $\mathbb{F}_4$ can be established as a special case of [4], where cyclic codes of length p^s over the Galois field $\mathbb{F}_{p^\alpha}$ were investigated. In [2], Cao et al. determined the structures

Received March 15, 2023; Accepted July 3, 2023.
2020 *Mathematics Subject Classification.* 94B15, 16S36.
Key words and phrases. Chain ring, cyclic code, torsion code.

of repeated-root $(\delta+\alpha u^2)$-constacyclic codes over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^e\rangle}$ for any $\delta,\alpha\in\mathbb{F}_{p^m}^*$. This class is a significant subclass of constacyclic codes over finite chain rings of Type 2. In [6], Dinh et al. first classified and then investigated the structure and duals of several classes of repeated-root constacyclic codes over the ring $\frac{\mathbb{F}_{p^m}[u]}{\langle u^\alpha\rangle}$.

In this paper, we present the structure of cyclic codes of length p^s over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^e\rangle}$, where p is a prime number and $u^e=0$. In Section 2, we review some basic definitions and properties of a polynomial ring over a finite chain ring and present some main theorems that have been discussed in [4,5,10]. In Section 3, we specify the structure of cyclic codes of length p^s over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^e\rangle}$, where $u^e=0$. In Section 4, we study the cyclic codes of length p^s over $R_4=\frac{\mathbb{F}_{p^m}[u]}{\langle u^4\rangle}$. Also, we characterize the generator of the torsion code of these codes. Finally, we present some examples of cyclic codes of length p^s over R_4.

2. Preliminaries

A *principal ideal* is an ideal I of a ring R that is generated by a single element $a\in R$, that is $\langle a\rangle=\{ra : r\in R\}$. A ring R is a *principal ideal ring* if it has unity and if every ideal is principally generated. R is called a *local ring* if R has a unique maximal ideal. Furthermore, a ring R is called a chain ring if the set of all ideals of R is linearly ordered under set-theoretic inclusion.

A code C of length n over R is a non-empty subset of R^n, and the ring R is referred to as the alphabet of the code. If this subset is also an R-submodule of R^n, then C is called linear.

For a unit λ of R, the λ-constacyclic (λ-twisted) shift τ_λ on R^n is the shift $\tau_\lambda(x_0,x_1,\dots,x_{n-1})=(\lambda x_{n-1},x_0,x_1,\dots,x_{n-2})$, and a code C is said to be λ-constacyclic if $\tau_\lambda(C)=C$, i.e., if C is closed under the λ-constacyclic shift τ_λ. In case $\lambda=1$, those λ-constacyclic codes are called cyclic codes.

Proposition 2.1 ([7, Proposition 2.1])**.** *Let R be a finite commutative ring. Then the following conditions are equivalent*:

(i) *R is a local ring and the maximal ideal M of R is principal, i.e., $M=\langle\Gamma\rangle$ for some $\Gamma\in R$.*

(ii) *R is a local principal ideal ring.*

(iii) *R is a chain ring.*

Proposition 2.2 ([5, Proposition 2.2])**.** *Let R be a finite commutative ring. A linear code C of length n over R is cyclic if and only if C is an ideal of $\frac{R[x]}{\langle x^n-1\rangle}$.*

Throughout this paper, we use the following symbols for simplicity:

- $R_e=\frac{\mathbb{F}_{p^m}[u]}{\langle u^e\rangle}=\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+\cdots+u^{e-1}\mathbb{F}_{p^m}$, where $u^e=0$.
- $\mathcal{R}_e=\frac{R_e[x]}{\langle x^{p^s}-1\rangle}$.

Lemma 2.3 ([5])**.** *Let $h(x)=a_0+\sum_{i=1}^{p^s-1}a_i(x-1)^i$ be a polynomial in $\mathcal{R}_1$, where $a_0\neq 0$ and $a_i\in\mathbb{F}_{p^m}$. Then $h(x)$ is a unit in $\mathcal{R}_1$.*

Proposition 2.4 ([4]). *The ring $\mathcal{R}_1$ is a chain ring with exactly the following ideals*:

$$\mathcal{R}_1 = \langle (x-1)^0\rangle \supsetneq \langle (x-1)^1\rangle \supsetneq \cdots \supsetneq \langle (x-1)^{p^s-1}\rangle \supsetneq \langle (x-1)^{p^s}\rangle = 0.$$

Theorem 2.5 ([10]). *Cyclic codes of length p^s over R_3, i.e., ideals in $\mathcal{R}_3$, are*

- *Type* 1 : 0, $\mathcal{R}_3$.
- *Type* 2 : $\langle u^2(x-1)^i\rangle$, *where* $0 \leqslant i \leqslant p^s-1$.
- *Type* 3 : $\langle u(x-1)^i + u^2h(x)(x-1)^t\rangle$, *where* $0 \leqslant i \leqslant p^s-1$, $0 \leq t < i$, *and either* $h(x)$ *is* 0 *or is a unit, which it can be represented as* $h(x) = \sum_j h_j(x-1)^j$.
- *Type* 4 : $\langle u(x-1)^i + u^2h(x)(x-1)^t, u^2(x-1)^\omega\rangle$, *where* $0 \leq i \leq p^s-1$, $0 \leq t < w < i$, *and* $h(x)$ *as in Type* 3.
- *Type* 5 : $\langle (x-1)^i + uh_1(x)(x-1)^t + u^2h_2(x)(x-1)^z\rangle$, *where* $1 \leqslant i \leqslant p^s-1$, $0 \leq t, z < i$, *and* $h_1(x)$, $h_2(x)$ *as in Type* 3.
- *Type* 6 : $\langle (x-1)^i + uh_1(x)(x-1)^t + u^2h_2(x)(x-1)^z, u^2(x-1)^\sigma\rangle$, *where* $1 \leqslant i \leqslant p^s-1$, $0 \leq t < \sigma$, $0 \leq z < \sigma$, $\sigma < i$, *with* $h_1(x)$ *and* $h_2(x)$ *as in Type* 3.
- *Type* 7 : $\langle (x-1)^i + uh_1(x)(x-1)^t + u^2h_2(x)(x-1)^z, u(x-1)^{q_1} + u^2h_3(x)(x-1)^{q_2}\rangle$, *where* $1 \leqslant i \leqslant p^s-1$, $0 \leq t < i$, $0 \leq z < i$, $q_2 < q_1 < i$, *and* $h_1(x), h_2(x)$, $h_3(x)$ *as in Type* 3.
- *Type* 8 : $\langle (x-1)^i + uh_1(x)(x-1)^t + u^2h_2(x)(x-1)^z, u(x-1)^{q_1} + u^2h_3(x)(x-1)^{q_2}, u^2(x-1)^\omega\rangle$, *where* $1 \leqslant i \leqslant p^s-1$, $0 \leq t < \omega$, $0 \leq z < \omega$, $q_2 < q_1 < i$, $\omega < i$, *and* $h_1(x), h_2(x)$ *and* $h_3(x)$ *as in Type* 3.

3. Cyclic codes of length p^s over R_e

In this section, we determine the algebraic structure of all cyclic codes of length p^s over R_e, where $u^e = 0$. The ring R_e is a finite chain ring of nilpotency index e and characteristic p. Its only maximal ideal is $\langle u\rangle$.

The mapping π_e, which is defined as follows, is a surjective ring endomorphism:

$$\pi_e : R_e \longrightarrow R_{e-1},$$
$$\sum_{j=0}^{e-1} u^j a_j(x) \longmapsto \sum_{j=0}^{e-2} u^j a_j(x).$$

and we can extend it as follows:

$$\pi_e : \mathcal{R}_e \longrightarrow \mathcal{R}_{e-1},$$
$$\sum_{j=0}^{e-1} u^j g_j(x) \longmapsto \sum_{j=0}^{e-2} u^j g_j(x)$$

and the mapping μ_e, which is defined as follows, is a surjective ring endomorphism:

$$\mu_e : \mathcal{R}_e \longrightarrow \mathcal{R}_1,$$

$$\sum_{j=0}^{e-1} u^j g_j(x) \longmapsto g_0(x).$$

Remark 3.1. Every element $f(x) \in \mathcal{R}_e$ can be uniquely expressed as

$$f(x) = \sum_{j=0}^{p^s-1} a_{0,j}(x-1)^j + u\sum_{j=0}^{p^s-1} a_{1,j}(x-1)^j + \cdots + u^{e-1}\sum_{j=0}^{p^s-1} a_{e-1,j}(x-1)^j,$$

where $a_{0,j}, a_{1,j}, \dots, a_{e-1,j} \in \mathbb{F}_{p^m}$.

Theorem 3.2. *Let $\mathcal{I}$ be an ideal in $\mathcal{R}_e$. Then*

$$\mathcal{I} = \langle (x-1)^i + uh_1(x)(x-1)^{t_1} + \cdots + u^{e-1}h_{e-1}(x)(x-1)^{t_{e-1}} \rangle + u{\pi_e}^{-1}(\pi_e(\mathcal{I} :_{\mathcal{R}_e} u)),$$

where $0 \le t_j < i$ and either $h_j(x)$'s are 0 or are units for $1 \le j \le e-1$ and $\pi_e(\mathcal{I} :_{\mathcal{R}_e} u)$ is an ideal of $\mathcal{R}_{e-1}$.

Proof. We may assume that $\mathcal{I} = \frac{I}{\langle (x-1)^{p^s} \rangle}$, where I is an ideal in $R_e[x]$ containing $\langle (x-1)^{p^s} \rangle$. Since $\mu_e : R_e[x] \longrightarrow \mathbb{F}_{p^m}[x]$ is an epimorphism, $\mu_e(I)$ is an ideal of $\mathbb{F}_{p^m}[x]$ and there exists a polynomial $g \in R_e[x]$ such that $\mu_e(I) = \langle \mu_e(g) \rangle$. Inasmuch as $\mu_e|_I : I \longrightarrow \mu_e(I)$ is surjective, there is a polynomial $f \in I$ such that $\mu_e(f) = \mu_e(g)$. Let f_1 be an arbitrary polynomial in I. Then $\mu_e(f_1) \in \mu_e(I) = \langle \mu_e(f) \rangle$, and so there exists a polynomial $h \in R_e[x]$ such that $\mu_e(f_1) = \mu_e(h)\mu_e(f) = \mu_e(hf)$. Then $f_1 = hf + r$ for some $r \in \langle u \rangle$. Since $r = f_1 - hf \in I \cap \langle u \rangle$, then $f_1 = hf + r \in \langle f \rangle + (I \cap \langle u \rangle)$ and this implies that $I = \langle f \rangle + (I \cap \langle u \rangle)$. Therefore

$$\begin{aligned} \mathcal{I} = \frac{I}{\langle (x-1)^{p^s} \rangle} &= \frac{\langle f \rangle + \langle (x-1)^{p^s} \rangle}{\langle (x-1)^{p^s} \rangle} + \big(\frac{I}{\langle (x-1)^{p^s} \rangle} \cap \frac{\langle u \rangle + \langle (x-1)^{p^s} \rangle}{\langle (x-1)^{p^s} \rangle} \big) \\ &= \langle f \rangle + (\mathcal{I} \cap \langle u \rangle). \end{aligned}$$

First we show that

$$\langle f \rangle = \langle (x-1)^i + uh_1(x)(x-1)^{t_1} + \cdots + u^{e-1}h_{e-1}(x)(x-1)^{t_{e-1}} \rangle.$$

To see this, inasmuch as $\mathcal{R}_1$ is a chain ring, then $\mu_e(\mathcal{I}) = \langle \mu_e(f) \rangle = \langle (x-1)^i \rangle$, where $0 \le i \le p^s$. Hence, there exists $k(x) \in \mathcal{R}_1$ such that $(x-1)^i = k(x)\mu_e(f)$. Therefore $\mu_e(f)$ is a factor of $(x-1)^i$. Without loss of generality we may assume that $f(x) = (x-1)^i + ug_1(x) + \cdots + u^{e-1}g_{e-1}(x)$, where $g_k(x) \in \mathcal{R}_1$, $\deg(g_k(x)) \le p^s - 1$ and $g_k(x) = \sum_{j=0}^{p^s-1} g_{kj}(x-1)^j$ for $1 \le k \le e-1$. Thus we can write

$$\begin{aligned} f(x) &= (x-1)^i + u\sum_{j=0}^{p^s-1} g_{1j}(x-1)^j + \cdots + u^{e-1}\sum_{j=0}^{p^s-1} g_{e-1j}(x-1)^j \\ &= (x-1)^i + uh_1(x)(x-1)^{t_1} + \cdots + u^{e-1}h_{e-1}(x)(x-1)^{t_{e-1}} \end{aligned}$$

such that $h_k(x) = h_{k0} + \sum_{j=1}^{p^s-1} h_{kj}(x-1)^j$ and $h_{k0} \neq 0$. By Lemma 2.3, $h_k(x)$ is a unit. Therefore

$$\langle f\rangle = \langle (x-1)^i + uh_1(x)(x-1)^{t_1} + \cdots + u^{e-1}h_{e-1}(x)(x-1)^{t_{e-1}}\rangle.$$

Furthermore, we have

$$\mathcal{I} \cap \langle u\rangle = u(\mathcal{I} :_{\mathcal{R}_e} u) = u{\pi_e}^{-1}(\pi_e(\mathcal{I} :_{\mathcal{R}_e} u)),$$

where $\pi_e(\mathcal{I} :_{\mathcal{R}_e} u)$ is an ideal of $\mathcal{R}_{e-1}$. Consequently,

$$\mathcal{I} = \langle (x-1)^i + uh_1(x)(x-1)^{t_1} + \cdots + u^{e-1}h_{e-1}(x)(x-1)^{t_{e-1}}\rangle + u{\pi_e}^{-1}(\pi_e(\mathcal{I} :_{\mathcal{R}_e} u)).$$

□

It is obvious to see that $\langle 0\rangle$ and $\langle 1\rangle$ are cyclic codes of length p^s over R_e, which are the trivial ideals of $\mathcal{R}_e$. In the following theorem, we classify all non-trivial cyclic codes of length p^s over R_e.

Theorem 3.3. *Non-trivial cyclic codes of length p^s over R_e, i.e., non-trivial ideals in $\mathcal{R}_e$, are*

$$\begin{aligned}
&\langle \alpha_1 u^{e-1}(x-1)^{t_1}, \alpha_2(u^{e-2}(x-1)^{t_2} + u^{e-1}h_{11}(x)(x-1)^{t_{11}}), \ldots,\\
&\alpha_{e-1}(u(x-1)^{t_{e-1}} + \sum_{j=1}^{e-2} u^{j+1}h_{e-2,j}(x)(x-1)^{t_{e-2,j}}),\\
&\alpha_e((x-1)^{t_e} + \sum_{j=1}^{e-1} u^j h_{e-1,j}(x)(x-1)^{t_{e-1,j}})\rangle,
\end{aligned}$$

where $0 \leq t_{k,\nu} < t_{k+1}$, $1 \leq t_e \leq p^s - 1$, $h_{k,\nu}(x) \in \mathcal{R}_1$ and either $h_{k,\nu}(x)$'s are 0 or are units for $1 \leq k \leq e-1$, $1 \leq \nu \leq k$ and $t_{k+1} < t_e$ for $k \neq e-1$ and $\alpha_k = 0$ or 1 for $1 \leq k \leq e$ and $(\alpha_1, \alpha_2, \ldots, \alpha_e) \neq (0, 0, \ldots, 0)$.

Proof. Let $\mathcal{I}$ be an arbitrary non-trivial ideal of $\mathcal{R}_e$. By using Theorem 3.2 and using induction on e, we establish all possible forms that the non-trivial ideal $\mathcal{I}$ can have. Thanks to [5, Theorem 5.4] and Theorem 2.5, we have the results for $e = 2$ and 3, respectively. In the first case, assume that $\mathcal{I} \subseteq \langle u\rangle$. Then $\mathcal{I} = u{\pi_e}^{-1}(\pi_e(\mathcal{I} :_{\mathcal{R}_e} u))$, where $\pi_e(\mathcal{I} :_{\mathcal{R}_e} u)$ is an ideal of $\mathcal{R}_{e-1}$. By induction hypothesis we have

$$\begin{aligned}
\pi_e(\mathcal{I} :_{\mathcal{R}_e} u) = \langle &\alpha_1 u^{e-2}(x-1)^{t_1}, \alpha_2(u^{e-3}(x-1)^{t_2} + u^{e-2}h_{11}(x)(x-1)^{t_{11}}),\\
&\ldots, \alpha_{e-2}(u(x-1)^{t_{e-2}} + \sum_{j=1}^{e-3} u^{j+1}h_{e-3,j}(x)(x-1)^{t_{e-3,j}}),\\
&\alpha_{e-1}((x-1)^{t_{e-1}} + \sum_{j=1}^{e-2} u^j h_{e-2,j}(x)(x-1)^{t_{e-2,j}})\rangle
\end{aligned}$$

such that $\alpha_k = 0$ or 1 for $1 \leq k \leq e-1$ and $(\alpha_1, \alpha_2, \ldots, \alpha_{e-1}) \neq (0, 0, \ldots, 0)$. Therefore,

$$\begin{aligned}\mathcal{I} = \langle &\alpha_1 u^{e-1}(x-1)^{t_1}, \alpha_2(u^{e-2}(x-1)^{t_2} + u^{e-1}h_{11}(x)(x-1)^{t_{11}}), \ldots,\\ &\alpha_{e-2}(u^2(x-1)^{t_{e-2}} + \sum_{j=1}^{e-3} u^{j+2}h_{e-3,j}(x)(x-1)^{t_{e-3,j}}),\\ &\alpha_{e-1}(u(x-1)^{t_{e-1}} + \sum_{j=1}^{e-2} u^{j+1}h_{e-2,j}(x)(x-1)^{t_{e-2,j}})\rangle.\end{aligned}$$

Now, we consider the case where $\mathcal{I} \nsubseteq \langle u \rangle$. Then

$$\mathcal{I} = \langle (x-1)^{t_e} + \sum_{j=1}^{e-1} u^j h_{e-1,j}(x)(x-1)^{t_{e-1,j}} \rangle + u{\pi_e}^{-1}(\pi_e(\mathcal{I} :_{\mathcal{R}_e} u)),$$

where $\pi_e(\mathcal{I} :_{\mathcal{R}_e} u)$ is an ideal of $\mathcal{R}_{e-1}$. By induction hypothesis we have

$$\begin{aligned}\mathcal{I} = \langle &\alpha_1 u^{e-1}(x-1)^{t_1}, \alpha_2(u^{e-2}(x-1)^{t_2} + u^{e-1}h_{11}(x)(x-1)^{t_{11}}), \ldots,\\ &\alpha_{e-1}(u(x-1)^{t_{e-1}} + \sum_{j=1}^{e-2} u^{j+1}h_{e-2,j}(x)(x-1)^{t_{e-2,j}}),\\ &(x-1)^{t_e} + \sum_{j=1}^{e-1} u^j h_{e-1,j}(x)(x-1)^{t_{e-1,j}}\rangle,\end{aligned}$$

where $\alpha_k = 0$ or 1 for $1 \leq k \leq e-1$ and the proof is complete. $\square$

Here, we provide an optimal cyclic codes of length p^s over R_5. Let us start with the following definition.

Definition. Define the *Gray map* $\rho : R_5 \longrightarrow \mathbb{F}_{p^m}^{16}$ by

$$\begin{aligned}\rho(a_0 + ua_1 + u^2a_2 + u^3a_3 + u^4a_4) = (&a_4, a_4 + a_0, a_4 + a_1, a_4 + a_2, a_4 + a_3,\\ &a_4 + a_0 + a_1, a_4 + a_0 + a_2, a_4 + a_0 + a_3,\\ &a_4 + a_1 + a_2, a_4 + a_1 + a_3, a_4 + a_2 + a_3,\\ &a_4 + a_0 + a_1 + a_2, a_4 + a_0 + a_1 + a_3,\\ &a_4 + a_0 + a_2 + a_3, a_4 + a_1 + a_2 + a_3,\\ &a_4 + a_0 + a_1 + a_2 + a_3).\end{aligned}$$

We can generalize this Gray map for all $x = (x_0, x_1, \ldots, x_{p^s-1}) \in R_5^{p^s}$ as follows:

$$\varrho : R_5^{p^s} \longrightarrow \mathbb{F}_{p^m}^{16p^s},$$
$$\varrho(x_0, x_1, \ldots, x_{p^s-1}) = (\rho(x_0), \rho(x_1), \ldots, \rho(x_{p^s-1})).$$

Therefore, $\mathcal{C} = \varrho(C)$ is a cyclic code of length $16p^s$ over $\mathbb{F}_{p^m}$.

Example 3.4. Let $\mathcal{R}_5 = \frac{(\mathbb{F}_{5^5}+u\mathbb{F}_{5^5}+u^2\mathbb{F}_{5^5}+u^3\mathbb{F}_{5^5}+u^4\mathbb{F}_{5^5})[x]}{\langle x^5-1\rangle}$ and δ be a primitive (5^5-1)th root of unity in $\mathbb{F}_{5^5}$. Consider the following code:

$$\begin{aligned} C &= \langle u^2(x-1)^4 + u^3\delta\big((\delta^3+\delta^2+1)+(1+2\delta^3)(x-1)+\delta^3(x-1)^2\big) \\ &\quad + u^4\delta^3\big((1+\delta+\delta^2+\delta^4)+(1+2\delta^2-3\delta^4)(x-1) \\ &\quad + (\delta^2-3\delta^4)(x-1)^2+\delta^4(x-1)^3\big)\rangle \\ &= \langle(u^2+u^3\delta^3+u^4\delta^4)+(u^2+u^3\delta+u^4\delta^3)x+(u^2+u^3\delta^4+u^4\delta^5)x^2 \\ &\quad + (u^2+u^4\delta^7)x^3+u^2x^4\rangle. \end{aligned}$$

Then, C has a generator matrix of the form

$$\begin{bmatrix} u^2+u^3\delta^3+u^4\delta^4 & u^2+u^3\delta+u^4\delta^3 & u^2+u^3\delta^4+u^4\delta^5 & u^2+u^4\delta^7 & u^2 \end{bmatrix},$$

and so $\varrho(C)$ is an optimal code with parameters $[80, 3, 64]$.

4. Cyclic codes of length p^s over $R_4 = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m} + u^3\mathbb{F}_{p^m}$

In this section, we determine the algebraic structure of all cyclic codes of length p^s over R_e, in the case that $e = 4$. Recall that R_4 is a finite chain ring of nilpotency index 4 and characteristic p. Its only maximal ideal is $u\mathbb{F}_{p^m}$.

Proposition 4.1. *Every element $f(x) \in \mathcal{R}_4$ can be uniquely expressed as*

$$\begin{aligned} f(x) = &\sum_{j=0}^{p^s-1} a_{0j}(x-1)^j + u\sum_{j=0}^{p^s-1} a_{1j}(x-1)^j + u^2\sum_{j=0}^{p^s-1} a_{2j}(x-1)^j \\ &+ u^3\sum_{j=0}^{p^s-1} a_{3j}(x-1)^j, \end{aligned}$$

where $a_{kj} \in \mathbb{F}_{p^m}$ for $0 \le k \le 4$.

Definition. The mapping π_4, which is defined as follows, is a surjective ring endomorphism:

$$\begin{aligned} \pi_4 : R_4 &\longrightarrow R_3, \\ \sum_{j=0}^{3} u^j a_j &\longmapsto \sum_{j=0}^{2} u^j a_j, \end{aligned}$$

and we can extend it as follows:

$$\begin{aligned} \pi_4 : \mathcal{R}_4 &\longrightarrow \mathcal{R}_3, \\ \sum_{j=0}^{3} u^j g_j(x) &\longmapsto \sum_{j=0}^{2} u^j g_j(x). \end{aligned}$$

Remark 4.2. We extend the natural ring morphism $\mu_4 : R_4 \longrightarrow \mathbb{F}_{p^m}$, where $\mu_4(a_0 + ua_1 + u^2a_2 + u^3a_3) = a_0$, as follows:

$$\mu_4 : R_4[x] \longrightarrow \mathbb{F}_{p^m}[x],$$

$$\sum_{j=0}^{3} u^j g_j(x) \longmapsto g_0(x).$$

Note that it can be even extended to $\mu_4 : \mathcal{R}_4 \longrightarrow \mathcal{R}_1$. For each ideal $\mathcal{I}$ in $\mathcal{R}_4$, the image $\mu_4(\mathcal{I} :_{\mathcal{R}_4} u^i) = \mu_4(\{v \in \mathcal{R}_4 : vu^i \in \mathcal{I}\})$ is an ideal in $\mathcal{R}_1$ for $i = 0, 1, 2, 3$. Inasmuch as every cyclic code C over the ring R_4 is an ideal of $\mathcal{R}_4$, so $\mu_4(C :_{\mathcal{R}_4} u^i)$ is in fact a cyclic code over $\mathbb{F}_{p^m}$ which is called the *torsion code* associated to C and it is denoted by $\mathrm{Tor}_i(C)$. By Proposition 2.4, $\mathrm{Tor}_i(C) = \langle (x-1)^{T_i} \rangle$, where $0 \le T_i \le p^s$.

As a consequence of Theorem 3.3, we classify the cyclic codes of length p^s over R_4 as following.

Theorem 4.3. *Cyclic codes of length p^s over R_4, i.e., ideals of the ring $\mathcal{R}_4$, can be separated into the following types*:

- *Type* 1 : $\langle 0 \rangle$, $\langle 1 \rangle$.
- *Type* 2 : $\langle u^3(x-1)^i \rangle$, *where* $0 \leqslant i \leqslant p^s - 1$.
- *Type* 3 : $\langle u^2(x-1)^i + u^3 h(x)(x-1)^t \rangle$, *where* $0 \le i \le p^s - 1$, $0 \le t < i$, *and either* $h(x)$ *is* 0 *or* $h(x)$ *is a unit, which can be represented as* $h(x) = \sum_j h_j(x-1)^j$ *with* $h_j \in \mathbb{F}_{p^m}$, *and* $h_0 \neq 0$.
- *Type* 4 : $\langle u^2(x-1)^i + u^3 h(x)(x-1)^t, u^3(x-1)^{\omega} \rangle$, *where* $0 \le i \le p^s - 1$, $0 \le t < i$, $\omega < i$, $h(x)$ *as in Type* 3, *and* $\deg(h(x)) \le \omega - t - 1$.
- *Type* 5 : $\langle u(x-1)^i + u^2 h_1(x)(x-1)^{t_1} + u^3 h_2(x)(x-1)^{t_2} \rangle$, *where* $0 \le i \le p^s - 1$, $0 \le t_1 < i$, $0 \le t_2 < i$, *and* $h_1(x)$, $h_2(x)$ *are similar to* $h(x)$ *in Type* 3.
- *Type* 6 : $\langle u(x-1)^i + u^2 h_1(x)(x-1)^{t_1} + u^3 h_2(x)(x-1)^{t_2}, u^3(x-1)^{\omega} \rangle$, *where* $0 \le i \le p^s - 1$, $0 \le t_1 < i$, $0 \le t_2 < i$, $\omega < i$, *and* $h_1(x), h_2(x)$ *are similar to* $h(x)$ *in Type* 3.
- *Type* 7 : $\langle u(x-1)^i + u^2 h_1(x)(x-1)^{t_1} + u^3 h_2(x)(x-1)^{t_2},\ u^2(x-1)^{q_1} + u^3 h_3(x)(x-1)^{q_2} \rangle$, *where* $0 \le i \le p^s - 1$, $0 \le t_1 < i$, $0 \le t_2 < i$, $0 \le q_2 < q_1 < i$, *and* $h_1(x), h_2(x), h_3(x)$ *are similar to* $h(x)$ *in Type* 3.
- *Type* 8 : $\langle u(x-1)^i + u^2 h_1(x)(x-1)^{t_1} + u^3 h_2(x)(x-1)^{t_2}, u^2(x-1)^{q_1} + u^3 h_3(x)(x-1)^{q_2}, u^3(x-1)^{\omega} \rangle$, *where* $0 \le i \le p^s - 1$, $0 \le t_1 < i$, $0 \le t_2 < i$, $0 \le q_2 < q_1 < i$, *and* $\omega < i$, *and* $h_1(x), h_2(x), h_3(x)$ *are similar to* $h(x)$ *in Type* 3.
- *Type* 9 : $\langle (x-1)^i + u h_1(x)(x-1)^{t_1} + u^2 h_2(x)(x-1)^{t_2} + u^3 h_3(x)(x-1)^{t_3} \rangle$, *where* $1 \le i \le p^s - 1$, $0 \le t_1 < i$, $0 \le t_2 < i$, $0 \le t_3 < i$, *and* $h_1(x), h_2(x), h_3(x)$ *are similar to* $h(x)$ *in Type* 3.
- *Type* 10 : $\langle (x-1)^i + u h_1(x)(x-1)^{t_1} + u^2 h_2(x)(x-1)^{t_2} + u^3 h_3(x)(x-1)^{t_3}, u^3(x-1)^{\omega} \rangle$, *where* $1 \le i \le p^s - 1$, $0 \le t_1 < i$, $0 \le t_2 < i$, $0 \le t_3 < i$, *and* $h_1(x), h_2(x), h_3(x)$ *are similar to* $h(x)$ *in Type* 3.
- *Type* 11 : $\langle (x-1)^i + u h_1(x)(x-1)^{t_1} + u^2 h_2(x)(x-1)^{t_2} + u^3 h_3(x)(x-1)^{t_3}, u^2(x-1)^{q_1} + u^3 h_4(x)(x-1)^{q_2} \rangle$, *where* $1 \le i \le p^s - 1$, $0 \le t_1 < i$, $0 \le t_2 < i$, $0 \le t_3 < i$, $0 \le q_1 < i$, $0 \le q_2 < q_1$ *and* $h_1(x), h_2(x), h_3(x), h_4(x)$ *are similar to* $h(x)$ *in Type* 3.

• *Type* 12 : $\langle (x-1)^i + uh_1(x)(x-1)^{t_1} + u^2h_2(x)(x-1)^{t_2} + u^3h_3(x)(x-1)^{t_3}, u^2(x-1)^{q_1} + u^3h_4(x)(x-1)^{q_2}, u^3(x-1)^{\omega}\rangle$, *where* $1 \le i \le p^s-1$, $0 \le t_1 < i$, $0 \le t_2 < i$, $0 \le t_3 < i$, $0 \le q_2 < q_1 < i$, *and* $\omega < i$, *and* $h_1(x), h_2(x), h_3(x), h_4(x)$ *are similar to* $h(x)$ *in Type* 3, $\deg(h_4(x)) < \omega - q_2$.

• *Type* 13 : $\langle (x-1)^i + uh_1(x)(x-1)^{t_1} + u^2h_2(x)(x-1)^{t_2} + u^3h_3(x)(x-1)^{t_3}, u(x-1)^{q_1} + u^2h_4(x)(x-1)^{q_2} + u^3h_5(x)(x-1)^{q_3}\rangle$, *where* $1 \le i \le p^s-1$, $0 \le t_1 < i$, $0 \le t_2 < i$, $0 \le t_3 < i$, $0 \le q_2, q_3 < q_1 < i$, *and* $h_j(x)$ *is similar to* $h(x)$ *in Type* 3 *for* $1 \le j \le 5$.

• *Type* 14 : $\langle (x-1)^i + uh_1(x)(x-1)^{t_1} + u^2h_2(x)(x-1)^{t_2} + u^3h_3(x)(x-1)^{t_3} u(x-1)^{q_1} + u^2h_4(x)(x-1)^{q_2} + u^3h_5(x)(x-1)^{q_3}, u^3(x-1)^{\omega}\rangle$, *where* $1 \le i \le p^s-1$, $0 \le t_1 < i$, $0 \le t_2 < i$, $0 \le t_3 < i$, $0 \le q_2 < q_1 < i$, $0 \le q_3 < q_1$, $\omega < i$, *and* $h_j(x)$ *is similar to* $h(x)$ *in Type* 3 *for* $1 \le j \le 5$. *Also* $\deg(h_5(x)) < \omega - q_3$.

• *Type* 15 : $\langle (x-1)^i + uh_1(x)(x-1)^{t_1} + u^2h_2(x)(x-1)^{t_2} + u^3h_3(x)(x-1)^{t_3}, u(x-1)^{q_1} + u^2h_4(x)(x-1)^{q_2} + u^3h_5(x)(x-1)^{q_3}, u^2(x-1)^{z_1} + u^3h_6(x)(x-1)^{z_2}\rangle$, *where* $1 \le i \le p^s-1$, $0 \le t_1 < i$, $0 \le t_2 < i$, $0 \le t_3 < i$, $0 \le q_2 < q_1 < i$, $0 \le q_3 < q_1$, $0 \le z_2 < z_1 < i$, *and* $h_j(x)$ *is similar to* $h(x)$ *in Type* 3 *for* $1 \le j \le 6$.

• *Type* 16 : $\langle (x-1)^i + uh_1(x)(x-1)^{t_1} + u^2h_2(x)(x-1)^{t_2} + u^3h_3(x)(x-1)^{t_3}, u(x-1)^{q_1} + u^2h_4(x)(x-1)^{q_2} + u^3h_5(x)(x-1)^{q_3}, u^2(x-1)^{z_1} + u^3h_6(x)(x-1)^{z_2}, u^3(x-1)^{\omega}\rangle$, *where* $1 \le i \le p^s-1$, $0 \le t_1 < i$, $0 \le t_2 < i$, $0 \le t_3 < i$, $0 \le q_2 < q_1 < i$, $0 \le q_3 < q_1$, $0 \le z_2 < z_1 < i$, $\omega < i$ *and* $h_j(x)$ *is similar to* $h(x)$ *in Type* 3 *for* $1 \le j \le 6$. *Also* $\deg(h_6(x)) < \omega - z_2$.

Let C be a cyclic code of length p^s over R_4. As we mentioned in Remark 4.2, $\mathrm{Tor}_i(C)$ is of the form $\langle (x-1)^{T_i}\rangle$. Now, we determine the integer T_1 for different types presented in Theorem 4.3. It is easy to see that in Type 1, T_1 is p^s or 0, and in Types $2-4$, T_1 is p^s. Furthermore in Types $5-8$, T_1 is i, and in Types $13-16$, T_1 is q_1. In the following, we obtain the integer T_1 for other types.

Proposition 4.4. *In Type* 9,

$$T_1 = \begin{cases} i, & \text{if } \ h_1(x) = 0, \\ \min\{p^s - i + t_1, i\}, & \text{if } \ h_1(x) \neq 0. \end{cases}$$

Proof. The integer T_1 is the smallest non-negative integer satisfying

$$\begin{aligned} &u(x-1)^{T_1} + u^2\ell_1(x) + u^3\ell_2(x) \\ &\in \langle (x-1)^i + uh_1(x)(x-1)^{t_1} + u^2h_2(x)(x-1)^{t_2} + u^3h_3(x)(x-1)^{t_3}\rangle \end{aligned}$$

for some $\ell_1(x)$ and $\ell_2(x) \in \mathcal{R}_1$. Inasmuch as

$$\begin{aligned} &u(x-1)^i + u^2h_1(x)(x-1)^{t_1} + u^3h_2(x)(x-1)^{t_2} \\ &= u\big[(x-1)^i + uh_1(x)(x-1)^{t_1} + u^2h_2(x)(x-1)^{t_2} + u^3h_3(x)(x-1)^{t_3}\big] \\ &\in \langle (x-1)^i + uh_1(x)(x-1)^{t_1} + u^2h_2(x)(x-1)^{t_2} + u^3h_3(x)(x-1)^{t_3}\rangle, \end{aligned}$$

therefore $T_1 \leq i$. If $h_1(x) \neq 0$, then we have

$$\begin{aligned}
&u(x-1)^{p^s-i+t_1} + u^2(h_1(x))^{-1}h_2(x)(x-1)^{p^s-i+t_2} \\
&+ u^3(h_1(x))^{-1}h_3(x)(x-1)^{p^s-i+t_3} \\
=\ &(h_1(x))^{-1}(x-1)^{p^s-i}\big[(x-1)^i + uh_1(x)(x-1)^{t_1} + u^2h_2(x)(x-1)^{t_2} \\
&+ u^3h_3(x)(x-1)^{t_3}\big] \\
\in\ &\langle (x-1)^i + uh_1(x)(x-1)^{t_1} + u^2h_2(x)(x-1)^{t_2} + u^3h_3(x)(x-1)^{t_3}\rangle,
\end{aligned}$$

implying that $T_1 \leq p^s - i + t_1$. Hence $T_1 \leq \min\{p^s - i + t_1, i\}$. Since

$$\begin{aligned}
&u(x-1)^{T_1} + u^2\ell_1(x) + u^3\ell_2(x) \\
\in\ &\langle (x-1)^i + uh_1(x)(x-1)^{t_1} + u^2h_2(x)(x-1)^{t_2} + u^3h_3(x)(x-1)^{t_3}\rangle,
\end{aligned}$$

there exists $f(x) \in \mathcal{R}_4$ such that

$$\begin{aligned}
&u(x-1)^{T_1} + u^2\ell_1(x) + u^3\ell_2(x) \\
=\ &f(x)\big((x-1)^i + uh_1(x)(x-1)^{t_1} + u^2h_2(x)(x-1)^{t_2} + u^3h_3(x)(x-1)^{t_3}\big),
\end{aligned}$$

where $f(x)$ is of the form

$$\sum_{j=0}^{p^s-1} a_{0j}(x-1)^j + u\sum_{j=0}^{p^s-1} a_{1j}(x-1)^j + u^2\sum_{j=0}^{p^s-1} a_{2j}(x-1)^j + u^3\sum_{j=0}^{p^s-1} a_{3j}(x-1)^j,$$

and $a_{kj} \in \mathbb{F}_{p^m}$ for $0 \leq k \leq 3$. Thus $u(x-1)^{T_1}$ can be expressed as

$$\begin{aligned}
&u(x-1)^{T_1} \\
=\ &(x-1)^i \sum_{j=0}^{p^s-1} a_{0j}(x-1)^j \\
&+ uh_1(x)(x-1)^{t_1}\sum_{j=0}^{p^s-1} a_{0j}(x-1)^j + u(x-1)^i\sum_{j=0}^{p^s-1} a_{1j}(x-1)^j \\
=\ &u[h_1(x)(x-1)^{t_1}\sum_{j=0}^{p^s-1} a_{0j}(x-1)^j + (x-1)^i \sum_{j=0}^{p^s-i-1} a_{1j}(x-1)^j] \\
=\ &u[h_1(x)(x-1)^{t_1}\sum_{j=p^s-i}^{p^s-1} a_{0j}(x-1)^j + (x-1)^i \sum_{j=0}^{p^s-i-1} a_{1j}(x-1)^j] \\
=\ &u[(x-1)^{p^s-i+t_1}h_1(x)\sum_{j=0}^{i-1} a_{0,j+p^s-i}(x-1)^j + (x-1)^i \sum_{j=0}^{p^s-i-1} a_{1j}(x-1)^j].
\end{aligned}$$

Hence $T_1 \geq \min\{p^s - i + t_1, i\}$, which means that

$$T_1 = \min\{p^s - i + t_1, i\}. \qquad \square$$

By a similar argument as the proof of Proposition 4.4, we have the following result.

Proposition 4.5. *In Types* 10, 11 *and* 12, *we have*

$$T_1 = \begin{cases} i, & \text{if } \ h_1(x) = 0, \\ \min\{p^s - i + t_1, i\}, & \text{if } \ h_1(x) \neq 0. \end{cases}$$

4.1. Examples

In this subsection, we provide some optimal cyclic codes of length p^s over R_4.

Definition. Define the *Gray map* $\psi : R_4 \longrightarrow \mathbb{F}_{p^m}^8$ by

$$\begin{aligned} \psi(a_0 + ua_1 + u^2a_2 + u^3a_3) = (&a_3, a_3 + a_0, a_3 + a_1, a_3 + a_2, a_3 + a_0 + a_1, \\ &a_3 + a_0 + a_2, a_3 + a_1 + a_2, a_3 + a_0 + a_1 + a_2). \end{aligned}$$

We can generalize this Gray map for all $x = (x_0, x_1, \dots, x_{p^s-1}) \in R_4^{p^s}$ as follows:

$$\phi : R_4^{p^s} \longrightarrow \mathbb{F}_{p^m}^{8p^s},$$
$$\phi(x_0, x_1, \dots, x_{p^s-1}) = (\psi(x_0), \psi(x_1), \dots, \psi(x_{p^s-1})).$$

Hence, $\mathcal{C} = \phi(C)$ is a cyclic code of length $8p^s$ over $\mathbb{F}_{p^m}$.

Inasmuch as ϕ is a linear map, we get the following lemma.

Lemma 4.6. $\phi : (R_4^{p^s}, \text{Lee distances}) \longrightarrow (\mathbb{F}_{p^m}^{8p^s}, \text{Hamming distances})$ *is a distance preserving map.*

Example 4.7. Let $\mathcal{R}_4 = \frac{(\mathbb{F}_{16} + u\mathbb{F}_{16} + u^2\mathbb{F}_{16} + u^3\mathbb{F}_{16})[x]}{\langle x^4 - 1 \rangle}$ and δ be a primitive 15th root of unity in $\mathbb{F}_{16}$, i.e., $\mathbb{F}_{16} = \{0, \delta, \dots, \delta^{15}, \delta^{16} = 1\}$. Consider the following code:

$$\begin{aligned} C &= \langle (x-1)^3 + ux(x-1) + u^2\delta(x-1)^2 + u^3\delta^2(x-1) \rangle \\ &= \langle (1 + u^2\delta + u^3\delta^2) + (1 + u + u^3\delta^2)x + (1 + u + u^2\delta)x^2 + x^3 \rangle. \end{aligned}$$

Then, C has a generator matrix of the form

$$\begin{bmatrix} 1 + u^2\delta + u^3\delta^2 & 1 + u + u^3\delta^2 & 1 + u + u^2\delta & 1 \end{bmatrix}.$$

$\phi(C)$ has the following generator matrix

$$\left[\begin{smallmatrix} \delta^2 & \delta^2+1 & \delta^2 & \delta^2+\delta & \delta^2+1 & \delta^2+\delta+1 & \delta^2+\delta & \delta^2+\delta+1 & \delta^2 & \delta^2+1 & \delta^2+1 & \delta^2 & \delta^2 & \delta^2+1 & \delta^2+1 & \delta^2 & 0 & 1 & 1 & \delta & 0 & \delta+1 & \delta+1 & \delta & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ \delta & \delta & \delta+1 & \delta & \delta+1 & \delta & \delta+1 & \delta+1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \delta & \delta & \delta+1 & \delta+1 & \delta+1 & \delta+1 & \delta & \delta & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{smallmatrix}\right].$$

Hence, $\phi(C)$ is an optimal code with parameters $[32, 4, 16]$.

Example 4.8. Let $\mathcal{R}_4=\frac{(\mathbb{F}_{27}+u\mathbb{F}_{27}+u^2\mathbb{F}_{27}+u^3\mathbb{F}_{27})[x]}{\langle x^3-1\rangle}$ and δ be a primitive 26th root of unity in $\mathbb{F}_{27}$, i.e., $\mathbb{F}_{27}=\{0,\delta,\ldots,\delta^{26},\delta^{27}=1\}$. Consider the following codes:

• $C=\langle (x-1)+u\delta+u^2\delta^2\rangle=\langle(-1+u\delta+u^2\delta^2)+x\rangle$.

Thus, C has a generator matrix of the form

$$\begin{bmatrix} -1+u\delta+u^2\delta^2 & 1 & 0 \\ \\ 0 & -1+u\delta+u^2\delta^2 & 1 \end{bmatrix}.$$

$\phi(C)$ has the following generator matrix

$$\left[\begin{array}{cccccccccccccccccccccccc}
0 & 2 & \delta & \delta^2 & \delta+2 & \delta^2+2 & \delta+\delta^2 & \delta+\delta^2+2 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & \delta & \delta^2 & \delta+2 & \delta^2+2 & \delta+\delta^2 & \delta+\delta^2+2 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
\delta^2 & \delta^2 & \delta^2+2 & \delta^2+\delta & \delta^2+2 & \delta^2+\delta & \delta^2+\delta+2 & \delta^2+\delta+2 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \delta^2 & \delta^2 & \delta^2+2 & \delta^2+\delta & \delta^2+2 & \delta^2+\delta & \delta^2+\delta+2 & \delta^2+\delta+2 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
\delta & \delta & \delta & \delta-1 & \delta & \delta-1 & \delta-1 & \delta-1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \delta & \delta & \delta & \delta-1 & \delta & \delta-1 & \delta-1 & \delta-1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right].$$

Hence, $\phi(C)$ is an optimal code with parameters $[24,8,11]$.

• $C=\langle (x-1)^2+u(x-1)+u^2\delta\rangle=\langle(1-u+u^2\delta)+(1+u)x+x^2\rangle$ is a cyclic code over R_4. Therefore, C has a generator matrix of the form

$$\begin{bmatrix} 1-u+u^2\delta & 1+u & 1 \end{bmatrix}.$$

$\phi(C)$ has the following generator matrix

$$\left[\begin{array}{cccccccccccccccccccccccc}
0 & 1 & 2 & \delta & 0 & \delta+1 & \delta-1 & \delta & 0 & 1 & 1 & 0 & 2 & 1 & 1 & 2 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
\delta & \delta & \delta+1 & \delta-1 & \delta+1 & \delta-1 & \delta & \delta & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
2 & 2 & 2 & 0 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right].$$

So, $\phi(C)$ is an optimal code with parameters $[24,4,15]$.

5. Conclusion

In this paper, we first studied the structure of cyclic codes of length p^s over R_e. We determined the generator polynomials of this family of codes. Then, we specified the structures of cyclic codes of length p^s over R_4. Also, we obtained the torsion codes of these codes. Finally, we provided several examples of optimal cyclic codes over R_4 and R_5.

References

[1] T. Abualrub and I. Siap, *Cyclic codes over the rings Z_2+uZ_2 and $Z_2+uZ_2+u^2Z_2$*, Des. Codes Cryptogr. **42** (2007), no. 3, 273–287. https://doi.org/10.1007/s10623-006-9034-5

[2] Y. Cao, Y. Cao, H. Q. Dinh, F. Fu, J. Gao, and S. Sriboonchitta, *A class of repeated-root constacyclic codes over* $\mathbb{F}_{p^m}[u]/\langle u^e \rangle$ *of Type* 2, Finite Fields Appl. **55** (2019), 238–267. `https://doi.org/10.1016/j.ffa.2018.10.003`

[3] H. Q. Dinh, *Negacyclic codes of length* 2^s *over Galois rings*, IEEE Trans. Inform. Theory **51** (2005), no. 12, 4252–4262. `https://doi.org/10.1109/TIT.2005.859284`

[4] H. Q. Dinh, *On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions*, Finite Fields Appl. **14** (2008), no. 1, 22–40. `https://doi.org/10.1016/j.ffa.2007.07.001`

[5] H. Q. Dinh, *Constacyclic codes of length* p^s *over* $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, J. Algebra **324** (2010), no. 5, 940–950. `https://doi.org/10.1016/j.jalgebra.2010.05.027`

[6] H. Q. Dinh, S. Dhompongsa, and S. Sriboonchitta, *Repeated-root constacyclic codes of prime power length over* $\frac{\mathbb{F}_{p^m}[u]}{\langle u^a \rangle}$ *and their duals*, Discrete Math. **339** (2016), no. 6, 1706–1715. `https://doi.org/10.1016/j.disc.2016.01.020`

[7] H. Q. Dinh and S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory **50** (2004), no. 8, 1728–1744. `https://doi.org/10.1109/TIT.2004.831789`

[8] J. Gao, F. Fu, L. Xiao, and R. K. Bandi, *Some results on cyclic codes over* $\mathbb{Z}_q + u\mathbb{Z}_q$, Discrete Math. Algorithms Appl. **7** (2015), no. 4, 1550058, 9 pp. `https://doi.org/10.1142/S1793830915500585`

[9] X. Liu, *A note on cyclic codes over* $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$, J. Math. **36** (2016), No. 5.

[10] X. Liu and X. Xu, *Some classes of repeated-root constacyclic codes over* $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$, J. Korean Math. Soc. **51** (2014), no. 4, 853–866. `https://doi.org/10.4134/JKMS.2014.51.4.853`

Roghayeh Mohammadi Hesari
Department of Mathematics
Malayer University
Malayer, Iran
Email address: `r.mohammadi1363@yahoo.com`

Masoumeh Mohebbei
Department of Mathematics
Malayer University
Malayer, Iran
Email address: `masum.moheby@yahoo.com`

Rashid Rezaei
Department of Mathematics
Malayer University
Malayer, Iran
Email address: `ras_rezaei@yahoo.com, r.rezaei@malayeru.ac.ir`

Karim Samei
Department of Mathematics
Bu Ali Sina University
Hamedan, Iran
Email address: `samei@ipm.ir`