Journal of Algebra and Its Applications
(2018) 1950022 (25 pages)

DOI: 10.1142/S0219498819500221

On a class of constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

Hai Q. Dinh[*,†,‡,††], Bac T. Nguyen[‡,§,¶,‡‡], Songsak Sriboonchitta[‖,§§] and Thang M. Vo[‡,**,¶¶]

[*]*Division of Computational Mathematics and Engineering*
Institute for Computational Science, Ton Duc Thang University
Ho Chi Minh City, Vietnam

[†]*Faculty of Mathematics and Statistics, Ton Duc Thang University*
Ho Chi Minh City, Vietnam

[‡]*Department of Mathematical Sciences, Kent State University*
4314 Mahoning Avenue, Warren, OH 44483, USA

[§]*Department of Basic Sciences, University of Economics*
and Business Administration, Thai Nguyen University
Thai Nguyen Province, Vietnam

[¶]*Nguyen Tat Thanh University, 300 A Nguyen Tat Thanh Street*
Ho Chi Minh City, Vietnam

[‖]*Faculty of Economics, Chiang Mai University*
Chiang Mai 52000, Thailand

[**]*Department of Personnel and Organization*
Vinh University of Technology Education
Vinh City, Nghe An, Vietnam
[††]*dinhquanghai@tdt.edu.vn*
[‡‡]*bacnt2008@gmail.com*
[§§]*songsakecon@gmail.com*
[¶¶]*vomanhthang@vute.edu.vn*

Received 24 December 2017
Accepted 5 January 2018
Published 26 March 2018

Communicated by S. R. López-Permouth

Let p be a prime such that $p^m \equiv 3 \pmod 4$. For any unit λ of $\mathbb{F}_{p^m}$, we determine the algebraic structures of λ-constacyclic codes of length $4p^s$ over the finite commutative chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, $u^2 = 0$. If the unit $\lambda \in \mathbb{F}_{p^m}$ is a square, each λ-constacyclic code of length $4p^s$ is expressed as a direct sum of an -α-constacyclic code and an α-constacyclic code of length $2p^s$. If the unit λ is not a square, then $x^4 - \lambda_0$ can be decomposed into a product of two irreducible coprime quadratic polynomials which are $x^2 + \gamma x + \frac{\gamma^2}{2}$ and $x^2 - \gamma x + \frac{\gamma^2}{2}$, where $\lambda_0^{p^s} = \lambda$ and $\gamma^4 = -4\lambda_0$. By showing that the quotient rings $\frac{\mathcal{R}}{\left\langle \left(x^2+\gamma x+\frac{\gamma^2}{2}\right)^{p^s} \right\rangle}$ and $\frac{\mathcal{R}}{\left\langle \left(x^2-\gamma x+\frac{\gamma^2}{2}\right)^{p^s} \right\rangle}$ are local, non-chain rings, we can

compute the number of codewords in each of λ-constacyclic codes. Moreover, the duals of such codes are also given.

Keywords: Constacyclic codes; dual codes; repeated-root codes; chain rings; local rings.

Mathematics Subject Classification: 94B15, 94B05, 11T71

1. Introduction

Codes over finite rings are intensive studied from the 1990s because of their new role in algebraic coding theory and their successful applications. In an important paper [14], Hammons *et al.* 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. Since then, codes over finite chain rings received attention. Since 2003, special classes of repeated-root codes over certain classes of finite chain rings have been studied by numerous other authors (see, for example, [1, 4, 11]).

Linear and cyclic codes over the finite commutative chain ring $\mathbb{F}_2 + u\mathbb{F}_2$, where $u^2 = 0$, are studied by a lot of researchers (see, for example, [2, 3, 5]). 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. The classification of codes plays an important role in studying their structures, but in general, it is very difficult. In a recent work [7], we classified and gave the detailed structures of all constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$; and in 2012 [8], we provided that for all constacyclic codes of length $2p^s$ over the finite field $\mathbb{F}_{p^m}$.

Recently, in [10], we established successfully the detailed structures of all constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ when $p^m \equiv 1 \pmod 4$. The key result of the technique in [10] is the observation that, for $p^m \equiv 1 \pmod 4$, when λ is not a square in $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, any nonzero polynomial of degree < 4 over $\mathbb{F}_{p^m}$ is invertible in the ambient ring $\frac{(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x]}{\langle x^{4p^s} - \lambda \rangle}$. We showed that this is no longer true for $p^m \equiv 3 \pmod 4$, as in this case, -1 is not a square, but there are non-invertible quadratic polynomials in the ambient ring $\frac{(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x]}{\langle x^{4p^s} + 1 \rangle}$, and moreover, $x^4 + 1$ factors into a product of two irreducible coprime quadratic polynomials. Therefore, we cannot use the method given in [10] to study codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ when $p^m \equiv 3 \pmod 4$.

The units of $\mathcal{R}$ can be expressed as two types, namely, $\lambda \in \mathbb{F}_{p^m} - \{0\}$, and $\alpha + u\beta$, where α, β are nonzero. To continue the line of study, this paper investigates the λ-constacyclic codes of length $4p^s$ over $\mathcal{R}$, where $p^m \equiv 3 \pmod 4$ and $\lambda \in \mathbb{F}_{p^m}$. The remaining case of $(\alpha + u\beta)$-constacyclic codes is considered in our recent paper [12].

The rest of the paper is arranged as follows. After presenting preliminary concepts and results in Sec. 2, Sec. 3 presents the main results of this paper. If λ is not a square, then the algebraic structure of λ-constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ where $p^m \equiv 3 \pmod 4$ and $\lambda \in \mathbb{F}_{p^m}$ is investigated in Theorem 3.3. We also establish the number of codewords in each of these codes (Theorem 3.11).

The duals of each λ-constacyclic code are provided in Sec. 4, as particular cases of our results.

2. Preliminaries

An ideal I of a ring R is called *principal* if it is generated by one element. A ring R is a principal ideal ring if its ideals are principal. R is called a local ring if $R/\operatorname{rad} R$ is a division ring, or equivalently, if R has a unique maximal right (left) ideal. Furthermore, a ring R is called a chain ring if the set of all right (left) ideals of R is linearly ordered under set-theoretic inclusion.

By [11, Proposition 2.1], we have some characterizations of chain rings as follows.

Proposition 2.1 ([11, Proposition 2.1]). *Let R be a finite commutative ring, then the following conditions are equivalent*:

(i) *R is a local ring and the maximal ideal M of R is principal, i.e. $M = \langle\gamma\rangle$ for some $\gamma \in R$,*
(ii) *R is a local principal ideal ring,*
(iii) *R is a chain ring whose ideals are $\langle\gamma^i\rangle$, $0 \leq i \leq \varpi$, where ϖ is the nilpotency of γ.*

For a unit λ of R, the λ-constacyclic (λ-twisted) shift τ_λ on R^n is the shift

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

and a code C is said to be λ-constacyclic if $\tau_\lambda(C) = C$, i.e. if C is closed under the λ-constacyclic shift τ_λ.

The codeword $c = (c_0, c_1, \ldots, c_{n-1})$ is represented its polynomial representation $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, using the obvious one-to-one correspondence. So multiplication by x in the ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^n-\lambda\rangle}$ corresponds to a λ-constacyclic shift of $c(x)$. From this, we have the following result appeared in [15].

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

The inner product of vectors $x = (x_0, x_1, \ldots, x_{n-1}), y = (y_0, y_1, \ldots, y_{n-1}) \in R^n$ is defined by

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

Once we have specified a family of codes called the dual of a code C to be

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

A code C is called *self-orthogonal* if $C \subseteq C^\perp$, and it is called *self-dual* if $C = C^\perp$. An important result is cited here to use later on.

Proposition 2.3. *Let p be a prime and R be a finite chain ring of size p^α. The number of codewords in any linear code C of length n over R is p^k, for some integer*

$k \in \{0, 1, \ldots, \alpha n\}$. *Moreover, the dual code* $C^{\perp}$ *has* p^l *codewords, where* $k + l = \alpha n$, *i.e.* $|C| \cdot |C^{\perp}| = |R|^n$.

The dual of a cyclic code is a cyclic code, and the dual of a negacyclic code is a negacyclic code. In general, we have the following implication of the dual of a λ-constacyclic code.

Proposition 2.4 ([7]). *The dual of a* λ*-constacyclic code is a* λ^{-1}*-constacyclic code.*

We give the definition of reciprocal polynomials.

Definition 2.5. If $f(x) = a_0 + a_1 x + \cdots + a_r x^r$, where $a_r \neq 0$, then the reciprocal of $f(x)$ is the polynomial

$$f^{\star}(x) = a_r + a_{r-1}x + a_{r-2}x^2 + \cdots + a_0 x^r.$$

Symbolically, $f^{\star}(x)$ can be expressed by $f^{\star}(x) = x^r f(\frac{1}{x})$. If I is an ideal of $\frac{\mathcal{R}[x]}{\langle x^n - 1\rangle}$, then $I^{\star} = \{f^{\star}(x) : f(x) \in I\}$ is also an ideal of $\frac{\mathcal{R}[x]}{\langle x^n - 1\rangle}$.

The following result is useful in Sec. 4.

Lemma 2.6 ([13, Lemma 2.8]).

(a) *If* $\deg f \geq \deg g$, *then*

$$(f(x) + g(x))^{\star} = f^{\star}(x) + x^{\deg f - \deg g} g^{\star}(x).$$

(b) $(f(x)g(x))^{\star} = f^{\star}(x)g^{\star}(x)$.

Definition 2.7. Let I be an ideal of $\mathcal{R}$. 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, which is also an ideal of $\mathcal{R}$.

Remark 2.8. From the above definition we can see that if C is a constacyclic code of length n over R with associated ideal I, then the associated ideal of $C^{\perp}$ is $\mathcal{A}(I)^{\star}$.

Let ξ be a primitive element of $\mathbb{F}_{p^m}$. This means that $\mathbb{F}_{p^m} = \{0, \xi, \ldots, \xi^{p^m-2}, \xi^{p^m-1} = 1\}$. Denote $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where $u^2 = 0$ and $\mathcal{R}_{\lambda} = \frac{\mathcal{R}[x]}{\langle x^{4p^s} - \lambda\rangle}$. Then constacyclic codes of length $4p^s$ over $\mathcal{R}$ are precisely the ideals of the ambient ring $\mathcal{R}_{\lambda}$. To study the structure of ideals of $\mathcal{R}_{\lambda}$, we need to express the polynomial $x^{4p^s} - \lambda$ as a product of irreducible polynomials over $\mathcal{R}$.

3. Structure of λ-Constacyclic Codes when $p^m \equiv 3 \pmod 4$

If $\lambda = \alpha^2$, then we have $x^{4p^s} - \lambda = x^{4p^s} - \alpha^2 = (x^{2p^s} + \alpha)(x^{2p^s} - \alpha)$. And hence, by the Chinese reminder theorem,

$$\mathcal{R}_{\lambda} \cong \frac{R[x]}{\langle x^{2p^s} + \alpha\rangle} \oplus \frac{R[x]}{\langle x^{2p^s} - \alpha\rangle}.$$

It follows that ideals of $\mathcal{R}_\lambda$ are of the form $A \oplus B$, where A and B are ideals of $\frac{R[x]}{\langle x^{2p^s}+\alpha\rangle}$ and $\frac{R[x]}{\langle x^{2p^s}-\alpha\rangle}$, respectively, i.e. they are $-\alpha$- and α-constacyclic codes of length $4p^s$ over R. It means that any λ-constacyclic code of length $4p^s$ over R, i.e. an ideal C of $\mathcal{R}$, is represented as a direct sum of C_+ and C_-:

$$C = C_+ \oplus C_-,$$

where C_+ and C_- are ideals of $\frac{R[x]}{\langle x^{2p^s}+\alpha\rangle}$ and $\frac{R[x]}{\langle x^{2p^s}-\alpha\rangle}$, respectively. Thus, the classification, detailed structure, and number of codewords of constacyclic codes C of length $4p^s$ over R can be obtained from that of the direct summands C_+ and C_- (cf. [6]). It turns out that the dual code $C^\perp$ of C is also a direct sum of the dual codes of the direct summands $C_+^\perp$ and $C_-^\perp$.

We now consider the main case that the unit λ is not a square in $\mathbb{F}_{p^m}$. From now on throughout this section, we always assume that p is a (odd) prime such that $p^m \equiv 3 \pmod 4$. As mentioned in [7], there exists $\lambda_0 \in \mathbb{F}_{p^m}$ such that $\lambda_0^{p^s} = \lambda$. It is easy to check that the equation $\frac{x^4}{4} + \lambda_0 = 0$ has two roots in $\mathbb{F}_{p^m}$ exactly. We assume that $\gamma \in \mathbb{F}_{p^m}$ is a root of the equation $\frac{x^4}{4} + \lambda_0 = 0$. This implies that $\gamma^4 = -4\lambda_0$. We have

$$x^4 - \lambda_0 = x^4 + \frac{\gamma^4}{4} = \left(x^2 + \frac{\gamma^2}{2}\right)^2 - (\gamma x)^2 = \left(x^2 + \gamma x + \frac{\gamma^2}{2}\right)\left(x^2 - \gamma x + \frac{\gamma^2}{2}\right).$$

Therefore, $x^{4p^s} - \lambda$ can be expressed as

$$x^{4p^s} - \lambda = \left(x^2 + \gamma x + \frac{\gamma^2}{2}\right)^{p^s}\left(x^2 - \gamma x + \frac{\gamma^2}{2}\right)^{p^s}.$$

To simplify notations, we put $\delta \in \{-1, 1\}$. We start with the following two lemmas.

Lemma 3.1. *The polynomial $x^2 + \delta\gamma x + \frac{\gamma^2}{2}$ is irreducible over $\mathbb{F}_{p^m}$.*

Proof. Suppose that $x^2 + \delta\gamma x + \frac{\gamma^2}{2}$ is reducible over $\mathbb{F}_{p^m}$, then there exists an element $\beta \in \mathbb{F}_{p^m}$ such that

$$\beta^2 + \delta\gamma\beta + \frac{\gamma^2}{2} = 0.$$

We can see that $\beta^2 + \delta\gamma\beta + \frac{\gamma^2}{2} = (\beta + \frac{\gamma}{2})^2 + \frac{\gamma^2}{4} = 0$, implying that $\frac{\gamma^2}{4} = 0$. This is a contradiction. Hence, $x^2 + \delta\gamma x + \frac{\gamma^2}{2}$ is irreducible over $\mathbb{F}_{p^m}$. □

Lemma 3.2. *The polynomial $x^2 + \delta\gamma x + \frac{\gamma^2}{2}$ is irreducible over $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s}\right\rangle}$ for all $\delta \in \{1, -1\}$.*

Proof. Suppose that $x^2 + \delta\gamma x + \frac{\gamma^2}{2}$ is reducible over $\mathcal{R}$. Then there exists an element $\alpha \in \mathcal{R}$ such that $\alpha^2 + \delta\gamma\alpha + \frac{\gamma^2}{2} = 0$, where $\alpha = \alpha_1 + u\alpha_2, \alpha_1, \alpha_2 \in \mathbb{F}_{p^m}$.

We have

$$\begin{aligned}0 &= \alpha^2 + \delta\gamma\alpha + \frac{\gamma^2}{2}\\ &= (\alpha_1 + u\alpha_2)^2 + \delta\gamma(\alpha_1 + u\alpha_2) + \frac{\gamma^2}{2}\\ &= \left(\alpha_1^2 + \delta\gamma\alpha_1 + \frac{\gamma^2}{2}\right) + u(2\alpha_1\alpha_2 + \delta\gamma\alpha_2).\end{aligned}$$

From this, we can see that $\alpha_1^2 + \delta\gamma\alpha_1 + \frac{\gamma^2}{2} = 0$ and $2\alpha_1\alpha_2 + \delta\gamma\alpha_2 = 0$. If $2\alpha_1\alpha_2 + \delta\gamma\alpha_2 = 0$, then either $\alpha_2 = 0$ or $\alpha_1 = \frac{-\delta\gamma}{2}$. If $\alpha_2 = 0$, then $\alpha = \alpha_1 \in \mathbb{F}_{p^m}$, i.e. $x^2 + \delta\gamma x + \frac{\gamma^2}{2}$ is reducible over $\mathbb{F}_{p^m}$, which is a contradiction. If $\alpha_1 = \frac{-\delta\gamma}{2}$, then

$$\begin{aligned}0 &= \alpha_1^2 + \delta\gamma\alpha_1 + \frac{\gamma^2}{2}\\ &= \left(\frac{-\delta\gamma}{2}\right)^2 + \delta\gamma\left(\frac{-\delta\gamma}{2}\right) + \frac{\gamma^2}{2}\\ &= -\frac{\delta^2\gamma^2}{4} + \frac{\gamma^2}{2}\\ &= \frac{\gamma^2}{4}.\end{aligned}$$

That means $\gamma = 0$, a contradiction. Therefore, $x^2 + \delta\gamma x + \frac{\gamma^2}{2}$ is irreducible over $\mathcal{R}$. □

We now obtain λ-constacyclic codes of length $4p^s$ over $\mathcal{R}$ and their duals.

Theorem 3.3. *Let C be a λ-constacyclic code of length $4p^s$ over $\mathcal{R}$.*

(i) *λ-constacyclic codes of length $4p^s$ over $\mathcal{R}$ can be expressed as $C = C_1 \oplus C_2$, where C_i are ideals of the ring $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s}\right\rangle}$.*

(ii) $|C| = |C_1||C_2|$.

(iii) *The dual code $C^\perp$ of C is given by $C^\perp = C_1^\perp \oplus C_2^\perp$.*

(iv) $C_i^\perp = \mathrm{ann}(C_i)^\star$.

Proof. By Lemma 3.2, and the Chinese Remainder Theorem, we get the isomorphism

$$\frac{\mathcal{R}[x]}{\langle x^{4p^s} - \lambda\rangle} \cong \bigoplus_{\delta\in\{-1,1\}} \frac{\mathcal{R}[x]}{\left\langle \left(x^2 + \delta\alpha x + \frac{\gamma^2}{2}\right)^{p^s}\right\rangle}.$$

Hence, every λ-constacyclic code C of length $4p^s$ over $\mathcal{R}$ can be expressed as $C = C_1 \oplus C_2$, where C_i are ideals of the ring $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\alpha x+\frac{\gamma^2}{2}\right)^{p^s}\right\rangle}$, proving (i). It is easy to check that $|C| = |C_1||C_2|$, giving (ii). By Proposition 2.4, we can conclude that the

dual code $C^\perp$ of C is given by $C^\perp = C_1^\perp \oplus C_2^\perp$. It is well-known from [9] that if C is a λ-constacyclic code of length n over the ring R, then $C^\perp = \mathrm{ann}(C)^\star$, completing the proof of (iv). □

To investigate λ-constacyclic codes of length $4p^s$ over $\mathcal{R}$, and their duals, we need to determine all ideals of the ambient rings $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s}\right\rangle}$. The following result shows that any nonzero polynomial $cx+d \in \mathbb{F}_{p^m}[x]$ is invertible in $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s}\right\rangle}$.

Lemma 3.4. *Any nonzero polynomial $cx+d \in \mathbb{F}_{p^m}[x]$ is invertible in $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s}\right\rangle}$.*

Proof. If $c=0$, then $d\neq 0$. This means that d is invertible in $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s}\right\rangle}$. If $c\neq 0$, we have

$$\begin{aligned}
&c(x+c^{-1}d)^{-1}\\
&\quad= c^{-1}(x+c^{-1}d)^{p^s-1}(x-c^{-1}d+\delta\gamma)^{p^s}(x+c^{-1}d)^{-p^s}(x-c^{-1}d+\delta\gamma)^{-p^s}\\
&\quad= c^{-1}(x+c^{-1}d)^{p^s-1}(x-c^{-1}d+\delta\gamma)^{p^s}(x^2+\delta\gamma x-(c^{-1}d)^2+\delta\gamma(c^{-1}d))^{-p^s}\\
&\quad= c^{-1}(x+c^{-1}d)^{p^s-1}(x-c^{-1}d+\delta\gamma)^{p^s}\left(\left(\frac{\gamma^2}{2}\right)^{p^s}-(c^{-1}d)^{2p^s}+(\delta\gamma c^{-1}d)^{p^s}\right)^{-1}\\
&\quad= -c^{-1}(x+c^{-1}d)^{p^s-1}(x-c^{-1}d+\delta\gamma)^{p^s}\left(\frac{\gamma^2}{2}+(c^{-1}d)^2-(\delta\gamma)c^{-1}d\right)^{-p^s}.
\end{aligned}$$

It implies that $cx+d$ is invertible if and only if $\frac{\gamma^2}{2}+(c^{-1}d)^2-(\delta\gamma)c^{-1}d$ is invertible in $\mathbb{F}_{p^m}$, i.e. $(c^{-1}d)^2-(\delta\gamma)c^{-1}d+\frac{\gamma^2}{2}$ is nonzero. Since $x^2+\delta\gamma x+\frac{\gamma^2}{2}$ is irreducible over $\mathbb{F}_{p^m}$, we can see that $(c^{-1}d)^2-(\delta\gamma)c^{-1}d+\frac{\gamma^2}{2}$ is nonzero. This follows that $cx+d$ is invertible in $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s}\right\rangle}$. □

Lemma 3.5. *Let $f(x) \in \frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s}\right\rangle}$. Then $f(x)$ can be uniquely expressed as*

$$\begin{aligned}
f(x) &= \sum_{i=0}^{p^s-1}(c_{0i}x+d_{0i})(x^2+\delta\alpha x+\eta)^i + u\sum_{i=0}^{p^s-1}(c_{1i}x+d_{1i})(x^2+\delta\alpha x+\eta)^i\\
&= c_{00}x+d_{00}+(x^2+\delta\alpha x+\eta)\sum_{i=1}^{p^s-1}(c_{0i}x+d_{0i})(x^2+\delta\alpha x+\eta)^{i-1}\\
&\quad+u\sum_{i=0}^{p^s-1}(c_{1i}x+d_{1i})(x^2+\delta\alpha x+\eta)^i,
\end{aligned}$$

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

Proof. The representation of $f(x)$ follows from the fact that it can be viewed as polynomials of degree less than p^s over $\mathcal{R}$. From $(x^2 + \delta\gamma x + \frac{\gamma^2}{2}) = 0$ and $u^2 = 0$ in $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s} \right\rangle}$, we can see that $(x^2 + \delta\gamma x + \frac{\gamma^2}{2})$ is a nilpotent element of $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s} \right\rangle}$. By applying Lemma 3.4, $f(x)$ is non-invertible if and only if $c_{00} = d_{00} = 0$. □

Combining Lemmas 3.4 and 3.5, we give some characterizations of the ring $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s} \right\rangle}$ in the following theorem.

Theorem 3.6. *The quotient ring* $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\alpha x+\eta\right)^{p^s} \right\rangle}$ *is a local ring with maximal ideal* $\langle x^2 + \delta\gamma x + \frac{\gamma^2}{2}, u\rangle$, *but not a chain ring. In particular,* $x^2 + \delta\gamma x + \frac{\gamma^2}{2}$ *is a nilpotent element of* $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s} \right\rangle}$, *with the nilpotency index* p^s.

Proof. From Lemma 3.4, we can prove that the ideal $\langle x^2 + \delta\gamma x + \frac{\gamma^2}{2}, u\rangle$ contains all the non-invertible elements of $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s} \right\rangle}$. Hence, $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s} \right\rangle}$ is a local ring with the maximal ideal $\langle x^2 + \delta\gamma x + \frac{\gamma^2}{2}, u\rangle$. It is routine to check that $u \notin \langle x^2 + \delta\gamma x + \frac{\gamma^2}{2}\rangle$. Obviously, $x^2 + \delta\gamma x + \frac{\gamma^2}{2} \notin \langle u\rangle$. Therefore, $\langle x^2 + \delta\gamma x + \frac{\gamma^2}{2}, u\rangle$ is not a principal ideal of $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s} \right\rangle}$, showing that $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s} \right\rangle}$ is not a chain ring according to Proposition 2.1. □

We can now determine all ideals of $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s} \right\rangle}$.

Theorem 3.7. *All ideals in* $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s} \right\rangle}$ *are listed as follows*:

- *Type* 1: (*Trivial ideals*)

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

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

$$\left\langle u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^i \right\rangle,$$

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

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

$$\left\langle \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^i + u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^t h(x) \right\rangle,$$

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

- *Type* 4: (*Nonprincipal ideals*)

$$\left\langle \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^i + u\sum_{j=0}^{\omega-1}(c_j x + d_j)\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^j, \right.$$
$$\left. u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^\omega \right\rangle,$$

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

$$u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^T \in \left\langle \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^i + u\sum_{j=0}^{i-1}(c_j x + d_j)\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^j \right\rangle;$$

or equivalently,

$$\left\langle \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^i + u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^t h(x), u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^\omega \right\rangle,$$

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

Proof. First of all, it is obvious to see that ideals of Type 1 are trivial ideals. Let I be an arbitrary nontrivial ideal of $\frac{\mathcal{R}[x]}{\left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s}\right\rangle}$. We proceed 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 $u\sum_{i=0}^{p^s-1}(c_{1i}x + d_{1i})\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^i$, where $c_{1i}, d_{1i} \in \mathbb{F}_{p^m}$. This shows that there exists an element $a \in I$ that has the smallest k such that $c_{1k}x + d_{1k} \neq 0$. Therefore, each element $c(x) \in I$ has the form $c(x) = u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^k \sum_{i=k}^{p^s-1}(c_{1i}x + d_{1i})\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{i-k}$, showing that $I \subseteq \langle u(x^2 + \delta\gamma x + \frac{\gamma^2}{2})^k \rangle$. Since $a \in I$, we can

express a as follows:

$$a = u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k \sum_{i=k}^{p^s-1}(c_{1i}x+d_{1i})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{i-k}$$

$$= u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k \left[c_{1k}x+d_{1k}+\sum_{i=k+1}^{p^s-1}(c_{1i}x+d_{1i})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{i-k}\right].$$

From $c_{1k}x+d_{1k}\neq 0$, it implies that $c_{1k}x+d_{1k}+\sum_{i=k+1}^{p^s-1}(c_{1i}x+d_{1i})(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{i-k}$ is invertible. Hence, $u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^k \in I$. From this, we can see that $I = \langle u\big(x^2+\delta\gamma x+\frac{\gamma^2}{2}\big)^k\rangle$. Therefore, the nontrivial ideals of $\frac{\mathcal{R}[x]}{\langle\big(x^2+\delta\gamma x+\frac{\gamma^2}{2}\big)^{p^s}\rangle}$ contained in $\langle u\rangle$ are $\langle u\big(x^2+\delta\gamma x+\frac{\gamma^2}{2}\big)^k\rangle, 0\leq k\leq p^s-1$, which are ideals of Type 2.

Case 2. $I\not\subseteq\langle u\rangle$: Let I_u denote the set of elements in I which are reduced modulo u. By applying [8, Theorem 3.2], one can see that I_u is a nonzero ideal of the ring $\frac{\mathbb{F}_{p^m}[x]}{\langle\big(x^2+\delta\gamma x+\frac{\gamma^2}{2}\big)^{p^s}\rangle}$, which is a finite chain ring with ideals $\langle\big(x^2+\delta\gamma x+\frac{\gamma^2}{2}\big)^j\rangle$, where $0\leq j\leq p^s$. Then there is an integer $i\in\{0,1,\ldots,p^s-1\}$ such that $I_u = \langle\big(x^2+\delta\gamma x+\frac{\gamma^2}{2}\big)^i\rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle\big(x^2+\delta\gamma x+\frac{\gamma^2}{2}\big)^{p^s}\rangle}$. Thus, there exists an element

$$c(x) = \sum_{j=0}^{p^s-1}(c_{0j}x+d_{0j})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j + u\sum_{j=0}^{p^s-1}(c_{1j}x+d_{1j})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j$$

$$\in \frac{\mathcal{R}[x]}{\langle\big(x^2+\delta\gamma x+\frac{\gamma^2}{2}\big)^{p^s}\rangle},$$

where $c_{0j},c_{1j},d_{0j},d_{1j}\in\mathbb{F}_{p^m}$, such that $\big(x^2+\delta\gamma x+\frac{\gamma^2}{2}\big)^i + uc(x)\in I$. Since

$$\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i + uc(x)$$

$$= \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i + u\sum_{j=0}^{p^s-1}(c_{0j}x+d_{0j})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j \in I,$$

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

Case 2a. $I = \langle\big(x^2+\delta\gamma x+\frac{\gamma^2}{2}\big)^i + u\sum_{j=0}^{i-1}(c_jx+d_j)\big(x^2+\delta\gamma x+\frac{\gamma^2}{2}\big)^j\rangle$, then I can be expressed as

$$I = \left\langle\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i + u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^t h(x)\right\rangle,$$

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

Case 2b. $\langle (x^2+\delta\gamma x+\frac{\gamma^2}{2})^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})(x^2+\delta\gamma x+\frac{\gamma^2}{2})^j\rangle \subsetneq I$. Then there exists

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

It follows that there is a polynomial $g(x) \in \frac{\mathcal{R}[x]}{\langle (x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s}\rangle}$ such that

$$\begin{aligned} &0 \neq h(x) \\ &= f(x) - g(x)\left[\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j\right] \in I, \end{aligned}$$

implying that $h(x)$ can be expressed as

$$h(x) = \sum_{j=0}^{i-1}(h_{0j}x+h'_{0j})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j + u\sum_{j=0}^{i-1}(h_{1j}x+h'_{1j})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j,$$

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

$$\begin{aligned} h(x) &= u\sum_{j=k}^{i-1}(h_{1j}x+h'_{1j})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j \\ &= u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k \\ &\quad \times \left[h_{1k}x+h'_{1k}+\sum_{j=k+1}^{i-1}(h_{1j}x+h'_{1j})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{j-k}\right]. \end{aligned}$$

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

$$\begin{aligned} &u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k \\ &\quad = \left(h_{1k}x+h'_{1k}+\sum_{j=k+1}^{i-1}(h_{1j}x+h'_{1j})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{j-k}\right)^{-1} h(x) \in I. \end{aligned}$$

It has been shown that for any $f(x) \in I \backslash \langle (x^2+\delta\gamma x+\frac{\gamma^2}{2})^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})(x^2+\delta\gamma x+\frac{\gamma^2}{2})^j\rangle$, there is an integer k with $0 \leq k \leq i-1$ such that $u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^k \in I$. Put

$$\omega = \min\left\{ k \,\middle|\, f(x) \in I \backslash \left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j \right\rangle \right\}.$$

Then we have $\langle (x^2+\delta\alpha x+\eta)^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})(x^2+\delta\gamma x+\frac{\gamma^2}{2})^j, u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^\omega\rangle \subseteq I$. By the above construction, for any $f(x) \in I$, there exists a polynomial $g(x) \in I$ satisfying

$$f(x) - g(x)\left[\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j\right] \in \left\langle u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^\omega \right\rangle.$$

It follows that

$$f(x) \in \left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j, u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^\omega \right\rangle.$$

Hence,

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

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

$$I = \left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i + u\sum_{j=0}^{\omega-1}(c_jx+d_j)\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j, \right.$$
$$\left. u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^\omega \right\rangle$$
$$= \left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i + u\sum_{j=0}^{i-1}(c_jx+d_j)\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j \right\rangle.$$

This is a contradiction with the assumption of this case. Thus, we can conclude that $\omega < T$, showing that I is of Type 4. □

In Theorem 3.7, the number T plays an important role in Type 4. The following result determines the number T.

Proposition 3.8. *Let T be the smallest integer such that*

$$u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^T \in \left\langle \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i + u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^t h(x)\right\rangle.$$

Then T can be determined as follows:

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

Proof. We first observe that $T \leq i$ with the reason that $u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i = u[(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i + u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^t h(x)] \in C$. If $h(x) = 0$, then $C = \langle (x^2+\delta\gamma x+\frac{\gamma^2}{2})^i\rangle$, showing that $T = i$. Now we consider the case $h(x) \neq 0$, where $h(x)$ is a unit. Since $u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^T \in \langle (x^2+\delta\gamma x+\frac{\gamma^2}{2})^i + u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^t h(x)\rangle$, we can find a polynomial $f(x) \in \frac{\mathcal{R}[x]}{\langle (x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s}\rangle}$ satisfying $u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^T = f(x)[(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i + u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^t h(x)]$. Hence, $f(x)$ can be written as

$$f(x) = \sum_{j=0}^{p^s-1}(a_{0j}x+b_{0j})\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j + u\sum_{j=0}^{p^s-1}(a_{1j}x+b_{1j})$$
$$\times\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j,$$

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

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

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

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

$$\times\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j.$$

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

$$\left[\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i + u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^t h(x)\right]\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s-i}$$

$$= u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s-i+t} h(x).$$

Hence,

$$u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s-i+t} = \left[\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i + u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^t h(x)\right]$$

$$\times\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s-i}[h(x)]^{-1} \in C.$$

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

Recall that for a code C of length n over $\mathcal{R}$, their torsion and residue codes are codes over $\mathbb{F}_{p^m}$, defined as follows:

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

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

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

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

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

Proposition 3.9. *Let C be a code of length n over R, whose torsion and residue codes are* $\mathrm{Tor}(C)$ *and* $\mathrm{Res}(C)$. *Then* $|C| = |\mathrm{Tor}(C)| \cdot |\mathrm{Res}(C)|$.

In order to give the number of elements in each ideal I of the ring $\frac{\mathcal{R}[x]}{\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s}\rangle}$, we need to determine torsion and residue codes of I. By definition and the classification in Theorem 3.7, $\mathrm{Res}(I)$ and $\mathrm{Tor}(I)$ can be readily obtained.

Lemma 3.10. *Let I be ideals of the ring $\frac{\mathcal{R}[x]}{\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s}\rangle}$, then the torsion and residue codes of I are determined as follows*:

(i) *Type* 1:

- *If* $I=\langle 0\rangle$, *then* $\mathrm{Res}(I)=\mathrm{Tor}(I)=\langle 0\rangle$. *This implies that* $|\mathrm{Res}(I)|=|\mathrm{Tor}(I)|=1$.
- *If* $I=\langle 1\rangle$, *then* $\mathrm{Res}(I)=\mathrm{Tor}(I)=\langle 1\rangle$. *Hence*, $|\mathrm{Res}(I)|=|\mathrm{Tor}(I)|=p^{2mp^s}$

(ii) *Type* 2: *If* $I=\langle u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i\rangle$, *where* $0\leq i\leq p^s-1$, *then* $\mathrm{Res}(I)=\langle 0\rangle$ *and* $\mathrm{Tor}(I)=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i\rangle$. *Therefore*, $|\mathrm{Res}(I)|=1$ *and* $|\mathrm{Tor}(I)|=p^{2m(p^s-i)}$.

(iii) *Type* 3: *If* $I=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i+u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^t h(x)\rangle$, *where* $1\leq i\leq p^s-1, 0\leq t<i$ *and either* $h(x)$ *is* 0 *or* $h(x)$ *is a unit. Then* $\mathrm{Res}(I)=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i\rangle$ *and* $\mathrm{Tor}(I)=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^T\rangle$, *where* T *is the smallest integer such that* $u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^T\in I$, *which is given by*

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

From this, we have $|\mathrm{Res}(I)|=p^{2m(p^s-i)}$ *and* $|\mathrm{Tor}(I)|=p^{2m(p^s-T)}$.

(iv) *Type* 4: *If* $I=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i+u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^t h(x), u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^\kappa\rangle$, *where* $1\leq i\leq p^s-1, 0\leq t<i$, *either* $h(x)$ *is* 0 *or* $h(x)$ *is a unit, and* $\kappa<T$, *then* $\mathrm{Res}(I)=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i\rangle$ *and* $\mathrm{Tor}(I)=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^\kappa\rangle$. *This follows that* $|\mathrm{Res}(I)|=p^{2m(p^s-i)}$ *and* $|\mathrm{Tor}(I)|=p^{2m(p^s-\kappa)}$.

By multiplying the sizes of $\mathrm{Res}(I)$ and $\mathrm{Tor}(I)$ in each case, we can now give the number of elements in each ideal of the ring $\frac{\mathcal{R}[x]}{\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s}\rangle}$ as follows.

Theorem 3.11. *Let I be an ideal of the ring $\frac{\mathcal{R}[x]}{\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s}\rangle}$, then the number of elements of I, denoted by n_I, is determined as follows*:

- *If* $I=\langle 0\rangle$, *then* $n_I=1$.
- *If* $I=\langle 1\rangle$, *then* $n_I=p^{4mp^s}$.
- *If* $I=\langle u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i\rangle$, *where* $0\leq i\leq p^s-1$, *then* $n_I=p^{2m(p^s-i)}$.
- *If* $I=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i\rangle$, *where* $1\leq i\leq p^s-1$, *then* $n_I=p^{4m(p^s-i)}$.
- *If* $I=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i+u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^t h(x)\rangle$, *where* $1\leq i\leq p^s-1, 0\leq t<i$, *and* $h(x)$ *is a unit, then*

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

- *If* $I=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i+u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^t h(x), u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^\kappa\rangle$, *where* $1\le i\le p^s-1, 0\le t<i$, *either* $h(x)$ *is* 0 *or* $h(x)$ *is a unit, and*

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

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

4. Duals of λ-Constacyclic Codes

Suppose that C is a λ-constacyclic code of length $4p^s$ over $\mathcal{R}$ with the dual code as $C^\perp$. We start with a couple of lemmas.

Lemma 4.1. *Let* $f(x)=(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i-u\sum_{j=0}^{t}(a_jx+b_j)(x^2+\delta\gamma x+\frac{\gamma^2}{2})^j$, *be an element of* $\frac{\mathcal{R}[x]}{\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s}\rangle}$, *where* $t<i$. *Then*

$$\begin{aligned} f^\star(x)=&\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i-u\sum_{k=1}^{t}\left[\sum_{j=0}^{k-1}b_j\binom{i-j-1}{k-j-1}\right](-1)^{i-k}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k\\ &-u\sum_{k=t+1}^{i}\left[\sum_{j=0}^{t}b_j\binom{i-j-1}{k-j-1}\right](-1)^{i-k}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k\\ &-u\sum_{k=0}^{t}\left[\sum_{j=0}^{k}(a_jx-b_j)\binom{i-j-1}{k-j}\right](-1)^{i-k-1}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k\\ &-u\sum_{k=t+1}^{i-1}\left[\sum_{j=0}^{t}(a_jx-b_j)\binom{i-j-1}{k-j}\right](-1)^{i-k-1}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k. \end{aligned}$$

Proof. By Lemma 2.6, we have

$$\begin{aligned} f^\star(x)&=\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i-u\sum_{j=0}^{t}(b_jx+a_j)\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j x^{2i-2j-1}\\ &=\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i-u\sum_{j=0}^{t}(b_jx+a_j)x\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j\\ &\quad\times\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{i-j-1} \end{aligned}$$

$$
\begin{aligned}
&= \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i - u\sum_{j=0}^{t}(b_jx^2+a_jx)\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j\\
&\quad\times\sum_{k=0}^{i-j-1}\binom{i-j-1}{k}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k(-1)^{i-j-k-1}\\
&= \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i - u\sum_{j=0}^{t}\left(b_j\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)+a_jx-b_j\right)\\
&\quad\times\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j\sum_{k=0}^{i-j-1}\binom{i-j-1}{k}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k(-1)^{i-j-k-1}\\
&= \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i - u\sum_{j=0}^{t}b_j\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{j+1}\sum_{k=0}^{i-j-1}\binom{i-j-1}{k}\\
&\quad\times\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k(-1)^{i-j-k-1} - u\sum_{j=0}^{t}(a_jx-b_j)\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^j\\
&\quad\times\sum_{k=0}^{i-j-1}\binom{i-j-1}{k}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k(-1)^{i-j-k-1}\\
&= \left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i - u\sum_{k=1}^{t}\left[\sum_{j=0}^{k-1}b_j\binom{i-j-1}{k-j-1}\right](-1)^{i-k}\\
&\quad\times\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k\\
&\quad- u\sum_{k=t+1}^{i}\left[\sum_{j=0}^{t}b_j\binom{i-j-1}{k-j-1}\right](-1)^{i-k}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k\\
&\quad- u\sum_{k=0}^{t}\left[\sum_{j=0}^{k}(a_jx-b_j)\binom{i-j-1}{k-j}\right](-1)^{i-k-1}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k\\
&\quad- u\sum_{k=t+1}^{i-1}\left[\sum_{j=0}^{t}(a_jx-b_j)\binom{i-j-1}{k-j}\right](-1)^{i-k-1}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k. \qquad \square
\end{aligned}
$$

To determine the annihilator of I, where I is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s}\rangle}$, we first observe the following.

Lemma 4.2. *If* $I=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i+u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^th(x),u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^\omega\rangle$, *then* p^s-i *is the smallest positive integer* r *such that* $u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^r\in\mathcal{A}(I)$.

Proof. Consider

$$\left[\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^i+u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^t h(x)\right]u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^r=0.$$

Clearly, we must have $i+r\geq p^s$. So we have the smallest value of r, namely, p^s-i. Hence, $u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s-i}\in\mathcal{A}(I)$. □

Theorem 4.3. *Let the λ-constacyclic code C be associated to the ideal $I=\langle u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i\rangle$ of $\frac{\mathcal{R}[x]}{\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s}\rangle}$. Then $\mathcal{A}(C)^\star=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s-i},u\rangle$.*

Proof. From $C\subseteq\langle u\rangle$ and $C\subseteq\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i\rangle$, we have $\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s-i}\rangle=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i\rangle^\perp\subseteq C^\perp$ and $\langle u\rangle=\langle u\rangle^\perp\subseteq C^\perp$, implying that $\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s-i},u\rangle\subseteq C^\perp$. Since the coefficient vector of $(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s-i}$ is orthogonal to the coefficient vector of $u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i$ and all its negacyclic shift, the other inclusion is proved, completing the proof. □

Theorem 4.4. *Let the λ-constacyclic code C be associated to the ideal $I=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i+u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^th(x)\rangle$ of the ring $\frac{\mathcal{R}[x]}{\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s}\rangle}$, where $h(x)$ is 0 or $h(x)$ is a unit. Then we can determine $\mathcal{A}(C)^\star$ as follows*:

(1) *If $h(x)$ is 0, then $\mathcal{A}(C)^\star=\langle(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s-i}\rangle$.*
(2) *If $1\leq i\leq\frac{p^s+t}{2}$ and $h(x)$ is a unit, then $\mathcal{A}(C)^\star=\langle a(x)\rangle$, where*

$$\begin{aligned}a(x)=&\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s-i}-u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s-2i+t}\sum_{k=1}^{i-t-1}\\&\times\left[\sum_{j=0}^{k-1}b_j\binom{i-t-j-1}{k-j-1}\right](-1)^{i-t-k}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k\\&-u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s-2i+t}\sum_{k=0}^{i-t-1}\left[\sum_{j=0}^{k}(a_jx-b_j)\binom{i-t-j-1}{k-j}\right]\\&\times(-1)^{i-t-k-1}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k.\end{aligned}$$

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

$$\begin{aligned}b(x)=&\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{i-t}-u\sum_{k=1}^{p^s-i-1}\left[\sum_{j=0}^{k-1}b_j\binom{i-t-j-1}{k-j-1}\right]\\&\times(-1)^{i-t-k}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k\end{aligned}$$

$$- u \sum_{k=0}^{p^s-i-1} \left[\sum_{j=0}^{k} (a_j x - b_j) \binom{i-t-j-1}{k-j} \right] \times (-1)^{i-t-k-1} \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^k.$$

Proof. The proof of (1) is straightforward. We will give the proof of (2). The proof of (3) is similar. From $[(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i+u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^t h(x)][(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s-i} - u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s-2i+t}h(x)] = 0$, we can see that

$$\left\langle \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^{p^s-i} - u \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^{p^s-2i+t} h(x) \right\rangle \subseteq \mathcal{A}(C).$$

Let $\mathcal{A}(C) = \langle f(x), u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^k \rangle$, where $f(x) = (x^2+\delta\gamma x+\frac{\gamma^2}{2})^a + u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^b g(x)$. By Lemma 4.2, p^s-i is the smallest integer r such that $u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^r \in \mathcal{A}(C)$. Hence, $k = p^s-i$. We can see that $f(x)[(x^2+\delta\gamma x+\frac{\gamma^2}{2})^i+u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^t h(x)]$ is equal to

$$\begin{aligned} &\left[\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^a + u \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^b g(x) \right] \\ &\quad \times \left[\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^i + u \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^t h(x) \right] \\ &= \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^{a+i} + u \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^{a+t} h(x) \\ &\quad + u \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^{b+i} g(x) = 0. \end{aligned}$$

We must 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 concludes that

$$f(x) = \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^a + u \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^b g(x) \in \left\langle \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^{p^s-i} - u \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^{p^s+t-2i} h(x), u \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^{p^s-i} \right\rangle$$

and

$$\mathcal{A}(C) = \left\langle \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^{p^s-i} - u \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^{p^s+t-2i} h(x), u \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2} \right)^{p^s-i} \right\rangle.$$

Since $u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s-i} \in \langle (x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s-i} - u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^{p^s+t-2i}h(x)\rangle$, it follows that

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

Let $h(x) = \sum_j (a_j x+b_j)(x^2+\delta\gamma x+\frac{\gamma^2}{2})^j$, where $a_0x+b_0 \neq 0$ and $a_j, b_j \in \mathbb{F}_{p^m}$. Since $1 \leq i \leq \frac{p^s+t}{2}$, we have $t+j < T = \min\{i, p^s-i+t\} = i$. Therefore, $j \leq i-t-1$. Let

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

By Lemma 4.1 and removing all terms $u(x^2+\delta\gamma x+\frac{\gamma^2}{2})^j$ with $j \geq p^s-i$, it implies that

$$\begin{aligned} l^\star(x) = &\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s-i} - u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s-2i+t} \sum_{k=1}^{i-t-1} \\ &\times \left[\sum_{j=0}^{k-1} b_j \binom{i-t-j-1}{k-j-1}\right] (-1)^{i-t-k}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k \\ &- u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s-2i+t} \sum_{k=0}^{i-t-1} \left[\sum_{j=0}^{k} (a_j x-b_j)\binom{i-t-j-1}{k-j}\right] \\ &\times (-1)^{i-t-k-1}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k. \end{aligned}$$

Thus, we have

$$\begin{aligned} \mathcal{A}(C)^\star = \Bigg\langle &\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s-i} - u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s-2i+t} \sum_{k=1}^{i-t-1} \\ &\times \left[\sum_{j=0}^{k-1} b_j \binom{i-t-j-1}{k-j-1}\right] (-1)^{i-t-k}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k \\ &- u\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^{p^s-2i+t} \sum_{k=0}^{i-t-1} \left[\sum_{j=0}^{k} (a_j x-b_j)\binom{i-t-j-1}{k-j}\right] \\ &\times (-1)^{i-t-k-1}\left(x^2+\delta\gamma x+\frac{\gamma^2}{2}\right)^k \Bigg\rangle. \end{aligned}$$

The proof of part (2) is now complete. □

Theorem 4.5. *Let the λ-constacyclic code C be associated to the ideal*

$$I = \left\langle \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^i + u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^t h(x), u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^\omega \right\rangle,$$

where $h(x)$ is 0 or $h(x)$ is a unit. Then $\mathcal{A}(C)^\star$ is determined as follows:

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

$$\begin{aligned} d(x) = {} & \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-\omega} - u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-i-\omega+t} \sum_{k=1}^{\omega-t-1} \\ & \times \left[\sum_{j=0}^{k-1} b_j \binom{i-t-j-1}{k-j-1}\right] (-1)^{i-t-k} \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^k \\ & - u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-i-\omega+t} \sum_{k=0}^{\omega-t-1} \left[\sum_{j=0}^{k} (a_j x - b_j) \binom{i-t-j-1}{k-j}\right] \\ & \times (-1)^{i-t-k-1} \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^k. \end{aligned}$$

Proof. It is routine to check that if $h(x) = 0$, then $\mathcal{A}(C)^\star = \langle (x^2 + \delta\gamma x + \frac{\gamma^2}{2})^{p^s-\omega}, u(x^2 + \delta\gamma x + \frac{\gamma^2}{2})^{p^s-i}\rangle$, proving (1). We now give the proof of (2). A simple calculation shows that

$$\begin{aligned} I = \Bigg\langle & \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-\omega} - u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-i-\omega+t} h(x), \\ & u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-i} \Bigg\rangle \subseteq \mathcal{A}(C) \end{aligned}$$

and $n_C = p^{2m(i+\omega)}$. Then we can see that

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

Therefore, $\langle (x^2 + \delta\gamma x + \frac{\gamma^2}{2})^{p^s-\omega} - u(x^2 + \delta\gamma x + \frac{\gamma^2}{2})^{p^s-i-\omega+t} h(x), u(x^2 + \delta\gamma x + \frac{\gamma^2}{2})^{p^s-i}\rangle = \mathcal{A}(C)$. Let $h(x) = \sum_j (a_j x + b_j)(x^2 + \delta\gamma x + \frac{\gamma^2}{2})^j$, where $a_0 x + b_0 \neq 0$

and $a_j, b_j \in \mathbb{F}_{p^m}$. In this case $j \leq \omega - t - 1$. Let

$$l(x) = \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-\omega} - u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-i-\omega+t} \sum_{j=0}^{\omega-t-1} (a_j x + b_j) \times \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^j,$$

by Lemma 4.1 and removing all terms $u(x^2 + \delta\gamma x + \frac{\gamma^2}{2})^j$ with $j \geq p^s - i$, we get

$$\begin{aligned} l^\star(x) = {} & \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-\omega} - u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-i-\omega+t} \sum_{k=1}^{\omega-t-1} \\ & \times \left[\sum_{j=0}^{k-1} b_j \binom{i-t-j-1}{k-j-1}\right] (-1)^{i-t-k} \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^k \\ & - u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-i-\omega+t} \sum_{k=0}^{\omega-t-1} \left[\sum_{j=0}^{k} (a_j x - b_j) \binom{i-t-j-1}{k-j}\right] \\ & \times (-1)^{i-t-k-1} \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^k. \end{aligned}$$

Hence,

$$\begin{aligned} C^\perp = {} & \mathcal{A}(C)^\star \\ = {} & \left\langle \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-\omega} - u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-i-\omega+t} \sum_{k=1}^{\omega-t-1} \right. \\ & \times \left[\sum_{j=0}^{k-1} b_j \binom{i-t-j-1}{k-j-1}\right] (-1)^{i-t-k} \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^k \\ & - u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-i-\omega+t} \sum_{k=0}^{\omega-t-1} \left[\sum_{j=0}^{k} (a_j x - b_j) \binom{i-t-j-1}{k-j}\right] \\ & \left. \times (-1)^{i-t-k-1} \left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^k, u\left(x^2 + \delta\gamma x + \frac{\gamma^2}{2}\right)^{p^s-i} \right\rangle, \end{aligned}$$

completing the proof. □

In [10], we gave a new way to study the algebraic structures of λ-constacyclic codes of length $4p^s$ over $\mathcal{R}$. We proved an important observation that any nonzero polynomial of degree less than 4 in $\mathbb{F}_{p^m}[x]$ is invertible in $\frac{\mathcal{R}[x]}{\langle x^{4p^s}-\lambda\rangle}$, where λ is not a square in $\mathcal{R}$. This key result was then used to obtain that the ambient

ring $\frac{\mathcal{R}[x]}{\langle x^{4p^s}-\lambda\rangle}$ is a chain ring with maximal ideal $\langle x^4 - \alpha_0\rangle$, where $\lambda_0^{p^s} = \lambda$. However, as mentioned in [10], we only establish the algebraic structures of λ-constacyclic codes of length $4p^s$ over $\mathcal{R}$ for any prime p with $p^m \equiv 1 \pmod 4$ because otherwise, when $p^m \equiv 3 \pmod 4$, the polynomial $x^4 - \lambda_0$ can be decomposed as a product of two quadratic irreducible factors. This is the reason why the method in [10] cannot be used for studying the λ-constacyclic codes of length $4p^s$ for any prime p with $p^m \equiv 3 \pmod 4$. We can see that the unit elements of $\mathcal{R}$ can be expressed as two types, namely, $\lambda \in \mathbb{F}_{p^m} - \{0\}$, and $\alpha + u\beta$, where α, β are nonzero. This paper considered the λ-constacyclic codes of length $4p^s$ over $\mathcal{R}$, where $\lambda \in \mathbb{F}_{p^m} - \{0\}$. The class of $(\alpha + u\beta)$-constacyclic codes of length $4p^s$ over $\mathcal{R}$, where α, β are nonzero, is investigated in our other paper [12].

Acknowledgments

H. Q. Dinh and S. Sriboonchitta are grateful to the Central of Excellence in Econometrics of the Faculty of Economics, Chiang Mai University, for partial financial support. This paper was done during the visit of B. T. Nguyen and T. M. Vo to H. Q. Dinh at the Department of Mathematical Sciences, Kent State University, Ohio, USA, in November 2017 to January 2018. B. T. Nguyen and T. M. Vo are thankful for the hospitality and support of the Department of Mathematical Sciences, Kent State University. This work was also partially supported by a grant from the Simons Foundation. B. T. Nguyen is grateful to the Foundation for Science and Technology Development, Nguyen Tat Thanh University, for partial financial support.

References

[1] T. Abualrub and R. Oehmke, On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e, *IEEE Trans. Inform. Theory* **49** (2003) 2126–2133.
[2] M. M. Al-Ashker, Simplex codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, *Arab. J. Sci. Eng. Sect. A Sci.* **30** (2005) 277–285.
[3] E. Bannai, M. Harada, T. Ibukiyama, A. Munemasa and M. Oura, Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and applications to Hermitian modular forms, *Abh. Math. Sem. Univ. Hamburg* **73** (2003) 13–42.
[4] T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, *Discrete Appl. Math.* **128** (2003) 27–46.
[5] 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.
[6] 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.
[7] 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.
[8] H. Q. Dinh, Repeated-root constacyclic codes of length $2p^s$, *Finite Fields Appl.* **18** (2012) 133–143.
[9] H. Q. Dinh, Structure of repeated-root constacyclic codes of length $3p^s$ and their duals, *Discrete Math.* **313** (2013) 983–991.

[10] 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.
[11] H. Q. Dinh and S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inform. Theory* **50** (2004) 1728–1744.
[12] H. Q. Dinh, B. T. Nguyen, S. Sriboonchitta and T. M. Vo, On $(\alpha + \beta)$-constacyclic codes length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *J. Algebra Appl.* (2018), accepted for publication.
[13] H. Q. Dinh, L. Wang and S. Zhu, Negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *Finite Fields Appl.* **31** (2015) 178–201.
[14] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* **40** (1994) 301–319.
[15] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes* (Cambridge University Press, Cambridge, 2003).