Filomat 37:26 (2023), 9009–9038
https://doi.org/10.2298/FIL2326009D

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

Cyclic codes of length $5p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and their duals

Hai Q Dinh[a], Bac T Nguyen[b,c], Roengchai Tansuchat[d], Hiep L. Thi[e,*]

[a] *Department of Mathematical Sciences, Kent State University, Ohio, USA*
[b] *Institute of Fundamental and Applied Sciences, Duy Tan University, Ho Chi Minh City 700000, Vietnam*
[c] *Faculty of Natural Sciences, Duy Tan University, Da Nang, 550000, Vietnam*
[d] *Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University, Thailand*
[e] *Faculty of Education, Thu Dau Mot University, Binh Duong, Vietnam*

Abstract. For an odd prime $p \neq 5$, the structures of cyclic codes of length $5p^s$ over $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}(u^2 = 0)$ are completely determined. Cyclic codes of length $5p^s$ over $\mathcal{R}$ are considered in 3 cases, namely, $p \equiv 1 \pmod 5$, $p \equiv 4 \pmod 5$, $p \equiv 2$ *or* $3 \pmod 5$. When $p \equiv 1 \pmod 5$, a cyclic code of length $5p^s$ over $\mathcal{R}$ can be expressed as a direct sum of a cyclic code and $\gamma_i^{p^s}$-constacyclic codes of length p^s over $\mathcal{R}$, where $\gamma_i^{p^s} = -\frac{i(p^m-1)p^s}{10}, i = 1,3,7,9$. When $p \equiv 4 \pmod 5$, it is equivalent to $p^m \equiv 1 \pmod 5$ when m is even and $p^m \equiv 4 \pmod 5$ when m is odd. If $p^m \equiv 1 \pmod 5$ when m is even, then a cyclic code of length $5p^s$ over $\mathcal{R}$ can be obtained as a direct sum of a cyclic code and $\gamma_i^{p^s}$-constacyclic codes of length p^s over $\mathcal{R}$, where $\gamma_i^{p^s} = -\frac{i(p^m-1)p^s}{10}, i = 1,3,7,9$. If $p^m \equiv 4 \pmod 5$ when m is odd, then a cyclic code of length $5p^s$ over $\mathcal{R}$ can be expressed as a direct sum of a cyclic code of length p^s over $\mathcal{R}$ and an α_1 and α_2-constacyclic code of length $2p^s$ over $\mathcal{R}$, for some $\alpha_1, \alpha_2 \in \mathbb{F}_{p^m} \setminus \{0\}$. If $p \equiv 2$ *or* $3 \pmod 5$ such that $p^m \not\equiv 1 \pmod 5$, then a cyclic code of length $5p^s$ over $\mathcal{R}$ can be expressed as $C_1 \oplus C_2$, where C_1 is an ideal of $\frac{\mathcal{R}[x]}{\langle x^{p^s}-1\rangle}$ and C_2 is an ideal of $\frac{\mathcal{R}[x]}{\langle (x^4+x^3+x^2+x+1)^{p^s}\rangle}$. We also investigate all ideals of $\frac{\mathcal{R}[x]}{\langle (x^4+x^3+x^2+x+1)^{p^s}\rangle}$ to study detail structure of a cyclic code of length $5p^s$ over $\mathcal{R}$. In addition, dual codes of all cyclic codes of length $5p^s$ over $\mathcal{R}$ are also given. Furthermore, we give the number of codewords in each of those cyclic codes of length $5p^s$ over $\mathcal{R}$. As cyclic and negacyclic codes of length $5p^s$ over $\mathcal{R}$ are in a one-by-one equivalent via the ring isomorphism $x \mapsto -x$, all our results for cyclic codes hold true accordingly to negacyclic codes.
Keywords. Cyclic codes, constacyclic codes, dual codes, repeated-root codes.

1. Introduction

Let p be a prime number and $\mathbb{F}_{p^m}$ a finite field. An $[n,k]$ linear code C over $\mathbb{F}_{p^m}$ is a k-dimensional subspace of $\mathbb{F}_{p^m}^n$. A linear code C of length n over $\mathbb{F}_{p^m}$ is called a *cyclic code*, *negacyclic code* and *λ-constacyclic code* if it is an ideal of the ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^n-1\rangle}$, $\frac{\mathbb{F}_{p^m}[x]}{\langle x^n+1\rangle}$, and $\frac{\mathbb{F}_{p^m}[x]}{\langle x^n-\lambda\rangle}$, respectively. The classes of cyclic and negacyclic codes have been well studied since the late 1960's.

2020 *Mathematics Subject Classification*. Primary 94B15, 94B05; Secondary 11T71.
Keywords. Cyclic codes, constacyclic codes, dual codes, repeated-root codes.
Received: 01 December 2022; Accepted: 10 April 2023
Communicated by Paola Bonacini
* Corresponding author: Hiep L. Thi
Email addresses: hdinh@kent.edu (Hai Q Dinh), nguyentrongbac@duytan.edu.vn (Bac T Nguyen), roengchaitan@gmail.com (Roengchai Tansuchat), lthiep@tdmu.edu.vn (Hiep L. Thi)

Cyclic codes are the most studied of all codes. Many well-known codes, such as BCH, Kerdock, Golay, Reed-Muller, Preparata, Justesen, and binary Hamming codes, are either cyclic codes or constructed from cyclic codes. The class of cyclic codes is very interesting because cyclic codes are easy to encode and decode. Cyclic codes are especially fast when implemented in hardware. Therefore, they are a good option for many networks.

In 1957, Prange [40] first studied the class of cyclic codes over finite fields. In 1968, Berlakamp [5] first initiated the class of negacyclic codes over finite fields. In 1967, Berman [6] considered the case when $(n, p) = p$ yields the so-called repeated-root codes. Recently, λ-constacyclic codes of lengths $2p^s$, $3p^s$, ℓp^s over $\mathbb{F}_{p^m}$ are investigated in [17], [18], [13], respectively.

In 1994, Hammons *et al.* [28] showed that good non-linear codes can be constructed from linear codes over $\mathbb{Z}_4$ via the Gray map. After that, [1], [8], [19] studied repeated-root codes over certain classes of finite chain rings. In 1999, A. Bonnecaze and P. Udaya studied codes over $\mathbb{F}_2 + u\mathbb{F}_2$, where $u^2 = 0$ and then [2, 3] also considered codes over $\mathbb{F}_2 + u\mathbb{F}_2$, where $u^2 = 0$. In 2010, Dinh [16] established the structures of all constacyclic codes of length p^s over $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. After that, in [17], he gave the structures of all constacyclic codes of length $2p^s$ over the finite field $\mathbb{F}_{p^m}$. In 2018, Dinh *et al.* investigated all negacyclic and constacyclic codes of length $4p^s$ over $\mathcal{R}$ [20], [22], [23], [24]. In 2020, constacyclic codes of length $3p^s$ over $\mathcal{R}$ is studied in [21].

Motivated by that, in this paper, we investigate all cyclic codes of length $5p^s$ over $\mathcal{R}$ for an odd prime $p \neq 5$. The rest of the paper is arranged as follows. Section 2 gives preliminary concepts. Sections 3, 4, 5 present the main results of this paper. Section 3 provides the algebraic structures of all cyclic codes of length $5p^s$ over $\mathcal{R}$ when $p \equiv 1 \pmod 5$. We proceed by first obtaining the algebraic structures of all cyclic codes of length $5p^s$ over $\mathcal{R}$ when $p \equiv 1 \pmod 5$ in Theorem 3.1. All cyclic codes of length $5p^s$ over $\mathcal{R}$ when $p \equiv 4 \pmod 5$ are studied in Section 4. Theorem 4.4 gives the structure of cyclic codes of length $5p^s$ over $\mathcal{R}$ when $p^m \equiv 4 \pmod 5$. Sections 5 focuses on the case that $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$. The structures of cyclic codes and their dual are given in Theorem 5.1, and the number of codewords is completely described in Theorem 5.1. By Remark 5.15, cyclic and negacyclic codes of length $5p^s$ over $\mathcal{R}$ are equivalent via the ring isomorphism $\delta : \frac{\mathcal{R}[x]}{\langle x^{5p^s}-1\rangle} \to \frac{\mathcal{R}[x]}{\langle x^{5p^s}+1\rangle}$ given by $x \mapsto -x$. So all the results of the paper hold true for negacyclic codes via that isomorphism. We give some examples to illustrate our work in Section 6.

2. Preliminaries

Let R be a finite commutative ring with identity 1. An ideal I of R is said to be *principal* if $I = \langle x \rangle$, where $x \in R$. If all ideals of R are principal, then R is called *a principal ideal ring*. If R has a unique maximal ideal, R is called a *local ring*. Furthermore, R is called a *chain ring* if the set of all ideals of R is linearly ordered under set-theoretic inclusion. The following result is given in [19, Proposition 2.1].

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 whose ideals are $\langle \gamma^i \rangle$, $0 \leq i \leq N(\gamma)$, where $N(\gamma)$ is the nilpotency of γ.*

Recall that a code C of length n over R is a nonempty subset of R^n. A code C is called *linear* if the subset of R^n is an R-submodule of R^n. For a unit λ of R, the λ-constacyclic (λ-twisted) shift τ_λ on R^n is the shift

$$\tau_\lambda(x_0, x_1, \ldots, x_{n-1}) = (\lambda x_{n-1}, x_0, x_1, \ldots, x_{n-2}),$$

and a code C is said to be λ-constacyclic if $\tau_\lambda(C) = C$. If $\lambda = 1$, those λ-constacyclic codes are called cyclic codes, and if $\lambda = -1$, such λ-constacyclic codes are called negacyclic codes.

The following proposition is given in [30, 33].

Proposition 2.2. [30, 33] *A linear code C of length n is λ-constacyclic over R if and only if C is an ideal of $\frac{R[x]}{\langle x^n-\lambda\rangle}$.*

Given n-tuples $v = (v_0, v_1, \ldots, v_{n-1}), t = (t_0, t_1, \ldots, t_{n-1}) \in R^n$, their inner product or dot product is defined as follows

$$v \cdot t = v_0t_0 + v_1t_1 + \cdots + v_{n-1}t_{n-1}.$$

Two n-tuples v, t are called *orthogonal* if $v \cdot t = 0$. For a linear code C over R, its *dual code* $C^\perp$ is the set of n-tuples over R that are orthogonal to all codewords of C, i.e.,

$$C^\perp = \{v \mid v \cdot t = 0, \forall t \in C\}.$$

A code C is called *self-orthogonal* if $C \subseteq C^\perp$, and it is called *self-dual* if $C = C^\perp$. The following result is provided in [14]).

Proposition 2.3. *Let R be a finite chain ring of size p^ω, where p be a prime. Then a linear code C has p^t codewords, for some integer $t \in \{0, 1, \ldots, \omega n\}$. Moreover, $|C| \cdot |C^\perp| = |R|^n$.*

The following proposition allows us to determine the dual of a λ-constacyclic code in general.

Proposition 2.4. [16, Proposition 2.4] *The dual of a λ-constacyclic code is a λ^{-1}-constacyclic code.*

The definition of reciprocal polynomials is given as follows.

Definition 2.5. *Let*

$$m(x) = m_0 + m_1x + \cdots + m_tx^t$$

then the reciprocal of $m(x)$ is the polynomial

$$m^*(x) = m_t + m_{t-1}x + m_{t-2}x^2 + \cdots + m_0x^t.$$

We see that $m^*(x) = x^t m(\frac{1}{x})$. Assume that J is an ideal of $\mathcal{R}$, then $J^* = \{m^*(x) : m(x) \in J\}$ is also an ideal.

Definition 2.6. *Let J be an ideal of $\mathcal{R}$. We define $\mathcal{A}(J) = \{v(x) | m(x)v(x) = 0, \forall m(x) \in J\}$. Then $\mathcal{A}(J)$ is called the annihilator of J, which is also an ideal of $\mathcal{R}$.*

Using the above definition, the associated ideal of $C^\perp$ is $\mathcal{A}(J)^*$, where C is a constacyclic code of length n over $\mathcal{R}$ with associated ideal J. Then we provide two following lemmas which will be used in Section 5.

Lemma 2.7. *a) If* $\deg m \geq \deg v$, *then*

$$(m(x) + v(x))^* = m^*(x) + x^{\deg m - \deg v}v^*(x).$$

b) $(m(x)v(x))^* = m^*(x)v^*(x)$.

Lemma 2.8. *Assume that $J = \langle m(x), uv(x)\rangle$, then $J^* = \{h^*(x) | h(x) \in J\} = \langle m^*(x), uv^*(x)\rangle$.*

The following lemma is given in [45, Chapter 21].

Lemma 2.9. [45, Chapter 21] *For any odd prime $p \neq 5$, we have two cases as follows:*

(i) If $p \equiv 1 \pmod 5$ or $p \equiv 4 \pmod 5$, then 5 is a square in $\mathbb{F}_p$.

(ii) If $p \equiv 2$ or $3 \pmod 5$, then 5 is not a square in $\mathbb{F}_p$.

We have a small lemma as follows.

Lemma 2.11. *Let ξ be a primitive $(p-1)$th root of unity, so that $\mathbb{F}_p = \{0, \xi, \xi^2, \ldots, \xi^{p-2}, \xi^{p-1} = 1\}$.*

(i) If $p \equiv 1 \pmod 5$, then $x^5 - 1$ factors into linear polynomials over $\mathbb{F}_p$.

(ii) If $p \equiv 4 \pmod 5$, then $x^5 - 1$ factors into a linear polynomial and two quadratic irreducible polynomials over $\mathbb{F}_p$ and $x^5 - 1 = (x-1)(x^2 + \frac{1+\gamma}{2}x + 1)(x^2 + \frac{1-\gamma}{2}x + 1)$, where $\gamma^2 = 5$.

(iii) If $p \equiv 2$ or $3 \pmod 5$, then $x^5 - 1$ factors into a linear and degree 4 irreducible polynomial over $\mathbb{F}_p$ and $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$.

Proof.

(i) If $p \equiv 1 \pmod 5$, then $\xi^{\frac{p-1}{2}} = -1$. We see that $(-\xi^{\frac{(p-1)}{10}})^5 = 1$, i.e., $-\xi^{\frac{(p-1)}{10}}$ is a root of the equation $x^5 - 1 = 0$. Similar to $-\xi^{\frac{(p-1)}{10}}$, it is easy to see that $-\xi^{\frac{3(p-1)}{10}}, -\xi^{\frac{7(p-1)}{10}}, -\xi^{\frac{9(p-1)}{10}}$ are also roots of the equation $x^5 - 1 = 0$. Put $\gamma_1 = -\xi^{\frac{(p-1)}{10}}, \gamma_3 = -\xi^{\frac{3(p-1)}{10}}, \gamma_7 = -\xi^{\frac{7(p-1)}{10}}$, and $\gamma_9 = -\xi^{\frac{9(p-1)}{10}}$. Then $x^5 - 1$ can express as follows:

$$x^5 - 1 = (x-1)(x-\gamma_1)(x-\gamma_3)(x-\gamma_7)(x-\gamma_9),$$

proving (*i*).

(ii) Suppose that $x^4 + x^3 + x^2 + x + 1 = (x^2 + a_1x + a_2)(x^2 + a_3x + a_4) = x^4 + (a_1 + a_3)x^3 + (a_4 + a_1a_3 + a_2)x^2 + (a_1a_4 + a_2a_3)x + a_2a_4$. It implies that

$$\begin{cases} a_1 + a_3 = 1 \\ a_1a_3 + a_2 + a_4 = 1 \\ a_1a_4 + a_2a_3 = 1 \\ a_2a_4 = 1. \end{cases} \tag{1}$$

Hence,

$$\begin{cases} a_1 = 1 - a_3 \\ a_1a_3 + a_2 + a_4 = 1 \\ a_1a_4 + a_2a_3 = 1 \\ a_4 = \frac{1}{a_2}. \end{cases} \tag{2}$$

This implies that $\frac{a_1}{a_2} + a_2(1 - a_1) = 1$, i.e., $(1 - a_1)a_2^2 - a_2 + a_1 = 0$. It means that $a_2 = 1$ or $a_2 = \frac{a_1}{1-a_1}$. If $a_2 = 1$, we have $a_1^2 - a_1 - 1 = 0$. By Lemma 2.9, there exists $\gamma \in \mathbb{F}_p$ such that $\gamma^2 = 5$. Therefore, $a_1 = \frac{1\pm\gamma}{2}$. If $a_1 = \frac{1+\gamma}{2}$, then $a_3 = 1 - \frac{1+\gamma}{2} = \frac{1-\gamma}{2}$ and $a_4 = 1$. If $a_1 = \frac{1-\gamma}{2}$, then $a_3 = \frac{1+\gamma}{2}$ and $a_4 = 1$. Therefore, if $p \equiv 4 \pmod 5$, then $x^5 - 1$ factors into $(x-1)$, $(x^2 + \frac{1+\gamma}{2}x + 1)$ and $(x^2 + \frac{1-\gamma}{2}x + 1)$ over $\mathbb{F}_p$. Assume that $x^2 + (1+\gamma)2^{-1}x + 1$ is reducible over $\mathbb{F}_p$. Then there exists $\alpha \in \mathbb{F}_p$ such that $\alpha^2 + (1+\gamma)2^{-1}\alpha + 1 = 0$. This implies that $\alpha^5 - 1 = 0$, and so $\alpha^5 = 1$. It is easy to check that $\alpha = 1$ is not a root of the equation $\alpha^2 + (1+\gamma)2^{-1}\alpha + 1 = 0$ because $\frac{5+\gamma}{2} \neq 0$, i.e., $\alpha \neq 1$. Since $p \equiv 4 \pmod 5$, the order of the multiplicative group of $\mathbb{F}_p$ is not divisible by 5. It means that $\alpha \notin \mathbb{F}_p$, which is a contradiction. Therefore, $x^2 + (1+\gamma)2^{-1}x + 1$ is irreducible over $\mathbb{F}_p$. Using similar argument, we get that $x^2 + (1-\gamma)2^{-1}x + 1$ is irreducible over $\mathbb{F}_p$, showing (*ii*).

(iii) Put $f(x) = x^4 + x^3 + x^2 + x + 1$. Since $x^5 - 1 = (x-1)f(x)$, we see that any root of $f(x) = 0$ has order 5 or 1. Assume that $f(x)$ has a linear factor over $\mathbb{F}_p[x]$. Then $f(x) = 0$ has a root in $\mathbb{F}_p$. It is easy to see that 1 is not a root of $f(x) = 0$ because $1 + 1 + 1 + 1 + 1 \neq 0$. Therefore, any possible root must have order 5. Since 5 is not divisible $p - 1$, $f(x) = 0$ has not a root in $\mathbb{F}_p$, i.e., $f(x)$ has not a linear factor in $\mathbb{F}_p[x]$. Assume that $f(x)$ has an irreducible quadratic factor $g(x)$ in $\mathbb{F}_p[x]$. Then $f(x) = 0$ has a root in a quadratic extension k of $\mathbb{F}_p$. Since $[k : \mathbb{F}_p] = 2$, the field k has p^2 elements, and the cardinality of the multiplicative group of k is $|k^\star| = p^2 - 1 = (p-1)(p+1)$. By using Lagrange's theorem, the order of any element of $k^\star$ is a divisor of $p^2 - 1$. Since $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$, we see that 5 does not divide $p^2 - 1$, i.e., there is no element in k of order 5, a contradiction. Hence, $f(x)$ has not an irreducible quadratic factor, proving (iii). □

We end this section by the following lemma.

Lemma 2.12. [32, Theorem 1.69] *The polynomial $f(x) \in \mathbb{F}[x]$ of degree 2 or 3 is irreducible in $\mathbb{F}[x]$ if and only if $f(x)$ has no root in $\mathbb{F}$.*

3. $p \equiv 1 \pmod 5$

It is well-known from Proposition 2.2 that cyclic codes of length $5p^s$ over $\mathcal{R}$ are ideals of the ring $\mathcal{R}_1 = \frac{\mathcal{R}[x]}{\langle x^{5p^s}-1\rangle}$. We see that $x^5 - 1 = (x-1)\left(x^4 + x^3 + x^2 + x + 1\right)$. Let ξ be a primitive $(p^m - 1)$th root of unity, so that $\mathbb{F}_{p^m} = \{0, \xi, \xi^2, \ldots, \xi^{p^m-2}, \xi^{p^m-1} = 1\}$. Throughout this section, we always assume that $p \equiv 1 \pmod 5$, i.e., $p^m \equiv 1 \pmod 5$, where m is a positive integer. This means that $p^m \equiv 1 \pmod{10}$ and $p^m \equiv 1 \pmod 2$. Hence, $\xi^{\frac{p^m-1}{2}} = -1$. We see that $(-\xi^{\frac{(p^m-1)}{10}})^5 = 1$, i.e., $-\xi^{\frac{(p^m-1)}{10}}$ is a root of the equation $x^5 - 1 = 0$. Similar to $-\xi^{\frac{(p^m-1)}{10}}$, it is easy to see that $-\xi^{\frac{3(p^m-1)}{10}}, -\xi^{\frac{7(p^m-1)}{10}}, -\xi^{\frac{9(p^m-1)}{10}}$ are also roots of the equation $x^5 - 1 = 0$. By Remark 2.10, the equation $x^5 - 1 = 0$ has five distinct roots in $\mathcal{R}$. They are $1, -\xi^{\frac{(p^m-1)}{10}}, -\xi^{\frac{3(p^m-1)}{10}}, -\xi^{\frac{7(p^m-1)}{10}}, -\xi^{\frac{9(p^m-1)}{10}}$. Put $\gamma_1 = -\xi^{\frac{(p^m-1)}{10}}, \gamma_3 = -\xi^{\frac{3(p^m-1)}{10}}, \gamma_7 = -\xi^{\frac{7(p^m-1)}{10}}$, and $\gamma_9 = -\xi^{\frac{9(p^m-1)}{10}}$. Then $(x^4 + x^3 + x^2 + x + 1)^{p^s}$ can express as follows:

$$(x^4 + x^3 + x^2 + x + 1)^{p^s} = \left(x^{p^s} - \gamma_1^{p^s}\right)\left(x^{p^s} - \gamma_3^{p^s}\right)\left(x^{p^s} - \gamma_7^{p^s}\right)\left(x^{p^s} - \gamma_9^{p^s}\right).$$

This implies that

$$x^{5p^s} - 1 = \left(x^5 - 1\right)^{p^s} = \left(x^{p^s} - 1\right)\left(x^{p^s} - \gamma_1^{p^s}\right)\left(x^{p^s} - \gamma_3^{p^s}\right)\left(x^{p^s} - \gamma_7^{p^s}\right)\left(x^{p^s} - \gamma_9^{p^s}\right).$$

By Chinese Reimainder Theorem, we have

$$\begin{aligned}
\mathcal{R}_1 &= \frac{\mathcal{R}[x]}{\langle x^{5p^s}-1\rangle} \\
&\cong \frac{\mathcal{R}[x]}{\langle (x^{p^s}-1)\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^{p^s}-\gamma_1^{p^s})\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^{p^s}-\gamma_3^{p^s})\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^{p^s}-\gamma_7^{p^s})\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^{p^s}-\gamma_9^{p^s})\rangle} \\
&\cong \mathcal{R}_+ \bigoplus \mathcal{R}_{\gamma_1} \bigoplus \mathcal{R}_{\gamma_3} \bigoplus \mathcal{R}_{\gamma_7} \bigoplus \mathcal{R}_{\gamma_9},
\end{aligned}$$

where $\mathcal{R}_+ = \frac{\mathcal{R}[x]}{\langle (x^{p^s}-1)\rangle}$ and $\mathcal{R}_{\gamma_i} = \frac{\mathcal{R}[x]}{\langle (x^{p^s}-\gamma_i^{p^s})\rangle}$ $(i = 1, 3, 7, 9)$. Hence, ideals of $\mathcal{R}_1$ are of the form $\mathrm{C}_+ \bigoplus \mathrm{C}_{\gamma_1} \bigoplus \mathrm{C}_{\gamma_3} \bigoplus \mathrm{C}_{\gamma_7} \bigoplus \mathrm{C}_{\gamma_9}$, where C_+ is a cyclic code of length p^s over $\mathcal{R}$ and C_{γ_i} is a γ_i-constacyclic code of length p^s over $\mathcal{R}$ $(i = 1, 3, 7, 9)$. Then the algebraic structures of all constacyclic codes of length p^s over $\mathcal{R}$ studied in [16] allow us to determine the algebraic structure of all cyclic codes of length $5p^s$ over $\mathcal{R}$ when $p \equiv 1 \pmod 5$. In [16], Dinh determined the number of codewords in each constacyclic code of length p^s over $\mathcal{R}$. Therefore, the number of codewords in each cyclic code of length $5p^s$ over $\mathcal{R}$ can be obtained. Then we have the following theorem.

Theorem 3.1. *Let C be a cyclic code of length $5p^s$ over $\mathcal{R}$. Then*

$$C = \mathrm{C}_+ \bigoplus \mathrm{C}_{\gamma_1} \bigoplus \mathrm{C}_{\gamma_3} \bigoplus \mathrm{C}_{\gamma_7} \bigoplus \mathrm{C}_{\gamma_9},$$

where C_+ is a cyclic code, C_{γ_1} is a γ_1-constacyclic code, C_{γ_3} is a γ_3-constacyclic code, C_{γ_7} is a γ_7-constacyclic code, C_{γ_9} is a γ_9-constacyclic code of length p^s over $\mathcal{R}$. Moreover, $|C| = |C_+||C_{\gamma_1}||C_{\gamma_3}||C_{\gamma_7}||C_{\gamma_9}|$ and $C^\perp = C_+^\perp \bigoplus C_{\gamma_1}^\perp \bigoplus C_{\gamma_3}^\perp \oplus C_{\gamma_7}^\perp \bigoplus C_{\gamma_9}^\perp$.

Proof. It is easy to verify that $C_+^\perp \bigoplus C_{\gamma_1}^\perp \bigoplus C_{\gamma_3}^\perp \oplus C_{\gamma_7}^\perp \bigoplus C_{\gamma_9}^\perp \subseteq C^\perp$. We now consider

$$\begin{aligned}
|C_+^\perp \bigoplus C_{\gamma_1}^\perp \bigoplus C_{\gamma_3}^\perp \oplus C_{\gamma_7}^\perp \bigoplus C_{\gamma_9}^\perp| &= |C_+^\perp||C_{\gamma_1}^\perp||C_{\gamma_3}^\perp||C_{\gamma_7}^\perp||C_{\gamma_9}^\perp| \\
&= \frac{|\mathcal{R}|^{p^s}}{|C_+|}\frac{|\mathcal{R}|^{p^s}}{|C_{\gamma_1}|}\frac{|\mathcal{R}|^{p^s}}{|C_{\gamma_3}|}\frac{|\mathcal{R}|^{p^s}}{|C_{\gamma_7}|}\frac{|\mathcal{R}|^{p^s}}{|C_{\gamma_9}|} \\
&= \frac{|\mathcal{R}|^{5p^s}}{|C_+||C_{\gamma_1}||C_{\gamma_3}||C_{\gamma_7}||C_{\gamma_9}|} \\
&= \frac{|\mathcal{R}|^{5p^s}}{|C|} \\
&= |C^\perp|,
\end{aligned}$$

proving that $C^{\perp} = C_{+}^{\perp} \bigoplus C_{\gamma_1}^{\perp} \bigoplus C_{\gamma_3}^{\perp} \oplus C_{\gamma_7}^{\perp} \bigoplus C_{\gamma_9}^{\perp}$. □

Using Theorem 3.1, we have the following result.

Theorem 3.2. *Let $C = \mathrm{C}_{+} \bigoplus \mathrm{C}_{\gamma_1} \bigoplus \mathrm{C}_{\gamma_3} \bigoplus \mathrm{C}_{\gamma_7} \bigoplus \mathrm{C}_{\gamma_9}$ be a cyclic code of length $5p^s$ over $\mathcal{R}$, where C_{+} is a cyclic code, C_{γ_1} is a γ_1-constacyclic code, C_{γ_3} is a γ_3-constacyclic code, C_{γ_7} is a γ_7-constacyclic code, C_{γ_9} is a γ_9-constacyclic code of length p^s over $\mathcal{R}$. Then C is a self-dual cyclic code of length $5p^s$ over $\mathcal{R}$ if and only if*

(i) $C = \mathrm{C}_{+} \bigoplus \mathrm{C}_{\gamma_1} \bigoplus \mathrm{C}_{\gamma_3} \bigoplus \mathrm{C}_{\gamma_7} \bigoplus \mathrm{C}_{\gamma_9}$, where $C_{+} = \langle u_{\mathcal{R}_+} \rangle$ and $C_{\gamma_i} = \langle u_{\mathcal{R}_i} \rangle$ $(i = 1, 3, 7, 9)$.

(ii) $C = \mathrm{C}_{+} \bigoplus \mathrm{C}_{\gamma_1} \bigoplus \mathrm{C}_{\gamma_3} \bigoplus \mathrm{C}_{\gamma_7} \bigoplus \mathrm{C}_{\gamma_9}$, where $C_{+} = \langle (x-1)^t, u(x-1)^{\omega} \rangle$ and $C_{\gamma_i} = \langle u_{\mathcal{R}_i} \rangle$ $(i = 1, 3, 7, 9)$ such that $t + \omega = p^s$, where $1 \leq t \leq p^s - 1$, and $\omega < t$.

(iii) $C = \mathrm{C}_{+} \bigoplus \mathrm{C}_{\gamma_1} \bigoplus \mathrm{C}_{\gamma_3} \bigoplus \mathrm{C}_{\gamma_7} \bigoplus \mathrm{C}_{\gamma_9}$, where $C_{+} = \left\langle (x-1)^v + u \sum_{j=0}^{\omega-1} c_j (x-1)^j, u(x-1)^{\omega} \right\rangle$ and $C_{\gamma_i} = \langle u_{\mathcal{R}_i} \rangle$ $(i = 1, 3, 7, 9)$ such that $v + \omega = p^s$, and $M(v, \omega)(c_0, c_1, \ldots, c_{v-1})^T = (0, 0, \ldots, 0)^T$, for any $p > 5, s \geq 1$, where $M(v, \omega)(c_0, c_1, \ldots, c_{v-1})^T$ is given in [25]).

Proof. Assume that $C = \mathrm{C}_{+} \bigoplus \mathrm{C}_{\gamma_1} \bigoplus \mathrm{C}_{\gamma_3} \bigoplus \mathrm{C}_{\gamma_7} \bigoplus \mathrm{C}_{\gamma_9}$ is a cyclic code of length $5p^s$ over $\mathcal{R}$. By using [16, Lemma 4.1], we can see that $C_{+} = \langle u_{\mathcal{R}_+} \rangle$ is a self-dual cyclic code of length p^s over $\mathcal{R}$ and $C_{\gamma_i} = \langle u_{\mathcal{R}_i} \rangle$ $(i = 1, 3, 7, 9)$ is a self-dual γ_1-constacyclic code, γ_3-constacyclic code, γ_7-constacyclic code, γ_9-constacyclic code of length p^s over $\mathcal{R}$, respectively. From Theorem 3.1, we have $C^{\perp} = C_{+}^{\perp} \oplus C_{\gamma_1}^{\perp} \oplus C_{\gamma_3}^{\perp} \oplus C_{\gamma_7}^{\perp} \oplus C_{\gamma_9}^{\perp} = \langle u_{\mathcal{R}_1} \rangle = C$. Hence, C is a self-dual cyclic code of length $5p^s$ over $\mathcal{R}$, showing (i). If $C_{+} = \langle (x-1)^t, u(x-1)^{\omega} \rangle$ and $C_{\gamma_i} = \langle u_{\mathcal{R}_i} \rangle$ $(i = 1, 3, 7, 9)$ satisfying $t + \omega = p^s$, where $1 \leq t \leq p^s - 1$, and $\omega < t$, by Theorem 4.12 in [25], then

$$\begin{aligned} C^{\perp} &= C_{+}^{\perp} \oplus C_{\gamma_1}^{\perp} \oplus C_{\gamma_3}^{\perp} \oplus C_{\gamma_7}^{\perp} \oplus C_{\gamma_9}^{\perp} \\ &= \mathrm{C}_{+} \bigoplus \mathrm{C}_{\gamma_1} \bigoplus \mathrm{C}_{\gamma_3} \bigoplus \mathrm{C}_{\gamma_7} \bigoplus \mathrm{C}_{\gamma_9} \\ &= C. \end{aligned}$$

Hence, C is a self-dual cyclic code of length $5p^s$ over $\mathcal{R}$, proving (ii). If $C_{+} = \left\langle (x-1)^v + u \sum_{j=0}^{\omega-1} c_j (x-1)^j, u(x-1)^{\omega} \right\rangle$, by applying Theorem 4.15 in [25], $C_{+}^{\perp} = C_{+}$. Then

$$\begin{aligned} C^{\perp} &= C_{+}^{\perp} \oplus C_{\gamma_1}^{\perp} \oplus C_{\gamma_3}^{\perp} \oplus C_{\gamma_7}^{\perp} \oplus C_{\gamma_9}^{\perp} \\ &= \mathrm{C}_{+} \bigoplus \mathrm{C}_{\gamma_1} \bigoplus \mathrm{C}_{\gamma_3} \bigoplus \mathrm{C}_{\gamma_7} \bigoplus \mathrm{C}_{\gamma_9} \\ &= C, \end{aligned}$$

showing (iii). □

It is well-known from [25, Theorem 4.4] that the number of distinct constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ is computed as follows.

Theorem 3.3. (cf. [25, Theorem 4.4]) *Let p be an odd prime. The number of distinct constacyclic codes of length p^s over $\mathcal{R}$ is*

$$\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}} - 2p^{2m} - 2}{(p^m-1)^2} + \frac{(2p^m+3)(p^m)^{\frac{p^s-1}{2}} - 2p^s - 1}{p^m - 1} + (p^m)^{\frac{p^s-1}{2}} + 2.$$

From Theorem 3.3, the number of cyclic codes of length $5p^s$ over $\mathcal{R}$ is determined as follows.

Theorem 3.4. *The number of cyclic codes of length $5p^s$ over $\mathcal{R}$ is*

$$\left[\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}} - 2p^{2m} - 2}{(p^m-1)^2} + \frac{(2p^m+3)(p^m)^{\frac{p^s-1}{2}} - 2p^s - 1}{p^m - 1} + (p^m)^{\frac{p^s-1}{2}} + 2 \right]^5.$$

Proof. Applying Theorems 3.1 and 3.3, we complete our proof. □

4. $p \equiv 4 \pmod 5$

Assume that $p \equiv 4 \pmod 5$, i.e., $p^m \equiv 4 \pmod 5$ when m is odd and $p^m \equiv 1 \pmod 5$ when m is even. If $p^m \equiv 1 \pmod 5$ when m is even, then cyclic codes of length $5p^s$ over $\mathcal{R}$ are studied in Section 3. Therefore, in this section, we consider the remaining case that is $p^m \equiv 4 \pmod 5$ when m is odd. By Lemma 2.11, $x^{5p^s} - 1$ can be expressed as

$$x^{5p^s} - 1 = \left(x^{p^s} - 1\right)\left(x^2 + (1-\gamma)2^{-1}x + 1\right)^{p^s}\left(x^2 + (1+\gamma)2^{-1}x + 1\right)^{p^s}.$$

To obtain cyclic codes of length $5p^s$ over $\mathcal{R}$, we need to have the following lemma.

Lemma 4.1. *The polynomials $x^2 + (1-\gamma)2^{-1}x + 1$ and $x^2 + (1+\gamma)2^{-1}x + 1$ are irreducible over $\mathcal{R}$.*

Proof. First, we prove that $x^2 + (1-\gamma)2^{-1}x + 1$ and $x^2 + (1+\gamma)2^{-1}x + 1$ are irreducible over $\mathbb{F}_{p^m}$. Assume that $x^2 + (1-\gamma)2^{-1}x + 1$ is reducible over $\mathbb{F}_{p^m}$. Then there exists $\alpha \in \mathbb{F}_{p^m}$ such that $\alpha^2 + (1-\gamma)2^{-1}\alpha + 1 = 0$. This implies that $\alpha^5 - 1 = 0$, and so $\alpha^5 = 1$. It is easy to check that $\alpha = 1$ is not a root of the equation $\alpha^2 + (1-\gamma)2^{-1}\alpha + 1 = 0$ because $\frac{5-\gamma}{2} \neq 0$, i.e., $\alpha \neq 1$. Since $p^m \equiv 4 \pmod 5$, the order of the multiplicative group of $\mathbb{F}_{p^m}$ is not divisible by 5. It means that $\alpha \notin \mathbb{F}_{p^m}$, which is a contradiction. Therefore, $x^2 + (1-\gamma)2^{-1}x + 1$ is irreducible over $\mathbb{F}_{p^m}$. Assume that $x^2 + (1-\gamma)2^{-1}x + 1$ is reducible over $\mathcal{R}$. Then there exists $\eta \in \mathcal{R}$ satisfying $\eta^2 + (1-\gamma)2^{-1}\eta + 1 = 0$, where $\eta = \lambda + u\beta$ and $\lambda, \beta \in \mathbb{F}_{p^m}$. Since $\eta^2 + (1-\gamma)2^{-1}\eta + 1 = 0$, we have $\eta^5 = 1$, i.e., $(\lambda + u\beta)^5 = \lambda^5 + 5\lambda^4\beta u = 1$. Hence, $\lambda^5 = 1$ and $5\lambda^4\beta u = 0$. As $\lambda^5 = 1$, we have $\lambda \neq 0$. Using $p \neq 5$, we see that $\beta = 0$. This implies that $\eta = \lambda \in \mathbb{F}_{p^m}$. Hence, $\lambda^2 + (1-\gamma)2^{-1}\lambda + 1 = 0$, which is a contradiction because $x^2 + (1-\gamma)2^{-1}x + 1$ is irreducible over $\mathbb{F}_{p^m}$. It means that $x^2 + (1-\gamma)2^{-1}x + 1$ is irreducible over $\mathcal{R}$. Using similar argument, we get that $x^2 + (1+\gamma)2^{-1}x + 1$ is irreducible over $\mathcal{R}$. □

We consider the map $\Theta_1 : \frac{\mathcal{R}[x]}{\langle (x^2+(1-\gamma)2^{-1}x+1)^{p^s}\rangle} \to \frac{\mathcal{R}[x]}{\langle (x^2+(5+\gamma)2^{-3})^{p^s}\rangle}$ defined by $f(x) \to f(x-(1-\gamma)2^{-2})$. For polynomials $f(x), g(x) \in \mathcal{R}[x]$, then $f(x) \equiv g(x) \pmod{\left(x^2 + (1-\gamma)2^{-1}x + 1\right)^{p^s}}$ if and only if there exists $q(x) \in R[x]$ such that $f(x) - g(x) = q(x)\left(\left(x^2 + (1-\gamma)2^{-1}x + 1\right)^{p^s}\right)$. Then we have

$$\begin{aligned} f(x-(1-\gamma)2^{-2}) - g(x-(1-\gamma)2^{-2}) &= q\left(x-(1-\gamma)2^{-2}\right)\left[\left(x-(1-\gamma)2^{-2}\right)^2 + (1-\gamma)2^{-1}\left(x-(1-\gamma)2^{-2}\right) + 1\right]^{p^s} \\ &= q\left(x-(1-\gamma)2^{-2}\right)\left[x^2 - (1-\gamma)^2 2^{-4} + 1\right]^{p^s} \\ &= q\left(x-(1-\gamma)2^{-2}\right)\left[x^2 - (6-2\gamma)2^{-4} + 1\right]^{p^s} \\ &= q\left(x-(1-\gamma)2^{-2}\right)\left(x^2 + (5+\gamma)2^{-3}\right)^{p^s}. \end{aligned}$$

This implies that $f(x-(1-\gamma)2^{-2}) \equiv g(x-(1-\gamma)2^{-2} \pmod{(x^2+(5+\gamma)2^{-3})^{p^s}}$. Hence, $\Theta_1(f(x)) = \Theta_1(g(x))$ in $\frac{\mathcal{R}[x]}{\langle (x^2+(5+\gamma)2^{-3})^{p^s}\rangle}$ if and only if $f(x) \equiv g(x)$ in $\frac{\mathcal{R}[x]}{\langle (x^2+(1-\gamma)2^{-1}x+1)^{p^s}\rangle}$. Therefore, Θ_1 is well-defined and one-to-one. It is easy to see that Θ_1 is onto and Θ_1 is a ring homomorphism. It means that Θ_1 is a ring isomorphism. Similar to the map Θ_1, we consider the map $\Theta_2 : \frac{\mathcal{R}[x]}{\langle (x^2+(1+\gamma)2^{-1}x+1)^{p^s}\rangle} \to \frac{\mathcal{R}[x]}{\langle (x^2-(\gamma-5)2^{-3})^{p^s}\rangle}$ defined by $f(x) \to f(x-(1+\gamma)2^{-2})$. Then we can prove that Θ_2 is a ring isomorphism. We summarize the discussion above by the following theorem.

Theorem 4.2.

(i) The map $\Theta_1 : \frac{\mathcal{R}[x]}{\langle (x^2+(1-\gamma)2^{-1}x+1)^{p^s}\rangle} \to \frac{\mathcal{R}[x]}{\langle (x^2+(5+\gamma)2^{-3})^{p^s}\rangle}$ defined by $f(x) \to f(x-(1-\gamma)2^{-2})$ is a ring isomorphism.

(ii) The map $\Theta_2 : \frac{\mathcal{R}[x]}{\langle (x^2+(1+\gamma)2^{-1}x+1)^{p^s}\rangle} \to \frac{\mathcal{R}[x]}{\langle (x^2+(\gamma-5)2^{-3})^{p^s}\rangle}$ defined by $f(x) \to f(x-(1+\gamma)2^{-2})$ is a ring isomorphism.

From Theorem 4.2, we have a direct consequence.

Corollary 4.3.

(i) Let $A \subseteq \frac{\mathcal{R}[x]}{\langle (x^2+(1-\gamma)2^{-1}x+1)^{p^s}\rangle}, B \subseteq \frac{\mathcal{R}[x]}{\langle (x^2+(5+\gamma)2^{-3})^{p^s}\rangle}$. *If* $\Theta_1(A) = B$, *then* A *is an ideal of* $\frac{\mathcal{R}[x]}{\langle (x^2+(1-\gamma)2^{-1}x+1)^{p^s}\rangle}$ *if and only if* B *is an ideal of* $\frac{\mathcal{R}[x]}{\langle (x^2+(5+\gamma)2^{-3})^{p^s}\rangle}$.

(ii) Let $D \subseteq \frac{\mathcal{R}[x]}{\langle (x^2+(1+\gamma)2^{-1}x+1)^{p^s}\rangle}, E \subseteq \frac{\mathcal{R}[x]}{\langle (x^2+(\gamma-5)2^{-3})^{p^s}\rangle}$. *If* $\Theta_2(D) = E$, *then* D *is an ideal of* $\frac{\mathcal{R}[x]}{\langle (x^2+(1+\gamma)2^{-1}x+1)^{p^s}\rangle}$ *if and only if* E *is an ideal of* $\frac{\mathcal{R}[x]}{\langle (x^2+(\gamma-5)2^{-3})^{p^s}\rangle}$.

Since $x^{5p^s}-1 = \left(x^{p^s}-1\right)\left(x^2+(1-\gamma)2^{-1}x+1\right)^{p^s}\left(x^2+(1+\gamma)2^{-1}x+1\right)^{p^s}$, we have

$$\mathcal{R}_1 = \frac{\mathcal{R}[x]}{\langle x^{5p^s}-1\rangle} \cong \frac{\mathcal{R}[x]}{\langle (x^{p^s}-1)\rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x^2+(1-\gamma)2^{-1}x+1)^{p^s}\rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x^2+(1+\gamma)2^{-1}x+1)^{p^s}\rangle}.$$

By Corollary 4.3, we have $\mathcal{R}_1 \cong \frac{\mathcal{R}[x]}{\langle (x^{p^s}-1)\rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x^{2p^s}-\alpha_1)\rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x^{2p^s}-\alpha_2)\rangle}$, where $\alpha_1 = [-(\gamma+5)2^{-3}]^{p^s}$ and $\alpha_2 = [-(\gamma-5)2^{-3}]^{p^s}$. Then we see that a cyclic code of length $5p^s$ over $\mathcal{R}$ is of the form $C_+ \bigoplus C_{\alpha_1} \bigoplus C_{\alpha_2}$, where C_+ is an ideal of $\frac{\mathcal{R}[x]}{\langle (x^{p^s}-1)\rangle}$, C_{α_1} is an ideal of $\frac{\mathcal{R}[x]}{\langle (x^{2p^s}-\alpha_1)\rangle}$, and C_{α_2} is an ideal of $\frac{\mathcal{R}[x]}{\langle (x^{2p^s}-\alpha_2)\rangle}$. The algebraic structures of all constacyclic codes of lengths $p^s, 2p^s$ over $\mathcal{R}$ studied in [16], [12] allow us to determine the algebraic structure of all cyclic codes of length $5p^s$ over $\mathcal{R}$. [16] and [12] determined the number of codewords in each constacyclic code of lengths $p^s, 2p^s$ over $\mathcal{R}$. Therefore, the number of codewords in each cyclic code of length $5p^s$ over $\mathcal{R}$ can be obtained in the following theorem.

Theorem 4.4. *If* C *is a cyclic code of length* $5p^s$ *over* $\mathcal{R}$, *then* C *can be represented as* $C = C_+ \bigoplus C_{\alpha_1} \bigoplus C_{\alpha_2}$, *where* C_+ *is a cyclic code of length* p^s *over* $\mathcal{R}$, C_{α_1} *is an* α_1*-constacyclic code and* C_{α_2} *is an* α_2*-constacyclic code of length* $2p^s$ *over* $\mathcal{R}$. *Moreover,* $|C| = |C_+||C_{\alpha_1}||C_{\alpha_2}|$ *and* $C^\perp = C_+^\perp \bigoplus C_{\alpha_1}^\perp \bigoplus C_{\alpha_2}^\perp$. *In particular,* $C = \langle u\rangle$ *is a self-dual cyclic code of length* $5p^s$ *over* $\mathcal{R}$.

Proof. It is clear to see that $C_+^\perp \bigoplus C_{\alpha_1}^\perp \bigoplus C_{\alpha_2}^\perp \subseteq C^\perp$. We now consider

$$\begin{aligned}
|C_+^\perp \bigoplus C_{\alpha_1}^\perp \bigoplus C_{\alpha_2}^\perp| &= |C_+^\perp||C_{\alpha_1}^\perp||C_{\alpha_2}^\perp| \\
&= \frac{|\mathcal{R}|^{p^s}}{|C_+|}\frac{|\mathcal{R}|^{2p^s}}{|C_{\alpha_1}|}\frac{|\mathcal{R}|^{2p^s}}{|C_{\alpha_2}|} \\
&= \frac{|\mathcal{R}|^{5p^s}}{|C_+||C_{\alpha_1}||C_{\alpha_2}|} \\
&= \frac{|\mathcal{R}|^{5p^s}}{|C|} \\
&= |C^\perp|,
\end{aligned}$$

proving that $C^\perp = C_+^\perp \bigoplus C_{\alpha_1}^\perp \bigoplus C_{\alpha_2}^\perp$. From [12], $C_+ = \langle u\rangle$ is a self-dual cyclic code of length p^s over $\mathcal{R}$, $C_{\alpha_1} = \langle u\rangle$ is a self-dual code of length $2p^s$ over $\mathcal{R}$ and $C_{\alpha_2} = \langle u\rangle$ is a self-dual code of length $2p^s$ over $\mathcal{R}$. Then $C = C_+ \bigoplus C_{\alpha_1} \bigoplus C_{\alpha_2} = \langle u\rangle$ is a self-dual code of length $5p^s$ over $\mathcal{R}$. □

The number of constacyclic codes of length $2p^s$ over $\mathcal{R}$ is given as follows.

Theorem 4.5. *The number of distinct constacyclic codes of length* $2p^s$ *over* $\mathcal{R}$ *is*

$$(p^m+1)\left[\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}}-2p^{2m}-2}{(p^m-1)^2} + \frac{(2p^m+3)(p^m)^{\frac{p^s-1}{2}}-2p^s-1}{p^m-1} + (p^m)^{\frac{p^s-1}{2}}\right] - \frac{p^m(p^s-1)p^s}{2} - p^m(2p^s-1)+2.$$

Proof. In [12], constacyclic codes of length $2p^s$ over $\mathcal{R}$ are classified into 4 distinct types of ideals.
• Type 1 constacyclic codes of length $2p^s$ over $\mathcal{R}$ are $\langle 0\rangle, \langle 1\rangle$, which are two distinct codes.
• Type 2 constacyclic codes of length $2p^s$ over $\mathcal{R}$ are $\langle u(x^2-\lambda_0)^i\rangle$, where $0 \le i \le p^s-1$. Therefore, there are p^s distinct constacyclic codes.
• Type 3 constacyclic codes of length $2p^s$ over $\mathcal{R}$ are $\langle (x^2-\lambda_0)^i + u(x^2-\lambda_0)^t h(x)\rangle$, where $1 \le i \le p^s-1, 0 \le t \le i$, and $h(x)$ is 0 or a unit.
◦ Case 3a: If $h(x) = 0$, then the constacyclic codes of length $2p^s$ over $\mathcal{R}$ are of the form $\langle (x^2-\lambda_0)^i\rangle$, where $1 \le i \le p^s-1$. It implies that there are p^s-1 distinct codes.
◦ Case 3b: If $h(x)$ is a unit, then $h(x)$ can be expressed as $h(x) = \sum\limits_j (h_{0j}x + h_{1j})(x^2-\lambda_0)^j$, where $h_{0j}, h_{1j} \in \mathbb{F}_{p^m}$ and $h_{00}x + h_{10} \neq 0$. Let T be the smallest integer such that $u(x^2-\lambda_0)^T \in \langle (x^2-\lambda_0)^i + u(x^2-\lambda_0)^t h(x)\rangle$. Using [12, Proposition 5.4], we have $T = \min\{i, p^s - i + t\}$. In order for the ideals to be distinct, we must have $t + j < T$, i.e., $0 \le j \le T - t - 1$. This means that the number of distinct ideals of this form is

$$\begin{aligned} S_1 &= \sum_{i=1}^{\frac{p^s-1}{2}} \sum_{t=0}^{i-1} (p^{2m}-1)(p^m)^{i-t-1} + \sum_{i=\frac{p^s+1}{2}}^{p^s-1} \sum_{t=0}^{2i-p^s-1} (p^{2m}-1)(p^m)^{p^s-i-1} + \sum_{i=\frac{p^s+1}{2}}^{p^s-1} \sum_{t=2i-p^s}^{i-1} (p^{2m}-1)(p^m)^{i-t-1} \\ &= (p^m+1)\left[\sum_{i=1}^{\frac{p^s-1}{2}} (p^m-1) \sum_{t=0}^{i-1} (p^m)^{i-t-1} + (p^m-1)\left(\sum_{i=\frac{p^s+1}{2}}^{p^s-1} \sum_{t=0}^{2i-p^s-1} (p^m)^{p^s-i-1}\right) + \sum_{i=\frac{p^s+1}{2}}^{p^s-1} (p^m-1) \sum_{i=2i-p^s}^{i-1} (p^m)^{i-t-1}\right]. \end{aligned}$$

From this, we have

$$S_1 = (p^m+1)\left[\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}} - 4}{p^m-1} + (p^m)^{\frac{p^s-1}{2}} - 2p^s - 1\right].$$

• Type 4 constacyclic codes are $\langle (x^2-\lambda_0)^i + u(x^2-\lambda_0)^t h(x), u(x^2-\lambda_0)^\kappa\rangle$, where $1 \le i \le p^s-1, 0 \le t < i, h(x)$ is 0 or a unit, $0 \le \kappa < T$.
◦ Case 4a: By using [12, Proposition 5.4], if $h(x) = 0$, then $T = i$. It implies that $\langle (x^2-\lambda_0)^i + u(x^2-\lambda_0)^t h(x), u(x^2-\lambda_0)^\kappa\rangle = \langle (x^2-\lambda_0)^i, u(x^2-\lambda_0)^\kappa\rangle$, where $1 \le i \le p^s-1$ and $0 \le \kappa < i$. Hence, the number of distinct codes of this form is $\sum\limits_{i=1}^{p^s-1} i = \frac{p^s(p^s-1)}{2}$.
◦ Case 4b: By using [12, Proposition 5.4], if $h(x)$ is a unit, then $T = \min\{i, p^s - i + t\}$. Hence, $h(x)$ can be expressed as $h(x) = \sum\limits_j (h_{0j}x + h_{1j})(x^2-\lambda_0)^j$, where $h_{0j}, h_{1j} \in \mathbb{F}_{p^m}$ and $h_{00}x + h_{10} \neq 0$. In order for the ideals to be distinct, $t + j < \kappa$, i.e., $0 \le j \le \kappa - t - 1$. It follows that the number of distinct ideals of this form

$$S_2 = (p^m+1)\left[\sum_{i=2}^{\frac{p^s-1}{2}} \sum_{t=0}^{i-2} (p^{m(i-t-1)} - 1) + \sum_{i=\frac{p^s+1}{2}}^{p^s-2} \sum_{t=0}^{2i-p^s-1} (p^{m(p^s-i-1)} - 1) + \sum_{i=\frac{p^s+1}{2}}^{p^s-2} \sum_{t=2i-p^s}^{i-2} (p^{m(i-t-1)} - 1)\right].$$

We abbreviate and hence,

$$S_2 = (p^m+1)\left[\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}} - 2p^{2m} - 2}{(p^m-1)^2} + \frac{(p^m)^{\frac{p^s-1}{2}} - 2p^s + 3}{p^m-1} + \frac{p^s - p^{2s}}{2} + 2\right].$$

Then the number of distinct constacyclic codes of length $2p^s$ over $\mathcal{R}$ is the sum of numbers of distinct constacyclic codes of each type:

$$S = (p^m+1)\left[\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}} - 2p^{2m} - 2}{(p^m-1)^2} + \frac{(2p^m+3)(p^m)^{\frac{p^s-1}{2}} - 2p^s - 1}{p^m-1} + (p^m)^{\frac{p^s-1}{2}}\right] - \frac{p^m(p^s-1)p^s}{2} - p^m(2p^s-1) + 2. \ \square$$

Using Theorems 3.4 and 4.5, we determine the number of cyclic codes of length $5p^s$ over $\mathcal{R}$.

Theorem 4.6. *The number of cyclic codes of length $5p^s$ over $\mathcal{R}$ is*

$$\left[(p^m+1)\left(\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}}-2p^{2m}-2}{(p^m-1)^2}+\frac{(2p^m+3)(p^m)^{\frac{p^s-1}{2}}-2p^s-1}{p^m-1}+(p^m)^{\frac{p^s-1}{2}}\right)-\frac{p^m(p^s-1)p^s}{2}-p^m(2p^s-1)+2\right]^2$$
$$\cdot\left[\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}}-2p^{2m}-2}{(p^m-1)^2}+\frac{(2p^m+3)(p^m)^{\frac{p^s-1}{2}}-2p^s-1}{p^m-1}+(p^m)^{\frac{p^s-1}{2}}+2\right].$$

Proof. From Theorem 4.4, if C is a cyclic code of length $5p^s$ over $\mathcal{R}$, then $C = \mathrm{C}_+ \bigoplus \mathrm{C}_{\alpha_1} \bigoplus \mathrm{C}_{\alpha_2}$ where C_+ is a cyclic code of length p^s over $\mathcal{R}$, C_{α_1} is an α_1-constacyclic code and C_{α_2} is an α_2-constacyclic code of length $2p^s$ over $\mathcal{R}$, where $\alpha_1 = [-(\gamma+5)2^{-3}]^{p^s}$ and $\alpha_2 = [-(\gamma-5)2^{-3}]^{p^s}$. Using Theorems 3.3 and 4.5, we can compute the number of cyclic codes of length $5p^s$ over $\mathcal{R}$. □

5. $p \equiv 2$ or $3 \pmod 5$

Throughout this section, $p \equiv 2$ or $3 \pmod 5$ and $v(x) = x^4 + x^3 + x^2 + x + 1$. We divide $p \equiv 2 \pmod 5$ into 4 cases, namely, $p^m \equiv 1 \pmod 5$ when $m = 4t$, $p^m \equiv 2 \pmod 5$ when $m = 4t+1$, $p^m \equiv 4 \pmod 5$ when $m = 4t+2$ and $p^m \equiv 3 \pmod 5$ when $m = 4t+3$, where $t \in \mathbb{N}$. Similar to the case $p \equiv 2 \pmod 5$, we divide $p \equiv 3 \pmod 5$ into 4 cases, namely, $p^m \equiv 1 \pmod 5$ when $m = 4t$, $p^m \equiv 2 \pmod 5$ when $m = 4t+3$, $p^m \equiv 4 \pmod 5$ when $m = 4t+2$ and $p^m \equiv 3 \pmod 5$ when $m = 4t+1$. The case $p^m \equiv 1 \pmod 5$ is investigated in Section 3. Therefore, from now on, we proceed to obtain all cyclic codes of length $5p^s$ over $\mathcal{R}$ when $p \equiv 2$ or $3 \pmod 5$ such that $p^m \not\equiv 1 \pmod 5$. To do so, we need to have the following proposition.

Proposition 5.1 *Assume that $p \equiv 2$ or $3 \pmod 5$ such that $p^m \not\equiv 1 \pmod 5$. Then*

(i) The polynomial $v(x)$ is irreducible over $\mathcal{R}$.

(ii) There does not exist an element $\gamma \in \mathbb{F}_{p^m}$ such that $\gamma^2 = 5$.

Proof. (i) We see that $x^5 - 1$ can be expressed as $x^5 - 1 = (x-1)v(x)$. Assume that $v(x)$ is reducible over $\mathbb{F}_{p^m}$. Then there exists $\alpha \in \mathbb{F}_{p^m}$ such that $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$. This implies that $\alpha^5 - 1 = 0$, i.e., $\alpha^5 = 1$. From $p \neq 5$, we have $\alpha \neq 1$. Since $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$ ($p^m \not\equiv 1 \pmod 5$), the order of the multiplicative group of $\mathbb{F}_{p^m}$ is not divisible by 5. It follows that $\alpha \notin \mathbb{F}_{p^m}$, which is a contradiction. Therefore, $v(x)$ is irreducible over $\mathbb{F}_{p^m}$. Assume that $v(x)$ is reducible over $\mathcal{R}$. Then there exists $\eta \in \mathcal{R}$ satisfying $\eta^4 + \eta^3 + \eta^2 + \eta + 1 = 0$, where $\eta = \lambda + u\beta$ and $\lambda, \beta \in \mathbb{F}_{p^m}$. Since $\eta^4 + \eta^3 + \eta^2 + \eta + 1 = 0$, we have $\eta^5 = 1$. As mentioned in the proof of Lemma 4.1, we see that $\beta = 0$. This implies that $\eta = \lambda \in \mathbb{F}_{p^m}$. Hence, $\lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1 = 0$, which is a contradiction because $v(x)$ is irreducible over $\mathbb{F}_{p^m}$. It means that the polynomial $v(x)$ is irreducible over $\mathcal{R}$.
(ii) Assume that there is a $\gamma \in \mathbb{F}_{p^m}$ such that $\gamma^2 = 5$. Using same argument as in the proof of Lemma 2.11 part (ii), we have $v(x) = (x^2 + (1-\gamma)2^{-1}x + 1)(x^2 + (1+\gamma)2^{-1}x + 1)$, which is a contradiction with (i). Hence, it does not exist a $\gamma \in \mathbb{F}_{p^m}$ such that $\gamma^2 = 5$. □

Using Proposition 5.1, by the Chinese Remainder Theorem, we have the isomorphism:

$$\frac{\mathcal{R}[x]}{\langle x^{5p^s}-1\rangle} \cong \frac{\mathcal{R}[x]}{\langle (x^{p^s}-1)\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}.$$

Then cyclic codes and their dual of length $5p^s$ over $\mathcal{R}$ are studied in the following theorem.

Theorem 5.2. *Let C be a cyclic code of length $5p^s$ over $\mathcal{R}$ with associated ideal I. Then the following hold:*

(i) $I = I_1 \oplus I_2$, where I_1 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (x^{p^s}-1)\rangle}$ and I_2 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$.

(ii) $|I| = |I_1||I_2|$.

(*iii*) $\mathcal{A}(I) = \mathcal{A}(I_1) \bigoplus \mathcal{A}(I_2)$.

Proof. We have

$$\frac{\mathcal{R}[x]}{\langle x^{5p^s}-1\rangle} \cong \frac{\mathcal{R}[x]}{\langle (x-1)^{p^s}\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}.$$

Then $I = I_1 \oplus I_2$, where I_1 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (x-1)^{p^s}\rangle}$ and I_2 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$, proving (i). (ii) and (iii) can be easily seen from (i), completing our proof. □

Put $\mathcal{R}_\gamma = \frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$. We will investigate all ideals of $\mathcal{R}_\gamma$. In order to do so, we need to prove that any nonzero polynomial of degree less than 4 in $\mathbb{F}_{p^m}[x]$ is invertible in $\mathcal{R}_\gamma$.

Proposition 5.3. *Any nonzero polynomial of degree less than* 4 *in* $\mathbb{F}_{p^m}[x]$ *is invertible in* $\mathcal{R}_\gamma$.

Proof. Assume that $f(x) = ax^3 + bx^2 + cx + d$ is a nonzero polynomial in $\mathbb{F}_{p^m}[x]$. This means that $a, b, c, d \in \mathbb{F}_{p^m}$ such that not all of them are zero. If $\deg(f) = 0$, then $a = b = c = 0$ and $d \neq 0$. It is clear that $f(x) = d \neq 0$ which is invertible. We consider 3 cases, namely, $\deg(f) = 1, 2$ and 3.

- **Case 1: deg** $(f) = 1$**.** Since deg $(f) = 1$, we have $a = b = 0$, and $c \neq 0$, i.e, $f(x)$ can be expressed as $f(x) = cx + d$. In $\mathcal{R}_\gamma$, we see that

$$\begin{aligned}
c^{-1}(x+c^{-1}d)^{-1} &= c^{-1}(x+c^{-1}d)^{p^s-1}\left(x^3+(1-c^{-1}d)x^2+\left((c^{-1}d)^2-c^{-1}d+1\right)x-\left((c^{-1}d)^3-(c^{-1}d)^2+c^{-1}d-1\right)\right)^{p^s}\\
&\times (x+c^{-1}d)^{-p^s}\left(x^3+(1-c^{-1}d)x^2+\left((c^{-1}d)^2-c^{-1}d+1\right)x-\left((c^{-1}d)^3-(c^{-1}d)^2+c^{-1}d-1\right)\right)^{-p^s}\\
&= -c^{-1}(x+c^{-1}d)^{p^s-1}\left(x^3+(1-c^{-1}d)x^2+\left((c^{-1}d)^2-c^{-1}d+1\right)x-\left((c^{-1}d)^3-(c^{-1}d)^2+c^{-1}d-1\right)\right)^{p^s}\\
&\times\left[(c^{-1}d)^4-(c^{-1}d)^3+(c^{-1}d)^2-c^{-1}d+1\right]^{-p^s}.
\end{aligned}$$

  It is easy to see that $cx + d$ is invertible in $\mathcal{R}_\gamma$ if and only if $\left[(c^{-1}d)^4 - (c^{-1}d)^3 + (c^{-1}d)^2 - c^{-1}d + 1\right]^{-p^s}$ is invertible in $\mathbb{F}_{p^m}$. Since $x^4+x^3+x^2+x+1$ is irreducible over $\mathbb{F}_{p^m}$, $(-c^{-1}d)^4+(-c^{-1}d)^3+(-c^{-1}d)^2+(-c^{-1}d)+1 \neq 0$. Hence, $(c^{-1}d)^4 - (c^{-1}d)^3 + (c^{-1}d)^2 - c^{-1}d + 1$ is invertible in $\mathbb{F}_{p^m}$, proving that $cx + d$ is invertible in $\mathcal{R}_\gamma$.

- **Case 2: deg** $(f) = 2$**.** Since deg $(f) = 2$, we have $a = 0$, and $b \neq 0$. Hence, $f(x) = bx^2+cx+d$. In $\mathcal{R}_\gamma$, we see that

$$\begin{aligned}
f(x)^{-1} &= (bx^2+cx+d)^{-1}\\
&= b^{-1}\left(x^2+b^{-1}cx+b^{-1}d\right)^{-1}\\
&= b^{-1}\left(x^2+c_2x+d_2\right)^{-1}, \text{where } c_2 = b^{-1}c \text{ and } d_2 = b^{-1}d\\
&= b^{-1}\left(x^2+c_2x+d_2\right)^{p^s-1}\left(x^2+c_2x+d_2\right)^{-p^s}\left[x^2+(1-c_2)x+(c_2^2-c_2-d_2+1)\right]^{p^s}\\
&\times\left[x^2+(1-c_2)x+(c_2^2-c_2-d_2+1)\right]^{-p^s}\\
&= b^{-1}\left(x^2+c_2x+d_2\right)^{p^s-1}\left[x^2+(1-c_2)x+(c_2^2-c_2-d_2+1)\right]^{p^s}\\
&\times\left[(c_2^3-c_2^2-2c_2d_2+c_2+d_2-1)x+(c_2^2d_2-c_2d_2-d_2^2+d_2-1)\right]^{-p^s}.
\end{aligned}$$

  Hence, $f(x)$ is invertible if and only if $(c_2^3-c_2^2-2c_2d_2+c_2+d_2-1)x+(c_2^2d_2-c_2d_2-d_2^2+d_2-1)$ is invertible, which, by **Case 1**, is equivalent to $(c_2^3-c_2^2-2c_2d_2+c_2+d_2-1)x+(c_2^2d_2-c_2d_2-d_2^2+d_2-1) \neq 0$. If $d_2 = 0$, then $c_2^2d_2-c_2d_2-d_2^2+d_2-1 \neq 0$ implying $f(x)$ is invertible. If $d_2 = 1$, then $c_2^2d_2-c_2d_2-d_2^2+d_2-1 = c_2^2-c_2-1$. By Proposition 5.1 (ii), there is not a $\gamma \in \mathbb{F}_{p^m}$ such that $\gamma^2 = 5$. Hence, $c_2^2 - c_2 - 1 \neq 0$. Therefore, $c_2^2d_2 - c_2d_2 - d_2^2 + d_2 - 1 \neq 0$ when $d_2 = 1$. Thus, $f(x)$ is invertible when $d_2 = 1$. Suppose that

$(c_2^3 - c_2^2 - 2c_2d_2 + c_2 + d_2 - 1)x + (c_2^2d_2 - c_2d_2 - d_2^2 + d_2 - 1) = 0$ and $d_2 \notin \{0, 1\}$. That means that $c_2^3 - c_2^2 - 2c_2d_2 + c_2 + d_2 - 1 = 0$ and $c_2^2d_2 - c_2d_2 - d_2^2 + d_2 - 1 = 0$, where $d_2 \notin \{0, 1\}$. As the equation $c_2^2d_2 - c_2d_2 - d_2^2 + d_2 - 1 = 0$ has a root, it has two roots $c_2 = \frac{d_2 \pm e}{2d_2}$, where $4d_2^3 - 3d_2^2 + 4d_2 = e^2$ and $e \in \mathbb{F}_{p^m}$. We consider the first case of c_2, namely, $c_2 = \frac{d_2+e}{2d_2}$. Since $c_2^3 - c_2^2 - 2c_2d_2 + c_2 + d_2 - 1 = 0$, using $c_2 = \frac{d_2+e}{2d_2}$, we must have

$$\begin{aligned}
0 &= \Big(\frac{d_2+e}{2d_2}\Big)^3 - \Big(\frac{d_2+e}{2d_2}\Big)^2 - 2\Big(\frac{d_2+e}{2d_2}\Big)d_2 + \Big(\frac{d_2+e}{2d_2}\Big) + d_2 - 1 \\
&= (d_2+e)^3 - 2d_2(d_2+e)^2 - (2d_2)^3(d_2+e) + 4d_2^2(d_2+e) + 8d_2^3(d_2-1) \\
&= d_2^3 + 3d_2^2e + 3d_2e^2 + e^3 - 2d_2^3 - 4d_2^2e - 2d_2e^2 - 8d_2^4 - 8d_2^3e + 4d_2^3 + 4d_2^2e + 8d_2^4 - 8d_2^3 \\
&= -5d_2^3 + 3d_2^2e + d_2e^2 - 8d_2^3e + e^3 \\
&= e(e^2 - 8d_2^3 + 3d_2^2) - 5d_2^3 + d_2e^2 \\
&= ed_2(-4d_2^2 + 4) + 4d_2^4 - 8d_2^3 + 4d_2^2.
\end{aligned}$$

This implies that $4d_2^3 - 8d_2^2 + 4d_2 + e(-4d_2^2 + 4) = 0$. Therefore, $e(-4d_2^2 + 4) = -4d_2^3 + 8d_2^2 - 4d_2$. It follows that $e^2(-4d_2^2 + 4)^2 = (-4d_2^3 + 8d_2^2 - 4d_2)^2$. Hence, $(4d_2^2 - 3d_2 + 4)(-4d_2^2 + 4)^2 - d_2(4d_2^2 - 8d_2 + 4)^2 = 0$, i.e., $(d_2 - 1)^2(d_2^4 + d_2^3 + d_2^2 + d_2 + 1) = 0$. From $d_2 \neq 1$, we have $d_2^4 + d_2^3 + d_2^2 + d_2 + 1 = 0$, which is a contradiction with Proposition 5.1 (i). Similar to the case $c_2 = \frac{d_2+e}{2d_2}$, we have a contradiction to Proposition 5.1 (ii) when $c_2 = \frac{d_2-e}{2d_2}$. Hence, Hence, $(c_2^3 - c_2^2 - 2c_2d_2 + c_2 + d_2 - 1)x + (c_2^2d_2 - c_2d_2 - d_2^2 + d_2 - 1) \neq 0$, i.e., $f(x)$ is invertible.

• **Case 3: deg**$(f) = 3$**.** Since $\deg(f) = 3$, we have $a \neq 0$. Hence, $f(x) = ax^3 + bx^2 + cx + d$. In $\mathcal{R}_\gamma$, we see that

$$\begin{aligned}
f(x)^{-1} &= (ax^3 + bx^2 + cx + d)^{-1} \\
&= a^{-1}\left(x^3 + a^{-1}bx^2 + a^{-1}cx + a^{-1}d\right)^{-1} \\
&= a^{-1}\left(x^3 + b_3x^2 + c_3x + d_3\right)^{-1}, \text{where } b_3 = a^{-1}b, c_3 = a^{-1}c \text{ and } d_3 = a^{-1}d \\
&= a^{-1}\left(x^3 + b_3x^2 + c_3x + d_3\right)^{p^s-1}\left(x^3 + b_3x^2 + c_3x + d_3\right)^{-p^s}\left[x + (-b_3+1)\right]^{p^s}\left[x + (-b_3+1)\right]^{-p^s} \\
&= a^{-1}\left(x^3 + b_3x^2 + c_3x + d_3\right)^{p^s-1}(x + (-b_3+1))^{p^s}\left[\left(x^3 + b_3x^2 + c_3x + d_3\right)\left(x + (-b_3+1)\right)\right]^{-p^s} \\
&= a^{-1}\left(x^3 + b_3x^2 + c_3x + d_3\right)^{p^s-1}(x + (-b_3+1))^{p^s} \\
&\times \left[(-b_3^2 + b_3 + c_3 - 1)x^2 + (-b_3c_3 + c_3 + d_3 - 1)x + (-b_3d_3 + d_3 - 1)\right]^{-p^s}.
\end{aligned}$$

This shows that $f(x)$ is invertible if and only if $(-b_3^2 + b_3 + c_3 - 1)x^2 + (-b_3c_3 + c_3 + d_3 - 1)x + (-b_3d_3 + d_3 - 1)$ is invertible, i.e., by **Case 2**, $(-b_3^2 + b_3 + c_3 - 1)x^2 + (-b_3c_3 + c_3 + d_3 - 1)x + (-b_3d_3 + d_3 - 1) \neq 0$. Suppose that $(-b_3^2 + b_3 + c_3 - 1)x^2 + (-b_3c_3 + c_3 + d_3 - 1)x + (-b_3d_3 + d_3 - 1) = 0$. It implies that $-b_3^2 + b_3 + c_3 - 1 = 0$, $-b_3c_3 + c_3 + d_3 - 1 = 0$ and $-b_3d_3 + d_3 - 1 = 0$. If $b_3 = 1$, then $d_3 - d_3b_3 - 1 = -1 \neq 0$, which is a contradiction. Hence, $b_3 \neq 1$, implying $d_3 = \frac{1}{1-b_3}$. From $-b_3c_3 + c_3 + d_3 - 1 = 0$, it follows

that $c_3 = \frac{1-d_3}{1-b_3} = -\frac{b_3}{(1-b_3)^2}$. Thus, we have

$$\begin{aligned}
0 &= -b_3^2 + b_3 + c_3 - 1 \\
&= -b_3^2 + b_3 + \frac{-b_3}{(1-b_3)^2} - 1 \\
&= b_3^4 - 3b_3^3 + 4b_3^2 - 2b_3 + 1 \\
&= \left(b_3^4 + \frac{9}{4}b_3^2 + \frac{9}{4} - 3b_3^3 + 3b_3^2 - \frac{9}{2}b_3\right) - \frac{5}{4}\left(b_3^2 - 2b_3 + 1\right) \\
&= \left(b_3^2 - \frac{3}{2}b_3 + \frac{3}{2}\right)^2 - \frac{5}{4}\left(b_3 - 1\right)^2.
\end{aligned}$$

That means

$$5 = \frac{\left(b_3^2 - \frac{3}{2}b_3 + \frac{3}{2}\right)^2}{4\left(b_3 - 1\right)^2},$$

which is a square. By Proposition 5.1 (ii), this is impossible. Therefore, $f(x)$ is invertible. □

Proposition 5.4. *The polynomial $v(x)$ is nilpotent in $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$ with nilpotency index p^s. $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$ is a local ring with maximal ideal $\langle v(x), u\rangle$, but it is not a chain ring.*

Proof. In $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$, $(v(x))^{p^s} = 0$. Hence, $v(x)$ is nilpotent in $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$ with nilpotency index p^s. Assume that $f(x)$ is an arbitrary element of $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$. Then $f(x)$ can be seen as a polynomial of degree up to $4p^s - 1$ of $\mathcal{R}[x]$, and so $f(x) = f_1(x) + uf_2(x)$, where $f_1(x), f_2(x)$ are polynomials of degrees up to $4p^s - 1$ of $\mathbb{F}_{p^m}[x]$. Thus,

$$\begin{aligned}
f(x) &= \sum_{i=0}^{p^s-1}(a_{0i}x^3 + b_{0i}x^2 + c_{0i}x + d_{0i})(v(x))^i + u\sum_{i=0}^{p^s-1}(a_{1i}x^3 + b_{1i}x^2 + c_{0i}x + d_{0i})(v(x))^i \\
&= (a_{00}x^3 + b_{00}x^2 + c_{00}x + d_{00}) + (v(x))\sum_{i=1}^{p^s-1}(a_{0i}x^3 + b_{0i}x^2 + c_{0i}x + d_{0i})(v(x))^{i-1} \\
&+ u\sum_{i=0}^{p^s-1}(a_{1i}x^3 + b_{1i}x^2 + c_{0i}x + d_{0i})(v(x))^i,
\end{aligned}$$

where $a_{0i}, a_{1i}, b_{0i}, b_{1i}, c_{0i}, c_{1i}, d_{0i}, d_{1i} \in \mathbb{F}_{p^m}$. Since both $v(x)$ and u are nilpotent in $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$, $f(x)$ is non-invertible if and only if $a_{00} = b_{00} = c_{00} = d_{00} = 0$, *i.e.*, $f(x) \in \langle v(x), u\rangle$. It means that $\langle v(x), u\rangle$ forms the set of all non-invertible elements of $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$. Thus, $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$ is a local ring with maximal ideal $\langle v(x), u\rangle$. Moreover, it is easy to see that $u \notin \langle v(x)\rangle$, and $v(x) \notin \langle u\rangle$. Hence, the maximal ideal $\langle v(x), u\rangle$ is not principal, hence, Proposition 2.1 implies that $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$ is not a chain ring. □

Theorem 5.5. *Ideals of $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$ are*

- *Type 1: (trivial ideals)*

$$\langle 0\rangle,\ \langle 1\rangle.$$

- *Type 2: (principal ideals with nonmonic polynomial generators)*

$$\left\langle u(v(x))^i\right\rangle,$$

where $0 \le i \le p^s - 1$.

• *Type 3: (principal ideals with monic polynomial generators)*

$$\left\langle (v(x))^i + u(v(x))^t h(x) \right\rangle,$$

where $1 \le i \le p^s - 1, 0 \le t < i$, *and either* $h(x)$ *is 0 or* $h(x)$ *is a unit which can be represented as* $h(x) = \sum_j (h_{3j}x^3 + h_{2j}x^2 + h_{1j}x + h_{0j})(v(x))^j$, *with* $h_{3j}, h_{2j}, h_{1j}, h_{0j} \in \mathbb{F}_{p^m}$, *and* $h_{30}x^3 + h_{20}x^2 + h_{10}x + h_{00} \neq 0$.

• *Type 4: (nonprincipal ideals)*

$$\left\langle (v(x))^i + u\sum_{j=0}^{\omega-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j, u(v(x))^\omega \right\rangle,$$

where $1 \le i \le p^s - 1, a_j, b_j, c_j, d_j \in \mathbb{F}_{p^m}$, *and* $\omega < T$, *where* T *is the smallest integer such that*

$$u(v(x))^T \in \langle (v(x))^i + u\sum_{j=0}^{i-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j \rangle;$$

or equivalently,

$$\left\langle (v(x))^i + u(v(x))^t h(x), u(v(x))^\omega \right\rangle,$$

with $h(x)$ *as in Type 3, and* $\deg h(x) \le \omega - t - 1$.

Proof. We see that ideals of Type 1 are $\langle 0\rangle$, $\langle 1\rangle$.. Let I be an arbitrary nontrivial ideal of $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$. We consider all possible forms that the ideal I can have.

Case 1. $I \subseteq \langle u\rangle$: Then any element of I must be of the form $u\sum_{i=0}^{p^s-1}(a_{1i}x^3 + b_{1i}x^2 + c_{1i}x + d_{1i})(v(x))^i$, where $a_{1i}, b_{1i}, c_{1i}, d_{1i} \in \mathbb{F}_{p^m}$. Then there is an element $a \in I$ that has the smallest k satisfying $a_{1i}x^3 + b_{1i}x^2 + c_{0i}x + d_{0i} \neq 0$. Therefore, for any $c(x) \in I$, it has the form $c(x) = u(v(x))^k\sum_{i=k}^{p^s-1}(a'_{1i}x^3 + b'_{1i}x^2 + c'_{1i}x + d'_{1i})(v(x))^{i-k}$, which implies $I \subseteq \langle u(v(x))^k\rangle$. However, we have $a \in I$ with

$$\begin{aligned} a &= u(v(x))^k\sum_{i=k}^{p^s-1}(a_{1i}x^3 + b_{1i}x^2 + c_{1i}x + d_{1i})(v(x))^{i-k} \\ &= u(v(x))^k\left[a_{1k}x^3 + b_{1k}x^2 + c_{1k}x + d_{1k} + \sum_{i=k+1}^{p^s-1}(a_{1i}x^3 + b_{1i}x^2 + c_{1i}x + d_{1i})(v(x))^{i-k}\right]. \end{aligned}$$

Since $a_{1k}x^3 + b_{1k}x^2 + c_{1k}x + d_{1k} \neq 0, a_{1k}x^3 + b_{1k}x^2 + c_{1k}x + d_{1k} + \sum_{i=k+1}^{p^s-1}(a_{1i}x^3 + b_{1i}x^2 + c_{1i}x + d_{1i})(v(x))^{i-k}$ is invertible, hence, $u(v(x))^k \in I$. Therefore, $I = \langle u(v(x))^k\rangle$, which means that the nontrivial ideals of $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$ contained in $\langle u\rangle$ are $\langle u(v(x))^k\rangle, 0 \le k \le p^s - 1$, which are ideals of Type 2.

Case 2. $I \not\subseteq \langle u\rangle$: Let I_u denote the set of elements in I reduced modulo u. Then I_u is a nonzero ideal of the ring $\frac{\mathbb{F}_{p^m}[x]}{\langle (v(x))^{p^s}\rangle}$, which is a finite chain ring with ideals $\langle (v(x))^j\rangle$, where $0 \le j \le p^s$. Hence, there is an integer $i \in \{0, 1, \ldots, p^s - 1\}$ such that $I_u = \langle (v(x))^i\rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle (v(x))^{p^s}\rangle}$. Therefore, there exists an element $c(x) \in \frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$ and $c(x)$ can be expressed as

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

where $a_{0j}, a_{1j}, b_{0j}, b_{1j}, c_{0j}, c_{1j}, d_{0j}, d_{1j} \in \mathbb{F}_{p^m}$, such that $(v(x))^i + uc(x) \in I$. Since

$$(v(x))^i + uc(x) = (v(x))^i + u\sum_{j=0}^{p^s-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j \in I,$$

and

$$u(v(x))^k = u\left[(v(x))^i + uc(x)\right](v(x))^{k-i} \in I$$

with $i \le k \le p^s - 1$, it implies that that

$$(v(x))^i + u\sum_{j=0}^{i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j \in I.$$

We now consider two subcases.

Case 2a. $I = \left\langle (v(x))^i + u\sum_{j=0}^{i-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j \right\rangle$. Hence,

$$I = \left\langle (v(x))^i + u(v(x))^t h(x) \right\rangle,$$

where $h(x)$ is 0 or a unit which can be represented as $h(x) = \sum_j (h_{0j}x^3 + h_{1j}x^2 + h_{2j}x + h_{3j})(v(x))^j$, with $h_{0j}, h_{1j}, h_{2j}, h_{3j} \in \mathbb{F}_{p^m}$ and $h_{00}x^3 + h_{10}x^2 + h_{20}x + h_{30} \neq 0$. Thus, I is of Type 3.

Case 2b. $\left\langle (v(x))^i + u\sum_{j=0}^{i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j \right\rangle \subsetneq I$.
Since $\left\langle (v(x))^i + u\sum_{j=0}^{i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j \right\rangle \subsetneq I$, there exists

$$f(x) \in I \setminus \left\langle (v(x))^i + u\sum_{j=0}^{i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j \right\rangle.$$

Hence, there exists a polynomial $g(x) \in \frac{\mathcal{R}[x]}{\langle (v(x))^{p^s} \rangle}$ satisfying

$$0 \neq h(x) = f(x) - g(x)\left[(v(x))^i + u\sum_{j=0}^{i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j\right] \in I.$$

It shows that

$$h(x) = \sum_{j=0}^{i-1}(h_{0j}x^3 + h_{1j}x^2 + h_{2j}x + h_{3j})(v(x))^j + u\sum_{j=0}^{i-1}(h'_{0j}x^3 + h'_{1j}x^2 + h'_{2j}x + h'_{3j})(v(x))^j,$$

where $h_{0j}, h_{1j}, h_{2j}, h_{3j}, h'_{0j}, h'_{1j}, h'_{2j}, h'_{3j} \in \mathbb{F}_{p^m}$. Hence, $h(x)$ reduced modulo u is in $I_u = \langle (v(x))^i \rangle$, and thus, $h_{0j} = h_{1j} = h_{2j} = h_{3j} = 0$ for all $0 \le j \le i-1$, i.e., $h(x) = u\sum_{j=0}^{i-1}(h'_{0j}x^3 + h'_{1j}x^2 + h'_{2j}x + h'_{3j})(v(x))^j$. As $h(x) \neq 0$, there exists a smallest integer $k, 0 \le k \le i-1$, such that $h'_{0k}x^3 + h'_{1k}x^2 + h'_{2k}x + h'_{3k} \neq 0$. Then

$$\begin{aligned} h(x) &= u\sum_{j=k}^{i-1}(h'_{0j}x^3 + h'_{1j}x^2 + h'_{2j}x + h'_{3j})(v(x))^j \\ &= u(v(x))^k\left[h'_{0k}x^3 + h'_{1k}x^2 + h'_{2k}x + h'_{3k}\right] \\ &\quad + u(v(x))^k\left[\sum_{j=k+1}^{i-1}(h'_{0j}x^3 + h'_{1j}x^2 + h'_{2j}x + h'_{3j})(v(x))^{j-k}\right]. \end{aligned}$$

Since $h'_{0k}x^3 + h'_{1k}x^2 + h'_{2k}x + h'_{3k} \neq 0, h'_{0k}x^3 + h'_{1k}x^2 + h'_{2k}x + h'_{3k} + \sum_{j=k+1}^{i-1}(h'_{0j}x^3 + h'_{1j}x^2 + h'_{2j}x + h'_{3j})(v(x))^{j-k}$ is an invertible element in $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$. Put

$$m(x) = h'_{0k}x^3 + h'_{1k}x^2 + h'_{2k}x + h'_{3k} + \sum_{j=k+1}^{i-1}(h'_{0j}x^3 + h'_{1j}x^2 + h'_{2j}x + h'_{3j})(v(x))^{j-k}.$$

Then

$$u(v(x))^k = \left((m(x))^{j-k}\right)^{-1} h(x) \in I.$$

We have shown that for any

$$f(x) \in I \setminus \left\langle (v(x))^i + u\sum_{j=0}^{i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j \right\rangle,$$

there is an integer k with $0 \leq k \leq i-1$ such that $u(v(x))^k \in I$. Let

$$\omega = \min\left\{k | f(x) \in I \setminus \langle (v(x))^i + u\sum_{j=0}^{i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j \rangle\right\}.$$

Then

$$\left\langle (v(x))^i + u\sum_{j=0}^{i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j, u(v(x))^\omega \right\rangle \subseteq I.$$

Moreover, by the above construction, for any $f(x) \in I$, there is a polynomial $g(x) \in I$ such that

$$f(x) - g(x)[(v(x))^i + u\sum_{j=0}^{i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j] \in \langle u(v(x))^\omega \rangle,$$

showing that

$$f(x) \in \langle (v(x))^i + u\sum_{j=0}^{i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j, u(v(x))^\omega \rangle.$$

Thus,

$$\begin{aligned} I &= \left\langle (v(x))^i + u\sum_{j=0}^{i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j, u(v(x))^\omega \right\rangle \\ &= \left\langle (v(x))^i + u\sum_{j=0}^{\omega-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j, u(v(x))^\omega \right\rangle. \end{aligned}$$

Let T be the smallest integer such that

$$u(v(x))^T \in \langle (v(x))^i + u\sum_{j=0}^{i-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j \rangle.$$

If $\omega \geq T$, then

$$\begin{aligned} I &= \left\langle (v(x))^i + u\sum_{j=0}^{\omega-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j, u(v(x))^\omega \right\rangle \\ &= \left\langle (v(x))^i + u\sum_{j=0}^{i-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j \right\rangle, \end{aligned}$$

which contradicts the assumption of this case. Hence $\omega < T$, proving that I is of Type 4, as required. □

The following result helps us to determine T.

Proposition 5.6. *Let T be the smallest integer satisfying*

$$u(v(x)))^T \in \langle (v(x)))^i + u(v(x)))^t h(x) \rangle.$$

Then

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

Proof. Since $u(v(x)))^i = u[(v(x)))^i + u(v(x)))^t h(x)] \in C$, we see that $T \leq i$. If $h(x) = 0$, then $C = \langle (v(x)))^i \rangle$, showing that $T = i$. Assume that $h(x)$ is a unit, i.e., $h(x) \neq 0$. Since

$$u(v(x)))^T \in \langle (v(x)))^i + u(v(x)))^t h(x) \rangle,$$

there exists a polynomial $f(x) \in \frac{\mathcal{R}[x]}{\langle (v(x))^{p^s} \rangle}$ such that

$$u(v(x)))^T = f(x)[(v(x)))^i + u(v(x)))^t h(x)].$$

Then

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

where $a_{0j}, a_{1j}, b_{0j}, b_{1j}, c_{0j}, c_{1j}, d_{0j}, d_{1j} \in \mathbb{F}_{p^m}$. From this, we have

$$\begin{aligned}
u(v(x))^T &= \left[\sum_{j=0}^{p^s-1}(a_{0j}x^3 + b_{0j}z^2 + c_{0j}x + d_{0j})(v(x))^j\right] \\
&\times \left[(v(x))^i + u(v(x))^t h(x)\right] \\
&+ \left[u\sum_{j=0}^{p^s-1}(a_{1j}x^3 + b_{1j}x^2 + c_{1j}x + d_{1j})(v(x))^j\right] \\
&\times \left[(v(x))^i + u(v(x))^t h(x)\right] \\
&= (v(x))^i \sum_{j=0}^{p^s-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j \\
&+ u(v(x))^i \sum_{j=0}^{p^s-1}(a_{1j}x^3 + b_{1j}x^2 + c_{1j}x + d_{1j})(v(x))^j \\
&+ u(v(x))^t h(x) \sum_{j=0}^{p^s-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j \\
&= (v(x))^i \sum_{j=0}^{p^s-i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j \\
&+ (v(x))^{p^s} \sum_{j=p^s-i}^{p^s-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^{i+j-p^s} \\
&+ u(v(x))^i \sum_{j=0}^{p^s-i-1}(a_{1j}x^3 + b_{1j}x^2 + c_{1j}x + d_{1j})(v(x))^j \\
&+ u(v(x))^{p^s} \sum_{j=p^s-i}^{p^s-1}(a_{1j}x^3 + b_{1j}x^2 + c_{1j}x + d_{1j})(v(x))^{i+j-p^s} \\
&+ u(v(x))^t h(x) \sum_{j=0}^{p^s-i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j \\
&+ u(v(x))^t h(x) \sum_{j=p^s-i}^{p^s-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j \\
&= u(v(x))^i \sum_{j=0}^{p^s-i-1}(a_{1j}x^3 + b_{1j}x^2 + c_{1j}x + d_{1j})(v(x))^j \\
&+ u(v(x))^t h(x) \sum_{j=p^s-i}^{p^s-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(v(x))^j \\
&= u(v(x))^i \sum_{j=0}^{p^s-i-1}(a_{1j}x^3 + b_{1j}x^2 + c_{1j}x + d_{1j})(v(x))^j \\
&+ u(v(x))^{p^s-i+t} h(x) \sum_{j=0}^{i-1} q_{0,p^s-i+t}(x)(v(x))^j,
\end{aligned}$$

where $q_{0,p^s-i+t}(x) = a_{0,p^s-i+j}x^3 + b_{0,p^s-i+j}x^2 + c_{0,p^s-i+j}x + d_{0,p^s-i+j}$. Thus, $T \geq \min\{i, p^s - i + t\}$. Moreover,

$$\left[(v(x))^i + u(v(x))^t h(x)\right](v(x))^{p^s-i} = u(v(x))^{p^s-i+t}h(x).$$

Therefore,

$$u(v(x))^{p^s-i+t} = \left[(v(x))^i + u(v(x))^t h(x)\right](v(x))^{p^s-i}h(x)^{-1} \in C.$$

Thus, $T \leq p^s - i + t$, proving that $T = \min\{i, p^s - i + t\}$. □

Let C be a code of length n over R. We recall torsion and residue codes of C as follows:

$$\mathrm{Tor}(C) = \{\mathbf{a} \in \mathbb{F}_{p^m}^n \mid u\,\mathbf{a} \in C\},$$

$$\mathrm{Res}(C) = \{\mathbf{a} \in \mathbb{F}_{p^m}^n \mid \exists\, \mathbf{b} : \mathbf{a} + u\,\mathbf{b} \in C\}.$$

The reduction modulo u from C to $\mathrm{Res}(C)$ is given by

$$\phi : C \longrightarrow \mathrm{Res}(C), \qquad \phi(\mathbf{a} + u\,\mathbf{b}) = \mathbf{a}\,.$$

Clearly, ϕ is well-defined and onto, with $\mathrm{Ker}(\phi) = \mathrm{Tor}(C)$, and $\phi(C) = \mathrm{Res}(C)$. Therefore, $|\mathrm{Res}(C)| = \frac{|C|}{|\mathrm{Tor}(C)|}$. Thus, we have:

Proposition 5.7. *Let C be a code of length n over R, whose torsion and residue codes are* $\mathrm{Tor}(C)$ *and* $\mathrm{Res}(C)$. *Then* $|C| = |\mathrm{Tor}(C)| \cdot |\mathrm{Res}(C)|$.

We can now give the enumeration of elements in each ideal of the ring $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$.

Theorem 5.8. *Let I be an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$. Then the numbers of elements of I, denoted by n_I is determined as follows.*

- *If $I = \langle 0\rangle$, then $n_I = 1$.*
- *If $I = \langle 1\rangle$, then $n_I = p^{8mp^s}$.*
- *If $I = \langle u(v(x))^i\rangle$, where $0 \leq i \leq p^s - 1$, then $n_I = p^{4m(p^s-i)}$.*
- *If $I = \langle (v(x))^i\rangle$, where $1 \leq i \leq p^s - 1$, then $n_I = p^{8m(p^s-i)}$.*
- *If $I = \langle (v(x))^i + u(v(x))^t h(x)\rangle$, where $1 \leq i \leq p^s - 1, 0 \leq t < i$, and $h(x)$ is a unit, then*

$$n_I = \begin{cases} p^{8m(p^s-i)}, & \text{if } 1 \leq i \leq p^{s-1} + \frac{t}{2} \\ p^{4m(2p^s-i-T)}, & \text{if } p^{s-1} + \frac{t}{2} < i \leq p^s - 1 \end{cases}.$$

- *If $I = \langle (v(x))^i + u(v(x))^t h(x), u(v(x))^\kappa\rangle$, where $1 \leq i \leq p^s - 1, 0 \leq t < i$, either $h(x)$ is 0 or $h(x)$ is a unit, and*

$$\kappa < T = \begin{cases} i, & \text{if } h(x) = 0 \\ \min\{i, p^s - i + t\}, & \text{if } h(x) \neq 0\,, \end{cases}$$

then $n_I = p^{4m(2p^s-i-\kappa)}$.

Proof.

(i) Type 1:

- If $I = \langle 0\rangle$, then $\mathrm{Res}(I) = \mathrm{Tor}(I) = \langle 0\rangle$, proving (i).
- If $I = \langle 1\rangle$, then $\mathrm{Res}(I) = \mathrm{Tor}(I) = \langle 1\rangle$.

(ii) Type 2: If $I = \langle u(v(x))^i \rangle$, where $0 \le i \le p^s - 1$, then $\mathrm{Res}(I) = \langle 0 \rangle$ and $\mathrm{Tor}(I) = \langle (v(x))^i \rangle$.

(iii) Type 3: If $I = \langle (v(x))^i + u(v(x))^t h(x) \rangle$, where $1 \le i \le p^s - 1, 0 \le t < i$ and either $h(x)$ is 0 or $h(x)$ is a unit. Then $\mathrm{Res}(I) = \langle (v(x))^i \rangle$ and $\mathrm{Tor}(I) = \langle (v(x))^T \rangle$, where T is the smallest integers such that $u(v(x))^T \in I$, which is given by

$$T = \begin{cases} i, & \text{if } h(x) = 0 \\ \min\{i, p^s - i + t\}, & \text{if } h(x) \neq 0\,, \end{cases}$$

(iv) Type 4: If $I = \langle (v(x))^i + u(v(x))^t h(x), u(v(x))^\kappa \rangle$, where $1 \le i \le p^s - 1, 0 \le t < i$, either $h(x)$ is 0 or $h(x)$ is a unit, and $\kappa < T$, then $\mathrm{Res}(I) = \langle (v(x))^i \rangle$ and $\mathrm{Tor}(I) = \langle (v(x))^\kappa \rangle$. □

We need to have two following lemmas to determine the duals of all λ-constacyclic codes with respect to four types as classified in Theorem 5.5.

Lemma 5.9. *Let $f(x) = (v(x))^i - u\sum_{j=0}^{t}(a_j x^3 + b_j x + c_j x + d_j)(v(x))^j$ be a polynomial over $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s} \rangle}$, where $t < i$. Then*

$$f^*(x) = (v(x))^i - u\sum_{j=0}^{t}(d_j x^3 + c_j x^2 + b_j x + a_j)(v(x))^j x^{4i-4j-3}.$$

Proof. Using Lemma 2.8, $\left[(v(x))^k\right]^* = [(v(x))^*]^k = (v(x))^k$. Applying Lemma 2.8 again, we have

$$\begin{aligned} f^*(x) &= \left[(v(x))^i\right]^* - u\sum_{j=0}^{t}(a_j x^3 + b_j x + c_j x + d_j)^* \left[(v(x))^j\right]^* x^{4i-4j-3} \\ &= (v(x))^i - u\sum_{j=0}^{t}(d_j x^3 + c_j x^2 + b_j x + a_j)(v(x))^j x^{4i-4j-3}. \ \square \end{aligned}$$

Lemma 5.10. *If $I = \langle (v(x))^i + u(v(x))^t h(x), u(v(x))^\omega \rangle$, then $p^s - i$ is the smallest positive integer r such that $u(v(x))^r \in \mathcal{A}(I)$.*

Proof. Assume that

$$\left[(v(x))^i + u(v(x))^t h(x)\right] u(v(x))^r = 0.$$

Since the nilpotency index of $v(x)$ is p^s, $i + r \ge p^s$, i.e., $r \ge p^s - i$, as required. □

Theorem 5.11. *Let $I = \langle u(v(x))^i \rangle$ be an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s} \rangle}$, then $I^\perp = \langle (v(x))^{p^s - i}, u \rangle$.*

Proof. As $I \subseteq \langle u \rangle$ and $I \subseteq \langle (v(x))^i \rangle$, we see that $\langle (v(x))^{p^s - i} \rangle = \langle (v(x))^i \rangle^\perp \subseteq I^\perp$ and $\langle u \rangle = \langle u \rangle^\perp \subseteq I^\perp$. So $\langle (v(x))^{p^s - i}, u \rangle \subseteq I^\perp$. The other inequality follows from the fact that the coefficient vector of $(v(x))^{p^s - i}$ is orthogonal to the coefficient vector of $u(v(x))^i$. □

Theorem 5.12. *Let $I = \langle (v(x))^i + u(v(x))^t h(x) \rangle$ be an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s} \rangle}$, where $h(x)$ is 0 or $h(x)$ is a unit. Then the dual ideal $\mathcal{A}(I)^*$, determinded as follows.*

1) If $h(x)$ is 0, then $\mathcal{A}(I)^* = \langle (v(x))^{p^s - i} \rangle$.

2) If $h(x)$ is a unit and $1 \le i \le \frac{p^s + t}{2}$, then $\mathcal{A}(I)^* = \langle a(x) \rangle$, where

$$\begin{aligned} a(x) &= (v(x))^{p^s - i} \\ &\quad - u(v(x))^{p^s - 2i + t}\sum_{j=0}^{i-t-1}(d_j x^3 + c_j x^2 + b_j x + a_j)(v(x))^j x^{4i-4t-4j-3}. \end{aligned}$$

3) If $h(x)$ is a unit and $\frac{p^s+t}{2} < i \le p^s - 1$, then $\mathcal{A}(I)^* = \langle b(x), u(v(x))^{p^s-i}\rangle$, where

$$b(x) = (v(x))^{i-t} - u\sum_{j=0}^{p^s-i-1}(d_jx^3 + c_jx^2 + b_jx + a_j)(v(x))^j x^{4i-4t-4j-3}.$$

Proof. We see that 1) is obvious. We continue to prove 2) and 3). Let $h(x)$ be a unit. Since

$$[(v(x))^i + u(v(x))^t h(x)][(v(x))^{p^s-i} - u(v(x))^{p^s-2i+t}h(x)] = 0,$$

it implies that

$$\langle (v(x))^{p^s-i} - u(v(x))^{p^s-2i+t}h(x)\rangle \subseteq \mathcal{A}(I).$$

We see that $\mathcal{A}(I)$ can express as $\mathcal{A}(I) = \langle f(x), u(v(x))^k\rangle$, where $f(x) = (v(x))^a + u(v(x))^b g(x)$. We give the simpliest form for the generators $f(x)$ and $u(v(x))^k$. Using Lemma 5.10, $p^s - i$ is the smallest integer r such that $u(v(x))^r \in \mathcal{A}(I)$. Hence, $k = p^s - i$. On the other hand,

$$\begin{aligned} f(x)[(v(x))^i + u(v(x))^t h(x)] &= [(v(x))^a + u(v(x))^b g(x)] \\ &\quad \times [(v(x))^i + u(v(x))^t h(x)] \\ &= (v(x))^{a+i} + u(v(x))^{a+t}h(x) \\ &\quad + u(v(x))^{b+i}g(x) \\ &= 0. \end{aligned}$$

It is easy to see that $a + i \ge p^s$, i.e., $a \ge p^s - i$. We consider two ranges of i, namely, $1 \le i \le \frac{p^s+t}{2}$ and $\frac{p^s+t}{2} < i \le p^s - 1$.

- $1 \le i \le \frac{p^s+t}{2}$: Since $a \ge p^s - i$, we can choose $a = p^s - i$. Then we can set $b = p^s - 2i + t$ and $g(x) = -h(x)$. Hence,

$$\begin{aligned} f(x) &= (v(x))^a + u(v(x))^b g(x) \\ &\in \left\langle (v(x))^{p^s-i} - u(v(x))^{p^s+t-2i}h(x), u(v(x))^{p^s-i}\right\rangle \end{aligned}$$

and

$$\mathcal{A}(I) = \langle (v(x))^{p^s-i} - u(v(x))^{p^s+t-2i}h(x), u(v(x))^{p^s-i}\rangle.$$

As $u(v(x))^{p^s-i} = u\left[(v(x))^{p^s-i} - u(v(x))^{p^s+t-2i}h(x)\right]$, it implies that $u(v(x))^{p^s-i} \in \left\langle (v(x))^{p^s-i} - u(v(x))^{p^s+t-2i}h(x)\right\rangle$. Hence, we have

$$\mathcal{A}(I) = \left\langle (v(x))^{p^s-i} - u(v(x))^{p^s+t-2i}h(x)\right\rangle.$$

Let $h(x) = \sum_j (a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j$, where $a_0x^3 + b_0x^2 + c_0x + d_0 \ne 0$ and $a_j, b_j, c_j, d_j \in \mathbb{F}_{p^m}$. Since $1 \le i \le \frac{p^s+t}{2}$, $t + j < T = \min\{i, p^s - i + t\} = i$. Therefore $j \le i - t - 1$. Let

$$\ell_1(x) = (v(x))^{p^s-i} - u(v(x))^{p^s-2i+t}\sum_{j=0}^{i-t-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j.$$

Then $\langle \mathcal{A}(I)^*\rangle = \langle \ell_1^*(x)\rangle$, and by Lemma 5.8, we have

$$\ell_1^*(x) = (v(x))^{p^s-i} - u(v(x))^{p^s-2i+t}\sum_{j=0}^{i-t-1}(d_jx^3 + c_jx^2 + b_jx + a_j)(v(x))^j x^{4i-4t-4j-3},$$

proving 2).

- $\frac{p^s+t}{2} < i \le p^s - 1$: In this case, $p^s - i < i - t$, so we can choose $a = i - t$. That means, we need b and $g(x)$ such that
$$u(v(x))^i h(x) + u(v(x))^{b+i} g(x) = 0.$$
Thus, we can choose $b = 0$ and $g(x) = -h(x)$. Hence, $f(x) = (v(x))^{i-t} - uh(x)$. Let $h(x) = \sum_j (a_j x^3 + b_j x^2 + c_j x + d_j)(v(x))^j$, where $a_0 x^3 + b_0 x^2 + c_0 x + d_0 \neq 0$ and $a_j, b_j, c_j, d_j \in \mathbb{F}_{p^m}$. Since $\frac{p^s+t}{2} < i \le p^s - 1$, $t + j < T = \min\{i, p^s - i + t\} = p^s - i + t$, showing $j \le p^s - i - 1$. Let
$$\ell_2(x) = (v(x))^{i-t} - u \sum_{j=0}^{p^s-i-1} (a_j x + b_j)(v(x))^j.$$
Now $\langle \mathcal{A}(I)^* \rangle = \langle \ell_2^*(x), u(v(x))^{p^s-i} \rangle$, and by Lemma 5.9, we have
$$\ell_2^*(x) = (v(x))^{i-t} - u \sum_{j=0}^{p^s-i-1} (d_j x^3 + c_j x^2 + b_j x + a_j)(v(x))^j x^{4i-4t-4j-3},$$
which proves 3). □

Theorem 5.13. *Let $I = \langle (v(x))^i + u(v(x))^t h(x), u(v(x))^\omega \rangle$ be an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s} \rangle}$, where $h(x)$ is 0 or $h(x)$ is a unit. Then the dual ideal $\mathcal{A}(I)^*$ is determinded as follows.*

(1) If $h(x) = 0$, then $\mathcal{A}(I)^* = \left\langle (v(x))^{p^s-\omega}, u(v(x))^{p^s-i} \right\rangle$.

(2) If $h(x)$ is a unit, then $\mathcal{A}(I)^* = \left\langle c(x), u(v(x))^{p^s-i} \right\rangle$, where
$$c(x) = (-\gamma_0)^{i-t}(v(x))^{p^s-\omega} - u(v(x))^{p^s-i-\omega+t} \sum_{j=0}^{\omega-t-1} (d_j x^3 + c_j x^2 + b_j x + a_j)(v(x))^j x^{4i-4t-4j-3}.$$

Proof. If $h(x) = 0$, then $I = \langle (v(x))^i, u(v(x))^\omega \rangle$. Hence,
$$\mathcal{A}(I) = \left\langle (v(x))^{p^s-\omega}, u(v(x))^{p^s-i} \right\rangle.$$
Therefore,
$$\begin{aligned} \mathcal{A}(I)^* &= \left\langle \left[(v(x))^{p^s-\omega}\right]^*, \left[u(v(x))^{p^s-i}\right]^* \right\rangle \\ &= \left\langle (v(x))^{p^s-\omega}, u(v(x))^{p^s-i} \right\rangle \\ &= \left\langle (v(x))^{p^s-\omega}, u(v(x))^{p^s-i} \right\rangle, \end{aligned}$$
proving (1). Let $h(x)$ be a unit. Put
$$E = \left\langle (v(x))^{p^s-\omega} - u(v(x))^{p^s-i-\omega+t} h(x), u(v(x))^{p^s-i} \right\rangle.$$
Then $|E| = p^{4m(i+\omega)}$. It is easy to verify that $E \subseteq \mathcal{A}(I)$. On the other hand, we see that
$$p^{4m(i+\omega)} = |E| \le |\mathcal{A}(I)| = |\mathcal{A}(I)^*| = \frac{p^{8mp^s}}{n_I} \le \frac{p^{8mp^s}}{p^{4m(2p^s-i-\omega)}} = p^{4m(i+\omega)}.$$

It implies that $E = \mathcal{A}(I)$, i.e.,

$$\left\langle (v(x))^{p^s-\omega} - u(v(x))^{p^s-i-\omega+t}h(x), u(v(x))^{p^s-i} \right\rangle = \mathcal{A}(I).$$

Let $h(x) = \sum_j (a_j x^3 + b_j x^2 + c_j x + d_j)(v(x))^j$, where $a_0x^3 + b_0x^2 + c_0x + d_0 \neq 0$ and $a_j, b_j, c_j, d_j \in \mathbb{F}_{p^m}$. In this case, we have $j \leq \omega - t - 1$. Let

$$\ell(x) = (v(x))^{p^s-\omega} - u(v(x))^{p^s-i-\omega+t} \sum_{j=0}^{\omega-t-1} (a_j x^3 + b_j x^2 + c_j x + d_j)(v(x))^j.$$

Then $\mathcal{A}(I)^* = \left\langle \ell^*(x), u(v(x))^{p^s-i} \right\rangle$. From Lemma 5.8,

$$\ell^*(x) = (v(x))^{p^s-\omega} - u(v(x))^{p^s-i-\omega+t} \sum_{j=0}^{\omega-t-1} (d_j x^3 + c_j x^2 + b_j x + a_j)(v(x))^j x^{4i-4t-4j-3},$$

completing the proof of (2). □

Summarizing Theorems 5.2, 5.5, 5.12 and 5.13, we give the structure of cyclic codes of length $5p^s$ over $\mathcal{R}$ as follows.

Theorem 5.14. *Let C be a cyclic code of length $5p^s$ over $\mathcal{R}$. Then we have:*

(*i*) *Cyclic codes of length $5p^s$ over $\mathcal{R}$ can be represented as $C = \mathrm{C}_1 \bigoplus \mathrm{C}_2$, where C_1 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle x^{p^s}-1\rangle}$ which is determined in [16] and C_2 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$ which is determined as in Theorem 5.5.*

(*ii*) *$|C| = |C_1||C_2|$, where $|C_1|$ is given in [16], and $|C_2|$ is determined as in Theorem 5.8.*

(*iii*) *$C^\perp = C_1^\perp \bigoplus C_2^\perp$, where $C_1^\perp$ is determined in [16] and $C_2^\perp$ is determined as in Theorems 5.12 and 5.13.*

Remark 5.15. *Consider the map $\delta : \frac{\mathcal{R}[x]}{\langle x^{5p^s}-1\rangle} \to \frac{\mathcal{R}[x]}{\langle x^{5p^s}+1\rangle}$ given by $x \mapsto -x$. We see that δ is a ring isomorphism. Hence, cyclic and negacyclic codes of length $5p^s$ over $\mathcal{R}$ are equivalent via the ring isomorphism δ. So all the results of the paper hold true for negacyclic codes of length $5p^s$ over $\mathcal{R}$ via that isomorphism.*

6. Examples

We give some examples to illustrate our results in Sections 3, 4 and 5.

Example 6.1. Let C be a cyclic code of length 35 over $\mathcal{R} = \mathbb{F}_7 + u\mathbb{F}_7$. Here, $p = 7, s = 1$ and $m = 1$. Then we have a factorization of $x^{35} - 1$ as follows:

$$x^{35} - 1 = (x^7 - 1)(v(x))^7,$$

where $v(x) = x^4 + x^3 + x^2 + x + 1$. By the Chinese Remainder Theorem,

$$\mathcal{R}_1 \cong \frac{\mathcal{R}[x]}{\langle (x^7-1)\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (v(x))^7\rangle}.$$

By Theorem 5.14, $C = \mathrm{C}_1 \bigoplus \mathrm{C}_2$, where C_1 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (x^7-1)\rangle}$, whose structure is given in [16] and C_2 is an ideal of $\frac{\mathcal{R}[x]}{\langle (v(x))^7\rangle}$. Using Theorem 5.5, ideals of $\frac{\mathcal{R}[x]}{\langle (v(x))^7\rangle}$ are

- Type 1:

$$\langle 0\rangle,\ \langle 1\rangle.$$

- Type 2:
$$\left\langle u(v(x))^i \right\rangle,$$
where $0 \le i \le 6$.

- Type 3:
$$\left\langle (v(x))^i + u(v(x))^t h(x) \right\rangle,$$
where $1 \le i \le 6, 0 \le t < i$, and either $h(x)$ is 0 or $h(x)$ is a unit and $h(x) = \sum_j (h_{3j}x^3 + h_{2j}x^2 + h_{1j}x + h_{0j})(v(x))^j$, with $h_{3j}, h_{2j}, h_{1j}, h_{0j} \in \mathbb{F}_7$, and $h_{30}x^3 + h_{20}x^2 + h_{10}x + h_{00} \neq 0$.

- Type 4:
$$\left\langle (v(x))^i + u\sum_{j=0}^{\omega-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j, u(v(x))^\omega \right\rangle,$$
where $1 \le i \le 6, a_j, b_j, c_j, d_j \in \mathbb{F}_7$, and $\omega < T$, where T is the smallest integer satisfying
$$u(v(x))^T \in \langle (v(x))^i + u\sum_{j=0}^{i-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j \rangle;$$
or equivalently,
$$\left\langle (v(x))^i + u(v(x))^t h(x), u(v(x))^\omega \right\rangle,$$
with $h(x)$ as in Type 3, and $\deg h(x) \le \omega - t - 1$.

By part (ii) of Theorem 5.14, we see that $|C| = |C_1||C_2|$, where $|C_1|$ is given in [16], and $|C_2|$ is determined as follows:

- $|C_2| = 1$ when $C_2 = \langle 0 \rangle$.
- $|C_2| = 7^{56}$ when $C_2 = \langle 1 \rangle$.
- $|C_2| = 7^{4(7-i)}$ when $C_2 = \langle u(v(x))^i \rangle$, where $0 \le i \le 6$.
- $|C_2| = 7^{8(7-i)}$ when $C_2 = \langle (v(x))^i \rangle$, where $1 \le i \le 6$.
- $|C_2| = \begin{cases} 7^{8(7-i)}, & \text{in this case, } 1 \le i \le 1 + \frac{t}{2} \\ 7^{4(14-i-T)}, & \text{in this case, } 1 + \frac{t}{2} < i \le 6 \end{cases}$ when $C_2 = \langle (v(x))^i + u(v(x))^t h(x) \rangle$, where $1 \le i \le 6, 0 \le t < i$, and $h(x)$ is a unit.
- $|C_2| = 7^{4(14-i-\kappa)}$ when $C_2 = \langle (v(x))^i + u(v(x))^t h(x), u(v(x))^\kappa \rangle$, where $1 \le i \le 6, 0 \le t < i$, either $h(x)$ is 0 or $h(x)$ is a unit, and
$$\kappa < T = \begin{cases} i, & \text{if } h(x) = 0 \\ \min\{i, 7 - i + t\}, & \text{if } h(x) \neq 0 \end{cases}$$
.

Example 6.2. Let C be a cyclic code of length 65 over $\mathcal{R} = \mathbb{F}_{13} + u\mathbb{F}_{13}$. Here, $p = 13, s = 1$ and $m = 1$. Then we have a factorization of $x^{65} - 1$ as follows:
$$x^{65} - 1 = (x^{13} - 1)(v(x))^{13},$$
where $v(x) = x^4 + x^3 + x^2 + x + 1$. By the Chinese Remainder Theorem,
$$\mathcal{R}_1 \cong \frac{\mathcal{R}[x]}{\langle (x^{13} - 1) \rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (v(x))^{13} \rangle}.$$
By applying Theorem 5.14, $C = C_1 \bigoplus C_2$, where C_1 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (x^{13}-1) \rangle}$, whose structure is given in [16] and C_2 is an ideal of $\frac{\mathcal{R}[x]}{\langle (v(x))^{13} \rangle}$. Using Theorem 5.5, ideals of $\frac{\mathcal{R}[x]}{\langle (v(x))^{13} \rangle}$ are

- Type 1:
$$\langle 0\rangle,\ \langle 1\rangle.$$
- Type 2:
$$\left\langle u(v(x))^i\right\rangle,$$
where $0 \le i \le 12$.
- Type 3:
$$\left\langle (v(x))^i + u(v(x))^t h(x)\right\rangle,$$
where $1 \le i \le 12, 0 \le t < i$, and either $h(x)$ is 0 or $h(x)$ is a unit and $h(x) = \sum_j (h_{3j}x^3+h_{2j}x^2+h_{1j}x+h_{0j})(v(x))^j$, with $h_{3j}, h_{2j}, h_{1j}, h_{0j} \in \mathbb{F}_{13}$, and $h_{30}x^3 + h_{20}x^2 + h_{10}x + h_{00} \neq 0$.
- Type 4:
$$\left\langle (v(x))^i + u\sum_{j=0}^{\omega-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j, u(v(x))^\omega\right\rangle,$$
where $1 \le i \le 12, a_j, b_j, c_j, d_j \in \mathbb{F}_{13}$, and $\omega < T$, where T is the smallest integer satisfying
$$u(v(x))^T \in \langle (v(x))^i + u\sum_{j=0}^{i-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j\rangle;$$
or equivalently,
$$\left\langle (v(x))^i + u(v(x))^t h(x), u(v(x))^\omega\right\rangle,$$
with $h(x)$ as in Type 3, and $\deg h(x) \le \omega - t - 1$.

By part (ii) of Theorem 5.14, we see that $|C| = |C_1||C_2|$, where $|C_1|$ is given in [16], and $|C_2|$ is determined as follows:

- $|C_2| = 1$ when $C_2 = \langle 0\rangle$.
- $|C_2| = 13^{56}$ when $C_2 = \langle 1\rangle$.
- $|C_2| = 13^{4(13-i)}$ when $C_2 = \langle u(v(x))^i\rangle$, where $0 \le i \le 12$.
- $|C_2| = 13^{8(13-i)}$ when $C_2 = \langle (v(x))^i\rangle$, where $1 \le i \le 12$.
- $|C_2| = \begin{cases} 13^{8(13-i)}, & \text{in this case, } 1 \le i \le 1 + \frac{t}{2} \\ 13^{4(26-i-T)}, & \text{in this case, } 1 + \frac{t}{2} < i \le 12 \end{cases}$ when $C_2 = \langle (v(x))^i + u(v(x))^t h(x)\rangle$, where $1 \le i \le 12, 0 \le t < i$, and $h(x)$ is a unit.
- $|C_2| = 13^{4(26-i-\kappa)}$ when $C_2 = \langle (v(x))^i + u(v(x))^t h(x), u(v(x))^\kappa\rangle$, where $1 \le i \le 12, 0 \le t < i$, either $h(x)$ is 0 or $h(x)$ is a unit, and
$$\kappa < T = \begin{cases} i, & \text{if } h(x) = 0 \\ \min\{i, 13 - i + t\}, & \text{if } h(x) \neq 0 \end{cases}$$
.

Example 6.3. Let C be a cyclic code of length 115 over $\mathcal{R} = \mathbb{F}_{23} + u\mathbb{F}_{23}$. Here, $p = 23, s = 1$ and $m = 1$. Then we have a factorization of $x^{115} - 1$ as follows:
$$x^{115} - 1 = (x^{23} - 1)(v(x))^{23},$$

where $v(x) = x^4 + x^3 + x^2 + x + 1$. From the Chinese Remainder Theorem,

$$\mathcal{R}_1 \cong \frac{\mathcal{R}[x]}{\langle (x^{23}-1)\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (v(x))^{23}\rangle}.$$

By using Theorem 5.14, $C = C_1 \bigoplus C_2$, where C_1 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (x^{23}-1)\rangle}$, whose structure is given in [16] and C_2 is an ideal of $\frac{\mathcal{R}[x]}{\langle (v(x))^{23}\rangle}$. Using Theorem 5.5, ideals of $\frac{\mathcal{R}[x]}{\langle (v(x))^{23}\rangle}$ are

- Type 1:
$$\langle 0\rangle,\ \langle 1\rangle.$$
- Type 2:
$$\left\langle u(v(x))^i \right\rangle,$$
where $0 \le i \le 22$.
- Type 3:
$$\left\langle (v(x))^i + u(v(x))^t h(x) \right\rangle,$$
where $1 \le i \le 22, 0 \le t < i$, and either $h(x)$ is 0 or $h(x)$ is a unit and $h(x) = \sum_j (h_{3j}x^3 + h_{2j}x^2 + h_{1j}x + h_{0j})(v(x))^j$, with $h_{3j}, h_{2j}, h_{1j}, h_{0j} \in \mathbb{F}_{23}$, and $h_{30}x^3 + h_{20}x^2 + h_{10}x + h_{00} \neq 0$.
- Type 4:
$$\left\langle (v(x))^i + u\sum_{j=0}^{\omega-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j, u(v(x))^\omega \right\rangle,$$
where $1 \le i \le 22, a_j, b_j, c_j, d_j \in \mathbb{F}_{23}$, and $\omega < T$, where T is the smallest integer satisfying
$$u(v(x))^T \in \langle (v(x))^i + u\sum_{j=0}^{i-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(v(x))^j\rangle;$$
or equivalently,
$$\left\langle (v(x))^i + u(v(x))^t h(x), u(v(x))^\omega \right\rangle,$$
with $h(x)$ as in Type 3, and $\deg h(x) \le \omega - t - 1$.

By part (ii) of Theorem 5.14, we see that $|C| = |C_1||C_2|$, where $|C_1|$ is given in [16], and $|C_2|$ is determined as follows:

- $|C_2| = 1$ when $C_2 = \langle 0\rangle$.
- $|C_2| = 23^{56}$ when $C_2 = \langle 1\rangle$.
- $|C_2| = 23^{4(23-i)}$ when $C_2 = \langle u(v(x))^i\rangle$, where $0 \le i \le 22$.
- $|C_2| = 23^{8(23-i)}$ when $C_2 = \langle (v(x))^i\rangle$, where $1 \le i \le 22$.
- $|C_2| = \begin{cases} 23^{8(23-i)}, & \text{in this case, } 1 \le i \le 1 + \frac{t}{2} \\ 23^{4(46-i-T)}, & \text{in this case, } 1 + \frac{t}{2} < i \le 22 \end{cases}$ when $C_2 = \langle (v(x))^i + u(v(x))^t h(x)\rangle$, where $1 \le i \le 22, 0 \le t < i$, and $h(x)$ is a unit.
- $|C_2| = 23^{4(46-i-\kappa)}$ when $C_2 = \langle (v(x))^i + u(v(x))^t h(x), u(v(x))^\kappa\rangle$, where $1 \le i \le 22, 0 \le t < i$, either $h(x)$ is 0 or $h(x)$ is a unit, and
$$\kappa < T = \begin{cases} i, & \text{if } h(x) = 0 \\ \min\{i, 23 - i + t\}, & \text{if } h(x) \neq 0 \end{cases}$$
.

Example 6.4. Let C be a cyclic code of length 55 over $\mathcal{R} = \mathbb{F}_{11} + u\mathbb{F}_{11}$. Then C is an ideal of $\mathcal{R}_1 = \frac{(\mathbb{F}_{11}+u\mathbb{F}_{11})[x]}{\langle x^{55}-1\rangle}$. Here, $p = 11, s = 1$ and $m = 1$. We see that

$$v(x) = (x-4)(x-5)(x-9)(x-3).$$

Then we have a factorization of $x^{55} - 1$ as follows:

$$x^{55} - 1 = (x^{11} - 1)(x^{11} - 4)(x^{11} - 5)(x^{11} - 9)(x^{11} - 3),$$

where $v(x) = x^4 + x^3 + x^2 + x + 1$. By the Chinese Remainder Theorem, we have

$$\mathcal{R}_1 \cong \frac{\mathcal{R}[x]}{\langle (x^{11}-1)\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^{11}-4)\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^{11}-5)\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^{11}-9)\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^{11}-3)\rangle}.$$

By Theorem 3.1, $C = C_+ \bigoplus C_1 + \bigoplus C_2 \bigoplus C_3 \bigoplus C_4$, where C_+ is a cyclic code of length 11 over $\mathcal{R}$, C_1 is a 4-constacyclic code of length 11 over $\mathcal{R}$, C_2 is a 5-constacyclic code of length 11 over $\mathcal{R}$, C_3 is a 9-constacyclic code of length 11 over $\mathcal{R}$ and C_4 is a 3-constacyclic code of length 11 over $\mathcal{R}$. Their structures are given in [16]. By applying Theorem 3.1, $C^\perp = C_+^\perp \bigoplus C_1^\perp \bigoplus C_2^\perp \bigoplus C_3^\perp \bigoplus C_4^\perp$, where $C_+^\perp$ is a cyclic code of length 11 over $\mathcal{R}$, $C_1^\perp$ is a 3-constacyclic code of length 11 over $\mathcal{R}$, $C_2^\perp$ is a 9-constacyclic code of length 11 over $\mathcal{R}$, $C_3^\perp$ is a 5-constacyclic code of length 11 over $\mathcal{R}$ and $C_4^\perp$ is a 4-constacyclic code of length 11 over $\mathcal{R}$.

Example 6.5. Let C be a cyclic code of length 95 over $\mathcal{R} = \mathbb{F}_{19} + u\mathbb{F}_{19}$. Then C is an ideal of $\mathcal{R}_1 = \frac{(\mathbb{F}_{19}+u\mathbb{F}_{19})[x]}{\langle x^{95}-1\rangle}$. Here, $p = 19, s = 1$ and $m = 1$. Put $\gamma = 9 \in \mathbb{F}_{19}$. Then $\gamma^2 = 9^2 = 5 \in \mathbb{F}_{19}$. Put $\alpha_1 = [-(\gamma+5)2^{-3}]^{19} = 3^{19} = 3 \in \mathbb{F}_{19}$ and $\alpha_2 = [-(\gamma-5)2^{-3}]^{19} = -10^{19} = -13 = 6 \in \mathbb{F}_{19}$. Then we have a factorization of $x^{95} - 1$ as follows:

$$x^{95} - 1 = (x^{19} - 1)(x^2 - 4x + 1)^{19}(x^2 + 5x + 1)^{19}.$$

By the Chinese Remainder Theorem,

$$\mathcal{R}_1 \cong \frac{\mathcal{R}[x]}{\langle (x^{19}-1)\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^2-4x+1)^{19}\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^2+5x+1)^{19}\rangle}.$$

From Theorem 4.2, we have

$$\begin{aligned}\mathcal{R}_1 &\cong \frac{\mathcal{R}[x]}{\langle (x^{19}-1)\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^2-4x+1)^{19}\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^2+5x+1)^{19}\rangle} \\ &\cong \frac{\mathcal{R}[x]}{\langle (x^{19}-1)\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^{38}-3)\rangle} \bigoplus \frac{\mathcal{R}[x]}{\langle (x^{38}-6)\rangle}.\end{aligned}$$

By using Theorem 4.4, $C = C_+ \bigoplus C_{\alpha_1} \bigoplus C_{\alpha_2}$, where C_+ is a cyclic code of length 19 over $\mathcal{R}$, C_{α_1} is a 3-constacyclic code of length 38 over $\mathcal{R}$ and C_{α_2} is a 6-constacyclic code of length 38 over $\mathcal{R}$. Their structures are given in [12].

7. Conclusion

In this paper, for an odd prime $p \neq 5$, we study all cyclic codes of length $5p^s$ over $\mathcal{R}$, where $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}(u^2 = 0)$. We divide our considerations into 4 cases, namely, $p \equiv 1 \pmod 5$ (Section 3), $p \equiv 4 \pmod 5$ (Section 4), and $p \equiv 2$ *or* $3 \pmod 5$ (Section 5). When $p \equiv 1 \pmod 5$, we see that the polynomial $x^{5p^s} - 1$ can be expressed as

$$x^{5p^s} - 1 = (x^5 - 1)^{p^s} = (x^{p^s} - 1)(x^{p^s} - \gamma_1^{p^s})(x^{p^s} - \gamma_3^{p^s})(x^{p^s} - \gamma_7^{p^s})(x^{p^s} - \gamma_9^{p^s}),$$

where $\gamma_1^{p^s} = -\frac{(p^m-1)p^s}{10}, \gamma_3^{p^s} = -\frac{3(p^m-1)p^s}{10}, \gamma_7^{p^s} = -\frac{7(p^m-1)p^s}{10}, \gamma_9^{p^s} = -\frac{9(p^m-1)p^s}{10}$. By Theorem 3.1, the algebraic structures of all cyclic codes of length $5p^s$ over $\mathcal{R}$ when $p \equiv 1 \pmod 5$ are given. Following Theorem 3.1, a

cyclic code of length $5p^s$ over $\mathcal{R}$ is a direct sum of $C_+, C_{\gamma_1}, C_{\gamma_3}, C_{\gamma_7}, C_{\gamma_9}$, where C_+ is a cyclic code of length p^s over $\mathcal{R}$ and C_{γ_i} is a γ_i-constacyclic code of length p^s over $\mathcal{R}$ ($i = 1, 3, 7, 9$). From Theorem 3.1, we also see that the dual of all cyclic codes of length $5p^s$ over $\mathcal{R}$ is determined as

$$C^\perp = C_+^\perp \bigoplus C_{\gamma_1}^\perp \bigoplus C_{\gamma_3}^\perp \bigoplus C_{\gamma_7}^\perp \bigoplus C_{\gamma_9}^\perp,$$

where $C_+^\perp$ is the dual code of C_+ and $C_{\gamma_i}^\perp$ is the dual code of C_{γ_i} ($i = 1, 3, 7, 9$). In Section 3, Theorem 3.2 presents necessary and sufficient conditions for a self-dual cyclic code of length $5p^s$ over $\mathcal{R}$ and Theorem 3.4 provides the number of cyclic codes of length $5p^s$ over $\mathcal{R}$. When $p \equiv 4 \pmod 5$, we divide into 2 cases, namely, $p^m \equiv 1 \pmod 5$ when m is even and $p^m \equiv 4 \pmod 5$ when m is odd. If $p^m \equiv 1 \pmod 5$ when m is even, then cyclic codes of length $5p^s$ over $\mathcal{R}$ are studied in Section 3. Therefore, in Section 4, we study the remaining case that is $p^m \equiv 4 \pmod 5$ when m is odd. Since $p^m \equiv 4 \pmod 5$, there exists $\gamma \in \mathbb{F}_{p^m}$ such that $\gamma^2 = 5$. Then the polynomial $x^{5p^s} - 1$ can be expressed as

$$x^{5p^s} - 1 = (x-1)^{p^s} \left(x^2 + (1-\gamma)\,2^{-1}x + 1\right)^{p^s} \left(x^2 + (1+\gamma)\,2^{-1}x + 1\right)^{p^s}.$$

By constructing the ring isomorphism $\Theta_1 : \frac{\mathcal{R}[x]}{\langle (x^2+(1-\gamma)2^{-1}x+1)^{p^s}\rangle} \to \frac{\mathcal{R}[x]}{\langle (x^2+(5+\gamma)2^{-3})^{p^s}\rangle}$ defined by $f(x) \to f(x-(1-\gamma)2^{-2})$ and the ring isomorphism $\Theta_2 : \frac{\mathcal{R}[x]}{\langle (x^2+(1+\gamma)2^{-1}x+1)^{p^s}\rangle} \to \frac{\mathcal{R}[x]}{\langle (x^2+(\gamma-5)2^{-3})^{p^s}\rangle}$ defined by $f(x) \to f(x-(1+\gamma)2^{-2})$ (Theorem 4.2), we investigate all cyclic codes of length $5p^s$ over $\mathcal{R}$ when $p^m \equiv 4 \pmod 5$ in Theorem 4.4. Theorem 4.4 shows that if C is a cyclic code of length $5p^s$ over $\mathcal{R}$, then C can be represented as $C = C_+ \bigoplus C_{\alpha_1} \bigoplus C_{\alpha_2}$ where C_+ is a cyclic code of length p^s over $\mathcal{R}$, C_{α_1} is an α_1-constacyclic code and C_{α_2} is an α_2-constacyclic code of length $2p^s$ over $\mathcal{R}$ ($\alpha_1 = [-(\gamma+5)2^{-3}]^{p^s}$ and $\alpha_2 = [-(\gamma-5)2^{-3}]^{p^s}$). Theorem 4.4 also allows us to determine the dual of all cyclic codes of length $5p^s$ over $\mathcal{R}$ when $p^m \equiv 4 \pmod 5$ as follows:

$$C^\perp = C_+^\perp \bigoplus C_{\alpha_1}^\perp \bigoplus C_{\alpha_2}^\perp,$$

where $C_+^\perp$ is the dual code of C_+, $C_{\alpha_1}^\perp$ is the dual code of C_{α_1}, and $C_{\alpha_2}^\perp$ is the dual of C_{α_2}. In Theorem 4.6, we give the mass formulas to count all cyclic codes of length $5p^s$ over $\mathcal{R}$ when $p^m \equiv 4 \pmod 5$. When $p \equiv 2$ *or* $3 \pmod 5$ such that $p^m \not\equiv 1 \pmod 5$, cyclic codes and their dual of length $5p^s$ over $\mathcal{R}$ are studied in Theorem 5.14. By part (i) of Theorem 5.14, cyclic codes of length $5p^s$ over $\mathcal{R}$ is determined as $C = C_1 \bigoplus C_2$, where C_1 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle x^{p^s}-1\rangle}$ which is determined in [16], and C_2 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (v(x))^{p^s}\rangle}$ which is determined in Theorem 5.5. By part (ii) of Theorem 5.14, we have $|C| = |C_1||C_2|$, where $|C_1|$ is computed in [16] and $|C_2|$ is determined in Theorem 5.8. In addition, from part (iii) of Theorem 5.14, $C^\perp$ can be represented as $C^\perp = C_1^\perp \bigoplus C_2^\perp$, where $C_1^\perp$ is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle x^{p^s}-1\rangle}$ and $C_2^\perp$ is determined in Theorems 5.12 and 5.13.

As discussed in Remark 5.15, cyclic and negacyclic codes are equivalent via the ring isomorphism $\delta : \frac{\mathcal{R}[x]}{\langle x^{5p^s}-1\rangle} \to \frac{\mathcal{R}[x]}{\langle x^{5p^s}+1\rangle}$ given by $x \mapsto -x$. So all the results of the paper hold true for negacyclic codes via that isomorphism.

For future work, it is interesting to investigate λ-constacyclic codes of length $5p^s$ over $\mathcal{R}$, where $\lambda \in \mathbb{F}_{p^m} \setminus \{0\}$ or $\lambda = \alpha + u\beta$ ($\alpha, \beta \in \mathbb{F}_{p^m} \setminus \{0\}$).

Acknowledgement

H.Q. Dinh and W. Yamaka are grateful to the Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University, for partial financial support. This research is partially supported by the Research Administration Centre, Chiang Mai University.

References

[1] T. Abualrub and R. Oehmke, *On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e*, IEEE Trans. Inform. Theory **49** (2003), 2126-2133.
[2] M.M. Al-Ashker, *Simplex codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$*, Arab. J. Sci. Eng. Sect. A Sci. **30** (2005), 277-285.
[3] E. Bannai, M. Harada, T. Ibukiyama, A. Munemasa, and M. Oura, *Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and applications to Hermitian modular forms*, Abh. Math. Sem. Univ. Hamburg **73** (2003), 13-42.
[4] E.R. Berlekamp, *Algebraic Coding Theory*, revised 1984 edition, Aegean Park Press, 1984.
[5] E. R. Berlekamp, *Negacyclic codes for the Lee metric,* in: Proceedings of the Conference on Combinatorial Mathematics and Its Application, Chapel Hill, NC, 1968, 298-316.
[6] S.D. Berman, *Semisimple cyclic and Abelian codes. II*, Kibernetika (Kiev) **3** (1967), 21-30 (Russian); translated as Cybernetics **3** (1967), 17-23.
[7] T. Blackford, *Negacyclic codes over $\mathbb{Z}_4$ of even length*, IEEE Trans. Inform. Theory **49** (2003), 1417-1424.
[8] T. Blackford, *Cyclic codes over $\mathbb{Z}_4$ of oddly even length*, International Workshop on Coding and Cryptography (WCC 2001) (Paris), Appl. Discr. Math. **128** (2003), 27-46.
[9] A. Bonnecaze and P. Udaya, *Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$*, IEEE Trans. Inform. Theory **45** (1999), 1250-1255.
[10] A.R. Calderbank, A.R. Hammons, P.V. Kumar, N.J. A. Sloane, and P. Solé, *A linear construction for certain Kerdock and Preparata codes*, Bull. AMS **29** (1993), 218-222.
[11] G. Castagnoli, J.L. Massey, P.A. Schoeller, and N. von Seemann, *On repeated-root cyclic codes*, IEEE Trans. Inform. Theory **37** (1991), 337-342.
[12] B. Chen, H.Q. Dinh, H. Liu and L.Wang, *Constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, Finite Fields and Their Applications **36** (2016), 108-130.
[13] B. Chen, H.Q. Dinh, and H. Liu, *Repeated-root constacyclic codes of length ℓp^s and their duals*, Discrete Appl. Math., **177** (2014), 60-70.
[14] H.Q. Dinh, *Negacyclic codes of length 2^s over Galois rings*, IEEE Trans. Inform. Theory **51** (2005), 4252-4262.
[15] H. Q. Dinh, *Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$*, IEEE Trans. Inform. Theory **55** (2009), 1730-1740.
[16] H.Q. Dinh, *Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, J. Algebra **324** (2010), 940-950.
[17] H. Q. Dinh, *Repeated-root constacyclic codes of length $2p^s$*, Finite Fields & Appl. **18** (2012), 133-143.
[18] H. Q. Dinh, *Structure of repeated-root constacyclic codes of length $3p^s$ and their duals*, Discrete Appl. Math. **313** (2013), 983-991.
[19] H.Q. Dinh and S.R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory **50** (2004), 1728-1744.
[20] H.Q. Dinh, S. Dhompongsa, and S. Sriboonchitta, *On constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, Discrete Math. **340** (2017), 832-849.
[21] H. Q. Dinh, B.T. Nguyen, and W. Yamaka, "Constacyclic Codes of Length $3p^s$ Over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and their application in various distance distributions", *IEEE Access*, **8** (2020), pp. 204031-204056.
[22] H.Q. Dinh, B.T. Nguyen, S. Sriboonchitta, and T.M. Vo, *On a class of constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, J. Algebra Appl. **18** (2019), 1950022.
[23] H.Q. Dinh, B.T. Nguyen, S. Sriboonchitta, and T.M. Vo, *On $(\alpha + u\beta)$-constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, J. Algebra Appl. **18** (2019), 1950023.
[24] H. Q. Dinh, Bac. T. Nguyen, and Songsak Sriboonchitta, *Negacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, Discrete Mathematics **341** (2018), 1055-1071.
[25] H. Q.Dinh ,Y. Fan, H. Liu, X. Liu, S. Sriboonchitta, *On self-dual constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, Discrete Mathematics **341** (2018), 324-335.
[26] S.T. Dougherty, S. Ling, *Cyclic codes over $\mathbb{Z}_4$ of even length*, Des. Codes Cryptogr. **39** (2006), 127-153.
[27] G. Falkner, B. Kowol, W. Heise, and E. Zehendner, *On the existence of cyclic optimal codes*, Atti Sem. Mat. Fis. Univ. Modena **28** (1979), 326-341.
[28] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J. A. Sloane, and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301-319.
[29] W.C. Huffman, *On the decomposition of self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ with an automorphism of odd prime order*, Finite Fields & Appl. **13** (2007), 681-712.
[30] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.
[31] E. Kleinfeld, *Finite Hjelmslev planes*, Illinois J. Math. **3** (1959), 403-407.
[32] R. Lidl and H. Niederreiter, *Finite Field*, Encyclopedia of Mathematics and its Applications 20, Cambridge University Press, 1987.
[33] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, 10^{th} impression, North-Holland, Amsterdam, 1998.
[34] J.L. Massey, D.J. Costello, and J. Justesen, *Polynomial weights and code constructions*, IEEE Trans. Inform. Theory **19** (1973), 101-110.
[35] B.R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, **28**, Marcel Dekker, New York, 1974.
[36] A.A. Nechaev, *Kerdock code in a cyclic form*, (in Russian), Diskr. Math. (USSR) **1** (1989), 123-139. English translation: Discrete Math. and Appl. **1** (1991), 365-384.
[37] C.-S. Nedeloaia, *Weight distributions of cyclic self-dual codes*, IEEE Trans. Inform. Theory **49** (2003), 1582-1591.
[38] G. Norton and A. Sălăgean-Mandache, *On the structure of linear cyclic codes over finite chain rings*, Appl. Algebra Engrg. Comm. Comput. **10** (2000), 489–506.
[39] V. Pless and W.C. Huffman, *Handbook of coding theory*, Elsevier, Amsterdam, 1998.
[40] E. Prange, *Cyclic Error-Correcting Codes in Two Symbols*, (September 1957), TN-57-103.
[41] E. Prange, *Some cyclic error-correcting codes with simple decoding algorithms*, (April 1958), TN-58-156.
[42] E. Prange, *An algorithm for factoring $x^n - 1$ over a finite field*, (October 1959), TN-59-175.
[43] E. Prange, *The use of coset equivalence in the analysis and decoding of group codes*, (1959), TN-59-164.
[44] R.M. Roth and G. Seroussi, *On cyclic MDS codes of length q over* GF(q), IEEE Trans. Inform. Theory **32** (1986), 284-285.

[45] J. H. Silverman, *A friendly introduction to number theory*, Brown University, 2011.
[46] A. Sălăgean, *Repeated-root cyclic and negacyclic codes over finite chain rings*, Discrete Appl. Math. **154** (2006), 413-419.
[47] I. Siap, *Linear codes over* $\mathbb{F}_2 + u\mathbb{F}_2$ *and their complete weight enumerators*, Codes and designs (Columbus, OH, 2000), Ohio State Univ. Math. Res. Inst. Publ. **10** (2002), de Gruyter, Berlin, 259-271.
[48] J. Tang, *The root criterion of quadratic equations in the finite field* GF(2^m), (in Chinese), Math. Practice Theory **2** (1986), 57–59. Reviewed in Zentr. Math. 633 12010.
[49] L.-z. Tang, C.B. Soh and E. Gunawan, *A note on the q-ary image of a* q^m*-ary repeated-root cyclic code*, IEEE Trans. Inform. Theory **43** (1997), 732-737.
[50] P. Udaya and A. Bonnecaze, *Decoding of cyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory **45** (1999), 2148-2157.
[51] J.H. van Lint, *Repeated-root cyclic codes*, IEEE Trans. Inform. Theory **37** (1991), 343-345.
[52] J. Wolfmann, *Negacyclic and cyclic codes over* $\mathbb{Z}_4$, IEEE Trans. Inform. Theory **45** (1999), 2527-2532.
[53] K.-H. Zimmermann, *On generalizations of repeated-root cyclic codes*, IEEE Trans. Inform. Theory **42** (1996), 641-649.