สัญญาเลขที่ R2563C005

รายงานวิจัยฉบับสมบูรณ์

โครงการ : การสร้างของรหัสวัฏจักรและรหัสวัฏจักรเชิงลบเหนือริงจำกัดสลับที่

คณะผู้วิจัย สังกัด

รองศาสตราจารย์ ดร.จักรกฤษ กลิ่นเอี่ยม

ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร

สนับสนุนโดย

งบประมาณรายได้มหาวิทยาลัยนเรศวร

ปีงบประมาณ 2563

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my advisor, Professor Dr.Suthep Suantai, for providing me valuable guidance and support throughout the project. Additionally, I would like to thank to my love students, Jirayu Pluto, Wateekorn Sriwirach, who helped me in doing a lot of research and I came to know about so many things. Without your assistance, I would not be able to complete this project successfully.

Furthermore, I would like to thank Naresuan University, which provides supporting for research.

Last but not least, I would like to thank to my parents for providing me the moral support and encouragement.

Chakkrid Klin-eam

Title Constructions of cyclic and negacyclic codes over finite commutative rings

Researcher Associate Professor Chakkrid Klin-eam, Ph.D.
Department of Mathematics, Faculty of Science
Naresuan University

Keywords Cyclic codes, Negacyclic codes, Finite commutative rings

Abstract

Let p be a prime such that $p \neq 3$. The algebraic structures of all cyclic and negacyclic codes of length $3p^s$ over the finite commutative chain ring $R := \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} (u^2 = 0)$ are obtained that the conditions depend on the factorization of polynomial $x^2 + x + 1$ over R. Therefore, we classify the structures of cyclic and negacyclic codes of length $3p^s$ over R into 2 cases, i.e., $p^m \equiv 1 \pmod 3$ and $p^m \equiv 2 \pmod 3$. From that, we obtain the number of all cyclic and negacyclic codes of length $3p^s$ over R. After that, we give some situations for such cyclic and negacyclic codes are self-dual codes.

ชื่อเรื่อง การสร้างของรหัสวัฏจักรและรหัสวัฏจักรเชิงลบที่ชัดเจนเหนือริงจำกัดสลับที่

ผู้วิจัย รองศาสตราจารย์ ดร.จักรกฤษ กลิ่นเอี่ยม

ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร

คำสำคัญ รหัสวัฏจักร รหัสวัฏจักรเชิงลบ ริงจำกัดสลับที่

บทคัดย่อ

ให้ p เป็นจำนวนเฉพาะ ซึ่ง $p \neq 3$ โครงสร้างเชิงพีชคณิตของรหัสวัฏจักรและรหัสวัฏจักรเชิงลบทั้งหมดของความยาว $3p^s$ เหนือริงจำกัดสลับที่ $R := \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} (u^2 = 0)$ ได้รับบนเงื่อนไขการแยกตัวประกอบของพหุนาม x^2+x+1 เหนือ R ดังนั้นเราสามารถจำแนกโครงสร้างของรหัสวัฏจักรและรหัสวัฏจักรเชิงลบของความยาว $3p^s$ เหนือ R ออกเป็น 2 กรณี นั่นคือ $p^m \equiv 1 \pmod 3$ และ $p^m \equiv 2 \pmod 3$ จากนั้นเราได้นับจำนวนรหัสวัฏจักรและรหัสวัฏจักรเชิงลบทั้งหมดของความยาว $3p^s$ เหนือ R หลังจากนั้นเราได้ให้รหัสคู่กันที่เหมาะสมกับรหัสวัฏจักรและรหัสวัฏจักรเชิงลบบางสถานการณ์

LIST OF CONTENTS

Chapter 1
Introduction

Let λ be a unit of a finite field. The class of λ-constacyclic codes is an important class of linear codes in coding theory. Many optimal linear codes are derived from λ-constacyclic codes. The class of λ-constacyclic codes includes as sub-classes of two classes, i.e., cyclic codes ($\lambda = 1$) and negacyclic codes ($\lambda = -1$). Cyclic codes over finite fields first were studied in 1957 by Prange which the cyclic codes have a rich algebraic structure. In 1967, Berman [1] introduce the codes in which length is divisible by the characteristics of the field, called *repeated-root codes*. In the 1970s and 1980s, several researchers, for example, Massey et al. [6], Falkner et al. [19], Roth and Seroussi [23] studied about repeated-root codes. Moreover, Castagnoli et al. [3] and van Lint [22], they showed that repeated-root cyclic codes have a concatenated construction, and are asymptotically bad in the 1990s.

After the 1990s, codes over finite rings are studied. In an important paper, Hammons et al. [20] proved that certain good nonlinear codes such as Kerdock and Preparata codes can be constructed from linear codes over $\mathbb{Z}_4$ via the Gray map. In 1999, Bonnecaze and Udaya [2] introduced cyclic codes and self-dual codes over the finite chain ring $\mathbb{F}_2+u\mathbb{F}_2$ where $u^2 = 0$. The ring $\mathbb{F}_2 + u\mathbb{F}_2$ shares some good properties of both $\mathbb{F}_4$ and $\mathbb{Z}_4$. This element is given by all binary polynomials in indeterminate u of degree less than 2 and is closed under usual binary addition but multiplication modulo u^2. In general, the class of finite rings of the form $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ has been widely used as alphabets of certain constacyclic codes.

In general, Zhao al et. [24] determined all $(\alpha + u\beta)$-constacyclic codes of length np^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ where α, β are units of $\mathbb{F}_{p^m}$ and $gcd(n, p) = 1$. Let $\alpha_0 \in \mathbb{F}_{p^m}$ such that $\alpha_0^{p^s} = \alpha$. They divide the structures of such constacyclic codes into 2 cases, i.e., $x^n - \alpha_0$ is irreducible in $\mathbb{F}_{p^m}$ and $x^n - \alpha_0$ is reducible in $\mathbb{F}_{p^m}$. Moreover, Cao al et. [5] also determine all α-constacyclic codes of length np^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ where α is a unit of $\mathbb{F}_{p^m}$ and $gcd(n, p) = 1$. Similarly, they divide the structures of such constacyclic codes that are similar to the above results. However, they do not give the condition that $x^n - \alpha_0$ is irreducible. It makes us interesting to such a condition. It is hard to find that condition in general form, i.e., constacyclic codes of length np^s. Therefore, it is a good reason to determine the codes of a specific length. The algebraic structures of repeated-

root constacyclic codes over $\mathbb{F}_{p^m}$ were studied in several lengths which include p^s, $2p^s$, $3p^s$ and $4p^s$ (see [9], [10], [11] and [12], repectively). In addition, the factorization of polynomials $x^2 - x + 1$ and $x^2 + x + 1$ over $\mathbb{F}_{p^m}$ were determined for construction of cyclic, negacyclic and constacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}$. Thus, we use those ideas to determine cyclic and negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$. After that, the structures of such repeated-root constacyclic codes over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ are interesting which consist of length p^s, $2p^s$ and $4p^s$. In 2010, Dinh [8] were studied the algebraic structures of constacyclic codes of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$. Moreover, the algebraic structures of self-dual constacyclic codes of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ were obtained by Dinh et al. [17] in 2018. Chen et al. [4] established all constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$. Recently, all constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ are studied by Dinh et al. [13], [15] and [14]. First, they were obtained that the structures of constacyclic codes of length $4p^s$ over such ring when $p^m \equiv 1 \pmod 4$. In 2018, the structures of constacyclic codes of length $4p^s$ when $p^m \equiv 3 \pmod 4$ were determined. We notice the algebraic structures of constacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ are not studied. Therefore, we focus on cyclic and negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ which are specifically of those constacyclic codes. Moreover, dual codes of cyclic codes are cyclic and dual codes of negacyclic codes are also negacyclic. This means that self-dual cyclic and negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ are existed.

The aims of this research are to obtain the algebraic structures of cyclic and negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ and their duals. Furthermore, the number of all distinct cyclic and negacyclic codes of length $3p^s$ over such ring are determined. Finally, we determine the conditions that cyclic and negacyclic codes are self-dual codes. The rest of the research is arranged as follows. After presenting preliminary in Chapter 2, we present the main results of this research in Chapter 3.1 and Section 3.2. Each section is divided into 2 subsections, i.e., $p^m \equiv 1 \pmod 3$ and $p^m \equiv 2 \pmod 3$. In Chapter 3.1, we focus on the structures of cyclic codes of length $3p^s$ and their dual codes. The remaining result, the number of all distinct cyclic codes are obtained in Section 3.2. Moreover, some conditions for self-dual cyclic codes are also obtained in the above section. In the case $p^m \equiv 2 \pmod 3$, it will be shown that each cyclic code of length $3p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ is a direct sum of a cyclic code of length p^s over such ring and an ideal of the quotient ring $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. However, we construct a ring isomorphism between the quotient rings $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ and $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle x^{2p^s}+(3\cdot 2^{-2})^{p^s}\rangle}$, i.e., each ideal of the quotient ring $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ is isomorphic to a $-(3\cdot 2^{-2})^{p^s}$-constacyclic codes of length $2p^s$ over

$\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ when p is an odd prime $p \neq 3$. In the remaining case $p = 2$, we obtain some properties of the quotient ring $\frac{(\mathbb{F}_{2^m}+u\mathbb{F}_{2^m})[x]}{\langle(x^2+x+1)^{2^s}\rangle}$ which bring to the properties of cyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$. After that, we define a ring isomorphism to obtain properties for negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$. Finally, The conclusion is mentioned in Chapter 4.

Chapter 2

Preliminaries

An ideal I of a finite commutative ring R with identity is called *principal* if it is generated by a single element. A ring R is a principal ideal ring if its ideals are principal. R is called a *local ring* if R has a unique maximal ideal. Furthermore, a ring R is called a *chain ring* if the set of all ideals of R is linearly ordered under set-theoretic inclusion. The *order* of an element a in R is the smallest positive integer n such that $a^n = 1$ where 1 is an identity of R and denoted by $ord(a)$. Moreover, the following equivalent conditions are known for the class of finite commutative rings with identity.

[18] If R is a finite commutative ring with identity, then the following conditions are equivalent:

1. R is a local ring and the maximal ideal M of R is principal, i.e., $M = \langle r \rangle$ for some $r \in R$,
2. R is a local principal ideal ring,
3. R is a chain ring with ideals $\langle r^i \rangle, 0 \leq i \leq N_r$, where N_r is the nilpotentcy of r.

Each *code* C of length n over a finite commutative ring R with identity is a nonempty subset of R^n, and ring R is referred to as the *alphabet* of the code. If C is an R-submodule of R^n, then C is called *a linear code* of length n over R. For a unit λ of R, the λ-constacyclic (λ-twisted) shift τ_λ on R^n is the shift

$$\tau_\lambda(c_0, c_1, ..., c_{n-1}) = (\lambda c_{n-1}, c_0, c_1, ..., c_{n-2})$$

and a linear code C is called *a λ-constacyclic code* if $\tau_\lambda(C) = C$, i.e., if C is closed under the λ-constacyclic shift τ_λ, for $\lambda = 1$, it is called *a cyclic code* and for $\lambda = -1$, it is called a *negacyclic code*.

Each codeword $c = (c_0, c_1, ..., c_{n-1})$ is identified with its polynomial representation as $c(x) = c_0 + c_1 x + ... + c_{n-1}x^{n-1}$ and the code C is identified with the set of all polynomial representations of its codewords. Then, in the quotient ring $\frac{R[x]}{\langle x^n - \lambda \rangle}$, $xc(x)$ corresponds to the λ-constacyclic shift of $c(x)$. Thus, the following fact is well known and straightforward:

[21] A linear code C of length n is a λ-constacyclic code over R if and only if C is an ideal of the quotient ring $\frac{R[x]}{\langle x^n-\lambda\rangle}$.(Hence, this quotient ring is referred to as the ambient ring of the code C.)

Given n-tuples $x = (x_0, x_1, ..., x_{n-1}), y = (y_0, y_1, ..., y_{n-1}) \in R^n$, their inner product is defined as usual

$$x \cdot y = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1},$$

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

$$C^\perp = \{x : x \cdot y = 0, \forall y \in C\}.$$

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 well known.

[18] Let p be a prime and R be a finite chain ring of size p^m. The number of codewords in each linear code C of length n over R is p^k, for some integer $k \in \{0, 1, ..., mn\}$. Moreover, the dual code $C^\perp$ has p^l codewords, where $k+l = mn$, i.e., $|C|\cdot|C^\perp| = |R|^n$.

In general, we have the following implication of the dual of a λ-constacyclic code.

[18] The dual of a λ-constacyclic code is a λ^{-1}-constacyclic code.

In this paper, we consider cyclic and negacyclic codes of length $3p^s$ over the ring $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ where $u^2 = 0$ and p is a prime with $p \neq 3$. The ring R consists of all p^m-ary polynomials of degree 0 and 1 in indeterminate u, it is closed under p^m-ary polynomial addition and multiplication modulo u^2. Thus, $R = \frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle} = \{a+ub : a, b \in \mathbb{F}_{p^m}\}$ is a local ring with maximal ideal $\langle u\rangle = u\mathbb{F}_{p^m}$, and hence, it is a chain ring.

Hereafter, we denote the ambient ring of cyclic and negacyclic codes of length $3p^s$ over R as

$$\mathcal{R}_1 = \frac{R[x]}{\langle x^{3p^s} - 1\rangle}.$$

and

$$\mathcal{R}_{-1} = \frac{R[x]}{\langle x^{3p^s} + 1\rangle},$$

respectively. From Proposition 2, λ-constacyclic codes of length n over R are ideals of $\mathcal{R}_\lambda = \dfrac{R[x]}{\langle x^n - \lambda\rangle}$.

[4] If $f(x) = a_0 + a_1x + \cdots + a_rx^r$ then the reciprocal of $f(x)$ is the polynomial $f^*(x) = a_r + a_{r-1}x + a_{r-2}x^2 + \cdots + a_0x^r$.

$f^*(x)$ can be expressed by $f^*(x) = x^r f(\frac{1}{x})$. If I is an ideal of $\mathcal{R}_\lambda$, then $I^* = \{f^*(x) : f(x) \in I\}$ is also an ideal of $\mathcal{R}_{\lambda^{-1}}$.

[4] Let I be an ideal of $\mathcal{R}_\lambda$. We define $\mathcal{A}(I) = \{g(x) : f(x)g(x) = 0, \forall f(x) \in I\}$. Then $\mathcal{A}(I)$ is called *the annihilator of* I.

From the above definition, We see that if I is an ideal of $\mathcal{R}_\lambda$, then $\mathcal{A}(I)$ is an ideal of $\mathcal{R}_\lambda$. Moreover, if C is a constacyclic code of length n over R with the associated ideal I (which is an ideal of $\mathcal{R}_\lambda$), then the associated ideal of $C^\perp$ is $\mathcal{A}(I)^*$ (which is an ideal of $\mathcal{R}_{\lambda^{-1}}$). The following lemma is easy to prove and will be used in Section 3.1.

[4]

1. $(f(x)g(x))^* = f^*(x)g^*(x)$.
2. If $\deg f(x) \geq \deg g(x)$, then $(f(x) + g(x))^* = f^*(x) + x^{\deg f(x) - \deg g(x)} g^*(x)$.
3. Let $I = \langle f(x), ug(x) \rangle$ be an ideal of $\mathcal{R}_\lambda$, then $I^* = \langle f^*(x), ug^*(x) \rangle$, which is an ideal of $\mathcal{R}_{\lambda^{-1}}$.

Let ξ be a primitive $(p^m - 1)$-th root of identity of $\mathbb{F}_{p^m}$. Then

$$\mathbb{F}_{p^m} = \{0, \xi, \xi^2, \cdots, \xi^{p^m - 1} = 1\}.$$

Chapter 3

Main Results

Firstly, we focus the structures of cyclic codes of length $3p^s$ over R as the following section.

3.1 Cyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

In this section, we focus on the algebraic structures of cyclic codes of length $3p^s$ over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. So, we divide this structures into 2 cases, namely, $p^m \equiv 1 \pmod 3$ and $p^m \equiv 2 \pmod 3$.

3.1.1 The case $p^m \equiv 1 \pmod 3$

By Proposition 2, each cyclic code of length $3p^s$ over R is an ideal of $\mathcal{R}_1 = \frac{R[x]}{\langle x^{3p^s}-1\rangle}$. In $R[x]$, we get

$$(\xi^{\frac{p^m-1}{3}})^3 - 1 = 0,$$
$$(\xi^{\frac{2(p^m-1)}{3}})^3 - 1 = 0 \text{ and}$$
$$(\xi^{\frac{3(p^m-1)}{3}})^3 - 1 = 0.$$

This means that $\xi^{\frac{p^m-1}{3}}$, $\xi^{\frac{2(p^m-1)}{3}}$ and $\xi^{\frac{3(p^m-1)}{3}}$ are roots of the polynomial $x^3 - 1$. Therefore, the polynomial $x^{3p^s} - 1$ can be expressed as

$$\begin{aligned} x^{3p^s} - 1 &= (x^3 - 1)^{p^s} \\ &= (x - \xi^{\frac{p^m-1}{3}})^{p^s}(x - \xi^{\frac{2(p^m-1)}{3}})^{p^s}(x - \xi^{\frac{3(p^m-1)}{3}})^{p^s} \\ &= (x^{p^s} - \xi^{\frac{(p^m-1)p^s}{3}})(x^{p^s} - \xi^{\frac{2(p^m-1)p^s}{3}})(x^{p^s} - \xi^{\frac{3(p^m-1)p^s}{3}}) \\ &= (x^{p^s} - \xi^{\frac{(p^m-1)p^s}{3}})(x^{p^s} - \xi^{\frac{2(p^m-1)p^s}{3}})(x^{p^s} - 1) \\ &= (x^{p^s} - 1)(x^{p^s} - \delta_1)(x^{p^s} - \delta_2), \end{aligned}$$

where $\delta_i = \xi^{\frac{i(p^m-1)p^s}{3}}$ for $i = 1, 2$.

Let $\delta_i = \xi^{\frac{i(p^m-1)p^s}{3}}$ for $i = 1, 2$.

1. $\delta_1\delta_2 = 1$.

2. $\delta_1 + \delta_2 = -1$.

Thus, we obtain that the algebraic structures of cyclic codes of length $3p^s$ over R as the following theorem.

Let C be a cyclic code of length $3p^s$ over R. Then $C = C_1 \oplus C_{\delta_1} \oplus C_{\delta_2}$ where C_1 is a cyclic code and C_{δ_i} is a δ_i-constacyclic code of length p^s over R where $\delta_i = \xi^{\frac{i(p^m-1)p^s}{3}}$ for $i = 1, 2$. Moreover, $|C| = |C_1||C_{\delta_1}||C_{\delta_2}|$.

It is a routine to show that $\langle x^{p^s} - 1\rangle$, $\langle x^{p^s} - \delta_1\rangle$ and $\langle x^{p^s} - \delta_2\rangle$ are pair-wises coprime ideals in $R[x]$ where $\delta_i = \xi^{\frac{i(p^m-1)p^s}{3}}$ for $i = 1, 2$. By Chinese Division Algorithm, we have

$$\frac{R[x]}{\langle x^{3p^s} - 1\rangle} \cong \frac{R[x]}{\langle x^{p^s} - 1\rangle} \oplus \frac{R[x]}{\langle x^{p^s} - \delta_1\rangle} \oplus \frac{R[x]}{\langle x^{p^s} - \delta_2\rangle}.$$

By Proposition 2, we obtain that C is an ideal of $\mathcal{R}_1$. Thus, $C = C_1 \oplus C_{\delta_1} \oplus C_{\delta_2}$ where C_1 is an ideal of $\frac{R[x]}{\langle x^{p^s}-1\rangle}$ and C_{δ_i} is an ideal of $\frac{R[x]}{\langle x^{p^s}-\delta_i\rangle}$ for $i = 1, 2$. By Proposition 2 again, C_1 is a cyclic code of length p^s over R and C_{δ_i} is a δ_i-constacyclic code of length p^s over R for $i = 1, 2$.

Therefore, by Theorem 3.1.1, each cyclic code of length $3p^s$ over R is a direct sum of cyclic and δ_1, δ_2-constacyclic codes of length p^s over R. However, the algebraic structures of all constacyclic codes of length p^s over R are obtained in [8]. Next, we investigate the dual of cyclic codes of length $3p^s$ over R as the following theorem. Let $C = C_1 \oplus C_{\delta_1} \oplus C_{\delta_2}$ be a cyclic code of length p^s over R where C_1 is a cyclic code and C_{δ_i} is a δ_i-constacyclic code of length $3p^s$ over R and $\delta_i = \xi^{\frac{i(p^m-1)}{3}}$ for $i = 1, 2$. Then $C^\perp = C_1^\perp \oplus C_{\delta_1}^\perp \oplus C_{\delta_2}^\perp$ where $C_1^\perp$ is a cyclic code, $C_{\delta_1}^\perp$ is a δ_2-constacyclic code and $C_{\delta_2}^\perp$ is a δ_1-constacyclic code of length p^s over R. In particular, $|C^\perp| = |C_1^\perp||C_{\delta_1}^\perp||C_{\delta_2}^\perp|$. It is obvious that

$$C_1^\perp \oplus C_{\delta_1}^\perp \oplus C_{\delta_2}^\perp \subseteq C^\perp.$$

We consider that

$$\begin{aligned}
|C_1^\perp||C_{\delta_1}^\perp||C_{\delta_2}^\perp| &= \frac{|R|^{p^s}}{|C_1|}\frac{|R|^{p^s}}{|C_{\delta_1}|}\frac{|R|^{p^s}}{|C_{\delta_2}|} \\
&= \frac{|R|^{3p^s}}{|C_1||C_{\delta_1}||C_{\delta_2}|} \\
&= \frac{|R|^{3p^s}}{|C|} \\
&= |C^\perp|.
\end{aligned}$$

Hence, $C^\perp = C_1^\perp \oplus C_{\delta_1}^\perp \oplus C_{\delta_2}^\perp$. Using Proposition 2, $C_1^\perp$ is a cyclic code of length p^s over R, $C_{\delta_1}^\perp$ is a δ_2-constacyclic code of length p^s over R and $C_{\delta_2}^\perp$ is a δ_1-constacyclic code of length p^s over R.

The following result can be found in [17, Section 5], and will apply to determine self-dual of cyclic codes of length $3p^s$ over R:

Let λ be a unit of $\mathbb{F}_{p^m}$. If $\lambda \neq \lambda^{-1}$, a λ-constacyclic code C of length p^s over R is self-dual if and only if it is the ideal $\langle u \rangle$ of the quotient ring $\frac{R[x]}{\langle x^{p^s}-\lambda \rangle}$. Hence, $\langle u \rangle$ is the unique self-dual λ-cosntacyclic code of length p^s over R.

Thus, The $\langle u \rangle$ is the unique self-dual δ_1, δ_2-constacyclic codes of length p^s over R.

Let $C = C_1 \oplus C_{\delta_1} \oplus C_{\delta_2}$ be a cyclic code of length $3p^s$ over R where C_1 is a cyclic code of length $3p^s$ over R and C_{δ_i} is a δ_i-constacyclic code of length $3p^s$ over R where $\delta_i = \xi^{\frac{i(p^m-1)}{3}}$ for $i = 1, 2$. If $C_1 = C_{\delta_1} = C_{\delta_2} = \langle u \rangle$, then C is a self-dual cyclic code of length $3p^s$ over R. Suppose that $C_1 = C_{\delta_1} = C_{\delta_2} = \langle u \rangle$. By assumtion, we have $C = \langle u \rangle$. Therefore, $C^{\perp} = \langle u \rangle$, implying that C is self-dual.

3.1.2 The case $p^m \equiv 2 \pmod 3$

First, we consider that

$$\begin{aligned} x^{3p^s} - 1 &= (x^3 - 1)^{p^s} \\ &= (x-1)^{p^s}(x^2+x+1)^{p^s} \\ &= (x^{p^s} - 1)(x^2+x+1)^{p^s}. \end{aligned}$$

Next, we give the following lemmas for properties of a polynomial $x^2 + x + 1$ to prove in this case. The polynomial x^2+x+1 is irreducible in $\mathbb{F}_{p^m}[x]$. Assume that x^2+x+1 is reducible in $\mathbb{F}_{p^m}[x]$. There exists $\alpha \in \mathbb{F}_{p^m}$ such that

$$\alpha^2 + \alpha + 1 = 0.$$

Note that

$$x^3 - 1 = (x-1)(x^2+x+1).$$

This implies that α is a root of $x^3 - 1 = 0$ over $\mathbb{F}_{p^m}$. That is $\alpha^3 = 1$. Thus, $ord(\alpha)|3$ If $ord(\alpha) = 1$, then $0 = \alpha^2 + \alpha + 1 = 1 + 1 + 1 = 3 \neq 0$ which is a contradiction. Now, we have $ord(\alpha) = 3$. This means that $3|(p^m - 1)$, implying that $p^m \equiv 1 \pmod 3$. It is a contradiction. Therefore, $x^2 + x + 1$ is irreducible in $\mathbb{F}_{p^m}[x]$. The polynomial $x^2 + x + 1$ is irreducible in $R[x]$. Assume that $x^2 + x + 1$ is reducible in $R[x]$. There exists $\alpha = \alpha_0 + u\alpha_1 \in R$ for some $\alpha_0, \alpha_1 \in \mathbb{F}_{p^m}$ such that

$$\alpha^2 + \alpha + 1 = 0.$$

So, $0 = (\alpha_0 + u\alpha_1)^2 + (\alpha_0 + u\alpha_1) + 1 = \alpha_0^2 + \alpha_0 + 1 + u(2\alpha_0\alpha_1 + \alpha_1)$. This implies that $\alpha_0^2 + \alpha_0 + 1 = 0$ and $2\alpha_0\alpha_1 + \alpha_1 = 0$. Thus, $\alpha_0 \in \mathbb{F}_{p^m}$ is a root of $x^2 + x + 1 = 0$. It is a contradiction with Lemma 3.1.2. Hence, $x^2 + x + 1$ is irreducible in $R[x]$.

Throughout this case, we consider that

$$\begin{aligned}
&(-3^{-1})^{p^s}(x+2)^{p^s}(x^{p^s}-1) + (-1)(-3^{-1})^{p^s}(x^2+x+1)^{p^s} \\
&= (-3^{-1})^{p^s}(x+2)^{p^s}(x-1)^{p^s} + (-1)(-3^{-1})^{p^s}(x^2+x+1)^{p^s} \\
&= (-3^{-1})^{p^s}[(x^2+x-2)^{p^s} - (x^2+x+1)^{p^s}] \\
&= (-3^{-1})^{p^s}(-3)^{p^s} \\
&= 1.
\end{aligned}$$

Thus, we obtain that $x^{p^s} - 1$ and $(x^2 + x + 1)^{p^s}$ are coprime in $R[x]$. This implies that $\langle x^{p^s} - 1\rangle$ and $\langle (x^2 + x + 1)^{p^s}\rangle$ are pair-wises coprime ideals in $R[x]$. By Chinese Remainder Theorem, we have

$$\frac{R[x]}{\langle x^{3p^s} - 1\rangle} \cong \frac{R[x]}{\langle x^{p^s} - 1\rangle} \oplus \frac{R[x]}{\langle (x^2 + x + 1)^{p^s}\rangle}. \tag{3.1}$$

By Proposition 2, each ideal of $\frac{R[x]}{\langle x^{p^s}-1\rangle}$ is a cyclic code of length p^s over R studied in [8]. Moreover, cyclic codes and their dual codes of length $3p^s$ over R are determined as follows: Let C be a cyclic code of length $3p^s$ over R. Then

1. $C = C_1 \oplus I$ where C_1 is a cyclic code of length p^s over R and I is an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. Moreover, $|C| = |C_1||I|$.
2. the dual code $C^\perp$ of C can be expressed as $C^\perp = C_1^\perp \oplus \mathcal{A}(I)^*$ where C_1 is a cyclic code of length p^s over R and I is an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. Moreover, $|C^\perp| = |C_1^\perp||\mathcal{A}(I)^*|$.

1. By Proposition 2, we have C is an ideal of $\frac{R[x]}{\langle x^{3p^s}-1\rangle}$. By Equation (3.1), we have C is a direct sum of an ideal of $\frac{R[x]}{\langle x^{p^s}-1\rangle}$ and an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. By Proposition 2 again, we have $C = C_1 \oplus I$ where C_1 is a cyclic code of length p^s over R and I is an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$.
2. Let $C^\perp$ be the dual code of each negacyclic code of length $3p^s$ over R. By 1, we have $C^\perp = C_1^\perp \oplus I^\perp$ where C_1 is a cyclic code of length p^s over R and I is an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. By Proposition 2, we have $C^\perp = C_1^\perp \oplus \mathcal{A}(I)^*$.

Next, we determine the algebraic structure of the ring $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. In $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$, we have

$$\begin{aligned} 0 &= (x^2+x+1)^{p^s} \\ &= x^{2p^s} + x^{p^s} + 1. \end{aligned} \tag{3.2}$$

By Equation (3.2), $-1 = x^{2p^s} + x^{p^s}$ in $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. Each non-zero polynomial of degree less than 2 in $\mathbb{F}_{p^m}[x]$ is invertible in $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. Let $f(x) = ax + b$ be a non-zero polynomial in $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ where $a, b \in \mathbb{F}_{p^m}$. If $a = 0$, then $ax + b = b \neq 0$. This implies that $ax + b$ is invertible in $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. If $a \neq 0$, then

$$\begin{aligned} a^{-1}(x+a^{-1}b)^{-1} &= a^{-1}(x+a^{-1}b)^{p^s-1}(x-a^{-1}b+1)^{p^s}(x+a^{-1}b)^{-p^s}(x-a^{-1}b+1)^{-p^s} \\ &= a^{-1}(x+a^{-1}b)^{p^s-1}(x-a^{-1}b+1)^{p^s}(x^2+x-(a^{-1}b)^2+a^{-1}b)^{-p^s} \\ &= a^{-1}(x+a^{-1}b)^{p^s-1}(x-a^{-1}b+1)^{p^s}(x^{2p^s}+x^{p^s}-(a^{-1}b)^{2p^s}+(a^{-1}b)^{p^s})^{-1} \\ &= a^{-1}(x+a^{-1}b)^{p^s-1}(x-a^{-1}b+1)^{p^s}(-1-(a^{-1}b)^{2p^s}-(-a^{-1}b)^{p^s})^{-1} \\ &= -a^{-1}(x+a^{-1}b)^{p^s-1}(x-a^{-1}b+1)^{p^s}((a^{-1}b)^{2p^s}+(-a^{-1}b)^{p^s}+1^{p^s})^{-1} \\ &= -a^{-1}(x+a^{-1}b)^{p^s-1}(x-a^{-1}b+1)^{p^s}([(a^{-1}b)^2+a^{-1}b+1]^{p^s})^{-1}. \end{aligned}$$

This means that $ax + b$ is invertible if and only if $(a^{-1}b)^2 + a^{-1}b + 1$ is invertible in $\mathbb{F}_{p^m}$. By Lemma 3.1.2, we have $(a^{-1}b)^2 + a^{-1}b + 1 \neq 0$. Hence, $ax + b$ is invertible in $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. Let $f(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. Then $f(x)$ can be uniquely expressed as

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

where $a_{0i}, a_{1i}, b_{0i}, b_{1i} \in \mathbb{F}_{p^m}$, $0 \leq i \leq p^s - 1$. Moreover, $f(x)$ is non-invertible if and only if $a_{00} = b_{00} = 0$. Since $f(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$, it can be viewed as polynomial of degree less than $2p^s$ over R. So, $f(x) = f_1(x) + uf_2(x)$ where $f_1(x), f_2(x)$ are polynomials in $\mathbb{F}_{p^m}[x]$. Thus, we have

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

where $a_{0i}, a_{1i}, b_{0i}, b_{1i} \in \mathbb{F}_{p^m}$, $0 \leq i \leq p^s - 1$. Since $(x^2+x+1)^{p^s} = 0$ and $u^2 = 0$, we have x^2+x+1 and u are nilpotent elements of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ with nilpotency indexes p^s and 2, respectively. Hence, $f(x)$ is non-invertible if and only if $a_{00} = b_{00} = 0$. The ring $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ is a local ring with the maximal ideal $\langle x^2+x+1, u \rangle$ and it is not a chain ring. By Lemma 3.1.2, the set of all non-invertible elements of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ forms the ideal $\langle x^2+x+1, u \rangle$. This means that $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ is a local ring with the maximal ideal $\langle x^2+x+1, u \rangle$. Next, we will show that $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ is not a chain ring. Claim that $u \notin \langle x^2+x+1 \rangle$ and $x^2+x+1 \notin \langle u \rangle$. Suppose that $u \in \langle x^2+x+1 \rangle$. Then $u = (x^2+x+1)(g_1(x)+ug_2(x))$ for some $g_1(x), g_2(x) \in \mathbb{F}_{p^m}[x]$. So, $(x^2+x+1)g_1(x) = 0$ and $(x^2+x+1)g_2(x) = 1$. This implies that x^2+x+1 is invertible. It is a contradiction because x^2+x+1 is a nilpotent element. Thus, $u \notin \langle x^2+x+1 \rangle$. Since nilpotentcy indexes of x^2+x+1 and u are p^s and 2, respectively, we have $x^2+x+1 \notin \langle u \rangle$. Hence, we obtain that $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ is not a chain ring. The ring $\frac{\mathbb{F}_{p^m}[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ is a chain ring whose each ideal forms $\langle (x^2+x+1)^i \rangle$, $0 \leq i \leq p^s$. Let $f(x) \in \frac{\mathbb{F}_{p^m}[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ Then

$$\begin{aligned} f(x) &= \sum_{i=0}^{p^s-1} (a_i x + b_i)(x^2+x+1)^i \\ &= a_0 x + b_0 + \sum_{i=1}^{p^s-1} (a_i x + b_i)(x^2+x+1)^i \\ &= a_0 x + b_0 + (x^2+x+1) \sum_{i=1}^{p^s-1} (a_i x + b_i)(x^2+x+1)^{i-1}, \end{aligned}$$

where $a_i, b_i \in \mathbb{F}_{p^m}$, $0 \leq i \leq p^s - 1$. Thus, $f(x)$ is non-invertible if and only if $a_0 = b_0 = 0$. This implies that the set of all non-invertible elements is $\langle x^2+x+1 \rangle$. So, The ring $\frac{\mathbb{F}_{p^m}[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ is a local ring with the maximal ideal $\langle x^2+x+1 \rangle$. Since the maximal ideal $\langle x^2+x+1 \rangle$ is a principal ideal and by Proposition 2, we have $\frac{\mathbb{F}_{p^m}[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ is a chain ring whose each ideal forms $\langle (x^2+x+1)^i \rangle$, $0 \leq i \leq p^s$.

Now, we characterize all ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ in the following theorem. All ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ are listed respectively as follows:

Type 1: (trivial ideals)

$$\langle 0 \rangle \text{ and } \langle 1 \rangle.$$

Type 2: (principal ideals with nonmonic polynomial generators)

$$\langle u(x^2+x+1)^i \rangle,$$

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

Type 3: (principal ideals with monic polynomial generators)

$$\langle (x^2+x+1)^i + u(x^2+x+1)^t h(x) \rangle,$$

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

Type 4: (non-principal ideals)

$$\langle (x^2+x+1)^i + u\sum_{j=0}^{\omega-1}(a_j x + b_j)(x^2+x+1)^j, u(x^2+x+1)^\omega \rangle,$$

where $1 \leq i \leq p^s - 1, a_j, b_j \in \mathbb{F}_{p^m}$, and $\omega < T$ where T is the smallest integer such that $u(x^2+x+1)^T \in \langle (x^2+x+1)^i + u\sum_{j=0}^{\omega-1}(a_j x + b_j)(x^2+x+1)^j \rangle$
or equivalently,
$\langle (x^2+x+1)^i + u(x^2+x+1)^t h(x), u(x^2+x+1)^\omega \rangle$, with $h(x)$ as in Type 3, and $\deg h(x) \leq \omega - t - 1$.

First of all, it is easy to see that ideals of Type 1 are trivial ideals. Let I be an arbitrary nontrivial ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. We processed by establishing all possible forms that this nontrivial ideal I can have.

Case 1: $I \subseteq \langle u \rangle$: Then any element of I must be of the form $c(x) = u\sum_{i=0}^{p^s-1}(a_{0i}x + b_{0i})(x^2+x+1)^i$ where $a_{0i}, b_{0i} \in \mathbb{F}_{p^m}$. This implies that there exists an element $l(x) \in I$ that has the smallest k such that $l_{0k}x + l_{1k} \neq 0$. Hence, each element $c(x) \in I$ have the form $c(x) = u(x^2+x+1)^k \sum_{i=k}^{p^s-1}(a_{0i}x + b_{0i})(x^2+x+1)^{i-k} \in \langle u(x^2+x+1)^k \rangle$, implying that $I \subseteq \langle u(x^2+x+1)^k \rangle$. However, we have $l(x) \in I$ with

$$\begin{aligned} l(x) &= u(x^2+x+1)^k \sum_{i=k}^{p^s-1}(l_{0i}x + l_{1i})(x^2+x+1)^{i-k} \\ &= u(x^2+x+1)^k \left[l_{0k}x + l_{1k} + \sum_{i=k+1}^{p^s-1}(l_{0i}x + l_{1i})(x^2+x+1)^{i-k} \right]. \end{aligned}$$

From $l_{0k}x + l_{1k} \neq 0$, we can see that $l_{0k}x + l_{1k} + \sum_{i=k+1}^{p^s-1}(l_{0i}x + l_{1i})(x^2+x+1)^{i-k}$ is invertible, proving that $u(x^2+x+1)^k \in I$. Therefore, $I = \langle u(x^2+x+1)^k \rangle$, which means that the nontrivial ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ contained in $\langle u \rangle$ are $\langle u(x^2+x+1)^k \rangle$, $0 \leq k \leq p^s - 1$, which are ideals of Type 2.

Case 2: $I \nsubseteq \langle u \rangle$: Let I_u denote the set of elements in I which are reduced modulo u. By Theorem 3.1.2, we have I_u is a non-zero ideal of the ring $\frac{\mathbb{F}_{p^m}[x]}{\langle (x^2+x+1)^{p^s} \rangle}$, which is a finite chain ring with ideals $\langle (x^2+x+1)^j \rangle$, where $0 \leq j \leq p^s$. Then there is an integer

$1 \leq i \leq p^s - 1$ such that $I_u = \langle (x^2+x+1)^i \rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. This follows that there exists an element

$$c(x) = \sum_{j=0}^{p^s-1}(a_{0j}x + b_{0j})(x^2+x+1)^j + u\sum_{j=0}^{p^s-1}(a_{1j}x + b_{1j})(x^2+x+1)^j \in \frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle},$$

where $a_{0j}, a_{1j}, b_{0j}, b_{1j} \in \mathbb{F}_{p^m}$ such that $(x^2+x+1)^i + uc(x) \in I$. Since

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

and $u(x^2+x+1)^k = u(x^2+x+1)^{k-i}[(x^2+x+1)^i + uc(x)] \in I$ with $i \leq k \leq p^s - 1$, we have $(x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j \in I$. We now consider two subcases.

Case 2a: $I = \langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j \rangle$, then I can be expressed as

$$I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x) \rangle,$$

where $0 \leq t < i$ and $h(x)$ is 0 or a unit. If $h(x)$ is a unit, then $h(x)$ can be represented as $h(x) = \sum_j (h_{1j}x + h_{0j})(x^2+x+1)^j$ with $h_{0j}, h_{1j} \in \mathbb{F}_{p^m}$ and $h_{10}x + h_{00} \neq 0$. It follows that I is of Type 3.

Case 2b: $\langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j \rangle \subsetneq I$. Then, there exists $f(x) \in I \backslash \langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j \rangle$. By Division Algorithm, there exist polynomials $q(x), r(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ such that

$$0 \neq r(x) = f(x) - q(x)\left[(x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j\right] \in I,$$

where $\deg r(x) < \deg((x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x + a_{1j})(x^2+x+1)^j)$. This implies that $r(x)$ can be expressed as

$$r(x) = \sum_{j=0}^{i-1}(r_{1j}x + r_{0j})(x^2+x+1)^j + u\sum_{j=0}^{i-1}(r'_{1j}x + r'_{0j})(x^2+x+1)^j,$$

where $r_{0j}, r_{1j}, r'_{0j}, r'_{1j} \in \mathbb{F}_{p^m}$. Hence, $r(x)$ reduced modulo u is in $I_u = \langle (x^2+x+1)^i \rangle$, and thus, $r_{0j}, r_{1j} = 0$ for all $0 \leq j \leq i-1$, i.e., $r(x) = u\sum_{j=0}^{i-1}(r'_{1j}x + r'_{0j})(x^2+x+1)^j$. Since $r(x) \neq 0$, there exists the smallest integer $k, 0 \leq k \leq i-1$, such that $r'_{1k}x + r'_{0k} \neq$

0. Then

$$r(x) = u\sum_{j=k}^{i-1}(r'_{1j}x + r'_{0j})(x^2+x+1)^j = u(x^2+x+1)^k \times \left[r'_{1k}x + r'_{0k} + \sum_{j=k+1}^{i-1}(h'_{1j}x + h'_{0j})(x^2+x+1)^{j-k}\right].$$

As $r'_{1k}x + r'_{0k} \neq 0, r'_{1k}x + r'_{0k} + \sum_{j=k+1}^{i-1}(r'_{1j}x + r'_{0j})(x^2+x+1)^{j-k}$ is an invertible element in $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$, hence,

$$u(x^2+x+1)^k = \left[r'_{1k}x + r'_{0k} + \sum_{j=k+1}^{i-1}(r'_{1j}x + r'_{0j})(x^2+x+1)^{j-k}\right]^{-1} r(x) \in I.$$

It has been shown that for any $f(x) \in I \backslash \langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j\rangle$, there is an integer k with $0 \leq k \leq i-1$ such that $u(x^2+x+1)^k \in I$. Let $\omega = \min\{k : f(x) \in I \backslash \langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j\rangle\}$. Then $\langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j, u(x^2+x+1)^\omega\rangle \subseteq I$. In addition, by the above construction, for any $f(x) \in I$, there exists a polynomial $g(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ satisfying

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

implying that

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

Thus, we get

$$I = \langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j, u(x^2+x+1)^\omega\rangle$$
$$= \langle (x^2+x+1)^i + u\sum_{j=0}^{\omega-1}(a_{0j}x + b_{0j})(x^2+x+1)^j, u(x^2+x+1)^\omega\rangle.$$

Let T be the smallest integer such that $u(x^2+x+1)^T \in \langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j\rangle$. If $\omega \geq T$, then

$$I = \langle (x^2+x+1)^i + u\sum_{j=0}^{\omega-1}(a_{0j}x + b_{0j})(x^2+x+1)^j, u(x^2+x+1)^\omega\rangle$$
$$= \langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j\rangle.$$

It is a contradiction by assumption of this case. This implies that $\omega < T$, proving that I is of Type 4.

Next, we focus on annihilator in $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ to characterize the dual codes of constacyclic codes of length $3p^s$ over R. We now investigate the dual codes and determine the annihilator of I where I is an ideal of the ring $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. We need to give the following lemma.

From Theorem 3.1.2, the number T is an important role in Type 4. So, we need to determine the number T as the following proposition. Let T be the smallest integer such that $u(x^2+x+1)^T \in C = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x) \rangle$, where $h(x)$ is 0 or a unit. Then

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

First of all, we see that $T \leq i$ because $u(x^2+x+1)^i = u[(x^2+x+1)^i + u(x^2+x+1)^t h(x)] \in C$. If $h(x) = 0$, then $C = \langle (x^2+x+1)^i \rangle$, implying that $T = i$. Now we consider that the case $h(x)$ is a unit. Since $u(x^2+x+1)^T \in \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x) \rangle$, there is a polynomial $f(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ satisfying $u(x^2+x+1)^T = f(x)[(x^2+x+1)^i + u(x^2+x+1)^t h(x)]$. So, $f(x)$ can be written as

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

where $a_{0j}, a_{1j}, b_{0j}, b_{1j} \in \mathbb{F}_{p^m}$. Then $u(x^2+x+1)^T$ can be expressed as follows:

$$\left[\sum_{j=0}^{p^s-1} (a_{0j}x + b_{0j})(x^2+x+1)^j + u \sum_{j=0}^{p^s-1} (a_{1j}x + b_{1j})(x^2+x+1)^j \right] \left[(x^2+x+1)^i + u(x^2+x+1)^t \right.$$

$$
\begin{aligned}
=&(x^2+x+1)^i\sum_{j=0}^{p^s-1}(a_{0j}x+b_{0j})(x^2+x+1)^j+u(x^2+x+1)^i\sum_{j=0}^{p^s-1}(a_{1j}x+b_{1j})(x^2+x+1)^j\\
&+u(x^2+x+1)^th(x)\sum_{j=0}^{p^s-1}(a_{0j}x+b_{0j})(x^2+x+1)^j\\
=&(x^2+x+1)^i\sum_{j=0}^{p^s-i-1}(a_{0j}x+b_{0j})(x^2+x+1)^j+(x^2+x+1)^{p^s}\sum_{j=p^s-i}^{p^s-1}(a_{0j}x+b_{0j})(x^2+x+1)^{i+j-1}\\
&+u(x^2+x+1)^i\sum_{j=0}^{p^s-i-1}(a_{1j}x+b_{1j})(x^2+x+1)^j\\
&+u(x^2+x+1)^{p^s}\sum_{j=p^s-i}^{p^s-1}(a_{1j}x+b_{1j})(x^2+x+1)^{i+j-p^s}\\
&+u(x^2+x+1)^th(x)\sum_{j=0}^{p^s-i-1}(a_{0j}x+b_{0j})(x^2+x+1)^j\\
&+u(x^2+x+1)^th(x)\sum_{j=p^s-i}^{p^s-1}(a_{0j}x+b_{0j})(x^2+x+1)^j\\
=&(x^2+x+1)^i\sum_{j=0}^{p^s-i-1}(a_{0j}x+b_{0j})(x^2+x+1)^j\\
&+u(x^2+x+1)^i\sum_{j=0}^{p^s-i-1}(a_{1j}x+b_{1j})(x^2+x+1)^j\\
&+u(x^2+x+1)^th(x)\sum_{j=0}^{p^s-i-1}(a_{0j}x+b_{0j})(x^2+x+1)^j\\
&+u(x^2+x+1)^th(x)\sum_{j=p^s-i}^{p^s-1}(a_{0j}x+b_{0j})(x^2+x+1)^j.
\end{aligned}
$$

We see that $(x^2+x+1)^i\sum_{j=0}^{p^s-i-1}(a_{0j}x+b_{0j})(x^2+x+1)^j=0$, implying that $a_{0j}=b_{0j}=0$ for all $0\le j\le p^s-i-1$. Thus,

$$
\begin{aligned}
u(x^2+x+1)^T=&u(x^2+x+1)^i\sum_{j=0}^{p^s-i-1}(a_{1j}x+b_{1j})(x^2+x+1)^j\\
&+u(x^2+x+1)^{p^s-i+t}h(x)\sum_{j=0}^{i-1}(a_{0,p^s-i+j}x+b_{0,p^s-i+j})(x^2+x+1)^j.
\end{aligned}
$$

Therefore, $T\ge\min\{i,p^s-i+t\}$. Moreover,

$$
[(x^2+x+1)^i+u(x^2+x+1)^th(x)](x^2+x+1)^{p^s-1}=u(x^2+x+1)^{p^s-i+t}h(x).
$$

Hence,

$$u(x^2+x+1)^{p^s-i+t} = [(x^2+x+1)^i + u(x^2+x+1)^t h(x)](x^2+x+1)^{p^s-i}h(x)^{-1} \in C.$$

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

We now investigate the dual codes and determine the annihilator of I where I is an ideal of the ring $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. We need to give the following lemma. Let I be an ideal of the ring $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. If $I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x), u(x^2+x+1)^\omega\rangle$ where $h(x)$ is 0 or a unit, then $p^s - i$ is the smallest positive integer r such that $u(x^2+x+1)^r \in \mathcal{A}(I)$. Since $(x^2+x+1)^i + u(x^2+x+1)^t h(x) \in I$ and $u(x^2+x+1)^r \in \mathcal{A}(I)$, we have

$$0 = [(x^2+x+1)^i + u(x^2+x+1)^t h(x)]u(x^2+x+1)^r = u(x^2+x+1)^{i+r}.$$

We see that $i + r \geq p^s$. So, we have the smallest value of r is $p^s - i$. Hence, $u(x^2 + x + 1)^{p^s-i} \in \mathcal{A}(I)$. Let $I = \langle u(x^2+x+1)^i\rangle$ be an ideal of the ring $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. Then $\mathcal{A}(I)^* = \langle (x^2+x+1)^{p^s-i}, u\rangle$. Since $I \subseteq \langle u\rangle$ and $I \subseteq \langle (x^2+x+1)^i\rangle$, we have $\langle (x^2+x+1)^{p^s-i}\rangle = \mathcal{A}(\langle (x^2+x+1)^i\rangle) \subseteq \mathcal{A}(I)$ and $\langle u\rangle = \langle u\rangle^\perp \subseteq \mathcal{A}(I)$. This implies that $\langle (x^2+x+1)^{p^s-i}, u\rangle \subseteq \mathcal{A}(I)$. The other inclusion follows from the fact that the coefficient vector of $(x^2+x+1)^{p^s-i}$ is orthogonal to the coefficient vector of $u(x^2 + x+1)^i$ and all its constacyclic shift. Thus, $\mathcal{A}(I) = \langle (x^2+x+1)^{p^s-i}, u\rangle$. By Lemma 2, we have $\mathcal{A}(I)^* = \langle (x^2+x+1)^{p^s-i}, u\rangle$. Let $I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x)\rangle$, where $h(x)$ is 0 or a unit. Then $\mathcal{A}(I)^*$ is determined as follows:

1. If $h(x)$ is 0, then $\mathcal{A}(I)^* = \langle (x^2+x+1)^{p^s-i}\rangle$.

2. If $1 \leq i \leq \frac{p^s+t}{2}$ and $h(x)$ is a unit, then

$$\begin{aligned}\mathcal{A}(I)^* =& \langle (x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s-2i+t}(x^2-1)\sum_{j=0}^{i-t-1} b_j(x^2+x+1)^j \\ & - u(x^2+x+1)^{p^s-2i+t}\sum_{j=0}^{i-t-1}(a_jx+b_j)(x^2+x+1)^j\rangle,\end{aligned}$$

   where $h(x) = \sum_j (a_jx + b_j)(x^2+x+1)^j$, $a_j, b_j \in \mathbb{F}_{p^m}$ and $a_0, b_0 \neq 0$.

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

$$\begin{aligned}b(x) =& (x^2+x+1)^{i-t} \\ & - ux^{4i-2p^s-2t-1}\sum_{j=0}^{p^s-i-1}(b_jx+a_j)(x^2+x+1)^j\end{aligned}$$

The proof of (i) is obvious. We will prove the case (ii).
Since

$$[(x^2+x+1)^i+u(x^2+x+1)^t h(x)][(x^2+x+1)^{p^s-i}-u(x^2+x+1)^{p^s-2i+t}h(x)]=0,$$

we have

$$\langle (x^2+x+1)^{p^s-i}-u(x^2+x+1)^{p^s-2i+t}h(x)\rangle \subseteq \mathcal{A}(I).$$

Let $\mathcal{A}(I)=\langle f(x), u(x^2+x+1)^k\rangle$ where $f(x)=(x^2+x+1)^a+u(x^2+x+1)^b g(x)$, $0\leq a,b,k\leq p^s-1$ and $g(x)\in \frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. By Lemma 3.1.2, p^s-i is the smallest integer such that $u(x^2+x+1)^{p^s-i}\in\mathcal{A}(I)$. Therefore, $k=p^s-i$. Since

$$\begin{aligned}0&=f(x)[(x^2+x+1)^i+u(x^2+x+1)^t h(x)]\\&=[(x^2+x+1)^a+u(x^2+x+1)^b g(x)][(x^2+x+1)^i+u(x^2+x+1)^t h(x)]\\&=(x^2+x+1)^{a+i}+u(x^2+x+1)^{a+t}h(x)+u(x^2+x+1)^{b+i}g(x),\end{aligned}$$

we have $a+i\geq p^s$. So we can take $a=p^s-i$. Then we have $b=p^s-2i+t$ and $g(x)=-h(x)$. This implies that

$$\mathcal{A}(I)=\langle (x^2+x+1)^{p^s-i}-u(x^2+x+1)^{p^s+t-2i}h(x), u(x^2+x+1)^{p^s-i}\rangle.$$

Since $u(x^2+x+1)^{p^s-i}\in\langle (x^2+x+1)^{p^s-i}-u(x^2+x+1)^{p^s+t-2i}h(x)\rangle$, we can see that $\mathcal{A}(I)=\langle (x^2+x+1)^{p^s-i}-u(x^2+x+1)^{p^s+t-2i}h(x)\rangle$. Let $h(x)=\sum_j(a_jx+b_j)(x^2+x+1)^j$ where $a_0x+b_0\neq 0$ and $a_j,b_j\in\mathbb{F}_{p^m}$. Since $1\leq i\leq \frac{p^s+t}{2}$ and property of T, we have $t+j<T=\min\{i,p^s-i+t\}=i$. So, $j\leq i-t-1$.
Let $l(x)=(x^2+x+1)^{p^s-i}-u(x^2+x+1)^{p^s-2i+t}\sum_{j=0}^{i-t-1}(a_jx+b_j)(x^2+x+1)^j$. By Lemma 2, we get that

$$\begin{aligned}l^*(x)=&(x^2+x+1)^{p^s-i}-u(x^2+x+1)^{p^s-2i+t}x\sum_{j=0}^{i-t-1}(b_jx+a_j)(x^2+x+1)^j\\=&(x^2+x+1)^{p^s-i}-u(x^2+x+1)^{p^s-2i+t}\sum_{j=0}^{i-t-1}(b_jx^2+a_jx)(x^2+x+1)^j\\=&(x^2+x+1)^{p^s-i}-u(x^2+x+1)^{p^s-2i+t}\sum_{j=0}^{i-t-1}(b_j(x^2-1)+a_jx+b_j)(x^2+x+1)^j\\=&(x^2+x+1)^{p^s-i}-u(x^2+x+1)^{p^s-2i+t}(x^2-1)\sum_{j=0}^{i-t-1}b_j(x^2+x+1)^j\\&-u(x^2+x+1)^{p^s-2i+t}\sum_{j=0}^{i-t-1}(a_jx+b_j)(x^2+x+1)^j.\end{aligned}$$

Hence

$$\mathcal{A}(I)^* = \langle (x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s-2i+t}(x^2-1)\sum_{j=0}^{i-t-1} b_j(x^2+x+1)^j$$
$$- u(x^2+x+1)^{p^s-2i+t}\sum_{j=0}^{i-t-1}(a_jx+b_j)(x^2+x+1)^j\rangle$$

The proof of (ii) is complete. Finally, we will show proof of (iii). It is similar to (ii), we have $\mathcal{A}(I) = \langle f(x), u(x^2+x+1)^{p^s-i}\rangle$ where $f(x) = (x^2+x+1)^a + u(x^2+x+1)^b g(x)$, $0 \le a, b \le p^s-1$ and $g(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. Since $\frac{p^s+t}{2} < i \le p^s-1$, we obtain that $p^s - i < i - t$. Now, we consider that

$$\begin{aligned} 0 &= f(x)[(x^2+x+1)^i + u(x^2+x+1)^t h(x)] \\ &= [(x^2+x+1)^a + u(x^2+x+1)^b g(x)][(x^2+x+1)^i + u(x^2+x+1)^t h(x)] \\ &= (x^2+x+1)^{a+i} + u(x^2+x+1)^{a+t}h(x) + u(x^2+x+1)^{b+i}g(x), \end{aligned}$$

and then $a \ge p^s - i$. So, we choose $a = i - t$. We need b and $g(x)$ such that

$$u(x^2+x+1)^i h(x) + u(x^2+x+1)^{b+i}g(x) = 0.$$

Thus, we choose $b = 0$ and $g(x) = -h(x)$. This implies that

$$\mathcal{A}(I) = \langle (x^2+x+1)^{i-t} - uh(x), u(x^2+x+1)^{p^s-i}\rangle$$

Let $h(x) = \sum_j (a_jx+b_j)(x^2+x+1)^j$, where $a_0, b_0 \ne 0$ and $a_j, b_j \in \mathbb{F}_{p^m}$. Since $\frac{p^s+t}{2} < i \le p^s-1$ and $t + j < T = \min\{i, p^s - i + t\} = p^s - i + t$, we have $j \le p^s - i - 1$. Let

$$l_2(x) = (x^2+x+1)^{i-t} - u\sum_{j=0}^{p^s-i-1}(a_jx+b_j)(x^2+x+1)^j.$$

Then

$$l_2^*(x) = (x^2+x+1)^{i-t} - ux^{4i-2t-2p^s+1}\sum_{j=0}^{p^s-i-1}(b_jx+a_j)(x^2+x+1)^j.$$

Therefore,

$$\mathcal{A}(I)^* = \langle (x^2+x+1)^{i-t} - ux^{4i-2t-2p^s+1}\sum_{j=0}^{p^s-i-1}(b_jx+a_j)(x^2+x+1)^j, u(x^2+x+1)^{p^s-i}\rangle.$$

Let $I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x), u(x^2+x+1)^\omega\rangle$, where $h(x)$ is 0 or a unit. Then $\mathcal{A}(I)^*$ is determined as follows:

1. If $h(x) = 0$, then $\mathcal{A}(I)^* = \langle (x^2+x+1)^{p^s-\omega}, u(x^2+x+1)^{p^s-i} \rangle$.

2. If $h(x)$ is a unit, then $\mathcal{A}(I)^* = \langle d(x), u(x^2+x+1)^{p^s-i} \rangle$, where

$$d(x) = (x^2+x+1)^{p^s-\omega} - ux^{2i-2\omega+1}(x^2+x+1)^{p^s-i-\omega+t} \sum_{j=0}^{\omega-t-1} (b_j x + a_j)(x^2+x+1)^j.$$

The proof of (i) is obvious. We will prove the case (ii). A simple calculation shows that

$$I = \langle (x^2+x+1)^{p^s-\omega} - u(x^2+x+1)^{p^s-i-\omega+t} h(x), u(x^2+x+1)^{p^s-i} \rangle \subseteq \mathcal{A}(I)$$

and $n_I = p^{2m(i+\omega)}$. Then

$$p^{2m(i+\omega)} = n_I \leq |\mathcal{A}(I)| \leq |\mathcal{A}(I)^*| = \frac{p^{4mp^s}}{n_I} = \frac{p^{4mp^s}}{p^{2m(2p^s-i-\omega)}} = p^{2m(i+\omega)}.$$

Therefore, $\langle (x^2+x+1)^{p^s-\omega} - u(x^2+x+1)^{p^s-i-\omega+t} h(x), u(x^2+x+1)^{p^s-i} \rangle = \mathcal{A}(I)$. Let $h(x) = \sum_j (a_j x + b_j)(x^2+x+1)^j$, where $a_0 x + b_0 \neq 0$ and $a_j, b_j \in \mathbb{F}_{p^m}$. In this case, we have $j \leq \omega - t - 1$. Let $d(x) = (x^2+x+1)^{p^s-\omega} - u(x^2+x+1)^{p^s-i-\omega+t} \sum_{j=0}^{\omega-t-1} (a_j x + b_j)(x^2+x+1)^j$. By Lemma 2, we get that

$$d(x)^* = (x^2+x+1)^{p^s-\omega} - u(x^2+x+1)^{p^s-i-\omega+t} x^{2i-2\omega+1} \sum_{j=0}^{\omega-t-1} (b_j x + a_j)(x^2+x+1)^j.$$

Hence,

$$\mathcal{A}(I)^* = \langle (x^2+x+1)^{p^s-\omega} - u(x^2+x+1)^{p^s-i-\omega+t} x^{2i-2\omega+1} \sum_{j=0}^{\omega-t-1} (b_j x + a_j)(x^2+x+1)^j, u(x^2+x+1)^{p^s-i} \rangle.$$

The proof is complete.

3.2 The number of cyclic codes and their self-dual codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

In this section, we separate structures of self-dual cyclic codes of length $3p^s$ over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ into 2 cases, i.e., $p^m \equiv 1 \pmod 3$ and $p^m \equiv 2 \pmod 3$.

3.2.1 The case $p^m \equiv 1 \pmod 3$

In paper [17, 7], the number of constacyclic codes and their self-dual codes of length p^s over R are obtained.

[17, 7] The number of distinct constacyclic codes of length p^s over R is equal to

- $\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}}-2p^{2m}-2}{(p^m-1)^2}+\frac{(2p^m+3)(p^m)^{\frac{p^s-1}{2}}-2p^s-1}{p^m-1}+(p^m)^{\frac{p^s-1}{2}}+2$ if p is an odd prime.
- $\frac{2^{m(2^{s-1}-1)}(2^{2m}+2^m+2)-2^{2m+1}-2}{(2^m-1)^2}+\frac{6\cdot 2^{m(2^s-1)}-2^{s+1}-1}{2^m-1}+2^{m2^{s-1}}+4\cdot 2^{m(2^{s-1}-1)}+3\cdot 2^{s-1}-1$ if $p=2$.

Applying Thoerem 3.1.1, the number of distinct cyclic codes of length $3p^s$ over R is obtained as the following theorem.

Let $p^m \equiv 1 \pmod 3$. Then the number of distinct cyclic codes of length $3p^s$ over R is equal to

- $(\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}}-2p^{2m}-2}{(p^m-1)^2}+\frac{(2p^m+3)(p^m)^{\frac{p^s-1}{2}}-2p^s-1}{p^m-1}+(p^m)^{\frac{p^s-1}{2}}+2)^3$ if p is an odd prime.
- $(\frac{2^{m(2^{s-1}-1)}(2^{2m}+2^m+2)-2^{2m+1}-2}{(2^m-1)^2}+\frac{6\cdot 2^{m(2^s-1)}-2^{s+1}-1}{2^m-1}+2^{m2^{s-1}}+4\cdot 2^{m(2^{s-1}-1)}+3\cdot 2^{s-1}-1)^3$ if $p=2$.

By Theorem 3.1.1, we obtain that the number of distinct cyclic codes of length $3p^s$ over R is the number to the third power of distinct constacyclic codes of length p^s. By Theorem 3.2.1, the number of distinct cyclic codes of length $3p^s$ is obtained.

Next, we determine the number of distinct self-dual cyclic codes of length $3p^s$ over R. We recall the result about dual cyclic codes of length $3p^s$.

For any $\alpha \in \mathbb{F}_{p^m}$ with $\alpha \neq \alpha^{-1}$, we obtain that self-dual code of each α-constacyclic code of length p^s over R is unique, i.e., $\langle u \rangle$ (see [17]). Moreover, the number of distinct self-dual cyclic codes of length p^s over R are obtained in [17].

As the fact $\delta_i^{-1} \neq \delta_i$ for $i = 1, 2$, we get the self-dual code of δ_1, δ_2-constacyclic codes of length p^s are $\langle u \rangle$ and then, the number of self-dual cyclic codes of length $3p^s$ over R is obtained as the following theorem. Let $p^m \equiv 1 \pmod 3$. Then the number of self-dual cyclic codes of length $3p^s$ over R is equal to the number of self-dual of cyclic codes of length p^s over R.

By Theorem 3.1.1, we obtain that each self-dual cyclic code of length $3p^s$ is a direct sum of a cyclic code, δ_1, δ_2-constacyclic codes of length p^s over R. Since $\delta_1 \neq \delta_1^{-1}$ and $\delta_2 \neq \delta_2^{-1}$, we have self-dual δ_1, δ_2-constacyclic codes are $\langle u \rangle$. Hence, the number of self-dual cyclic codes of length $3p^s$ is the number of self-dual cyclic codes of length p^s over R.

3.2.2 The case $p^m \equiv 2 \pmod 3$

The number of distinct cyclic codes of length $3p^s$ over R is a product of the number of distinct cyclic codes of length p^s over R and the number of distinct ideals of

$\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. In [17, 7], the number of distinct cyclic codes of length p^s over R are obtained.

The remaining part, we determine the number of distinct ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. By Theorem 3.1.2, we classify all ideals of such ring into 4 types.

Case 1: p is an odd prime.

First of all, we obtain 2 ideals of trivial type. In type 2, the number of distinct ideals $\langle u(x^2+x+1)^i\rangle$ where $0 \leq i \leq p^s-1$ is p^s. In type 3, we separate this type into 2 cases, i.e., $h(x)=0$ and $h(x)$ is a unit. If $h(x)=0$, the number of ideals $\langle (x^2+x+1)^i\rangle$ where $1 \leq i \leq p^s-1$ is p^s. If $h(x)$ is a unit, we have $h(x)=\sum_j (h_{1j}x+h_{0j})(x^2+x+1)^j$ where $h_{0j}, h_{1j} \in \mathbb{F}_{p^m}$ and $h_{10}x+h_{00} \neq 0$. Clearly, $t+j < T = \min\{i, p^s-i+t\}$ and then, $j \leq T-t-1$. Thus, the number of distinct ideals of this type is

$$\begin{aligned}
&\sum_{i=1}^{\frac{p^s-1}{2}} \sum_{t=0}^{i-1} (p^{2m}-1)(p^{2m})^{i-t-1} + \sum_{i=\frac{p^s+1}{2}}^{p^s-1} \sum_{t=0}^{2i-p^s-1} (p^{2m}-1)(p^{2m})^{p^s-i-1} \\
&+ \sum_{i=\frac{p^s+1}{2}}^{p^s-1} \sum_{t=2i-p^s}^{i-1} (p^{2m}-1)(p^{2m})^{i-t-1} \\
&= \sum_{i=1}^{\frac{p^s-1}{2}} (p^{2mi}-1) + (p^{2m}-1) \sum_{i=\frac{p^s+1}{2}}^{p^s-1} (2i-p^s)(p^{2m})^{p^s-i-1} \\
&+ \sum_{i=\frac{p^s+1}{2}}^{p^s-1} (p^{2m(p^s-i)}-1) \\
&= \frac{2p^{2m}(p^{2m(\frac{p^s-1}{2})}-1) + 2p^{2m}(p^{2m(\frac{p^s-1}{2}-1)}-1)}{p^{2m}-1} + p^{2m(\frac{p^s-1}{2})} - 2p^s + 3 \\
&= \frac{2(p^{2m}+1)(p^{2m})^{\frac{p^s-1}{2}}-4}{p^{2m}-1} + (p^{2m})^{\frac{p^s-1}{2}} - 2p^s - 1.
\end{aligned}$$

In type 4, we separate this type into 2 cases, i.e., $h(x)=0$ and $h(x)$ is a unit. If $h(x)=0$, the number of distinct ideals $\langle (x^2+x+1)^i, u(x^2+x+1)^\omega\rangle$ where $1 \leq i \leq p^s-1$ and $0 \leq \omega < T = i$, is

$$\sum_{i=1}^{p^s-1} i = \frac{(p^s-1)(p^s)}{2}.$$

If $h(x)=0$, we determine the number of distinct ideals of form $\langle (x^2+x+1)^i + u(x^2+x+1)^t h(x), u(x^2+x+1)^\omega\rangle$ where $1 \leq i \leq p^s-1, 0 \leq t < i, 0 \leq \omega < T$ and $h(x)$ is a unit. Since $t+j < \omega$ and $0 \leq j \leq \omega-t-1$, we have the number of distinct ideals of this form is

$$\sum_{i=2}^{\frac{p^s-1}{2}}\sum_{t=0}^{i-1}\sum_{\omega=t+1}^{i-1}(p^{2m}-1)(p^{2m})^{\omega-t-1}+\sum_{i=\frac{p^s+1}{2}}^{p^s-2}\sum_{t=0}^{2i-p^s-1}\sum_{\omega=t+1}^{p^s-i+t-1}(p^{2m}-1)(p^{2m})^{\omega-t-1}$$
$$+\sum_{i=\frac{p^s+1}{2}}^{p^s-1}\sum_{t=2i-p^s}^{i-2}\sum_{\omega=t+1}^{i-1}(p^{2m}-1)(p^{2m})^{\omega-t-1}$$
$$=\frac{2(p^{2m}+1)(p^{2m})^{\frac{p^s-1}{2}}-2p^{4m}-2}{(p^{2m}-1)^2}+\frac{(p^{2m})^{\frac{p^s-1}{2}}-2p^s+3}{p^{2m}-1}+\frac{p^s-p^{2s}}{2}+2.$$

Hence, we obtain that the number of distinct ideals when p is an odd prime is equal to

$$\frac{2(p^{2m}+1)(p^{2m})^{\frac{p^s-1}{2}}-2p^{4m}-2}{(p^{2m}-1)^2}+\frac{(2p^{2m}+3)(p^{2m})^{\frac{p^s-1}{2}}-2p^s-1}{p^{2m}-1}+(p^{2m})^{\frac{p^s-1}{2}}+2. \tag{3.3}$$

Case 2: $p=2$.

Clearly, we obtain 2 ideals in trivial type and the number of distinct ideals $\langle u(x^2+x+1)^i\rangle$ where $0\leq i\leq 2^s-1$ is 2^s in type 2. Now, in type 3, we separate this type into 2 cases, i.e., $h(x)=0$ and $h(x)$ is a unit. If $h(x)$ is a unit, the number of distinct ideals $\langle(x^2+x+1)^i\rangle$ where $1\leq i\leq 2^s-1$ is 2^s-1. If $h(x)$ is a unit, then $h(x)=\sum_j(h_{1j}x+h_{0j})(x^2+x+1)^j$ where $h_{1j},h_{2j}\in\mathbb{F}_{p^m}$ and $h_{1j}x+h_{0j}\neq 0$. Note that $t+j<T=\min\{i,2^s-i+t\}$. This means that $j\leq T-t-1$. Thus, the number of distinct ideals of this type is

$$\sum_{i=1}^{2^{s-1}}\sum_{t=0}^{i-1}(2^{2m}-1)(2^{2m})^{i-t-1}+\sum_{i=2^{s-1}+1}^{2^s-1}\sum_{t=0}^{2i-2^s-1}(2^{2m}-1)(2^{2m})^{2^s-i-1}$$
$$+\sum_{i=2^{s-1}+1}^{2^s-1}\sum_{t=2i-2^s}^{2^s-1}(2^{2m}-1)(2^{2m})^{i-t-1}$$
$$=2^{2m(2^{s-1})}+2^{2m(2^{s-1}-1)+2}-2^{s+1}-1.$$

Finally, we separate type 4 into 2 cases, i.e., $h(x)=0$ and $h(x)$ is a unit. If $h(x)=0$, then $T=i$. Thus, the number of distinct ideals $\langle(x^2+x+1)^i,u(x^2+x+1)^\omega\rangle$ where $1\leq i\leq 2^s-1$ and $\omega<T=i$ is

$$\sum_{i=1}^{2^s-1}i=\frac{(2^s-1)2^s}{2}=(2^s-1)2^{s-1}.$$

If $h(x)$ is a unit, then $h(x)=\sum_j(h_{1j}x+h_{0j})(x^2+x+1)^j$ where $h_{1j},h_{0j}\in\mathbb{F}_{p^m}$ and $h_{10}x+h_{00}\neq 0$. Note that $t+j<\omega$, or equivalently, $j\leq\omega-t-1$. Thus, the number of distinct ideals is

$$\sum_{i=2}^{2^{s-1}}\sum_{t=0}^{i-2}\sum_{\omega=t+1}^{i-1}(2^{2m}-1)(2^{2m})^{\omega-t-1}+\sum_{i=2^{s-1}+1}^{2^s-2}\sum_{t=0}^{2i-2^s-1}\sum_{\omega=t+1}^{2^s-i+t-1}(2^{2m}-1)(2^{2m})^{\omega-t-1}$$
$$+\sum_{i=2^{s-1}+1}^{2^s-2}\sum_{t=2i-2^s}^{i-2}\sum_{\omega=t+1}^{i-1}(2^{2m}-1)(2^{2m})^{\omega-t-1}$$
$$=\frac{2^{2m(2^{s-1}-1)}(2^{4m}+2^{2m}+2)-2^{4m+1}-2}{(2^{2m}-1)^2}+\frac{2^{m(2^{s-1}-1)+1}-2^{s+1}+3}{2^{2m}-1}+2^{2s-1}+2^{s+1}-1.$$

Hence, we obtain that the number of distinct ideals when $p=2$ is

$$\frac{2^{2m(2^{s-1}-1)}(2^{4m}+2^{2m}+2)-2^{4m+1}-2}{(2^{2m}-1)^2}+\frac{6\cdot 2^{2m(2^s-1)}-2^{s+1}-1}{2^{2m}-1}+2^{m2^{s-1}} \quad (3.4)$$
$$+4\cdot 2^{2m(2^{s-1}-1)}+3\cdot 2^{s-1}-1.$$

Therefore, we obtain all distinct cyclic codes of length $3p^s$ over R as follows:

Let $p^m\equiv 2 \pmod 3$. Then the number of distinct cyclic codes of length $3p^s$ over R is

- $\left(\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}}-2p^{2m}-2}{(p^m-1)^2}+\frac{(2p^m+3)(p^m)^{\frac{p^s-1}{2}}-2p^s-1}{p^m-1}+(p^m)^{\frac{p^s-1}{2}}+2\right)$
$\times\left(\frac{2(p^{2m}+1)(p^{2m})^{\frac{p^s-1}{2}}-2p^{4m}-2}{(p^{2m}-1)^2}+\frac{(2p^{2m}+3)(p^{2m})^{\frac{p^s-1}{2}}-2p^s-1}{p^{2m}-1}+(p^{2m})^{\frac{p^s-1}{2}}+2\right)$ if p is an odd prime.
- $\left(\frac{2^{m(2^{s-1}-1)}(2^{2m}+2^m+2)-2^{2m+1}-2}{(2^m-1)^2}+\frac{6\cdot 2^{m(2^s-1)}-2^{s+1}-1}{2^m-1}+2^{m2^{s-1}}+4\cdot 2^{m(2^{s-1}-1)}+3\cdot 2^{s-1}-1\right)$
$\times\left(\frac{2^{2m(2^{s-1}-1)}(2^{4m}+2^{2m}+2)-2^{4m+1}-2}{(2^{2m}-1)^2}+\frac{6\cdot 2^{2m(2^s-1)}-2^{s+1}-1}{2^{2m}-1}+2^{m2^{s-1}}+4\cdot 2^{2m(2^{s-1}-1)}+3\cdot 2^{s-1}-1\right)$ if $p=2$.

In case p is an odd prime, suppose that -3 is a square element in R, there exists $\alpha\in R$ such that $\alpha^2=-3$. We consider that

$$\begin{aligned}((-1+\alpha)2^{-1})^2+(-1+\alpha)2^{-1}+1 &=(-1-2\alpha-3)2^{-2}+(-1+\alpha)2^{-1}+1\\ &=(-1-\alpha)2^{-1}+(-1+\alpha)2^{-1}+1\\ &=0.\end{aligned}$$

It is a contradiction by Lemma 3.1.2. Thus, -3 is not a square which means that x^2+3 is irreducible over R. Let $p^m\equiv 2 \pmod 3$ and $\Phi:\frac{R[x]}{\langle(x^2+x+1)^{p^s}\rangle}\to\frac{R[x]}{\langle x^{2p^s}+(3\cdot 2^{-2})^{p^s}\rangle}$ by $\Phi(f(x))=f(x-2^{-1})$ where $p\neq 2$ and $f(x)\in\frac{R[x]}{\langle(x^2+x+1)^{p^s}\rangle}$. Then Φ is an isomorphism.

First of all, we will show that ϕ is well-defined and one-to-one. For polynomials $f(x)$ and $g(x) \in R[x]$, $f(x) \equiv g(x) \pmod{(x^2+x+1)^{p^s}}$ if and only if there exists a polynomial $h(x) \in R[x]$ such that $f(x) - g(x) = h(x)(x^2+x+1)^{p^s}$, if and only if

$$\begin{aligned} f(x-2^{-1}) - g(x-2^{-1}) &= h(x-2^{-1})((x-2^{-1})^2 + x - 2^{-1} + 1)^{p^s} \\ &= h(x-2^{-1})(x^2 - x + 2^{-2} + x - 2^{-1} + 1)^{p^s} \\ &= h(x-2^{-1})(x^2 + 3\cdot 2^{-2})^{p^s} \\ &= h(x-2^{-1})(x^{2p^s} + (3\cdot 2^{-2})^{p^s}), \end{aligned}$$

which is equivalent to $f(x-2^{-1}) \equiv g(x-2^{-1}) \pmod{(x^2+x+1)^{p^s}}$. Since $\Phi(f(x)) - \Phi(g(x)) = f(x) - g(x)$, we have, for $f(x), g(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$, $\Phi(f(x)) = \Phi(g(x))$ if and only if $f(x-2^{-1}) = g(x-2^{-1})$. Therefore, Φ is well defined and one-to-one. Next, it is a routine to show that Φ is onto and homomorphism. Hence, Φ is a ring isomorphism.

Let $p^m \equiv 2 \pmod 3$ and C be a cyclic code of length $3p^s$ over R where $p \neq 2$. Then

1. $C = C_1 \oplus C_3$ where C_1 is a cyclic code of length p^s over R and C_3 is a $-(3\cdot 2^{-2})^{p^s}$-constacyclic code of length $2p^s$ over R. Moreover, $|C| = |C_1||C_3|$.

2. the dual code $C^\perp$ of C can be expressed as $C^\perp = C_1^\perp \oplus C_3^\perp$ where C_1 is a cyclic code of length p^s over R and C_3 is a $-(3\cdot 2^{-2})^{p^s}$-constacyclic code of length $2p^s$ over R. Moreover, $|C^\perp| = |C_1^\perp||C_3^\perp|$.

The structures of $-(3\cdot 2^{-2})^{p^s}$-constacyclic codes of length $2p^s$ over R are obtained see in [4]. Moreover, the number of this constacyclic codes of $2p^s$ over R as the following theorem.

[4] The number of distinct $-(3\cdot 2^{-2})^{p^s}$-constacyclic codes of length $2p^s$ over R is equal to

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

From Equation (3.3), we notice that the number of distinct ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ in Theorem 3.2.2 is equal to the number of $-(3\cdot 2^{-2})^{p^s}$-constacyclic codes of length $2p^s$ over R.

In $p^m \equiv 2 \pmod 3$, we determine the condition $-(3 \cdot 2^{-2})^{p^s} = [-(3 \cdot 2^{-2})^{p^s}]^{-1}$ if and only if

$$\begin{aligned}(3 \cdot 2^{-2})^{2p^s} &= 1 \\ 3^{2p^s} &= 4^{2p^s} \\ (3-4)^{p^s}(3+4)^{p^s} &= 0 \\ 7^{p^s} &= 0.\end{aligned}$$

This means that the characteristic of R is equal to $p = 7$ if and only if $-(3 \cdot 2^{-2})^{p^s} = [-(3 \cdot 2^{-2})^{p^s}]^{-1}$. However, $7^m \equiv 1 \pmod 3$ for any positive integer m. Thus, this condition does not exist implying that $-(3 \cdot 2^{-2})^{p^s} \neq [-(3 \cdot 2^{-2})^{p^s}]^{-1}$, for any $p^m \equiv 2 \pmod 3$ with $p \neq 2$. Therefore, we divide them into 2 cases, i.e., the case $p^m \equiv 2 \pmod 3$ with $p \neq 2$ and the case $p^m \equiv 2 \pmod 3$ with $p = 2$ for self-dual codes.

The subcase $p^m \equiv 2 \pmod 3$ with $p \neq 2$

First of all, we give the condition of existence of self-dual constacyclic codes of length n over a finite commutative chain ring. [16] Let λ be a unit of the chain ring R with maximal ideal $\langle r \rangle$, such that $\lambda - \lambda^{-1}$ is a unit. Then there exists a self-dual λ-constacyclic code C of length n over R if and only if N_r is even. In such case, the number of C is $\frac{N_r}{2}$, and $C = \langle \gamma^{\frac{N_r}{2}} \rangle$ is the unique self-dual constacyclic code of length n over R.

In this subcase, as $-(3 \cdot 2^{-2})^{p^s} \neq [-(3 \cdot 2^{-2})^{p^s}]^{-1}$, we obtain that $\langle u \rangle$ is the unique self-dual code of $-(3 \cdot 2^{-2})^{p^s}$-constacyclic codes of length $2p^s$ over R. By Corollary 3.2.2, the number of self-dual cyclic codes of length p^s over R as follows:

Let $p^m \equiv 2 \pmod 3$ with $p \neq 2$. Then the number of self-dual cyclic codes of length $3p^s$ over R is the number of self-dual of cyclic codes of length p^s over R.

The subcase $p^m \equiv 2 \pmod 3$ with $p = 2$

We determine the number of self-dual cyclic codes of length $3 \cdot 2^s$ over R. From Theorem 3.1.2, we obtain the following theorem. The number of self-dual cyclic codes of length $3 \cdot 2^s$ over R is the product of the number of self-dual of cyclic codes of length 2^s over R and the number of distinct ideals I of $\frac{R[x]}{\langle (x^2+x+1)^{2^s} \rangle}$ which $I = \mathcal{A}(I)^*$.

Finally, we focus on ideals of $\frac{R[x]}{\langle (x^2+x+1)^{2^s} \rangle}$ for the situation each ideal I of $\frac{R[x]}{\langle (x^2+x+1)^{2^s} \rangle}$, $I = \mathcal{A}(I)^*$. We consider each ideals of such ring into 4 types from Theorem 3.1.2. Clearly, all ideals in trivial type, $\langle 0 \rangle$ and $\langle 1 \rangle$ are not satisfied the situation.

Let $I = \langle u(x^2+x+1)^i \rangle$ where $0 \leq i \leq 2^s - 1$ be an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{2^s} \rangle}$. Then $I = \mathcal{A}(I)^*$ if and only if $i = 0$, that is, $I = \langle u \rangle$. Suppose that $I = \mathcal{A}(I)^*$. If $i \neq 0$, Theorem 3.1.2, we get $\mathcal{A}(I)^* = \langle u, (x^2+x+1)^{2^s-i} \rangle$. This implies that $u \in \langle u(x^2+x+1)^i \rangle$. There exists $f(x) = \sum_{j=0}^{2^s-1}(a_{0j}x + b_{0j})(x^2+x+1)^j + u\sum_{j=0}^{2^s-1}(a_{1j}x + b_{1j})(x^2+x+1)^j \in \frac{R[x]}{\langle (x^2+x+1)^{2^s} \rangle}$ such that

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

Thus, $(x^2+x+1)^i \sum_{j=0}^{2^s-1}(a_{0j}x + b_{0j})(x^2+x+1)^j = 1$. This means that x^2+x+1 is invertible. It is a contradiction. Therefore, $i = 0$ which implies that $I = \langle u \rangle$. Conversely, suppose that $i = 0$. Clearly,

$$I = \langle u(x^2+x+1)^i \rangle = \langle u \rangle$$

and

$$\mathcal{A}(I)^* = \langle u, (x^2+x+1)^{2^s} \rangle = \langle u \rangle.$$

Therefore, we obtain that $I = \mathcal{A}(I)^*$.

From the above proposition, we obtain that the situation for ideals in type 2. Next, the condition $I = \mathcal{A}(I)^*$ of all ideals in type 3 are determined in the following proposition.

Next, we consider that condition $I = \mathcal{A}(I)^*$ for $I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x) \rangle$ where $1 \leq i \leq 2^s - 1$ and $h(x)$ is 0 or a unit. For $h(x) = 0$, we have $I = \langle (x^2+x+1)^i \rangle$ and $\mathcal{A}(I)^* = \langle (x^2+x+1)^{2^s-i} \rangle$.

Let $I = \langle (x^2+x+1)^i \rangle$ where $1 \leq i \leq 2^s-1$. Then $I = \mathcal{A}(I)^*$ if and only if $i = 2^{s-1}$. Suppose that $I = \mathcal{A}(I)^*$. Note that $I = \langle (x^2+x+1)^i \rangle = \mathcal{A}(I)^* = \langle (x^2+x+1)^{2^s-i} \rangle$. So,

$$(x^2+x+1)^i \in \langle (x^2+x+1)^{2^s-i} \rangle$$

and

$$(x^2+x+1)^{2^s-i} \in \langle (x^2+x+1)^i \rangle.$$

There exists $f(x), g(x) \in R[x]$ such that

$$(x^2+x+1)^{2^s-i} = (x^2+x+1)^i f(x)$$

and

$$(x^2+x+1)^i = (x^2+x+1)^{2^s-i} g(x).$$

This means that

$$\begin{aligned}(x^2+x+1)^{2^{s+1}-2i} &= (x^2+x+1)^{2^s-i}(x^2+x+1)^i f(x)\\ &= (x^2+x+1)^{2^s} f(x)\\ &= 0.\end{aligned}$$

$$\begin{aligned}(x^2+x+1)^{2i} &= (x^2+x+1)^i(x^2+x+1)^{2^s-i} g(x)\\ &= (x^2+x+1)^{2^s}\\ &= 0.\end{aligned}$$

So, $2^{s+1}-2i \geq 2^s$ and $2i \geq 2^s$. Thus, $2i = 2^s$. Hence, $i = 2^{s-1}$. On the other hand, suppose that $i = 2^{s-1}$. Clearly, $I = \langle (x^2+x+1)^{2^{s-1}} \rangle = \langle (x^2+x+1)^{2^s-2^{s-1}} \rangle = \mathcal{A}(I)^*$.

In type 3, we determine the condition of $I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x) \rangle$, $h(x)$ is a unit which satisfies $I = \mathcal{A}(I)^*$. Let $I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x) \rangle$ where $h(x) = \sum_j (a_j x + b_j)(x^2+x+1)^j$ is a unit and $1 \leq i \leq 2^s - 1$. Then $I = \mathcal{A}(I)^*$ if and only if $i = 2^{s-1}$ and $b_j = 0$. Suppose that $I = \mathcal{A}(I)^*$. By Theorem 3.1.2, $\frac{2^s+t}{2} < i < 2^s$, $I \neq \mathcal{A}(I)^*$ because $\mathcal{A}(I)^*$ is not principal. In $0 < i \leq \frac{2^s+t}{2}$, we have

$$\begin{aligned}\mathcal{A}(I)^* = \langle &(x^2+x+1)^{2^s-i} - u(x^2+x+1)^{2^s-2i+t}(x^2-1)\sum_{j=0}^{i-t-1} b_j(x^2+x+1)^j\\ &- u(x^2+x+1)^{2^s-2i+t}\sum_{j=0}^{i-t-1}(a_j x + b_j)(x^2+x+1)^j \rangle.\end{aligned}$$

There exist $f_1(x), f_2(x) \in \mathbb{F}_{2^m}[x]$ such that

$$\begin{aligned}&(x^2+x+1)^i + u(x^2+x+1)^t \sum_j (a_j x + b_j)(x^2+x+1)^j\\ &= \Big((x^2+x+1)^{2^s-i} - u(x^2+x+1)^{2^s-2i+t}(x^2-1)\sum_{j=0}^{i-t-1} b_j(x^2+x+1)^j\\ &- u(x^2+x+1)^{2^s-2i+t}\sum_{j=0}^{i-t-1}(a_j x + b_j)(x^2+x+1)^j\Big)\Big(f_1(x) + u f_2(x)\Big).\end{aligned}$$

Under modulo u, we have $(x^2+x+1)^i = (x^2+x+1)^{2^s-i} f_1(x)$ and then

$$\begin{aligned}(x^2+x+1)^{2i} &= (x^2+x+1)^{2^s} f_1(x)\\ &= 0.\end{aligned}$$

So, $2i \geq 2^s$. Moreover, there exist $g_1(x), g_2(x) \in \mathbb{F}_{2^m}[x]$ such that

$$\begin{aligned}
&(x^2+x+1)^{2^s-i} - u(x^2+x+1)^{2^s-2i+t}(x^2-1)\sum_{j=0}^{i-t-1} b_j(x^2+x+1)^j \\
&- u(x^2+x+1)^{2^s-2i+t}\sum_{j=0}^{i-t-1}(a_jx+b_j)(x^2+x+1)^j \\
&= \Big((x^2+x+1)^i + u(x^2+x+1)^t\sum_j (a_jx+b_j)(x^2+x+1)^j\Big)\Big(g_1(x)+ug_2(x)\Big).
\end{aligned}$$

Under Modulo u, we have

$$(x^2+x+1)^{2^s-i} = (x^2+x+1)^i g_1(x),$$

and then

$$\begin{aligned}
(x^2+x+1)^{2^{s+1}-2i} &= (x^2+x+1)^{2^s} g_1(x) \\
&= 0.
\end{aligned}$$

So, $2^{s+1}-2i \geq 2^s$, i.e., $2^s \geq 2i$. Thus, $2i = 2^s$ which means that $i = 2^{s-1}$. Note that

$$I = \langle (x^2+x+1)^{2^{s-1}} + u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1}(a_jx+b_j)(x^2+x+1)^j \rangle$$

and

$$\begin{aligned}
\mathcal{A}(I)^* =& \langle (x^2+x+1)^{2^{s-1}} - u(x^2+x+1)^t(x^2-1)\sum_{j=0}^{2^{s-1}-t-1} b_j(x^2+x+1)^j \\
&- u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1}(a_jx+b_j)(x^2+x+1)^j \rangle.
\end{aligned}$$

There exist $h_1(x), h_2(x) \in \mathbb{F}_{2^m}[x]$ such that

$$\begin{aligned}
&(x^2+x+1)^{2^{s-1}} + u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1}(a_jx+b_j)(x^2+x+1)^j \\
&= \Big((x^2+x+1)^{2^{s-1}} - u(x^2+x+1)^t(x^2-1)\sum_{j=0}^{2^{s-1}-t-1} b_j(x^2+x+1)^j \\
&- u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1}(a_jx+b_j)(x^2+x+1)^j\Big)\Big(h_1(x)+uh_2(x)\Big).
\end{aligned}$$

This implies that

$$(x^2+x+1)^{2^{s-1}} = (x^2+x+1)^{2^{s-1}} h_1(x)$$

and

$$u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1}(a_jx+b_j)(x^2+x+1)^j$$
$$= -u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1}\big((x^2-1)b_j+(a_jx+b_j)\big)(x^2+x+1)^j h_1(x)$$
$$+ u(x^2+x+1)^{2^{s-1}}h_2(x).$$

So, $h_1(x)=1$ and

$$u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1}(a_jx+b_j)(x^2+x+1)^j$$
$$= -u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1}\Big((x^2-1)b_j+(a_jx+b_j)\Big)(x^2+x+1)^j$$
$$+ u(x^2+x+1)^{2^{s-1}}h_2(x),$$

implying that

$$u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1}\big((x^2-1)b_j\big)(x^2+x+1)^j = u(x^2+x+1)^{2^{s-1}}h_2(x).$$

Multiplying $(x^2+x+1)^{2^{s-1}}$ both sides,

$$u(x^2+x+1)^{t+2^{s-1}} \sum_{j=0}^{2^{s-1}-t-1}\big((x^2-1)b_j\big)(x^2+x+1)^j = u(x^2+x+1)^{2^s}h_2(x) = 0.$$

This means that, for $0 \le j \le 2^{s-1}-t-1$, we get $b_j = 0$. Conversely, suppose that $i = 2^{s-1}$ and $b_j = 0$. It is easy to show that $I = \mathcal{A}(I)^*$.

Finally, we determine the situation $I = \mathcal{A}(I)^*$ where $I = \langle (x^2+x+1)^i, u(x^2+x+1)^\omega\rangle$ where $1 \le i \le 2^s-1, \omega \le i$. Let $I = \langle (x^2+x+1)^i, u(x^2+x+1)^\omega\rangle$ for $1 \le i \le 2^s-1$. Then $I = \mathcal{A}(I)^*$ if and only if $i+\omega = 2^s$. Suppose that $I = \mathcal{A}(I)^*$. By Theorem 3.1.2, we have

$$\mathcal{A}(I)^* = \langle (x^2+x+1)^{2^s-\omega}, u(x^2+x+1)^{2^s-i}\rangle.$$

So,

$$(x^2+x+1)^i \in \langle (x^2+x+1)^{2^s-\omega}, u(x^2+x+1)^{2^s-i}\rangle$$

and

$$(x^2+x+1)^{2^s-\omega} \in \langle (x^2+x+1)^i, u(x^2+x+1)^\omega\rangle.$$

There exist $f_1(x)+uf_2(x), g_1(x)+ug_2(x) \in R[x]$ such that

$$(x^2+x+1)^i = (x^2+x+1)^{2^s-\omega}(f_1(x)+uf_2(x)) + u(x^2+x+1)^{2^s-i}(g_1(x)+ug_2(x)).$$

Under modulo u, we have

$$(x^2+x+1)^i = (x^2+x+1)^{2^s-\omega}f_1(x),$$

which implies that $(x^2+x+1)^{i+\omega} = (x^2+x+1)^{2^s}f_1(x) = 0$. Thus, $i+\omega \geq 2^s$. Similarly, there exist $h_1(x)+uh_2(x), q_1(x)+uq_2(x) \in R[x]$ such that

$$(x^2+x+1)^{2^s-\omega} = (x^2+x+1)^i(h_1(x)+uh_2(x)) + u(x^2+x+1)^{\omega}(q_1(x)+uq_2(x)).$$

Under modulo u, we have $(x^2+x+1)^{2^s-\omega} = (x^2+x+1)^i h_1(x)$. We consider that

$$\begin{aligned}(x^2+x+1)^{2^{s+1}-\omega-i} &= (x^2+x+1)^{2^s}h_1(x)\\ &= 0.\end{aligned}$$

Thus, $2^{s+1}-i-\omega \geq 2^s$ which means that $2^s \geq i+\omega$. Therefore, $i+\omega = 2^s$. On the other hand, suppose that $i+\omega = 2^s$. Since

$$\mathcal{A}(I)^* = \langle (x^2+x+1)^{2^s-\omega}, u(x^2+x+1)^{2^s-i}\rangle,$$

we have

$$\begin{aligned}I &= \langle (x^2+x+1)^i, u(x^2+x+1)^{\omega}\rangle\\ &= \langle (x^2+x+1)^{2^s-\omega}, u(x^2+x+1)^{2^s-i}\rangle\\ &= \mathcal{A}(I)^*.\end{aligned}$$

3.3 Negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$

We now apply all results about cyclic codes of length $3p^s$ over $R = \mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ to negacyclic codes of same length over such ring by providing an isomorphism between cyclic and negacyclic codes of length $3p^s$ over R.

Let $\phi : \mathcal{R}_1 \to \mathcal{R}_{-1}$ by $\phi(f(x)) = f(-x)$ where $f(x) \in \mathcal{R}_1$. Then ϕ is an isomorphism. Moreover, I is an ideal of $\mathcal{R}_1$ if and only if $\phi(I)$ is an ideal of $\mathcal{R}_{-1}$.(C is a cyclic code of length $3p^s$ over R if and only if $\phi(C)$ is a negacyclic code of length $3p^s$ over R) First of all, we will show that ϕ is well-defined and one-to-one. For polynomials $f(x)$

and $g(x) \in R[x], f(x) \equiv g(x) \pmod{x^{3p^s}-1}$ if and only if there exists a polynomial $h(x) \in R[x]$ such that $f(x) - g(x) = h(x)(x^{3p^s}-1)$, if and only if

$$\begin{aligned} f(-x) - g(-x) &= h(-x)((-x)^{3p^s}-1) \\ &= -h(-x)(x^{3p^s}+1), \end{aligned}$$

which is equivalent to $f(-x) \equiv g(-x) \pmod{x^{3p^s}+1}$. Since $\phi(f(x)) - \phi(g(x)) = f(-x) - g(-x)$, we have, for $f(x), g(x) \in \frac{R[x]}{\langle x^{3p^s}-1\rangle}$, $\phi(f(x)) = \phi(g(x))$ if and only if $f(x) = g(x)$. Therefore, ϕ is well defined and one-to-one. Next, it is a rountine to show that ϕ is onto and homomorphism. Hence, ϕ is a ring isomorphism.

From Proposition 3.3 and Section 3.1, we obtain that the algebraic structures of cyclic code of length $3p^s$ over R, then we also the structures of negacyclic codes of length $3p^s$ over such ring. Moreover, our results about cyclic codes of length $3p^s$ over R in Section 3.2 can be carried over correspondingly to negacyclic codes of length $3p^s$ over R.

Chapter 4

Conclusion

Let p be a prime with $p \neq 3$. We obtain that the algebraic structures of the cyclic and negacyclic codes of length $3p^s$ over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ are isomorphic and the structures of such cyclic codes are in Table 4.1.

Table 4.1: The algebraic structures of each cyclic code C of length $3p^s$ over R

Cases	Algebraic structures
$p^m \equiv 1 \pmod 3$	$C = C_1 \oplus C_{\delta_1} \oplus C_{\delta_2}$ where C_1 is a cyclic code of length p^s over R and C_{δ_i} is a δ_i-constacyclic code of length p^s over R for all $i = 1, 2$ (see Theorem 3.1.1).
$2^m \equiv 2 \pmod 3$	$C = C_1 \oplus I$ where C_1 is a cyclic code of length p^s over R and I is an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$, respectively (see Theorem 3.1.2).
$p^m \equiv 2 \pmod 3$ $(p \neq 2)$	$C = C_1 \oplus C_3$ where C_1 is a cyclic code of length p^s over R and C_3 is a $-(3 \cdot 2^{-2})^{p^s}$-constacyclic code of length $2p^s$ over R, respectively (see Corollary 3.2.2).

Furthermore, we characterize the ideals of the quotient rings $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ into 4 types; trivial ideals, principal ideals with nonmonic polynomial generators, principal ideals with monic polynomial generators and non-principal ideals as follows from Theorem 3.1.2. The structures of such dual codes are determined in Theorem 3.1.1, 3.1.2, Theorem 3.1.2 and Theorem 3.1.2. In $p^m \equiv 1 \pmod 3$, the number of all cyclic codes of length $3p^s$ over R is mentioned in Theorem 3.2.1. On the other hand, $p^m \equiv 2 \pmod 3$, the number of all cyclic codes of length $3p^s$ over R is the product of number of all cyclic codes of length p^s over R and number of all ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. Moreover, the number of all cyclic code C of length $3p^s$ over R is shown in Table 4.2.

For the number of all self-dual cyclic codes of length $3p^s$ over R, it is the number

Table 4.2: Number of all cyclic code C of length $3p^s$ over R

Cases	Number of cyclic codes
$p^m \equiv 1 \pmod 3$	The third power of the number of all constacyclic codes of length p^s over R (see Theorem 3.2.1).
$p^m \equiv 2 \pmod 3$	The product of the number of all cyclic codes of length p^s over R and the number of all ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ (see Theorem 3.2.2).

of self-dual cyclic codes of length p^s over R with $p^m \equiv 1 \pmod 3$ (any p) or $p^m \equiv 2 \pmod 3$ $(p \neq 2)$ (see Theorem 3.2.1 and Theorem 3.2.2). In $p^m \equiv 2 \pmod 3$ with $p = 2$, the number of all self-dual cyclic codes is equal to the product of the number of self-dual cyclic codes of length p^s over R and the number of all ideals I of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$, $I = \mathcal{A}(I)^*$ (see Theorem 3.2.2). Finally, we determine the condition for each ideal I of $\frac{R[x]}{\langle (x^2+x+1)^{2^s} \rangle}$, $I = \mathcal{A}(I)^*$ in Proposition 3.2.2, Proposition 3.2.2, Proposition 3.2.2 and Proposition 3.2.2. However, for $I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x), u(x^2+x+1)^\omega \rangle$ where $h(x)$ is a unit, the condition $I = \mathcal{A}(I)^*$ is an open problem.

REFERENCES

[1] S. D. Berman, Semisimple cyclic and Abelian codes. II, *Kibernetika* (Kiev) **3** (1967) 21-30 (In Russian), *Cybernetic* **3** (1967) 17-23.

[2] 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.

[3] G. Castagnoli, J. L. Massey, P. A. Schoeller and N. von Seemann, On repeated-root cyclic codes, *IEEE Trans. Inf. Theory* **37** (1991) 337-342.

[4] 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 Appl.* **37** (2016) 108-130.

[5] Y. Cao, Y. Cao, H. Q. Dinh, F. W. Fu, J. Gao and S. Sriboonchitta, Constacyclic codes of length np^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, *Adv. Math. Commun.* **12**(2) (2018) 231.

[6] J. L. Massey, D. J. Costello and J. Justesen, Polynomial weights and code constructions, *IEEE Trans. Inf. Theory* **19** (1973) 101-110.

[7] H. Q. Dinh, Constacyclic Codes of Length 2^s Over Galois Extension Rings of $\mathbb{F}_2+u\mathbb{F}_2$, *IEEE Trans. Inf. Theory* **55** (2009) 1730-1740.

[8] 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.

[9] H. Q. Dinh, Repeated-root constacyclic codes of prime power length, *AMS Contemp. Math.* **480** (2009) 87-100.

[10] H. Q. Dinh, Repeated-root constacyclic codes of length $2p^s$, Finite Fields Appl. **18** (2012) 133-143.

[11] H. Q. Dinh, Structure of repeated-root constacyclic codes of length $3p^s$ and their duals, *Discrete Math.* **313** (2013) 983-991.

[12] H. Q. Dinh, On repeated-root constacyclic codes of length $4p^s$, *Asian-Eur. J. Math.* **6** (2013) https://doi.org/10.1142/S1793557113500204.

[13] 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.

[14] 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** (2018) https://doi.org/10.1142/S0219498819500221.

[15] 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** (2018) https://doi.org/10.1142/S0219498819500233.

[16] H. Q. Dinh, H. D. Nguyen, S. Sriboonchitta and T. M. Vo, Repeated-root constacyclic codes of prime power lengths over finite chain rings, *Finite Fields Appl.* **43** (2017) 22-41.

[17] H. Q. Dinh, Y. Fan, H. Liu, X. Liu and S. Sriboonchitta, On self-dual constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *Discrete Math.* **341** (2018) 324-335.

[18] H. Q. Dinh and S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inform. Theory* **50** (2004) 1728-1744.

[19] G. Falkner, B. Kowol, W. Heise and E. Zehendner, On the existence of cyclic optimal codes, *Atti Semin. Mat. Fis. Univ. Modena* **28** (1979) 326-341

[20] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* **40** (1994) 301-319.

[21] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, 10th impression, NorthHolland, Amsterdam, 1998.

[22] J. H. van Lint, Repeated-root cyclic codes, *IEEE Trans. Inf. Theory* **37** (1991) 343-345.

[23] R. M. Roth and G. Seroussi, On cyclic MDS codes of length q over $GF(q)$, *IEEE Trans. Inf. Theory* **32** (1986) 284-285.

[24] W. Zhao, X. Tang and Z. Gu, All $\alpha + u\beta$-constacyclic codes of length np^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *Finite Fields Appl.* **50** (2018) 1-16.

ภาคผนวก

Your Submission: DMAA-D-19-00245R1

em.dmaa.0.6ab793.690fd0c6@editorialmanager.com <em.dmaa.0.6ab793.690fd0c6@editorialmanager.com>
ในนามของ
Discrete Mathematics, Algorithms and Applications (DMAA) <em@editorialmanager.com>
อา 19/4/2020 16:01
ถึง:

☐ chakkrid klin-eam <chakkridk@nu.ac.th>

Ref.: Ms. No. DMAA-D-19-00245R1
Explicit constructions of cyclic and negacyclic codes of length 3ps over Fpm+ uFpm
Discrete Mathematics, Algorithms and Applications (DMAA)

Dear Asst.Prof.Dr. Chakkrid Klin-eam,

I am pleased to inform you that your work has now been accepted for publication in Discrete Mathematics, Algorithms and Applications (DMAA).

It was accepted on Apr 19, 2020.

If you wish to have your article published as Open Access, please note the Article-Processing Charge (APC) is USD2000. You may contact us or visit https://www.worldscientific.com/page/open for more details.

Comments from the Editor and Reviewers can be found below.

Thank you for submitting your work to this journal.

With kind regards

Suogang Gao
Editor
Discrete Mathematics, Algorithms and Applications (DMAA)

Comments from the Editors and Reviewers:

The revised version is good. This referee suggests the paper to be published.

In compliance with data protection regulations, you may request that we remove your personal registration details at any time. (Use the following URL: https://www.editorialmanager.com/dmaa/login.asp?a=r). Please contact the publication office if you have any questions.

Discrete Mathematics, Algorithms and Applications
(2020) 2050063 (35 pages)

DOI: 10.1142/S1793830920500639

Explicit constructions of cyclic and negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

Jirayu Phuto*,‡ and Chakkrid Klin-Eam*,†,§

*Department of Mathematics, Faculty of Science
Naresuan University, Phitsanulok 65000, Thailand

†Research Center for Academic Excellence in Mathematics
Naresuan University, Phitsanulok 65000, Thailand

‡jirayup60@email.nu.ac.th
§chakkridk@nu.ac.th

Received 1 November 2019
Accepted 19 April 2020
Published 4 June 2020

Let p be a prime such that $p \neq 3$. The algebraic structures of all cyclic and negacyclic codes of length $3p^s$ over the finite commutative chain ring $R := \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}(u^2 = 0)$ are obtained that the conditions depend on the factorization of polynomial $x^2 + x + 1$ over R. Therefore, we classify the structures of cyclic and negacyclic codes of length $3p^s$ over R into 2 cases, i.e., $p^m \equiv 1 \pmod 3$ and $p^m \equiv 2 \pmod 3$. From that we obtain the number of all cyclic and negacyclic codes of length $3p^s$ over R. After that, we give some situations for such cyclic and negacyclic codes are self-dual codes.

Keywords: Cyclic codes; chain rings; dual codes; negacyclic codes; repeated-root codes.

Mathematics Subject Classification 2020: 94B05, 13A99

1. Introduction

Let λ be a unit of a finite field. The class of λ-constacyclic codes is an important class of linear codes in coding theory. Many optimal linear codes are derived from λ-constacyclic codes. The class of λ-constacyclic codes includes as subclasses of two classes, i.e., cyclic codes ($\lambda = 1$) and negacyclic codes ($\lambda = -1$). Cyclic codes over finite fields were first studied in 1957 by Prange, which the cyclic codes have a rich algebraic structure. In 1967, Berman [1] introduced the codes in which length is divisible by the characteristics of the field, called *repeated-root codes*. In the 1970s and 1980s, several researchers, for example, Massey *et al.* [6], Falkner *et al.* [19], Roth and Seroussi [23] studied about repeated-root codes. Moreover, Castagnoli *et al.* [3] and van Lint [22], showed that repeated-root cyclic codes have a concatenated construction, and are asymptotically bad in the 1990s.

After the 1990s, codes over finite rings were studied. In an important paper, Hammons *et al.* [20] proved that certain good nonlinear codes such as Kerdock and Preparata codes can be constructed from linear codes over $\mathbb{Z}_4$ via the Gray map. In 1999, Bonnecaze and Udaya [2] introduced cyclic codes and self-dual codes over the finite chain ring $\mathbb{F}_2 + u\mathbb{F}_2$, where $u^2 = 0$. The ring $\mathbb{F}_2 + u\mathbb{F}_2$ shares some good properties of both $\mathbb{F}_4$ and $\mathbb{Z}_4$. This element is given by all binary polynomials in indeterminate u of degree less than 2 and is closed under usual binary addition but multiplication modulo u^2. In general, the class of finite rings of the form $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ has been widely used as alphabets of certain constacyclic codes.

In general, Zhao *et al.* [24] determined all $(\alpha + u\beta)$-constacyclic codes of length np^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where α, β are units of $\mathbb{F}_{p^m}$ and $\gcd(n, p) = 1$. Let $\alpha_0 \in \mathbb{F}_{p^m}$ such that $\alpha_0^{p^s} = \alpha$. They divide the structures of such constacyclic codes into 2 cases, i.e., $x^n - \alpha_0$ is irreducible in $\mathbb{F}_{p^m}$ and $x^n - \alpha_0$ is reducible in $\mathbb{F}_{p^m}$. Moreover, Cao *et al.* [5] also determined all α-constacyclic codes of length np^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where α is a unit of $\mathbb{F}_{p^m}$ and $\gcd(n, p) = 1$. Similarly, they divide the structures of such constacyclic codes that are similar to the above results. However, they do not give the condition that $x^n - \alpha_0$ is irreducible. It makes us interesting to such a condition. It is hard to find that condition in general form, i.e., constacyclic codes of length np^s. Therefore, it is a good reason to determine the codes of a specific length. The algebraic structures of repeated-root constacyclic codes over $\mathbb{F}_{p^m}$ were studied in several lengths which include p^s, $2p^s$, $3p^s$ and $4p^s$ (see [9–12], respectively). In addition, the factorization of polynomials $x^2 - x + 1$ and $x^2 + x + 1$ over $\mathbb{F}_{p^m}$ were determined for construction of cyclic, negacyclic and constacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}$. Thus, we use those ideas to determine cyclic and negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. After that, the structures of such repeated-root constacyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ are interesting which consist of length p^s, $2p^s$ and $4p^s$. In 2010, Dinh [8] were studied the algebraic structures of constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Moreover, the algebraic structures of self-dual constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ were obtained by Dinh *et al.* [17] in 2018. Chen *et al.* [4] established all constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Recently, all constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ are studied by Dinh *et al.* [13–15]. First, they obtained the structures of constacyclic codes of length $4p^s$ over such ring when $p^m \equiv 1 \pmod 4$. In 2018, the structures of constacyclic codes of length $4p^s$ when $p^m \equiv 3 \pmod 4$ were determined. We notice that the algebraic structures of constacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ are not studied. Therefore, we focus on cyclic and negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ which are specifically of those constacyclic codes. Moreover, dual codes of cyclic codes are cyclic and dual codes of negacyclic codes are also negacyclic. This means that self-dual cyclic and negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ exist.

The aims of this paper are to obtain the algebraic structures of cyclic and negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and their duals. Furthermore, the number of all distinct cyclic and negacyclic codes of length $3p^s$ over such ring are determined. Finally, we determine the conditions that cyclic and negacyclic codes are

self-dual codes. The rest of the paper is arranged as follows. After presenting preliminary in Sec. 2, we present the main results of this paper in Secs. 3 and 4. Each section is divided into 2 subsections, i.e., $p^m \equiv 1 \pmod 3$ and $p^m \equiv 2 \pmod 3$. In Sec. 3, we focus on the structures of cyclic codes of length $3p^s$ and their dual codes. The remaining result, the number of all distinct cyclic codes are obtained in Sec. 4. Moreover, some conditions for self-dual cyclic codes are also obtained in the above section. In the case $p^m \equiv 2 \pmod 3$, it will be shown that each cyclic code of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ is a direct sum of a cyclic code of length p^s over such ring and an ideal of the quotient ring $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. However, we construct a ring isomorphism between the quotient rings $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ and $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle x^{2p^s}+(3\cdot 2^{-2})^{p^s}\rangle}$, i.e., each ideal of the quotient ring $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ is isomorphic to a $-(3\cdot 2^{-2})^{p^s}$-constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ when p is an odd prime $p \neq 3$. In the remaining case $p = 2$, we obtain some properties of the quotient ring $\frac{(\mathbb{F}_{2^m}+u\mathbb{F}_{2^m})[x]}{\langle (x^2+x+1)^{2^s}\rangle}$ which bring to the properties of cyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. After that, we define a ring isomorphism to obtain properties for negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Finally, the conclusion is mentioned in Sec. 6.

2. Preliminaries

An ideal I of a finite commutative ring R with identity is called *principal* if it is generated by a single element. A ring R is a principal ideal ring if its ideals are principal. R is called a *local ring* if R has a unique maximal ideal. Furthermore, a ring R is called a *chain ring* if the set of all ideals of R is linearly ordered under set-theoretic inclusion. The *order* of an element a in R is the smallest positive integer n such that $a^n = 1$, where 1 is an identity of R and denoted by $\mathrm{ord}(a)$. Moreover, the following equivalent conditions are known for the class of finite commutative rings with identity.

Proposition 2.1 ([18]). *If R is a finite commutative ring with identity, then the following conditions are equivalent:*

(i) *R is a local ring and the maximal ideal M of R is principal, i.e., $M = \langle r\rangle$ for some $r \in R$,*
(ii) *R is a local principal ideal ring,*
(iii) *R is a chain ring with ideals $\langle r^i\rangle, 0 \leq i \leq N_r$, where N_r is the nilpotentcy of r.*

Each *code* C of length n over a finite commutative ring R with identity is a nonempty subset of R^n, and the ring R is referred to as the *alphabet* of the code. If C is an R-submodule of R^n, then C is called *a linear code* of length n over R. For a unit λ of R, the λ-constacyclic (λ-twisted) shift τ_λ on R^n is the shift

$$\tau_\lambda(c_0, c_1, \ldots, c_{n-1}) = (\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2})$$

and a linear code C is called *a λ-constacyclic code* if $\tau_\lambda(C) = C$, i.e., if C is closed under the λ-constacyclic shift τ_λ, for $\lambda = 1$, it is called *a cyclic code* and for $\lambda = -1$, it is called a *negacyclic code.*

Each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ is identified with its polynomial representation as $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ and the code C is identified with the set of all polynomial representations of its codewords. Then, in the quotient ring $\frac{R[x]}{\langle x^n - \lambda \rangle}$, $xc(x)$ corresponds to the λ-constacyclic shift of $c(x)$. Thus, the following fact is well known and straightforward.

Proposition 2.2 ([21]). *A linear code C of length n is a λ-constacyclic code over R if and only if C is an ideal of the quotient ring $\frac{R[x]}{\langle x^n - \lambda \rangle}$. (Hence, this quotient ring is referred to as the ambient ring of the code C.)*

Given n-tuples $x = (x_0, x_1, \ldots, x_{n-1}), y = (y_0, y_1, \ldots, y_{n-1}) \in R^n$, their inner product is defined as usual

$$x \cdot y = x_0 y_0 + x_1 y_1 + \cdots + x_{n-1} y_{n-1},$$

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

$$C^\perp = \{x : x \cdot y = 0, \forall\, y \in C\}.$$

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 well known.

Proposition 2.3 ([18]). *Let p be a prime and R be a finite chain ring of size p^m. The number of codewords in each linear code C of length n over R is p^k, for some integer $k \in \{0, 1, \ldots, mn\}$. Moreover, the dual code $C^\perp$ has p^l codewords, where $k + l = mn$, i.e., $|C| \cdot |C^\perp| = |R|^n$.*

In general, we have the following implication of the dual of a λ-constacyclic code.

Proposition 2.4 ([18]). *The dual of a λ-constacyclic code is a λ^{-1}-constacyclic code.*

In this paper, we consider cyclic and negacyclic codes of length $3p^s$ over the ring $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where $u^2 = 0$ and p is a prime with $p \neq 3$. The ring R consists of all p^m-ary polynomials of degree 0 and 1 in indeterminate u, it is closed under p^m-ary polynomial addition and multiplication modulo u^2. Thus, $R = \frac{\mathbb{F}_{p^m}[u]}{\langle u^2 \rangle} = \{a + ub : a, b \in \mathbb{F}_{p^m}\}$ is a local ring with maximal ideal $\langle u \rangle = u\mathbb{F}_{p^m}$, and hence, it is a chain ring.

Hereafter, we denote the ambient ring of cyclic and negacyclic codes of length $3p^s$ over R as

$$\mathcal{R}_1 = \frac{R[x]}{\langle x^{3p^s} - 1 \rangle},$$

and

$$\mathcal{R}_{-1} = \frac{R[x]}{\langle x^{3p^s} + 1 \rangle},$$

respectively. From Proposition 2.2, λ-constacyclic codes of length n over R are ideals of $\mathcal{R}_\lambda = \frac{R[x]}{\langle x^n - \lambda \rangle}$.

Definition 2.5 ([4]). If $f(x) = a_0 + a_1 x + \cdots + a_r x^r$, then the reciprocal of $f(x)$ is the polynomial $f^*(x) = a_r + a_{r-1}x + a_{r-2}x^2 + \cdots + a_0 x^r$.

$f^*(x)$ can be expressed by $f^*(x) = x^r f(\frac{1}{x})$. If I is an ideal of $\mathcal{R}_\lambda$, then $I^* = \{f^*(x) : f(x) \in I\}$ is also an ideal of $\mathcal{R}_{\lambda^{-1}}$.

Definition 2.6 ([4]). Let I be an ideal of $\mathcal{R}_\lambda$, we define $\mathcal{A}(I) = \{g(x) : f(x)\ g(x) = 0, \forall f(x) \in I\}$. Then $\mathcal{A}(I)$ is called *the annihilator of* I.

From the above definition, We see that if I is an ideal of $\mathcal{R}_\lambda$, then $\mathcal{A}(I)$ is an ideal of $\mathcal{R}_\lambda$. Moreover, if C is a constacyclic code of length n over R with the associated ideal I (which is an ideal of $\mathcal{R}_\lambda$), then the associated ideal of $C^\perp$ is $\mathcal{A}(I)^*$ (which is an ideal of $\mathcal{R}_{\lambda^{-1}}$). The following lemma is easy to prove and will be used in Sec. 3.

Lemma 2.7 ([4]). (i) $(f(x)g(x))^* = f^*(x)g^*(x)$.

(ii) *If* $\deg f(x) \geq \deg g(x)$, *then* $(f(x) + g(x))^* = f^*(x) + x^{\deg f(x) - \deg g(x)} g^*(x)$.

(iii) *Let* $I = \langle f(x), ug(x) \rangle$ *be an ideal of* $\mathcal{R}_\lambda$, *then* $I^* = \langle f^*(x), ug^*(x) \rangle$, *which is an ideal of* $\mathcal{R}_{\lambda^{-1}}$.

Let ξ be a primitive $(p^m - 1)$th root of identity of $\mathbb{F}_{p^m}$. Then

$$\mathbb{F}_{p^m} = \{0, \xi, \xi^2, \ldots, \xi^{p^m - 1} = 1\}.$$

Firstly, we focus the structures of cyclic codes of length $3p^s$ over R as the following section.

3. Cyclic Codes of Length $3p^s$ Over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

In this section, we focus on the algebraic structures of cyclic codes of length $3p^s$ over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. So, we divide this structures into 2 cases, namely, $p^m \equiv 1 \pmod 3$ and $p^m \equiv 2 \pmod 3$.

3.1. *The case* $p^m \equiv 1 \pmod 3$

By Proposition 2.2, each cyclic code of length $3p^s$ over R is an ideal of $\mathcal{R}_1 = \frac{R[x]}{\langle x^{3p^s} - 1 \rangle}$. In $R[x]$, we get

$$(\xi^{\frac{p^m - 1}{3}})^3 - 1 = 0,$$

$$(\xi^{\frac{2(p^m - 1)}{3}})^3 - 1 = 0 \quad \text{and}$$

$$(\xi^{\frac{3(p^m - 1)}{3}})^3 - 1 = 0.$$

This means that $\xi^{\frac{p^m-1}{3}}$, $\xi^{\frac{2(p^m-1)}{3}}$ and $\xi^{\frac{3(p^m-1)}{3}}$ are roots of the polynomial x^3-1. Therefore, the polynomial $x^{3p^s}-1$ can be expressed as

$$\begin{aligned} x^{3p^s}-1 &= (x^3-1)^{p^s} \\ &= (x-\xi^{\frac{p^m-1}{3}})^{p^s}(x-\xi^{\frac{2(p^m-1)}{3}})^{p^s}(x-\xi^{\frac{3(p^m-1)}{3}})^{p^s} \\ &= (x^{p^s}-\xi^{\frac{(p^m-1)p^s}{3}})(x^{p^s}-\xi^{\frac{2(p^m-1)p^s}{3}})(x^{p^s}-\xi^{\frac{3(p^m-1)p^s}{3}}) \\ &= (x^{p^s}-\xi^{\frac{(p^m-1)p^s}{3}})(x^{p^s}-\xi^{\frac{2(p^m-1)p^s}{3}})(x^{p^s}-1) \\ &= (x^{p^s}-1)(x^{p^s}-\delta_1)(x^{p^s}-\delta_2), \end{aligned}$$

where $\delta_i = \xi^{\frac{i(p^m-1)p^s}{3}}$ for $i=1,2$.

Remark 3.1. Let $\delta_i = \xi^{\frac{i(p^m-1)p^s}{3}}$ for $i=1,2$.

(i) $\delta_1\delta_2 = 1$.
(ii) $\delta_1+\delta_2 = -1$.

Thus, we obtain the algebraic structures of cyclic codes of length $3p^s$ over R as the following theorem.

Theorem 3.2. *Let C be a cyclic code of length $3p^s$ over R. Then $C = C_1 \oplus C_{\delta_1} \oplus C_{\delta_2}$, where C_1 is a cyclic code and C_{δ_i} is a δ_i-constacyclic code of length p^s over R, where $\delta_i = \xi^{\frac{i(p^m-1)p^s}{3}}$ for $i=1,2$. Moreover, $|C| = |C_1||C_{\delta_1}||C_{\delta_2}|$.*

Proof. It is a routine to show that $\langle x^{p^s}-1\rangle$, $\langle x^{p^s}-\delta_1\rangle$ and $\langle x^{p^s}-\delta_2\rangle$ are pairwises coprime ideals in $R[x]$, where $\delta_i = \xi^{\frac{i(p^m-1)p^s}{3}}$ for $i=1,2$. By Chinese Division Algorithm, we have

$$\frac{R[x]}{\langle x^{3p^s}-1\rangle} \cong \frac{R[x]}{\langle x^{p^s}-1\rangle} \oplus \frac{R[x]}{\langle x^{p^s}-\delta_1\rangle} \oplus \frac{R[x]}{\langle x^{p^s}-\delta_2\rangle}.$$

By Proposition 2.2, we obtain that C is an ideal of $\mathcal{R}_1$. Thus, $C = C_1 \oplus C_{\delta_1} \oplus C_{\delta_2}$, where C_1 is an ideal of $\frac{R[x]}{\langle x^{p^s}-1\rangle}$ and C_{δ_i} is an ideal of $\frac{R[x]}{\langle x^{p^s}-\delta_i\rangle}$ for $i=1,2$. By Proposition 2.2 again, C_1 is a cyclic code of length p^s over R and C_{δ_i} is a δ_i-constacyclic code of length p^s over R for $i=1,2$. □

Therefore, by Theorem 3.2, each cyclic code of length $3p^s$ over R is a direct sum of cyclic and δ_1,δ_2-constacyclic codes of length p^s over R. However, the algebraic structures of all constacyclic codes of length p^s over R are obtained in [8]. Next, we investigate the dual of cyclic codes of length $3p^s$ over R as the following theorem.

Theorem 3.3. *Let $C = C_1 \oplus C_{\delta_1} \oplus C_{\delta_2}$ be a cyclic code of length p^s over R, where C_1 is a cyclic code and C_{δ_i} is a δ_i-constacyclic code of length $3p^s$ over R and $\delta_i = \xi^{\frac{i(p^m-1)}{3}}$ for $i=1,2$. Then $C^\perp = C_1^\perp \oplus C_{\delta_1}^\perp \oplus C_{\delta_2}^\perp$, where $C_1^\perp$ is a cyclic code,*

$C_{\delta_1}^{\perp}$ is a δ_2-constacyclic code and $C_{\delta_2}^{\perp}$ is a δ_1-constacyclic code of length p^s over R. In particular, $|C^{\perp}| = |C_1^{\perp}||C_{\delta_1}^{\perp}||C_{\delta_2}^{\perp}|$.

Proof. It is obvious that

$$C_1^{\perp} \oplus C_{\delta_1}^{\perp} \oplus C_{\delta_2}^{\perp} \subseteq C^{\perp}.$$

We consider that

$$\begin{aligned} |C_1^{\perp}||C_{\delta_1}^{\perp}||C_{\delta_2}^{\perp}| &= \frac{|R|^{p^s}}{|C_1|}\frac{|R|^{p^s}}{|C_{\delta_1}|}\frac{|R|^{p^s}}{|C_{\delta_2}|} \\ &= \frac{|R|^{3p^s}}{|C_1||C_{\delta_1}||C_{\delta_2}|} \\ &= \frac{|R|^{3p^s}}{|C|} \\ &= |C^{\perp}|. \end{aligned}$$

Hence, $C^{\perp} = C_1^{\perp} \oplus C_{\delta_1}^{\perp} \oplus C_{\delta_2}^{\perp}$. Using Proposition 2.4, $C_1^{\perp}$ is a cyclic code of length p^s over R, $C_{\delta_1}^{\perp}$ is a δ_2-constacyclic code of length p^s over R and $C_{\delta_2}^{\perp}$ is a δ_1-constacyclic code of length p^s over R. □

The following result can be found in [17, Sec. 5], and will apply to determine self-dual of cyclic codes of length $3p^s$ over R.

Let λ be a unit of $\mathbb{F}_{p^m}$. If $\lambda \neq \lambda^{-1}$, a λ-constacyclic code C of length p^s over R is self-dual if and only if it is the ideal $\langle u \rangle$ of the quotient ring $\frac{R[x]}{\langle x^{p^s} - \lambda \rangle}$. Hence, $\langle u \rangle$ is the unique self-dual λ-constacyclic code of length p^s over R.

Thus, the $\langle u \rangle$ is the unique self-dual δ_1, δ_2-constacyclic codes of length p^s over R.

Proposition 3.4. *Let $C = C_1 \oplus C_{\delta_1} \oplus C_{\delta_2}$ be a cyclic code of length $3p^s$ over R where C_1 is a cyclic code of length $3p^s$ over R and C_{δ_i} is a δ_i-constacyclic code of length $3p^s$ over R where $\delta_i = \xi^{\frac{i(p^m-1)}{3}}$ for $i = 1, 2$. If $C_1 = C_{\delta_1} = C_{\delta_2} = \langle u \rangle$, then C is a self-dual cyclic code of length $3p^s$ over R.*

Proof. Suppose that $C_1 = C_{\delta_1} = C_{\delta_2} = \langle u \rangle$. By assumption, we have $C = \langle u \rangle$. Therefore, $C^{\perp} = \langle u \rangle$, implying that C is self-dual. □

3.2. *The case* $p^m \equiv 2 \pmod 3$

First, we consider that

$$\begin{aligned} x^{3p^s} - 1 &= (x^3 - 1)^{p^s} \\ &= (x-1)^{p^s}(x^2 + x + 1)^{p^s} \\ &= (x^{p^s} - 1)(x^2 + x + 1)^{p^s}. \end{aligned}$$

Next, we give the following lemmas for properties of a polynomial $x^2 + x + 1$ to prove in this case.

Lemma 3.5. *The polynomial x^2+x+1 is irreducible in $\mathbb{F}_{p^m}[x]$.*

Proof. Assume that x^2+x+1 is reducible in $\mathbb{F}_{p^m}[x]$. There exists $\alpha \in \mathbb{F}_{p^m}$ such that

$$\alpha^2+\alpha+1=0.$$

Note that

$$x^3-1=(x-1)(x^2+x+1).$$

This implies that α is a root of $x^3-1=0$ over $\mathbb{F}_{p^m}$. That is $\alpha^3=1$. Thus, $\text{ord}(\alpha)|3$ If $\text{ord}(\alpha)=1$, then $0=\alpha^2+\alpha+1=1+1+1=3\neq 0$ which is a contradiction. Now, we have $\text{ord}(\alpha)=3$. This means that $3|(p^m-1)$, implying that $p^m \equiv 1 \pmod 3$. It is a contradiction. Therefore, x^2+x+1 is irreducible in $\mathbb{F}_{p^m}[x]$. □

Lemma 3.6. *The polynomial x^2+x+1 is irreducible in $R[x]$.*

Proof. Assume that x^2+x+1 is reducible in $R[x]$. There exists $\alpha=\alpha_0+u\alpha_1 \in R$ for some $\alpha_0,\alpha_1 \in \mathbb{F}_{p^m}$ such that

$$\alpha^2+\alpha+1=0.$$

So, $0=(\alpha_0+u\alpha_1)^2+(\alpha_0+u\alpha_1)+1=\alpha_0^2+\alpha_0+1+u(2\alpha_0\alpha_1+\alpha_1)$. This implies that $\alpha_0^2+\alpha_0+1=0$ and $2\alpha_0\alpha_1+\alpha_1=0$. Thus, $\alpha_0 \in \mathbb{F}_{p^m}$ is a root of $x^2+x+1=0$. It is a contradiction with Lemma 3.5. Hence, x^2+x+1 is irreducible in $R[x]$. □

Throughout this case, we consider that

$$\begin{aligned}
&(-3^{-1})^{p^s}(x+2)^{p^s}(x^{p^s}-1)+(-1)(-3^{-1})^{p^s}(x^2+x+1)^{p^s}\\
&=(-3^{-1})^{p^s}(x+2)^{p^s}(x-1)^{p^s}+(-1)(-3^{-1})^{p^s}(x^2+x+1)^{p^s}\\
&=(-3^{-1})^{p^s}[(x^2+x-2)^{p^s}-(x^2+x+1)^{p^s}]\\
&=(-3^{-1})^{p^s}(-3)^{p^s}\\
&=1.
\end{aligned}$$

Thus, we obtain that $x^{p^s}-1$ and $(x^2+x+1)^{p^s}$ are coprime in $R[x]$. This implies that $\langle x^{p^s}-1\rangle$ and $\langle (x^2+x+1)^{p^s}\rangle$ are pair-wises coprime ideals in $R[x]$. By Chinese Remainder Theorem, we have

$$\frac{R[x]}{\langle x^{3p^s}-1\rangle} \cong \frac{R[x]}{\langle x^{p^s}-1\rangle} \oplus \frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}. \tag{1}$$

By Proposition 2.2, each ideal of $\frac{R[x]}{\langle x^{p^s}-1\rangle}$ is a cyclic code of length p^s over R studied in [8]. Moreover, cyclic codes and their dual codes of length $3p^s$ over R are determined as follows.

Theorem 3.7. *Let C be a cyclic code of length $3p^s$ over R. Then*

(i) *$C = C_1 \oplus I$, where C_1 is a cyclic code of length p^s over R and I is an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. Moreover, $|C| = |C_1||I|$.*

(ii) *The dual code $C^\perp$ of C can be expressed as $C^\perp = C_1^\perp \oplus \mathcal{A}(I)^*$, where C_1 is a cyclic code of length p^s over R and I is an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. Moreover, $|C^\perp| = |C_1^\perp||\mathcal{A}(I)^*|$.*

Proof. (i) By Proposition 2.2, we have C as an ideal of $\frac{R[x]}{\langle x^{3p^s}-1 \rangle}$. By Eq. (1), we have C as a direct sum of an ideal of $\frac{R[x]}{\langle x^{p^s}-1 \rangle}$ and an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. By Proposition 2.2 again, we have $C = C_1 \oplus I$, where C_1 an a cyclic code of length p^s over R and I is an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$.

(ii) Let $C^\perp$ be the dual code of each negacyclic code of length $3p^s$ over R. By (i), we have $C^\perp = C_1^\perp \oplus I^\perp$, where C_1 is a cyclic code of length p^s over R and I as an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. By Proposition 2.4, we have $C^\perp = C_1^\perp \oplus \mathcal{A}(I)^*$. □

Next, we determine the algebraic structure of the ring $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. In $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$, we have

$$\begin{aligned} 0 &= (x^2+x+1)^{p^s} \\ &= x^{2p^s} + x^{p^s} + 1. \end{aligned} \tag{2}$$

Remark 3.8. By Eq. (2), $-1 = x^{2p^s} + x^{p^s}$ in $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$.

Lemma 3.9. *Each nonzero polynomial of degree less than 2 in $\mathbb{F}_{p^m}[x]$ is invertible in $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$.*

Proof. Let $f(x) = ax+b$ be a nonzero polynomial in $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$, where $a, b \in \mathbb{F}_{p^m}$. If $a = 0$, then $ax + b = b \neq 0$. This implies that $ax + b$ is invertible in $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. If $a \neq 0$, then

$$\begin{aligned} &a^{-1}(x+a^{-1}b)^{-1} \\ &\quad = a^{-1}(x+a^{-1}b)^{p^s-1}(x-a^{-1}b+1)^{p^s}(x+a^{-1}b)^{-p^s}(x-a^{-1}b+1)^{-p^s} \\ &\quad = a^{-1}(x+a^{-1}b)^{p^s-1}(x-a^{-1}b+1)^{p^s}(x^2+x-(a^{-1}b)^2+a^{-1}b)^{-p^s} \\ &\quad = a^{-1}(x+a^{-1}b)^{p^s-1}(x-a^{-1}b+1)^{p^s}(x^{2p^s}+x^{p^s}-(a^{-1}b)^{2p^s}+(a^{-1}b)^{p^s})^{-1} \\ &\quad = a^{-1}(x+a^{-1}b)^{p^s-1}(x-a^{-1}b+1)^{p^s}(-1-(a^{-1}b)^{2p^s}-(-a^{-1}b)^{p^s})^{-1} \\ &\quad = -a^{-1}(x+a^{-1}b)^{p^s-1}(x-a^{-1}b+1)^{p^s}((a^{-1}b)^{2p^s}+(-a^{-1}b)^{p^s}+1^{p^s})^{-1} \\ &\quad = -a^{-1}(x+a^{-1}b)^{p^s-1}(x-a^{-1}b+1)^{p^s}([(a^{-1}b)^2+a^{-1}b+1]^{p^s})^{-1}. \end{aligned}$$

This means that $ax + b$ is invertible if and only if $(a^{-1}b)^2 + a^{-1}b + 1$ is invertible in $\mathbb{F}_{p^m}$. By Lemma 3.5, we have $(a^{-1}b)^2 + a^{-1}b + 1 \neq 0$. Hence, $ax + b$ is invertible in $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. □

Lemma 3.10. *Let* $f(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. *Then* $f(x)$ *can be uniquely expressed as*

$$f(x) = \sum_{i=0}^{p^s-1} (a_{0i}x + b_{0i})(x^2+x+1)^i + u\sum_{i=0}^{p^s-1} (a_{1i}x + b_{1i})(x^2+x+1)^i$$

$$= a_{00}x + b_{00} + \sum_{i=1}^{p^s-1} (a_{0i}x + b_{0i})(x^2+x+1)^i + u\sum_{i=0}^{p^s-1} (a_{1i}x + b_{1i})(x^2+x+1)^i,$$

where $a_{0i}, a_{1i}, b_{0i}, b_{1i} \in \mathbb{F}_{p^m}$, $0 \leq i \leq p^s - 1$. *Moreover,* $f(x)$ *is noninvertible if and only if* $a_{00} = b_{00} = 0$.

Proof. Since $f(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$, it can be viewed as polynomial of degree less than $2p^s$ over R. So, $f(x) = f_1(x) + uf_2(x)$, where $f_1(x), f_2(x)$ are polynomials in $\mathbb{F}_{p^m}[x]$. Thus, we have

$$f(x) = \sum_{i=0}^{p^s-1} (a_{0i}x + b_{0i})(x^2+x+1)^i + u\sum_{i=0}^{p^s-1} (a_{1i}x + b_{1i})(x^2+x+1)^i$$

$$= a_{00}x + b_{00} + \sum_{i=1}^{p^s-1} (a_{0i}x + b_{0i})(x^2+x+1)^i + u\sum_{i=0}^{p^s-1} (a_{1i}x + b_{1i})(x^2+x+1)^i$$

$$= a_{00}x + b_{00} + (x^2+x+1)\sum_{i=1}^{p^s-1} (a_{0i}x + b_{0i})(x^2+x+1)^{i-1}$$

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

where $a_{0i}, a_{1i}, b_{0i}, b_{1i} \in \mathbb{F}_{p^m}$, $0 \leq i \leq p^s - 1$. Since $(x^2+x+1)^{p^s} = 0$ and $u^2 = 0$, we have x^2+x+1 and u are nilpotent elements of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ with nilpotency indexes p^s and 2, respectively. Hence, $f(x)$ is noninvertible if and only if $a_{00} = b_{00} = 0$. □

Theorem 3.11. *The ring* $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ *is a local ring with the maximal ideal* $\langle x^2 + x + 1, u \rangle$ *and it is not a chain ring.*

Proof. By Lemma 3.10, the set of all noninvertible elements of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ forms the ideal $\langle x^2+x+1, u \rangle$. This means that $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ is a local ring with the maximal ideal $\langle x^2+x+1, u \rangle$. Next, we will show that $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ is not a chain ring. Claim that $u \notin \langle x^2+x+1 \rangle$ and $x^2+x+1 \notin \langle u \rangle$. Suppose that $u \in \langle x^2+x+1 \rangle$. Then $u = (x^2+x+1)(g_1(x)+ug_2(x))$ for some $g_1(x), g_2(x) \in \mathbb{F}_{p^m}[x]$. So, $(x^2+x+1)g_1(x) = 0$ and $(x^2+x+1)g_2(x) = 1$. This implies that x^2+x+1 is invertible. It is a contradiction because x^2+x+1 is a nilpotent element. Thus, $u \notin \langle x^2+x+1 \rangle$. Since nilpotentcy indexes of x^2+x+1 and u are p^s and 2, respectively, we have $x^2+x+1 \notin \langle u \rangle$. Hence, we obtain that $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ is not a chain ring. □

Proposition 3.12. *The ring* $\frac{\mathbb{F}_{p^m}[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ *is a chain ring whose each ideal forms* $\langle (x^2+x+1)^i\rangle$, $0 \le i \le p^s$.

Proof. Let $f(x) \in \frac{\mathbb{F}_{p^m}[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ Then

$$\begin{aligned} f(x) &= \sum_{i=0}^{p^s-1} (a_i x + b_i)(x^2+x+1)^i \\ &= a_0 x + b_0 + \sum_{i=1}^{p^s-1} (a_i x + b_i)(x^2+x+1)^i \\ &= a_0 x + b_0 + (x^2+x+1) \sum_{i=1}^{p^s-1} (a_i x + b_i)(x^2+x+1)^{i-1}, \end{aligned}$$

where $a_i, b_i \in \mathbb{F}_{p^m}$, $0 \le i \le p^s - 1$. Thus, $f(x)$ is noninvertible if and only if $a_0 = b_0 = 0$. This implies that the set of all noninvertible elements is $\langle x^2+x+1\rangle$. So, The ring $\frac{\mathbb{F}_{p^m}[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ is a local ring with the maximal ideal $\langle x^2+x+1\rangle$. Since the maximal ideal $\langle x^2+x+1\rangle$ is a principal ideal and by Proposition 2.1, we have $\frac{\mathbb{F}_{p^m}[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ is a chain ring whose each ideal forms $\langle (x^2+x+1)^i\rangle$, $0 \le i \le p^s$. □

Now, we characterize all ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ in the following theorem.

Theorem 3.13. *All ideals of* $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ *are listed respectively as follows*:

Type 1: (*trivial ideals*)

$$\langle 0\rangle \quad \text{and} \quad \langle 1\rangle.$$

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

$$\langle u(x^2+x+1)^i\rangle,$$

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

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

$$\langle (x^2+x+1)^i + u(x^2+x+1)^t h(x)\rangle,$$

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

Type 4: (*nonprincipal ideals*)

$$\left\langle (x^2+x+1)^i + u\sum_{j=0}^{\omega-1} (a_j x + b_j)(x^2+x+1)^j, u(x^2+x+1)^\omega \right\rangle,$$

where $1 \le i \le p^s - 1, a_j, b_j \in \mathbb{F}_{p^m}$, *and* $\omega < T$, *where* T *is the smallest integer such that* $u(x^2+x+1)^T \in \langle (x^2+x+1)^i + u\sum_{j=0}^{\omega-1}(a_j x + b_j)(x^2+x+1)^j\rangle$ *or equivalently,* $\langle (x^2+x+1)^i + u(x^2+x+1)^t h(x), u(x^2+x+1)^\omega\rangle$, *with* $h(x)$ *as in Type* 3, *and* $\deg h(x) \le \omega - t - 1$.

Proof. First of all, it is easy to see that ideals of Type 1 are trivial ideals. Let I be an arbitrary nontrivial ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. We processed by establishing all possible forms that this nontrivial ideal I can have.

Case 1: $I \subseteq \langle u\rangle$: Then any element of I must be of the form $c(x) = u\sum_{i=0}^{p^s-1}(a_{0i}x + b_{0i})(x^2+x+1)^i$, where $a_{0i}, b_{0i} \in \mathbb{F}_{p^m}$. This implies that there exists an element $l(x) \in I$ that has the smallest k such that $l_{0k}x + l_{1k} \neq 0$. Hence, each element $c(x) \in I$ have the form $c(x) = u(x^2+x+1)^k\sum_{i=k}^{p^s-1}(a_{0i}x + b_{0i})(x^2+x+1)^{i-k} \in \langle u(x^2+x+1)^k\rangle$, implying that $I \subseteq \langle u(x^2+x+1)^k\rangle$. However, we have $l(x) \in I$ with

$$\begin{aligned} l(x) &= u(x^2+x+1)^k \sum_{i=k}^{p^s-1}(l_{0i}x + l_{1i})(x^2+x+1)^{i-k} \\ &= u(x^2+x+1)^k \left[l_{0k}x + l_{1k} + \sum_{i=k+1}^{p^s-1}(l_{0i}x + l_{1i})(x^2+x+1)^{i-k} \right]. \end{aligned}$$

From $l_{0k}x + l_{1k} \neq 0$, we can see that $l_{0k}x + l_{1k} + \sum_{i=k+1}^{p^s-1}(l_{0i}x + l_{1i})(x^2+x+1)^{i-k}$ is invertible, proving that $u(x^2+x+1)^k \in I$. Therefore, $I = \langle u(x^2+x+1)^k\rangle$, which means that the nontrivial ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ contained in $\langle u\rangle$ are $\langle u(x^2+x+1)^k\rangle$, $0 \leq k \leq p^s - 1$, which are ideals of Type 2.

Case 2: $I \nsubseteq \langle u\rangle$: Let I_u denote the set of elements in I which are reduced modulo u. By Theorem 3.12, we have I_u is a nonzero ideal of the ring $\frac{\mathbb{F}_{p^m}[x]}{\langle (x^2+x+1)^{p^s}\rangle}$, which is a finite chain ring with ideals $\langle (x^2+x+1)^j\rangle$, where $0 \leq j \leq p^s$. Then there is an integer $1 \leq i \leq p^s - 1$ such that $I_u = \langle (x^2+x+1)^i\rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. This follows that there exists an element

$$\begin{aligned} c(x) &= \sum_{j=0}^{p^s-1}(a_{0j}x + b_{0j})(x^2+x+1)^j + u\sum_{j=0}^{p^s-1}(a_{1j}x + b_{1j})(x^2+x+1)^j \\ &\in \frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}, \end{aligned}$$

where $a_{0j}, a_{1j}, b_{0j}, b_{1j} \in \mathbb{F}_{p^m}$ such that $(x^2+x+1)^i + uc(x) \in I$. Since

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

and $u(x^2+x+1)^k = u(x^2+x+1)^{k-i}[(x^2+x+1)^i + uc(x)] \in I$ with $i \leq k \leq p^s - 1$, we have $(x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j \in I$. We now consider two subcases.

Case 2a: $I = \langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x+b_{0j})(x^2+x+1)^j\rangle$, then I can be expressed as

$$I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x)\rangle,$$

where $0 \leq t < i$ and $h(x)$ is 0 or a unit. If $h(x)$ is a unit, then $h(x)$ can be represented as $h(x) = \sum_j (h_{1j}x + h_{0j})(x^2+x+1)^j$ with $h_{0j}, h_{1j} \in \mathbb{F}_{p^m}$ and $h_{10}x + h_{00} \neq 0$. It follows that I is of Type 3.

Case 2b: $\langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x+b_{0j})(x^2+x+1)^j\rangle \subsetneq I$. Then, there exists $f(x) \in I \backslash \langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x+b_{0j})(x^2+x+1)^j\rangle$. By Division Algorithm, there exist polynomials $q(x), r(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ such that

$$0 \neq r(x) = f(x) - q(x)\left[(x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x+b_{0j})(x^2+x+1)^j\right] \in I,$$

where $\deg r(x) < \deg((x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x+a_{1j})(x^2+x+1)^j)$. This implies that $r(x)$ can be expressed as

$$r(x) = \sum_{j=0}^{i-1}(r_{1j}x+r_{0j})(x^2+x+1)^j + u\sum_{j=0}^{i-1}(r'_{1j}x+r'_{0j})(x^2+x+1)^j,$$

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

$$r(x) = u\sum_{j=k}^{i-1}(r'_{1j}x+r'_{0j})(x^2+x+1)^j = u(x^2+x+1)^k \times \left[r'_{1k}x + r'_{0k} + \sum_{j=k+1}^{i-1}(h'_{1j}x+h'_{0j})(x^2+x+1)^{j-k}\right].$$

As $r'_{1k}x + r'_{0k} \neq 0, r'_{1k}x + r'_{0k} + \sum_{j=k+1}^{i-1}(r'_{1j}x+r'_{0j})(x^2+x+1)^{j-k}$ is an invertible element in $\frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$, hence,

$$u(x^2+x+1)^k = \left[r'_{1k}x + r'_{0k} + \sum_{j=k+1}^{i-1}(r'_{1j}x+r'_{0j})(x^2+x+1)^{j-k}\right]^{-1} r(x) \in I.$$

It has been shown that for any $f(x) \in I \backslash \langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x+b_{0j})(x^2+x+1)^j\rangle$, there is an integer k with $0 \leq k \leq i-1$ such that $u(x^2+x+1)^k \in I$. Let $\omega = \min\{k : f(x) \in I \backslash \langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x+b_{0j})(x^2+x+1)^j\rangle\}$. Then $\langle (x^2+x+1)^i + u\sum_{j=0}^{i-1}(a_{0j}x+b_{0j})(x^2+x+1)^j, u(x^2+x+1)^\omega\rangle \subseteq I$. In

addition, by the above construction, for any $f(x) \in I$, there exists a polynomial $g(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ satisfying

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

implying that

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

Thus, we get

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

Let T be the smallest integer such that $u(x^2+x+1)^T \in \langle (x^2+x+1)^i + u\sum_{j=0}^{i-1} (a_{0j}x + b_{0j})(x^2+x+1)^j \rangle$. If $\omega \geq T$, then

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

It is a contradiction by assumption of this case. This implies that $\omega < T$, proving that I is of Type 4. □

Next, we focus on annihilator in $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ to characterize the dual codes of constacyclic codes of length $3p^s$ over R. We now investigate the dual codes and determine the annihilator of I, where I is an ideal of the ring $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. We need to give the following lemma.

From Theorem 3.13, the number T is an important role in Type 4. So, we need to determine the number T as the following proposition.

Proposition 3.14. *Let T be the smallest integer such that $u(x^2+x+1)^T \in C = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x) \rangle$, where $h(x)$ is 0 or a unit. Then*

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

Proof. First of all, we see that $T \leq i$ because $u(x^2+x+1)^i = u[(x^2+x+1)^i + u(x^2+x+1)^t h(x)] \in C$. If $h(x) = 0$, then $C = \langle (x^2+x+1)^i \rangle$, implying that

$T = i$. Now, we consider that the case $h(x)$ is a unit. Since $u(x^2+x+1)^T \in \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x)\rangle$, there is a polynomial $f(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$ satisfying $u(x^2+x+1)^T = f(x)[(x^2+x+1)^i + u(x^2+x+1)^t h(x)]$. So, $f(x)$ can be written as

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

where $a_{0j}, a_{1j}, b_{0j}, b_{1j} \in \mathbb{F}_{p^m}$. Then $u(x^2+x+1)^T$ can be expressed as follows:

$$\begin{aligned}
&\left[\sum_{j=0}^{p^s-1}(a_{0j}x + b_{0j})(x^2+x+1)^j + u\sum_{j=0}^{p^s-1}(a_{1j}x + b_{1j})(x^2+x+1)^j\right] \\
&\quad\times [(x^2+x+1)^i + u(x^2+x+1)^t h(x)] \\
&= (x^2+x+1)^i \sum_{j=0}^{p^s-1}(a_{0j}x + b_{0j})(x^2+x+1)^j \\
&\quad + u(x^2+x+1)^i \sum_{j=0}^{p^s-1}(a_{1j}x + b_{1j})(x^2+x+1)^j \\
&\quad + u(x^2+x+1)^t h(x) \sum_{j=0}^{p^s-1}(a_{0j}x + b_{0j})(x^2+x+1)^j \\
&= (x^2+x+1)^i \sum_{j=0}^{p^s-i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j + (x^2+x+1)^{p^s} \\
&\quad\times \sum_{j=p^s-i}^{p^s-1}(a_{0j}x + b_{0j})(x^2+x+1)^{i+j-p^s} \\
&\quad + u(x^2+x+1)^i \sum_{j=0}^{p^s-i-1}(a_{1j}x + b_{1j})(x^2+x+1)^j \\
&\quad + u(x^2+x+1)^{p^s} \sum_{j=p^s-i}^{p^s-1}(a_{1j}x + b_{1j})(x^2+x+1)^{i+j-p^s} \\
&\quad + u(x^2+x+1)^t h(x) \sum_{j=0}^{p^s-i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j \\
&\quad + u(x^2+x+1)^t h(x) \sum_{j=p^s-i}^{p^s-1}(a_{0j}x + b_{0j})(x^2+x+1)^j
\end{aligned}$$

$$= (x^2+x+1)^i \sum_{j=0}^{p^s-i-1} (a_{0j}x + b_{0j})(x^2+x+1)^j$$

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

$$+ u(x^2+x+1)^t h(x) \sum_{j=0}^{p^s-i-1} (a_{0j}x + b_{0j})(x^2+x+1)^j$$

$$+ u(x^2+x+1)^t h(x) \sum_{j=p^s-i}^{p^s-1} (a_{0j}x + b_{0j})(x^2+x+1)^j.$$

We see that $(x^2+x+1)^i \sum_{j=0}^{p^s-i-1}(a_{0j}x + b_{0j})(x^2+x+1)^j = 0$, implying that $a_{0j} = b_{0j} = 0$ for all $0 \le j \le p^s - i - 1$. Thus,

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

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

$$\times (x^2+x+1)^j.$$

Therefore, $T \ge \min\{i, p^s - i + t\}$. Moreover,

$$[(x^2+x+1)^i + u(x^2+x+1)^t h(x)](x^2+x+1)^{p^s-1} = u(x^2+x+1)^{p^s-i+t} h(x).$$

Hence,

$$u(x^2+x+1)^{p^s-i+t}$$
$$= [(x^2+x+1)^i + u(x^2+x+1)^t h(x)](x^2+x+1)^{p^s-i} h(x)^{-1} \in C.$$

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

We now investigate the dual codes and determine the annihilator of I, where I is an ideal of the ring $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. We need to give the following lemma.

Lemma 3.15. *Let I be an ideal of the ring $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. If $I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x), u(x^2+x+1)^\omega \rangle$, where $h(x)$ is 0 or a unit, then $p^s - i$ is the smallest positive integer r such that $u(x^2+x+1)^r \in \mathcal{A}(I)$.*

Proof. Since $(x^2+x+1)^i + u(x^2+x+1)^t h(x) \in I$ and $u(x^2+x+1)^r \in \mathcal{A}(I)$, we have

$$0 = [(x^2+x+1)^i + u(x^2+x+1)^t h(x)]u(x^2+x+1)^r = u(x^2+x+1)^{i+r}.$$

We see that $i + r \geq p^s$. So, we have the smallest value of r is $p^s - i$. Hence, $u(x^2+x+1)^{p^s-i} \in \mathcal{A}(I)$. □

Theorem 3.16. *Let $I = \langle u(x^2+x+1)^i \rangle$ be an ideal of the ring $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. Then $\mathcal{A}(I)^* = \langle (x^2+x+1)^{p^s-i}, u \rangle$.*

Proof. Since $I \subseteq \langle u \rangle$ and $I \subseteq \langle (x^2+x+1)^i \rangle$, we have $\langle (x^2+x+1)^{p^s-i} \rangle = \mathcal{A}(\langle (x^2+x+1)^i \rangle) \subseteq \mathcal{A}(I)$ and $\langle u \rangle = \langle u \rangle^\perp \subseteq \mathcal{A}(I)$. This implies that $\langle (x^2+x+1)^{p^s-i}, u \rangle \subseteq \mathcal{A}(I)$. The other inclusion follows from the fact that the coefficient vector of $(x^2+x+1)^{p^s-i}$ is orthogonal to the coefficient vector of $u(x^2+x+1)^i$ and all its constacyclic shift. Thus, $\mathcal{A}(I) = \langle (x^2+x+1)^{p^s-i}, u \rangle$. By Lemma 2.7, we have $\mathcal{A}(I)^* = \langle (x^2+x+1)^{p^s-i}, u \rangle$. □

Theorem 3.17. *Let $I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x) \rangle$, where $h(x)$ is 0 or a unit. Then $\mathcal{A}(I)^*$ is determined as follows:*

(i) *If $h(x)$ is 0, then $\mathcal{A}(I)^* = \langle (x^2+x+1)^{p^s-i} \rangle$.*

(ii) *If $1 \leq i \leq \frac{p^s+t}{2}$ and $h(x)$ is a unit, then*

$$\mathcal{A}(I)^* = \Bigg\langle (x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s-2i+t}(x^2-1) \times \sum_{j=0}^{i-t-1} b_j(x^2+x+1)^j - u(x^2+x+1)^{p^s-2i+t} \times \sum_{j=0}^{i-t-1} (a_j x + b_j)(x^2+x+1)^j \Bigg\rangle,$$

where $h(x) = \sum_j (a_j x + b_j)(x^2+x+1)^j$, $a_j, b_j \in \mathbb{F}_{p^m}$ and $a_0, b_0 \neq 0$.

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

$$b(x) = (x^2+x+1)^{i-t} - ux^{4i-2p^s-2t-1} \sum_{j=0}^{p^s-i-1} (b_j x + a_j)(x^2+x+1)^j.$$

Proof. The proof of (i) is obvious. We will prove the case (ii).

Since

$$[(x^2+x+1)^i + u(x^2+x+1)^t h(x)] \times [(x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s-2i+t}h(x)] = 0,$$

we have

$$\langle (x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s-2i+t}h(x)\rangle \subseteq \mathcal{A}(I).$$

Let $\mathcal{A}(I) = \langle f(x), u(x^2+x+1)^k\rangle$, where $f(x) = (x^2+x+1)^a + u(x^2+x+1)^b g(x)$, $0 \le a, b, k \le p^s - 1$ and $g(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. By Lemma 3.15, $p^s - i$ is the smallest integer such that $u(x^2+x+1)^{p^s-i} \in \mathcal{A}(I)$. Therefore, $k = p^s - i$. Since

$$\begin{aligned} 0 &= f(x)[(x^2+x+1)^i + u(x^2+x+1)^t h(x)] \\ &= [(x^2+x+1)^a + u(x^2+x+1)^b g(x)][(x^2+x+1)^i + u(x^2+x+1)^t h(x)] \\ &= (x^2+x+1)^{a+i} + u(x^2+x+1)^{a+t}h(x) + u(x^2+x+1)^{b+i}g(x), \end{aligned}$$

we have $a + i \ge p^s$. So we can take $a = p^s - i$. Then we have $b = p^s - 2i + t$ and $g(x) = -h(x)$. This implies that

$$\mathcal{A}(I) = \langle (x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s+t-2i}h(x), u(x^2+x+1)^{p^s-i}\rangle.$$

Since $u(x^2+x+1)^{p^s-i} \in \langle (x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s+t-2i}h(x)\rangle$, we can see that $\mathcal{A}(I) = \langle (x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s+t-2i}h(x)\rangle$. Let $h(x) = \sum_j (a_j x + b_j)(x^2+x+1)^j$, where $a_0 x + b_0 \ne 0$ and $a_j, b_j \in \mathbb{F}_{p^m}$. Since $1 \le i \le \frac{p^s+t}{2}$ and property of T, we have $t + j < T = \min\{i, p^s - i + t\} = i$. So, $j \le i - t - 1$.

Let $l(x) = (x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s-2i+t}\sum_{j=0}^{i-t-1}(a_j x + b_j)(x^2+x+1)^j$. By Lemma 2.7, we get that

$$\begin{aligned} l^*(x) &= (x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s-2i+t} x \sum_{j=0}^{i-t-1}(b_j x + a_j)(x^2+x+1)^j \\ &= (x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s-2i+t} \sum_{j=0}^{i-t-1}(b_j x^2 + a_j x)(x^2+x+1)^j \\ &= (x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s-2i+t} \\ &\quad \times \sum_{j=0}^{i-t-1}(b_j(x^2-1) + a_j x + b_j)(x^2+x+1)^j \\ &= (x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s-2i+t}(x^2-1)\sum_{j=0}^{i-t-1} b_j(x^2+x+1)^j \\ &\quad - u(x^2+x+1)^{p^s-2i+t}\sum_{j=0}^{i-t-1}(a_j x + b_j)(x^2+x+1)^j. \end{aligned}$$

Hence,

$$\mathcal{A}(I)^* = \Big\langle (x^2+x+1)^{p^s-i} - u(x^2+x+1)^{p^s-2i+t}(x^2-1)\sum_{j=0}^{i-t-1} b_j(x^2+x+1)^j - u(x^2+x+1)^{p^s-2i+t}\sum_{j=0}^{i-t-1}(a_jx+b_j)(x^2+x+1)^j \Big\rangle.$$

The proof of (ii) is complete. Finally, we will show proof of (iii). It is similar to (ii), we have $\mathcal{A}(I) = \langle f(x), u(x^2+x+1)^{p^s-i}\rangle$, where $f(x) = (x^2+x+1)^a + u(x^2+x+1)^b g(x)$, $0 \le a, b \le p^s-1$ and $g(x) \in \frac{R[x]}{\langle (x^2+x+1)^{p^s}\rangle}$. Since $\frac{p^s+t}{2} < i \le p^s-1$, we obtain that $p^s - i < i - t$. Now, we consider that

$$\begin{aligned} 0 &= f(x)[(x^2+x+1)^i + u(x^2+x+1)^t h(x)] \\ &= [(x^2+x+1)^a + u(x^2+x+1)^b g(x)][(x^2+x+1)^i + u(x^2+x+1)^t h(x)] \\ &= (x^2+x+1)^{a+i} + u(x^2+x+1)^{a+t}h(x) + u(x^2+x+1)^{b+i}g(x), \end{aligned}$$

and then $a \ge p^s - i$. So, we choose $a = i - t$. We need b and $g(x)$ such that

$$u(x^2+x+1)^i h(x) + u(x^2+x+1)^{b+i}g(x) = 0.$$

Thus, we choose $b = 0$ and $g(x) = -h(x)$. This implies that

$$\mathcal{A}(I) = \langle (x^2+x+1)^{i-t} - uh(x), u(x^2+x+1)^{p^s-i}\rangle$$

Let $h(x) = \sum_j (a_jx+b_j)(x^2+x+1)^j$, where $a_0, b_0 \ne 0$ and $a_j, b_j \in \mathbb{F}_{p^m}$. Since $\frac{p^s+t}{2} < i \le p^s-1$ and $t+j < T = \min\{i, p^s-i+t\} = p^s-i+t$, we have $j \le p^s-i-1$. Let

$$l_2(x) = (x^2+x+1)^{i-t} - u\sum_{j=0}^{p^s-i-1}(a_jx+b_j)(x^2+x+1)^j.$$

Then

$$l_2^*(x) = (x^2+x+1)^{i-t} - ux^{4i-2t-2p^s+1} \times \sum_{j=0}^{p^s-i-1}(b_jx+a_j)(x^2+x+1)^j.$$

Therefore,

$$\mathcal{A}(I)^* = \Big\langle (x^2+x+1)^{i-t} - ux^{4i-2t-2p^s+1} \times \sum_{j=0}^{p^s-i-1}(b_jx+a_j)(x^2+x+1)^j, u(x^2+x+1)^{p^s-i}\Big\rangle. \qquad \square$$

Theorem 3.18. *Let* $I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x), u(x^2+x+1)^\omega \rangle$, *where* $h(x)$ *is* 0 *or a unit. Then* $\mathcal{A}(I)^*$ *is determined as follows*:

(i) *If* $h(x) = 0$, *then* $\mathcal{A}(I)^* = \langle (x^2+x+1)^{p^s-\omega}, u(x^2+x+1)^{p^s-i} \rangle$.
(ii) *If* $h(x)$ *is a unit, then* $\mathcal{A}(I)^* = \langle d(x), u(x^2+x+1)^{p^s-i} \rangle$, *where*

$$d(x) = (x^2+x+1)^{p^s-\omega} - ux^{2i-2\omega+1}(x^2+x+1)^{p^s-i-\omega+t} \times \sum_{j=0}^{\omega-t-1} (b_j x + a_j)(x^2+x+1)^j.$$

Proof. The proof of (i) is obvious. We will prove the case (ii). A simple calculation shows that

$$I = \langle (x^2+x+1)^{p^s-\omega} - u(x^2+x+1)^{p^s-i-\omega+t} h(x), u(x^2+x+1)^{p^s-i} \rangle \subseteq \mathcal{A}(I)$$

and $n_I = p^{2m(i+\omega)}$. Then

$$p^{2m(i+\omega)} = n_I \leq |\mathcal{A}(I)| \leq |\mathcal{A}(I)^*| = \frac{p^{4mp^s}}{n_I} = \frac{p^{4mp^s}}{p^{2m(2p^s-i-\omega)}} = p^{2m(i+\omega)}.$$

Therefore, $\langle (x^2+x+1)^{p^s-\omega} - u(x^2+x+1)^{p^s-i-\omega+t} h(x), u(x^2+x+1)^{p^s-i} \rangle = \mathcal{A}(I)$. Let $h(x) = \sum_j (a_j x + b_j)(x^2+x+1)^j$, where $a_0 x + b_0 \neq 0$ and $a_j, b_j \in \mathbb{F}_{p^m}$. In this case, we have $j \leq \omega - t - 1$. Let $d(x) = (x^2+x+1)^{p^s-\omega} - u(x^2+x+1)^{p^s-i-\omega+t} \sum_{j=0}^{\omega-t-1} (a_j x + b_j)(x^2+x+1)^j$. By Lemma 2.7, we get that

$$d(x)^* = (x^2+x+1)^{p^s-\omega} - u(x^2+x+1)^{p^s-i-\omega+t} x^{2i-2\omega+1} \times \sum_{j=0}^{\omega-t-1} (b_j x + a_j)(x^2+x+1)^j.$$

Hence,

$$\mathcal{A}(I)^* = \left\langle (x^2+x+1)^{p^s-\omega} - u(x^2+x+1)^{p^s-i-\omega+t} x^{2i-2\omega+1} \times \sum_{j=0}^{\omega-t-1} (b_j x + a_j)(x^2+x+1)^j, u(x^2+x+1)^{p^s-i} \right\rangle.$$

The proof is complete. □

4. The Number of Cyclic Codes and Their Self-Dual Codes of Length $3p^s$ Over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

In this section, we separate structures of self-dual cyclic codes of length $3p^s$ over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ into 2 cases, i.e., $p^m \equiv 1 \pmod 3$ and $p^m \equiv 2 \pmod 3$.

4.1. *The case* $p^m \equiv 1 \pmod 3$

In paper [7, 17], the number of constacyclic codes and their self-dual codes of length p^s over R are obtained.

Theorem 4.1 ([7, 17]). *The number of distinct constacyclic codes of length p^s over R is equal to*

- $\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}}-2p^{2m}-2}{(p^m-1)^2} + \frac{(2p^m+3)(p^m)^{\frac{p^s-1}{2}}-2p^s-1}{p^m-1} + (p^m)^{\frac{p^s-1}{2}} + 2$ *if p is an odd prime.*
- $\frac{2^{m(2^{s-1}-1)}(2^{2m}+2^m+2)-2^{2m+1}-2}{(2^m-1)^2} + \frac{6\cdot 2^{m(2^s-1)}-2^{s+1}-1}{2^m-1} + 2^{m2^{s-1}} + 4\cdot 2^{m(2^{s-1}-1)} + 3\cdot 2^{s-1} - 1$ *if $p = 2$.*

Applying Theorem 3.2, the number of distinct cyclic codes of length $3p^s$ over R is obtained as the following theorem.

Theorem 4.2. *Let $p^m \equiv 1 \pmod 3$. Then the number of distinct cyclic codes of length $3p^s$ over R is equal to*

- $(\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}}-2p^{2m}-2}{(p^m-1)^2} + \frac{(2p^m+3)(p^m)^{\frac{p^s-1}{2}}-2p^s-1}{p^m-1} + (p^m)^{\frac{p^s-1}{2}} + 2)^3$ *if p is an odd prime.*
- $(\frac{2^{m(2^{s-1}-1)}(2^{2m}+2^m+2)-2^{2m+1}-2}{(2^m-1)^2} + \frac{6\cdot 2^{m(2^s-1)}-2^{s+1}-1}{2^m-1} + 2^{m2^{s-1}} + 4\cdot 2^{m(2^{s-1}-1)} + 3\cdot 2^{s-1} - 1)^3$ *if $p = 2$.*

Proof. By Theorem 3.2, we obtain that the number of distinct cyclic codes of length $3p^s$ over R is the number to the third power of distinct constacyclic codes of length p^s. By Theorem 4.1, the number of distinct cyclic codes of length $3p^s$ is obtained. □

Next, we determine the number of distinct self-dual cyclic codes of length $3p^s$ over R. We recall the result about dual cyclic codes of length $3p^s$.

For any $\alpha \in \mathbb{F}_{p^m}$ with $\alpha \neq \alpha^{-1}$, we obtain that self-dual code of each α-constacyclic code of length p^s over R is unique, i.e., $\langle u \rangle$ (see [17]). Moreover, the number of distinct self-dual cyclic codes of length p^s over R are obtained in [17].

As the fact $\delta_i^{-1} \neq \delta_i$ for $i = 1, 2$, we get the self-dual code of δ_1, δ_2-constacyclic codes of length p^s are $\langle u \rangle$ and then, the number of self-dual cyclic codes of length $3p^s$ over R is obtained as the following theorem.

Theorem 4.3. *Let $p^m \equiv 1 \pmod 3$. Then the number of self-dual cyclic codes of length $3p^s$ over R is equal to the number of self-dual of cyclic codes of length p^s over R.*

Proof. By Theorem 3.3, we obtain that each self-dual cyclic code of length $3p^s$ is a direct sum of a cyclic code, δ_1, δ_2-constacyclic codes of length p^s over R. Since

$\delta_1 \neq \delta_1^{-1}$ and $\delta_2 \neq \delta_2^{-1}$, we have self-dual δ_1, δ_2-constacyclic codes are $\langle u \rangle$. Hence, the number of self-dual cyclic codes of length $3p^s$ is the number of self-dual cyclic codes of length p^s over R. □

4.2. *The case* $p^m \equiv 2 \pmod 3$

The number of distinct cyclic codes of length $3p^s$ over R is a product of the number of distinct cyclic codes of length p^s over R and the number of distinct ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. In [7, 17], the number of distinct cyclic codes of length p^s over R are obtained.

The remaining part, we determine the number of distinct ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. By Theorem 3.13, we classify all ideals of such ring into 4 types.

Case 1: p is an odd prime.

First of all, we obtain 2 ideals of trivial type. In type 2, the number of distinct ideals $\langle u(x^2+x+1)^i \rangle$, where $0 \leq i \leq p^s - 1$ is p^s. In type 3, we separate this type into 2 cases, i.e., $h(x) = 0$ and $h(x)$ is a unit. If $h(x) = 0$, the number of ideals $\langle (x^2+x+1)^i \rangle$, where $1 \leq i \leq p^s - 1$ is p^s. If $h(x)$ is a unit, we have $h(x) = \sum_j (h_{1j}x + h_{0j})(x^2+x+1)^j$, where $h_{0j}, h_{1j} \in \mathbb{F}_{p^m}$ and $h_{10}x + h_{00} \neq 0$. Clearly, $t + j < T = \min\{i, p^s - i + t\}$ and then, $j \leq T - t - 1$. Thus, the number of distinct ideals of this type is

$$\begin{aligned}
&\sum_{i=1}^{\frac{p^s-1}{2}} \sum_{t=0}^{i-1} (p^{2m}-1)(p^{2m})^{i-t-1} + \sum_{i=\frac{p^s+1}{2}}^{p^s-1} \sum_{t=0}^{2i-p^s-1} (p^{2m}-1)(p^{2m})^{p^s-i-1} \\
&\quad + \sum_{i=\frac{p^s+1}{2}}^{p^s-1} \sum_{t=2i-p^s}^{i-1} (p^{2m}-1)(p^{2m})^{i-t-1} \\
&= \sum_{i=1}^{\frac{p^s-1}{2}} (p^{2mi}-1) + (p^{2m}-1) \sum_{i=\frac{p^s+1}{2}}^{p^s-1} (2i-p^s)(p^{2m})^{p^s-i-1} \\
&\quad + \sum_{i=\frac{p^s+1}{2}}^{p^s-1} (p^{2m(p^s-i)}-1) \\
&= \frac{2p^{2m}(p^{2m(\frac{p^s-1}{2})}-1) + 2p^{2m}(p^{2m(\frac{p^s-1}{2}-1)}-1)}{p^{2m}-1} + p^{2m(\frac{p^s-1}{2})} - 2p^s + 3 \\
&= \frac{2(p^{2m}+1)(p^{2m})^{\frac{p^s-1}{2}} - 4}{p^{2m}-1} + (p^{2m})^{\frac{p^s-1}{2}} - 2p^s - 1.
\end{aligned}$$

In type 4, we separate this type into 2 cases, i.e., $h(x) = 0$ and $h(x)$ is a unit. If $h(x) = 0$, the number of distinct ideals $\langle (x^2+x+1)^i, u(x^2+x+1)^\omega \rangle$, where

$1 \leq i \leq p^s - 1$ and $0 \leq \omega < T = i$, is

$$\sum_{i=1}^{p^s-1} i = \frac{(p^s-1)(p^s)}{2}.$$

If $h(x) = 0$, we determine the number of distinct ideals of form $\langle (x^2+x+1)^i + u(x^2+x+1)^t h(x), u(x^2+x+1)^\omega \rangle$, where $1 \leq i \leq p^s - 1, 0 \leq t < i, 0 \leq \omega < T$ and $h(x)$ is a unit. Since $t + j < \omega$ and $0 \leq j \leq \omega - t - 1$, we have the number of distinct ideals of this form is

$$\sum_{i=2}^{\frac{p^s-1}{2}} \sum_{t=0}^{i-1} \sum_{\omega=t+1}^{i-1} (p^{2m}-1)(p^{2m})^{\omega-t-1} + \sum_{i=\frac{p^s+1}{2}}^{p^s-2} \sum_{t=0}^{2i-p^s-1} \sum_{\omega=t+1}^{p^s-i+t-1} (p^{2m}-1)(p^{2m})^{\omega-t-1}$$

$$+ \sum_{i=\frac{p^s+1}{2}}^{p^s-1} \sum_{t=2i-p^s}^{i-2} \sum_{\omega=t+1}^{i-1} (p^{2m}-1)(p^{2m})^{\omega-t-1}$$

$$= \frac{2(p^{2m}+1)(p^{2m})^{\frac{p^s-1}{2}} - 2p^{4m} - 2}{(p^{2m}-1)^2} + \frac{(p^{2m})^{\frac{p^s-1}{2}} - 2p^s + 3}{p^{2m}-1} + \frac{p^s - p^{2s}}{2} + 2.$$

Hence, we obtain that the number of distinct ideals when p is an odd prime is equal to

$$\frac{2(p^{2m}+1)(p^{2m})^{\frac{p^s-1}{2}} - 2p^{4m} - 2}{(p^{2m}-1)^2} + \frac{(2p^{2m}+3)(p^{2m})^{\frac{p^s-1}{2}} - 2p^s - 1}{p^{2m}-1}$$

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

Case 2: $p = 2$.

Clearly, we obtain 2 ideals in trivial type and the number of distinct ideals $\langle u(x^2+x+1)^i \rangle$, where $0 \leq i \leq 2^s - 1$ is 2^s in type 2. Now, in type 3, we separate this type into 2 cases, i.e., $h(x) = 0$ and $h(x)$ is a unit. If $h(x)$ is a unit, the number of distinct ideals $\langle (x^2+x+1)^i \rangle$, where $1 \leq i \leq 2^s - 1$ is $2^s - 1$. If $h(x)$ is a unit, then $h(x) = \sum_j (h_{1j}x + h_{0j})(x^2+x+1)^j$ where $h_{1j}, h_{2j} \in \mathbb{F}_{p^m}$ and $h_{1j}x + h_{0j} \neq 0$. Note that $t + j < T = \min\{i, 2^s - i + t\}$. This means that $j \leq T - t - 1$. Thus, the number of distinct ideals of this type is

$$\sum_{i=1}^{2^{s-1}} \sum_{t=0}^{i-1} (2^{2m}-1)(2^{2m})^{i-t-1} + \sum_{i=2^{s-1}+1}^{2^s-1} \sum_{t=0}^{2i-2^s-1} (2^{2m}-1)(2^{2m})^{2^s-i-1}$$

$$+ \sum_{i=2^{s-1}+1}^{2^s-1} \sum_{t=2i-2^s}^{2^s-1} (2^{2m}-1)(2^{2m})^{i-t-1}$$

$$= 2^{2m(2^{s-1})} + 2^{2m(2^{s-1}-1)+2} - 2^{s+1} - 1.$$

Finally, we separate type 4 into 2 cases, i.e., $h(x) = 0$ and $h(x)$ is a unit. If $h(x) = 0$, then $T = i$. Thus, the number of distinct ideals $\langle (x^2+x+1)^i, u(x^2+x+1)^\omega \rangle$,

where $1 \leq i \leq 2^s - 1$ and $\omega < T = i$ is

$$\sum_{i=1}^{2^s-1} i = \frac{(2^s-1)2^s}{2} = (2^s-1)2^{s-1}.$$

If $h(x)$ is a unit, then $h(x) = \sum_j (h_{1j}x + h_{0j})(x^2+x+1)^j$, where $h_{1j}, h_{0j} \in \mathbb{F}_{p^m}$ and $h_{10}x + h_{00} \neq 0$. Note that $t + j < \omega$, or equivalently, $j \leq \omega - t - 1$. Thus, the number of distinct ideals is

$$\begin{aligned}
&\sum_{i=2}^{2^{s-1}} \sum_{t=0}^{i-2} \sum_{\omega=t+1}^{i-1} (2^{2m}-1)(2^{2m})^{\omega-t-1} \\
&\quad + \sum_{i=2^{s-1}+1}^{2^s-2} \sum_{t=0}^{2i-2^s-1} \sum_{\omega=t+1}^{2^s-i+t-1} (2^{2m}-1)(2^{2m})^{\omega-t-1} \\
&\quad + \sum_{i=2^{s-1}+1}^{2^s-2} \sum_{t=2i-2^s}^{i-2} \sum_{\omega=t+1}^{i-1} (2^{2m}-1)(2^{2m})^{\omega-t-1} \\
&= \frac{2^{2m(2^{s-1}-1)}(2^{4m}+2^{2m}+2) - 2^{4m+1} - 2}{(2^{2m}-1)^2} + \frac{2^{m(2^{s-1}-1)+1} - 2^{s+1} + 3}{2^{2m}-1} \\
&\quad + 2^{2s-1} + 2^{s+1} - 1.
\end{aligned}$$

Hence, we obtain that the number of distinct ideals when $p = 2$ is

$$\begin{aligned}
&\frac{2^{2m(2^{s-1}-1)}(2^{4m}+2^{2m}+2) - 2^{4m+1} - 2}{(2^{2m}-1)^2} + \frac{6 \cdot 2^{2m(2^s-1)} - 2^{s+1} - 1}{2^{2m}-1} + 2^{m2^{s-1}} \\
&\quad + 4 \cdot 2^{2m(2^{s-1}-1)} + 3 \cdot 2^{s-1} - 1. \qquad (4)
\end{aligned}$$

Therefore, we obtain all distinct cyclic codes of length $3p^s$ over R as follows.

Theorem 4.4. *Let $p^m \equiv 2 \pmod 3$. Then the number of distinct cyclic codes of length $3p^s$ over R is*

- $$\begin{aligned}
&\left(\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}} - 2p^{2m} - 2}{(p^m-1)^2} + \frac{(2p^m+3)(p^m)^{\frac{p^s-1}{2}} - 2p^s - 1}{p^m-1} \right. \\
&\quad \left. + (p^m)^{\frac{p^s-1}{2}} + 2 \right) \times \left(\frac{2(p^{2m}+1)(p^{2m})^{\frac{p^s-1}{2}} - 2p^{4m} - 2}{(p^{2m}-1)^2} \right. \\
&\quad \left. + \frac{(2p^{2m}+3)(p^{2m})^{\frac{p^s-1}{2}} - 2p^s - 1}{p^{2m}-1} + (p^{2m})^{\frac{p^s-1}{2}} + 2 \right)
\end{aligned}$$

if p is an odd prime.

- $$\left(\frac{2^{m(2^{s-1}-1)}(2^{2m}+2^m+2)-2^{2m+1}-2}{(2^m-1)^2}+\frac{6\cdot 2^{m(2^s-1)}-2^{s+1}-1}{2^m-1}\right.$$
$$\left.+2^{m2^{s-1}}+4\cdot 2^{m(2^{s-1}-1)}+3\cdot 2^{s-1}-1\right)$$
$$\times\left(\frac{2^{2m(2^{s-1}-1)}(2^{4m}+2^{2m}+2)-2^{4m+1}-2}{(2^{2m}-1)^2}+\frac{6\cdot 2^{2m(2^s-1)}-2^{s+1}-1}{2^{2m}-1}\right.$$
$$\left.+2^{m2^{s-1}}+4\cdot 2^{2m(2^{s-1}-1)}+3\cdot 2^{s-1}-1\right)$$

if $p=2$.

In case p is an odd prime, suppose that -3 is a square element in R, there exists $\alpha\in R$ such that $\alpha^2=-3$. We consider that

$$\begin{aligned}((-1+\alpha)2^{-1})^2+(-1+\alpha)2^{-1}+1&=(-1-2\alpha-3)2^{-2}+(-1+\alpha)2^{-1}+1\\&=(-1-\alpha)2^{-1}+(-1+\alpha)2^{-1}+1\\&=0.\end{aligned}$$

It is a contradiction by Lemma 3.6. Thus, -3 is not a square which means that x^2+3 is irreducible over R.

Proposition 4.5. *Let* $p^m\equiv 2 \pmod 3$ *and* $\Phi:\frac{R[x]}{\langle(x^2+x+1)^{p^s}\rangle}\to\frac{R[x]}{\langle x^{2p^s}+(3\cdot 2^{-2})^{p^s}\rangle}$ *by* $\Phi(f(x))=f(x-2^{-1})$, *where* $p\neq 2$ *and* $f(x)\in\frac{R[x]}{\langle(x^2+x+1)^{p^s}\rangle}$. *Then* Φ *is an isomorphism.*

Proof. First of all, we will show that ϕ is well-defined and one-to-one. For polynomials $f(x)$ and $g(x)\in R[x], f(x)\equiv g(x) \pmod{(x^2+x+1)^{p^s}}$ if and only if there exists a polynomial $h(x)\in R[x]$ such that $f(x)-g(x)=h(x)(x^2+x+1)^{p^s}$, if and only if

$$\begin{aligned}f(x-2^{-1})-g(x-2^{-1})&=h(x-2^{-1})((x-2^{-1})^2+x-2^{-1}+1)^{p^s}\\&=h(x-2^{-1})(x^2-x+2^{-2}+x-2^{-1}+1)^{p^s}\\&=h(x-2^{-1})(x^2+3\cdot 2^{-2})^{p^s}\\&=h(x-2^{-1})(x^{2p^s}+(3\cdot 2^{-2})^{p^s}),\end{aligned}$$

which is equivalent to $f(x-2^{-1})\equiv g(x-2^{-1}) \pmod{(x^2+x+1)^{p^s}}$. Since $\Phi(f(x))-\Phi(g(x))=f(x)-g(x)$, we have, for $f(x),g(x)\in\frac{R[x]}{\langle(x^2+x+1)^{p^s}\rangle}$, $\Phi(f(x))=\Phi(g(x))$ if and only if $f(x-2^{-1})=g(x-2^{-1})$. Therefore, Φ is well defined and one-to-one. Next, it is a routine to show that Φ is onto and homomorphism. Hence, Φ is a ring isomorphism. □

Corollary 4.6. *Let $p^m \equiv 2 \pmod 3$ and C be a cyclic code of length $3p^s$ over R, where $p \neq 2$. Then*

(i) *$C = C_1 \oplus C_3$, where C_1 is a cyclic code of length p^s over R and C_3 is a $-(3 \cdot 2^{-2})^{p^s}$-constacyclic code of length $2p^s$ over R. Moreover, $|C| = |C_1||C_3|$.*

(ii) *The dual code $C^\perp$ of C can be expressed as $C^\perp = C_1^\perp \oplus C_3^\perp$, where C_1 is a cyclic code of length p^s over R and C_3 is a $-(3 \cdot 2^{-2})^{p^s}$-constacyclic code of length $2p^s$ over R. Moreover, $|C^\perp| = |C_1^\perp||C_3^\perp|$.*

The structures of $-(3 \cdot 2^{-2})^{p^s}$-constacyclic codes of length $2p^s$ over R are obtained see in [4]. Moreover, the number of this constacyclic codes of $2p^s$ over R as the following theorem.

Theorem 4.7 ([4]). *The number of distinct $-(3 \cdot 2^{-2})^{p^s}$-constacyclic codes of length $2p^s$ over R is equal to*

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

From Eq. (3), we notice that the number of distinct ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ in Theorem 4.4 is equal to the number of $-(3 \cdot 2^{-2})^{p^s}$-constacyclic codes of length $2p^s$ over R.

In $p^m \equiv 2 \pmod 3$, we determine the condition $-(3 \cdot 2^{-2})^{p^s} = [-(3 \cdot 2^{-2})^{p^s}]^{-1}$ if and only if

$$\begin{aligned}(3 \cdot 2^{-2})^{2p^s} &= 1,\\ 3^{2p^s} &= 4^{2p^s},\\ (3-4)^{p^s}(3+4)^{p^s} &= 0,\\ 7^{p^s} &= 0.\end{aligned}$$

This means that the characteristic of R is equal to $p = 7$ if and only if $-(3 \cdot 2^{-2})^{p^s} = [-(3 \cdot 2^{-2})^{p^s}]^{-1}$. However, $7^m \equiv 1 \pmod 3$ for any positive integer m. Thus, this condition does not exist implying that $-(3 \cdot 2^{-2})^{p^s} \neq [-(3 \cdot 2^{-2})^{p^s}]^{-1}$, for any $p^m \equiv 2 \pmod 3$ with $p \neq 2$. Therefore, we divide them into 2 cases, i.e., the case $p^m \equiv 2 \pmod 3$ with $p \neq 2$ and the case $p^m \equiv 2 \pmod 3$ with $p = 2$ for self-dual codes.

4.2.1. *The subcase $p^m \equiv 2 \pmod 3$ with $p \neq 2$*

First of all, we give the condition of existence of self-dual constacyclic codes of length n over a finite commutative chain ring.

Proposition 4.8 ([16]). *Let λ be a unit of the chain ring R with maximal ideal $\langle r \rangle$, such that $\lambda - \lambda^{-1}$ is a unit. Then there exists a self-dual λ-constacyclic code C*

of length n over R if and only if N_r is even. In such case, the number of C is $\frac{N_r}{2}$, and $C = \langle \gamma^{\frac{N_r}{2}} \rangle$ is the unique self-dual constacyclic code of length n over R.

In this subcase, as $-(3 \cdot 2^{-2})^{p^s} \neq [-(3 \cdot 2^{-2})^{p^s}]^{-1}$, we obtain that $\langle u \rangle$ is the unique self-dual code of $-(3 \cdot 2^{-2})^{p^s}$-constacyclic codes of length $2p^s$ over R. By Corollary 4.6, the number of self-dual cyclic codes of length p^s over R as follows.

Theorem 4.9. *Let $p^m \equiv 2 \pmod 3$ with $p \neq 2$. Then the number of self-dual cyclic codes of length $3p^s$ over R is the number of self-dual of cyclic codes of length p^s over R.*

4.2.2. *The subcase $p^m \equiv 2 \pmod 3$ with $p = 2$*

We determine the number of self-dual cyclic codes of length $3 \cdot 2^s$ over R. From Theorem 3.7, we obtain the following theorem.

Theorem 4.10. *The number of self-dual cyclic codes of length $3 \cdot 2^s$ over R is the product of the number of self-dual of cyclic codes of length 2^s over R and the number of distinct ideals I of $\frac{R[x]}{\langle (x^2+x+1)^{2^s} \rangle}$ which $I = \mathcal{A}(I)^*$.*

Finally, we focus on ideals of $\frac{R[x]}{\langle (x^2+x+1)^{2^s} \rangle}$ for the situation each ideal I of $\frac{R[x]}{\langle (x^2+x+1)^{2^s} \rangle}$, $I = \mathcal{A}(I)^*$. We consider each ideals of such ring into 4 types from Theorem 3.13. Clearly, all ideals in trivial type, $\langle 0 \rangle$ and $\langle 1 \rangle$ are not satisfied the situation.

Proposition 4.11. *Let $I = \langle u(x^2+x+1)^i \rangle$, where $0 \leq i \leq 2^s - 1$ be an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{2^s} \rangle}$. Then $I = \mathcal{A}(I)^*$ if and only if $i = 0$, that is, $I = \langle u \rangle$.*

Proof. Suppose that $I = \mathcal{A}(I)^*$. If $i \neq 0$, Theorem 3.16, we get $\mathcal{A}(I)^* = \langle u, (x^2+x+1)^{2^s-i} \rangle$. This implies that $u \in \langle u(x^2+x+1)^i \rangle$. There exists $f(x) = \sum_{j=0}^{2^s-1}(a_{0j}x + b_{0j})(x^2+x+1)^j + u\sum_{j=0}^{2^s-1}(a_{1j}x + b_{1j})(x^2+x+1)^j \in \frac{R[x]}{\langle (x^2+x+1)^{2^s} \rangle}$ such that

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

Thus, $(x^2+x+1)^i \sum_{j=0}^{2^s-1}(a_{0j}x + b_{0j})(x^2+x+1)^j = 1$. This means that x^2+x+1 is invertible. It is a contradiction. Therefore, $i = 0$ which implies that $I = \langle u \rangle$. Conversely, suppose that $i = 0$. Clearly,

$$I = \langle u(x^2+x+1)^i \rangle = \langle u \rangle$$

and

$$\mathcal{A}(I)^* = \langle u, (x^2+x+1)^{2^s} \rangle = \langle u \rangle.$$

Therefore, we obtain that $I = \mathcal{A}(I)^*$. □

From the above proposition, we obtain that the situation for ideals in type 2. Next, the condition $I = \mathcal{A}(I)^*$ of all ideals in type 3 are determined in the following proposition.

Next, we consider that condition $I = \mathcal{A}(I)^*$ for $I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x)\rangle$, where $1 \leq i \leq 2^s - 1$ and $h(x)$ is 0 or a unit. For $h(x) = 0$, we have $I = \langle (x^2+x+1)^i\rangle$ and $\mathcal{A}(I)^* = \langle (x^2+x+1)^{2^s-i}\rangle$.

Proposition 4.12. *Let $I = \langle (x^2+x+1)^i\rangle$, where $1 \leq i \leq 2^s - 1$. Then $I = \mathcal{A}(I)^*$ if and only if $i = 2^{s-1}$.*

Proof. Suppose that $I = \mathcal{A}(I)^*$. Note that $I = \langle (x^2+x+1)^i\rangle = \mathcal{A}(I)^* = \langle (x^2+x+1)^{2^s-i}\rangle$. So,

$$(x^2+x+1)^i \in \langle (x^2+x+1)^{2^s-i}\rangle$$

and

$$(x^2+x+1)^{2^s-i} \in \langle (x^2+x+1)^i\rangle.$$

There exists $f(x), g(x) \in R[x]$ such that

$$(x^2+x+1)^{2^s-i} = (x^2+x+1)^i f(x)$$

and

$$(x^2+x+1)^i = (x^2+x+1)^{2^s-i} g(x).$$

This means that

$$\begin{aligned}(x^2+x+1)^{2^{s+1}-2i} &= (x^2+x+1)^{2^s-i}(x^2+x+1)^i f(x)\\ &= (x^2+x+1)^{2^s} f(x)\\ &= 0.\end{aligned}$$

$$\begin{aligned}(x^2+x+1)^{2i} &= (x^2+x+1)^i (x^2+x+1)^{2^s-i} g(x)\\ &= (x^2+x+1)^{2^s}\\ &= 0.\end{aligned}$$

So, $2^{s+1} - 2i \geq 2^s$ and $2i \geq 2^s$. Thus, $2i = 2^s$. Hence, $i = 2^{s-1}$. On the other hand, suppose that $i = 2^{s-1}$. Clearly, $I = \langle (x^2+x+1)^{2^{s-1}}\rangle = \langle (x^2+x+1)^{2^s-2^{s-1}}\rangle = \mathcal{A}(I)^*$. □

In type 3, we determine the condition of $I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x)\rangle$, $h(x)$ is a unit which satisfies $I = \mathcal{A}(I)^*$.

Proposition 4.13. *Let $I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x)\rangle$, where $h(x) = \sum_j (a_j x + b_j)(x^2+x+1)^j$ is a unit and $1 \leq i \leq 2^s - 1$. Then $I = \mathcal{A}(I)^*$ if and only if $i = 2^{s-1}$ and $b_j = 0$.*

Proof. Suppose that $I = \mathcal{A}(I)^*$. By Theorem 3.17, $\frac{2^s+t}{2} < i < 2^s$, $I \neq \mathcal{A}(I)^*$ because $\mathcal{A}(I)^*$ is not principal. In $0 < i \leq \frac{2^s+t}{2}$, we have

$$\mathcal{A}(I)^* = \Bigg\langle (x^2+x+1)^{2^s-i} - u(x^2+x+1)^{2^s-2i+t}(x^2-1)\sum_{j=0}^{i-t-1} b_j(x^2+x+1)^j - u(x^2+x+1)^{2^s-2i+t}\sum_{j=0}^{i-t-1}(a_jx+b_j)(x^2+x+1)^j \Bigg\rangle.$$

There exist $f_1(x), f_2(x) \in \mathbb{F}_{2^m}[x]$ such that

$$(x^2+x+1)^i + u(x^2+x+1)^t \sum_j (a_jx+b_j)(x^2+x+1)^j$$

$$= \Bigg((x^2+x+1)^{2^s-i} - u(x^2+x+1)^{2^s-2i+t}(x^2-1)\sum_{j=0}^{i-t-1} b_j(x^2+x+1)^j - u(x^2+x+1)^{2^s-2i+t}\sum_{j=0}^{i-t-1}(a_jx+b_j)(x^2+x+1)^j\Bigg)(f_1(x)+uf_2(x)).$$

Under modulo u, we have $(x^2+x+1)^i = (x^2+x+1)^{2^s-i}f_1(x)$ and then

$$(x^2+x+1)^{2i} = (x^2+x+1)^{2^s}f_1(x)$$
$$= 0.$$

So, $2i \geq 2^s$. Moreover, there exist $g_1(x), g_2(x) \in \mathbb{F}_{2^m}[x]$ such that

$$(x^2+x+1)^{2^s-i} - u(x^2+x+1)^{2^s-2i+t}(x^2-1)\sum_{j=0}^{i-t-1} b_j(x^2+x+1)^j$$
$$- u(x^2+x+1)^{2^s-2i+t}\sum_{j=0}^{i-t-1}(a_jx+b_j)(x^2+x+1)^j$$
$$= \Bigg((x^2+x+1)^i + u(x^2+x+1)^t\sum_j (a_jx+b_j)(x^2+x+1)^j\Bigg)$$
$$\times (g_1(x)+ug_2(x)).$$

Under Modulo u, we have

$$(x^2+x+1)^{2^s-i} = (x^2+x+1)^i g_1(x),$$

and then

$$(x^2+x+1)^{2^{s+1}-2i} = (x^2+x+1)^{2^s}g_1(x) = 0.$$

So, $2^{s+1} - 2i \geq 2^s$, i.e., $2^s \geq 2i$. Thus, $2i = 2^s$ which means that $i = 2^{s-1}$. Note that

$$I = \left\langle (x^2+x+1)^{2^{s-1}} + u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1} (a_j x + b_j)(x^2+x+1)^j \right\rangle$$

and

$$\mathcal{A}(I)^* = \left\langle (x^2+x+1)^{2^{s-1}} - u(x^2+x+1)^t(x^2-1) \sum_{j=0}^{2^{s-1}-t-1} b_j(x^2+x+1)^j \right.$$
$$\left. - u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1} (a_j x + b_j)(x^2+x+1)^j \right\rangle.$$

There exist $h_1(x), h_2(x) \in \mathbb{F}_{2^m}[x]$ such that

$$(x^2+x+1)^{2^{s-1}} + u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1} (a_j x + b_j)(x^2+x+1)^j$$
$$= \left((x^2+x+1)^{2^{s-1}} - u(x^2+x+1)^t(x^2-1) \sum_{j=0}^{2^{s-1}-t-1} b_j(x^2+x+1)^j \right.$$
$$\left. - u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1} (a_j x + b_j)(x^2+x+1)^j \right) (h_1(x) + uh_2(x)).$$

This implies that

$$(x^2+x+1)^{2^{s-1}} = (x^2+x+1)^{2^{s-1}} h_1(x)$$

and

$$u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1} (a_j x + b_j)(x^2+x+1)^j$$
$$= -u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1} ((x^2-1)b_j + (a_j x + b_j))(x^2+x+1)^j h_1(x)$$
$$+ u(x^2+x+1)^{2^{s-1}} h_2(x).$$

So, $h_1(x) = 1$ and

$$u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1} (a_j x + b_j)(x^2+x+1)^j$$

$$= -u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1} ((x^2-1)b_j + (a_jx+b_j))(x^2+x+1)^j$$

$$+ u(x^2+x+1)^{2^{s-1}} h_2(x),$$

implying that

$$u(x^2+x+1)^t \sum_{j=0}^{2^{s-1}-t-1} ((x^2-1)b_j)(x^2+x+1)^j = u(x^2+x+1)^{2^{s-1}} h_2(x).$$

Multiplying $(x^2+x+1)^{2^{s-1}}$ both sides,

$$u(x^2+x+1)^{t+2^{s-1}} \sum_{j=0}^{2^{s-1}-t-1} ((x^2-1)b_j)(x^2+x+1)^j = u(x^2+x+1)^{2^s} h_2(x) = 0.$$

This means that, for $0 \leq j \leq 2^{s-1}-t-1$, we get $b_j = 0$. Conversely, suppose that $i = 2^{s-1}$ and $b_j = 0$. It is easy to show that $I = \mathcal{A}(I)^*$. □

Finally, we determine the situation $I = \mathcal{A}(I)^*$, where $I = \langle (x^2+x+1)^i, u(x^2+x+1)^\omega \rangle$, where $1 \leq i \leq 2^s-1, \omega \leq i$.

Proposition 4.14. *Let $I = \langle (x^2+x+1)^i, u(x^2+x+1)^\omega \rangle$ for $1 \leq i \leq 2^s-1$. Then $I = \mathcal{A}(I)^*$ if and only if $i+\omega = 2^s$.*

Proof. Suppose that $I = \mathcal{A}(I)^*$. By Theorem 3.18, we have

$$\mathcal{A}(I)^* = \langle (x^2+x+1)^{2^s-\omega}, u(x^2+x+1)^{2^s-i} \rangle.$$

So,

$$(x^2+x+1)^i \in \langle (x^2+x+1)^{2^s-\omega}, u(x^2+x+1)^{2^s-i} \rangle$$

and

$$(x^2+x+1)^{2^s-\omega} \in \langle (x^2+x+1)^i, u(x^2+x+1)^\omega \rangle.$$

There exist $f_1(x)+uf_2(x), g_1(x)+ug_2(x) \in R[x]$ such that

$$(x^2+x+1)^i = (x^2+x+1)^{2^s-\omega}(f_1(x)+uf_2(x))$$
$$+ u(x^2+x+1)^{2^s-i}(g_1(x)+ug_2(x)).$$

Under modulo u, we have

$$(x^2+x+1)^i = (x^2+x+1)^{2^s-\omega} f_1(x),$$

which implies that $(x^2+x+1)^{i+\omega} = (x^2+x+1)^{2^s} f_1(x) = 0$. Thus, $i+\omega \geq 2^s$. Similarly, there exist $h_1(x)+uh_2(x), q_1(x)+uq_2(x) \in R[x]$ such that

$$(x^2+x+1)^{2^s-\omega} = (x^2+x+1)^i(h_1(x)+uh_2(x)) + u(x^2+x+1)^\omega(q_1(x)+uq_2(x)).$$

Under modulo u, we have $(x^2+x+1)^{2^s-\omega} = (x^2+x+1)^i h_1(x)$. We consider that

$$(x^2+x+1)^{2^{s+1}-\omega-i} = (x^2+x+1)^{2^s} h_1(x) = 0.$$

Thus, $2^{s+1}-i-\omega \geq 2^s$ which means that $2^s \geq i+\omega$. Therefore, $i+\omega = 2^s$. On the other hand, suppose that $i+\omega = 2^s$. Since

$$\mathcal{A}(I)^* = \langle (x^2+x+1)^{2^s-\omega}, u(x^2+x+1)^{2^s-i} \rangle,$$

we have

$$\begin{aligned} I &= \langle (x^2+x+1)^i, u(x^2+x+1)^\omega \rangle \\ &= \langle (x^2+x+1)^{2^s-\omega}, u(x^2+x+1)^{2^s-i} \rangle \\ &= \mathcal{A}(I)^*. \end{aligned}$$

□

5. Negacyclic Codes of Length $3p^s$ Over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

We now apply all results about cyclic codes of length $3p^s$ over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ to negacyclic codes of same length over such ring by providing an isomorphism between cyclic and negacyclic codes of length $3p^s$ over R.

Proposition 5.1. *Let $\phi : \mathcal{R}_1 \to \mathcal{R}_{-1}$ by $\phi(f(x)) = f(-x)$, where $f(x) \in \mathcal{R}_1$. Then ϕ is an isomorphism. Moreover, I is an ideal of $\mathcal{R}_1$ if and only if $\phi(I)$ is an ideal of $\mathcal{R}_{-1}$.(C is a cyclic code of length $3p^s$ over R if and only if $\phi(C)$ is a negacyclic code of length $3p^s$ over R)*

Proof. First of all, we will show that ϕ is well defined and one-to-one. For polynomials $f(x)$ and $g(x) \in R[x], f(x) \equiv g(x) \pmod{x^{3p^s}-1}$ if and only if there exists a polynomial $h(x) \in R[x]$ such that $f(x) - g(x) = h(x)(x^{3p^s}-1)$, if and only if

$$\begin{aligned} f(-x) - g(-x) &= h(-x)((-x)^{3p^s}-1) \\ &= -h(-x)(x^{3p^s}+1), \end{aligned}$$

which is equivalent to $f(-x) \equiv g(-x) \pmod{x^{3p^s}+1}$. Since $\phi(f(x)) - \phi(g(x)) = f(-x) - g(-x)$, we have, for $f(x), g(x) \in \frac{R[x]}{\langle x^{3p^s}-1 \rangle}$, $\phi(f(x)) = \phi(g(x))$ if and only if $f(x) = g(x)$. Therefore, ϕ is well defined and one-to-one. Next, it is a rountine to show that ϕ is onto and homomorphism. Hence, ϕ is a ring isomorphism. □

From Proposition 5.1 and Sec. 3, we obtain that the algebraic structures of cyclic code of length $3p^s$ over R, then we also the structures of negacyclic codes of length $3p^s$ over such ring. Moreover, our results about cyclic codes of length $3p^s$ over R in Sec. 4 can be carried over correspondingly to negacyclic codes of length $3p^s$ over R.

Table 1. The algebraic structures of each cyclic code C of length $3p^s$ over R.

Cases	Algebraic structures
$p^m \equiv 1 \pmod 3$	$C = C_1 \oplus C_{\delta_1} \oplus C_{\delta_2}$, where C_1 is a cyclic code of length p^s over R and C_{δ_i} is a δ_i-constacyclic code of length p^s over R for all $i = 1, 2$ (see Theorem 3.2).
$2^m \equiv 2 \pmod 3$	$C = C_1 \oplus I$, where C_1 is a cyclic code of length p^s over R and I is an ideal of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$, respectively (see Theorem 3.7).
$p^m \equiv 2 \pmod 3$ $(p \neq 2)$	$C = C_1 \oplus C_3$, where C_1 is a cyclic code of length p^s over R and C_3 is a $-(3 \cdot 2^{-2})^{p^s}$-constacyclic code of length $2p^s$ over R, respectively (see Corollary 4.6).

Table 2. Number of all cyclic code C of length $3p^s$ over R.

Cases	Number of cyclic codes
$p^m \equiv 1 \pmod 3$	The third power of the number of all constacyclic codes of length p^s over R (see Theorem 4.2).
$p^m \equiv 2 \pmod 3$	The product of the number of all cyclic codes of length p^s over R and the number of all ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ (see Theorem 4.4).

6. Conclusions

Let p be a prime with $p \neq 3$. We obtain that the algebraic structures of the cyclic and negacyclic codes of length $3p^s$ over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ are isomorphic and the structures of such cyclic codes are in Table 1.

Furthermore, we characterize the ideals of the quotient rings $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$ into 4 types; trivial ideals, principal ideals with nonmonic polynomial generators, principal ideals with monic polynomial generators and nonprincipal ideals as follows from Theorem 3.13. The structures of such dual codes are determined in Theorems 3.3, 3.16–3.18. In $p^m \equiv 1 \pmod 3$, the number of all cyclic codes of length $3p^s$ over R is mentioned in Theorem 4.2. On the other hand, $p^m \equiv 2 \pmod 3$, the number of all cyclic codes of length $3p^s$ over R is the product of number of all cyclic codes of length p^s over R and number of all ideals of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$. Moreover, the number of all cyclic code C of length $3p^s$ over R is shown in Table 2.

For the number of all self-dual cyclic codes of length $3p^s$ over R, it is the number of self-dual cyclic codes of length p^s over R with $p^m \equiv 1 \pmod 3$ (any p) or $p^m \equiv 2 \pmod 3$ $(p \neq 2)$ (see Theorems 4.3 and 4.9). In $p^m \equiv 2 \pmod 3$ with $p = 2$, the number of all self-dual cyclic codes is equal to the product of the number of self-dual cyclic codes of length p^s over R and the number of all ideals I of $\frac{R[x]}{\langle (x^2+x+1)^{p^s} \rangle}$, $I = \mathcal{A}(I)^*$ (see Theorem 4.10). Finally, we determine the condition for each ideal I of $\frac{R[x]}{\langle (x^2+x+1)^{2^s} \rangle}$, $I = \mathcal{A}(I)^*$ in Propositions 4.11–4.14. However, for

$I = \langle (x^2+x+1)^i + u(x^2+x+1)^t h(x), u(x^2+x+1)^\omega \rangle$, where $h(x)$ is a unit, the condition $I = \mathcal{A}(I)^*$ is an open problem.

Acknowledgments

The authors would like to thank Naresuan University and Science Achievement Scholarship of Thailand, which provides supporting for research.

References

[1] S. D. Berman, Semisimple cyclic and Abelian codes. II, *Kibernetika* (Kiev) **3** (1967) 21–30 (In Russian), *Cybernetic* **3** (1967) 17–23.

[2] 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.

[3] G. Castagnoli, J. L. Massey, P. A. Schoeller and N. von Seemann, On repeated-root cyclic codes, *IEEE Trans. Inf. Theory* **37** (1991) 337–342.

[4] 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 Appl.* **37** (2016) 108–130.

[5] Y. Cao, Y. Cao, H. Q. Dinh, F. W. Fu, J. Gao and S. Sriboonchitta, Constacyclic codes of length np^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *Adv. Math. Commun.* **12**(2) (2018) 231.

[6] J. L. Massey, D. J. Costello and J. Justesen, Polynomial weights and code constructions, *IEEE Trans. Inf. Theory* **19** (1973) 101–110.

[7] H. Q. Dinh, Constacyclic codes of length 2^s over galois extension Rings of $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Trans. Inf. Theory* **55** (2009) 1730–1740.

[8] 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.

[9] H. Q. Dinh, Repeated-root constacyclic codes of prime power length, *AMS Contemp. Math.* **480** (2009) 87–100.

[10] H. Q. Dinh, Repeated-root constacyclic codes of length $2p^s$, *Finite Fields Appl.* **18** (2012) 133–143.

[11] H. Q. Dinh, Structure of repeated-root constacyclic codes of length $3p^s$ and their duals, *Discr. Math.* **313** (2013) 983–991.

[12] H. Q. Dinh, On repeated-root constacyclic codes of length $4p^s$, *Asian-Eur. J. Math.* **6** (2013), https://doi.org/10.1142/S1793557113500204.

[13] H. Q. Dinh, S. Dhompongsa and S. Sriboonchitta, On constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *Discr. Math.* **340** (2017) 832–849.

[14] 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** (2018), https://doi.org/10.1142/S0219498819500221.

[15] 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** (2018), https://doi.org/10.1142/S0219498819500233.

[16] H. Q. Dinh, H. D. Nguyen, S. Sriboonchitta and T. M. Vo, Repeated-root constacyclic codes of prime power lengths over finite chain rings, *Finite Fields Appl.* **43** (2017) 22–41.

[17] H. Q. Dinh, Y. Fan, H. Liu, X. Liu and S. Sriboonchitta, On self-dual constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *Discr. Math.* **341** (2018) 324–335.

[18] H. Q. Dinh and S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inform. Theory* **50** (2004) 1728–1744.

[19] G. Falkner, B. Kowol, W. Heise and E. Zehendner, On the existence of cyclic optimal codes, *Atti Semin. Mat. Fis. Univ. Modena* **28** (1979) 326–341.

[20] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* **40** (1994) 301–319.

[21] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, 10th impression, (NorthHolland, Amsterdam, 1998).

[22] J. H. van Lint, Repeated-root cyclic codes, *IEEE Trans. Inf. Theory* **37** (1991) 343–345.

[23] R. M. Roth and G. Seroussi, On cyclic MDS codes of length q over $GF(q)$, *IEEE Trans. Inf. Theory* **32** (1986) 284–285.

[24] W. Zhao, X. Tang and Z. Gu, All $\alpha + u\beta$-constacyclic codes of length np^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *Finite Fields Appl.* **50** (2018) 1–16.