Bull. Korean Math. Soc. **56** (2019), No. 6, pp. 1385–1422
https://doi.org/10.4134/BKMS.b180721
pISSN: 1015-8634 / eISSN: 2234-3016

NEGACYCLIC CODES OF LENGTH $8p^s$ OVER $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

Chakkrid Klin-eam and Jirayu Phuto

Abstract. Let p be an odd prime. The algebraic structure of all negacyclic codes of length $8p^s$ over the finite commutative chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ where $u^2 = 0$ is studied in this paper. Moreover, we classify all negacyclic codes of length $8p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ into 5 cases, i.e., $p^m \equiv 1 \pmod{16}$, $p^m \equiv 3, 11 \pmod{16}$, $p^m \equiv 5, 13 \pmod{16}$, $p^m \equiv 7, 15 \pmod{16}$ and $p^m \equiv 9 \pmod{16}$. From that, the structures of dual and some self-dual negacyclic codes and number of codewords of negacyclic codes are obtained.

1. Introduction

The class of constacyclic codes is an important class of linear codes in coding theory. Many optimal linear codes are directly derived from constacyclic codes. It includes a subclass of two classes, i.e., cyclic codes and negacyclic codes. Constacyclic codes have practical application as they can improve efficiency for encoding with shift registers. Moreover, in negacyclic codes, the dual code of each negacyclic code is a negacyclic code. This is the reason why negacyclic codes are interesting.

The negacyclic codes of length n over a finite field $\mathbb{F}$ are classified as polynomial generators $\langle g(x)\rangle$ of the ambient ring $\frac{\mathbb{F}[x]}{\langle x^n+1\rangle}$ where $g(x)$ is a divisor of $x^n + 1$. When the code-length n is relatively prime to the characteristic of the finite field $\mathbb{F}$, the code to be *simple root code*. Otherwise, it is called a *repeated-root code* which was first studied since the 1970's and 1980's by several authors such as Massey et al. [2], Falkner et al. [15], Roth and Seroussi [19]. Nonetheless, the repeated-root codes over finite fields were researched in the more general properties in the 1990's by Castagnoli et al. [2] and van Lint [17] where they showed that repeated-root cyclic codes have a concatenated construction, and asymptotically bad. Therefore, the repeated-root codes are interesting because they have rich algebraic structures.

The constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ are very interesting because the structure of $\mathbb{F}_2 + u\mathbb{F}_2$ is lying between $\mathbb{F}_{2^2}$ and $\mathbb{Z}_4$ in the sense that it is additively

Received August 1, 2018; Revised December 7, 2018; Accepted April 25, 2019.
2010 *Mathematics Subject Classification.* Primary 94B15, 94B05; Secondary 11T71.
Key words and phrases. negacyclic codes, finite chain rings, constacyclic codes, repeated-root codes.

analogous to $\mathbb{F}_{2^2}$ and multiplication analogous to $\mathbb{Z}_4$ (see [1,5]). Moreover, the cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$ can construct to be DNA codes for computing which is important for biology (see [16]). So, many mathematicians are interested in cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$ and study the codes which are more general than cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$, i.e., constacyclic codes of length n over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$. The classification of codes is important in studying their structures but it is hard to classify them. In studying the repeated-root constacyclic codes over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, it is difficult to study the codes of length n. In number theory, we see that any integer n can be expressed as $n=p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k}$ where i,k,s_i are positive integers and p_i is a distinct prime, $1\leq i\leq k$. Therefore, we first study the codes of length p^s and generalize to qp^s where p and q are relatively primes. Dinh et al. got the results of classifying constacyclic codes of certain lengths over certain finite fields or finite chain rings. Furthermore, they established the structures of constacyclic codes of length $2p^s$ and $3p^s$ over $\mathbb{F}_{p^m}$ (see [7,8]). In 2004, cyclic and negacyclic codes over finite chain rings are studied by Dinh and López-Permouth (see [11]). They have obtained the algebraic structure of negacyclic codes and self-dual negacyclic codes of length 2^t over $\mathbb{Z}_{2^m}$. In 2005, Dihn [4] determine the algebraic structure of negacyclic codes of length 2^s over Galois rings. However, they obtain that Hamming distance and the weight distribitions of such negacyclic codes. In 2009, Dihn [5] investigated all constacyclic codes of length 2^s over the Galois ring $\mathbb{F}_2+u\mathbb{F}_2$ where $u^2=0$. They first obtain the structure of $(1+u\gamma)$-constacyclic codes of length 2^s over $GR(\mathbb{F}_2+u\mathbb{F}_2,m)$ for any nonzero element $\gamma\in\mathbb{F}_{2^m}$. Using the structure, they derive the Hamming distances of all codes. In addition, they get the structure of cyclic codes of length 2^s over $GR(\mathbb{F}_2+u\mathbb{F}_2,m)$ and the number of codewords. After that, they define one-to-one correspondence between cyclic and α-constacyclic codes, including $(1+u\gamma)$-constacyclic and $(\alpha+u\beta)$-constacyclic codes where nonzero elements $\alpha,\beta\in\mathbb{F}_{2^m}$. In 2010, Dihn [6] determined in the algebraic structures of constacyclic codes of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ and their dual codes. He obtained that the all ideals of a local ring $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle x^{p^s}-\lambda\rangle}$ when $\lambda\in\mathbb{F}_{p^m}\backslash\{0\}$ but it is not a chain ring. For $\lambda=\alpha+u\beta$ where $\alpha,\beta\in\mathbb{F}_{p^m}\backslash\{0\}$, he got $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle x^{p^s}-\lambda\rangle}$ is a chain ring. In 2014, X. Liu and X. Xu [18] obtained that the algebraic structure of cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$. Using Chinese Remainder Theorem, they obtain that the structure of such cyclic and negacyclic codes for $p\equiv 1 \pmod 4$, or $p\equiv 3 \pmod 3$ and m is even. For $p\equiv 3 \pmod 4$ and m is odd, they derive the algebraic structure of the quotient ring $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle x^{2p^s}+1\rangle}$ is a local ring with the maximal ideal $\langle u,x^2+1\rangle$. In 2015, Dinh et al. [14] got the algebraic structures of negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ and their dual codes. They divide the structures of such negacyclic codes into 2 cases: $p^m\equiv 1 \pmod 4$ and $p^m\equiv 3 \pmod 4$. When $p^m\equiv 1 \pmod 4$, each negacyclic code is represented as a direct sum of a $-\alpha$-constacyclic code and

an α-constacyclic code of length p^s. For $p^m \equiv 3 \pmod 4$, each negacyclic code is classified into 4 distinct types of ideals. Moreover, they get the algebraic structures of constacyclic codes of same length over same ring (see [3]). For such λ-constacyclic codes, they divide the structures into 2 cases: $\lambda = \alpha + u\beta$ or $\lambda \in \mathbb{F}_{p^m}$. When λ is a square, by Chinese Remainder Theorem, they obtain the structure of such constacyclic codes. For λ is not a square and $\lambda = \alpha + u\beta$, they get that $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle x^{2p^s}-(\alpha+u\beta)\rangle}$ is a chain ring. The remaining case, λ is not a square and $\lambda \in \mathbb{F}_{p^m}$, such constacyclic codes are classified into 4 distinct types of ideals. In 2018, Dinh et al. [12] determined the algebraic structures of negacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and their dual codes. Moreover, they determined the ideals of the rings $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle(x^2+\mu\nu x+1)^{p^s}\rangle}$ and $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle(x^2+\mu\delta x-1)^{p^s}\rangle}$ where $\delta^2 = -2$ or $\nu^2 = 2$ and $\mu \in \{-1, 1\}$. Thus, we focus on the negacyclic codes of length $8p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ to determine the structures of such negacyclic codes and their dual codes.

The aim of this paper is to determine structures of negacyclic codes of length $8p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}(u^2 = 0)$ where p is an odd prime. We divide the structures of such negacyclic codes into 5 cases: $p^m \equiv 1 \pmod{16}$, $p^m \equiv 3, 11 \pmod{16}$, $p^m \equiv 5, 13 \pmod{16}$, $p^m \equiv 7, 15 \pmod{16}$ or $p^m \equiv 9 \pmod{16}$. Moreover, we obtained that the number of codewords for each negacyclic codes and the algebraic structures of dual codes of such negacyclic codes. However, we use the technique in the paper [12] to investigate our aim. The remainder of this paper is organized as follows. Preliminary concepts is shown in Section 2. In Sections 3, 4, 5, 6 and 7; we give the structures of negacyclic codes of length $8p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. When $p^m \equiv 1 \pmod{16}$ (Section 3) or $p^m \equiv 5, 13 \pmod{16}$ (Section 5) or $p^m \equiv 9 \pmod{16}$ (Section 7), using Chinese Remainder Theorem, we obtained the structures of such negacyclic codes. For $p^m \equiv 3, 11 \pmod{16}$ (Section 4) or $p^m \equiv 7, 15 \pmod{16}$ (Section 6), we use some square elements to obtain that the structures of such negacyclic codes.

2. Preliminaries

All rings are commutative rings with identity. An ideal I of a ring is called a *principal ideal* if it is generated by a single element. A ring R is said to be a *principal ideal ring* if its ideals are principal ideals. R is called a *local ring* 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. The following equivalent conditions are known for the class of finite commutative rings with identity.

Proposition 2.1 ([14]). *Let R be 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 $\langle r^i \rangle$, $0 \leqslant i \leqslant N(r)$, where $N(r)$ is the nilpotency index of r.*

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

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

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. If $\lambda = -1$, this code is called a *negacyclic code* and if $\lambda = 1$, it is called a *cyclic 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. So, in the quotient ring $\frac{R[x]}{\langle x^n - \lambda \rangle}$, $xc(x)$ corresponds to the λ-constacyclic shift of c. Thus, the following fact is well known and straightforward:

Proposition 2.2 ([14]). *A linear code C of length n over a ring R is a λ-constacyclic code if and only if C is an ideal of the quotient ring $\frac{R[x]}{\langle x^n - \lambda \rangle}$.*

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 $C = C^\perp$. Moreover, C is called *isodual* if C permutationally and monomially is equivalent to $C^\perp$ (that is, $C^\perp$ can be obtained from C by permuting the coordinates and multiplying certain coordinates by certain constants). The following result is well known.

Proposition 2.3 ([14]). *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 ([14]). *The dual of each λ-constacyclic code is a λ^{-1}-constacyclic code.*

In this paper, we determine of the algebraic structure of all negacyclic codes of length $8p^s$ over the ring $R = \frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$. 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 the maximal ideal $\langle u\rangle$, and then, it is a chain ring.

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

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

Moreover, we denote *the order of element* a by $ord(a)$. Hereafter, we denote the quotient ring of negacyclic codes of length $8p^s$ over R as

$$\mathcal{R} = \frac{R[x]}{\langle x^{8p^s} + 1\rangle}.$$

From Proposition 2.2, each negacyclic code of length $8p^s$ over R is an ideal of $\mathcal{R}$. Moreover, by Proposition 2.4, the dual code of each negacyclic code of length $8p^s$ over R is a negacyclic code.

Definition 2.5 ([14])**.** If $f(x) = a_0 + a_1x + \cdots + a_rx^r$, then *the reciprocal of* $f(x)$ is the polynomial $f^*(x) = a_r + a_{r-1}x + a_{r-2}x^2 + \cdots + a_0x^r$.

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

Definition 2.6 ([14])**.** 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 $\mathcal{R}$.

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

Lemma 2.7 ([14])**.**

(i) $(f(x)g(x))^* = f^*(x)g^*(x)$.
(ii) *If* $\deg f \geq \deg g$, *then* $(f(x) + g(x))^* = f^*(x) + x^{\deg f - \deg g}g^*(x)$.
(iii) *Let* $I = \langle f(x), ug(x)\rangle$ *be an ideal of* $\mathcal{R}$. *Then* $I^* = \langle f^*(x), ug^*(x)\rangle$.

For each code C of length n over R, their *torsion and residue codes* are codes over $\mathbb{F}_{p^m}$, defined as follows:

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

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

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

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

Proposition 2.8 ([14]). *Let C be a code of length n over R whose torsion and residue codes are* $\mathrm{Tor}(C)$ *and* $\mathrm{Res}(C)$*, respectively. Then*

$$|C| = |\,\mathrm{Tor}(C)| \cdot |\,\mathrm{Res}(C)|.$$

To study the structure of all negacyclic codes of length $8p^s$ over R, we need to separate such negacyclic codes into 5 cases, that is, $p^m \equiv 1 \pmod{16}$, $p^m \equiv 3, 11 \pmod{16}$, $p^m \equiv 5, 13 \pmod{16}$, $p^m \equiv 7, 15 \pmod{16}$ and $p^m \equiv 9 \pmod{16}$. Firstly, we determine the algebraic structure and number of codewords of negacyclic codes of length $8p^s$ over R with $p^m \equiv 1 \pmod{16}$ in Section 3.

3. The case $p^m \equiv 1 \pmod{16}$

In this section, we always assume that $p^m \equiv 1 \pmod{16}$. By Proposition 2.2, we have that each negacyclic code of length $8p^s$ over R is an ideal of the quotient ring $\frac{R[x]}{\langle x^{8p^s}+1\rangle}$. Since ξ is a primitive (p^m-1)th root of identity in $\mathbb{F}_{p^m}$, the polynomial $x^{8p^s}+1$ can be expressed as

$$\begin{aligned} x^{8p^s}+1 &= (x^8+1)^{p^s} \\ &= (x-\gamma)^{p^s}(x-\gamma^3)^{p^s}(x-\gamma^5)^{p^s}(x-\gamma^7)^{p^s}(x-\gamma^9)^{p^s}(x-\gamma^{11})^{p^s} \\ &\quad (x-\gamma^{13})^{p^s}(x-\gamma^{15})^{p^s} \\ &= (x^{p^s}-\gamma^{p^s})(x^{p^s}-\gamma^{3p^s})(x^{p^s}-\gamma^{5p^s})(x^{p^s}-\gamma^{7p^s})(x^{p^s}-\gamma^{9p^s}) \\ &\quad (x^{p^s}-\gamma^{11p^s})(x^{p^s}-\gamma^{13p^s})(x^{p^s}-\gamma^{15p^s}), \end{aligned}$$

where $\gamma = \xi^{(p^m-1)/16}$.

Remark 3.1. $\gamma^{ip^s}\gamma^{jp^s} = 1$ where $i, j = 1, 3, 5, 7, 9, 11, 13, 15$ and $i + j = 16$.

By using Chinese Remainder Theorem, we obtain that the algebraic structure of each negacyclic code of length $8p^s$ over R in the following theorem.

Theorem 3.2. *Each negacyclic code of length $8p^s$ over R is a direct sum of γ^{p^s}, γ^{3p^s}, γ^{5p^s}, γ^{7p^s}, γ^{9p^s}, γ^{11p^s}, γ^{13p^s} and γ^{15p^s}-constacyclic codes of length p^s over R. Moreover, $|C| = |C_1||C_3||C_5||C_7||C_9||C_{11}||C_{13}||C_{15}|$ where C is a negacyclic code of length $8p^s$ over R and C_i is a γ^{ip^s}-constacyclic code of length p^s over R where $i = 1, 3, 5, 7, 9, 11, 13, 15$.*

Proof. Clearly, for each $i, j = 1, 3, 5, 7, 9, 11, 13, 15$ with $i \neq j$, $\langle x^{p^s} - \gamma^{ip^s}\rangle$ and $\langle x^{p^s} - \gamma^{jp^s}\rangle$ are pairwise coprime. By Chinese Remainder Theorem, we have

$$\begin{aligned} \frac{R[x]}{\langle x^{8p^s}+1\rangle} \cong\ & \frac{R[x]}{\langle x^{p^s}-\gamma^{p^s}\rangle} \oplus \frac{R[x]}{\langle x^{p^s}-\gamma^{3p^s}\rangle} \oplus \frac{R[x]}{\langle x^{p^s}-\gamma^{5p^s}\rangle} \oplus \frac{R[x]}{\langle x^{p^s}-\gamma^{7p^s}\rangle} \\ & \oplus \frac{R[x]}{\langle x^{p^s}-\gamma^{9p^s}\rangle} \oplus \frac{R[x]}{\langle x^{p^s}-\gamma^{11p^s}\rangle} \oplus \frac{R[x]}{\langle x^{p^s}-\gamma^{15p^s}\rangle}. \end{aligned}$$

Let C be a negacyclic code of length $8p^s$ over R. In light of Proposition 2.2, C is an ideal of $\frac{R[x]}{\langle x^{8p^s}+1\rangle}$. So, $C = C_1 \oplus C_3 \oplus C_5 \oplus C_7 \oplus C_9 \oplus C_{11} \oplus C_{13} \oplus C_{15}$

where C_i is an ideal of $\frac{R[x]}{\langle x^{p^s}-\gamma^{ip^s}\rangle}$ where $i = 1, 3, 5, 7, 9, 11, 13, 15$. This means that C_i is an γ^{ip^s}-constacyclic code of length p^s over R. □

Thus, the negacyclic codes C of length $8p^s$ over R can be represented as a direct sum of γ^{p^s}, γ^{3p^s}, γ^{5p^s}, γ^{7p^s}, γ^{9p^s}, γ^{11p^s}, γ^{13p^s} and γ^{15p^s}-constacyclic codes of length p^s over R. Note that the algebraic structures of all constacyclic codes of length p^s over R have been studied in [6]. Furthermore, by Proposition 2.4, the algebraic structures of dual codes of such negacyclic codes are obtained as the following theorem.

Theorem 3.3. *Let $C = C_1 \oplus C_3 \oplus C_5 \oplus C_7 \oplus C_9 \oplus C_{11} \oplus C_{13} \oplus C_{15}$ be a negacyclic code of length $8p^s$ over R where C_i is a γ^{ip^s}-constacyclic code of length p^s over R for $i = 1, 3, 5, 7, 9, 11, 13, 15$. Then $C^\perp = C_{15} \oplus C_{13} \oplus C_{11} \oplus C_9 \oplus C_7 \oplus C_5 \oplus C_3 \oplus C_1$. In particular, $|C^\perp| = |C_1||C_3||C_5||C_7||C_9||C_{11}||C_{11}||C_{13}||C_{15}|$.*

Proof. It is obvious that

$$C_1^\perp \oplus C_3^\perp \oplus C_5^\perp \oplus C_7^\perp \oplus C_9^\perp \oplus C_{11}^\perp \oplus C_{11}^\perp \oplus C_{13}^\perp \oplus C_{15}^\perp \subseteq C^\perp.$$

We consider that

$$\begin{aligned}
&|C_1^\perp||C_3^\perp||C_5^\perp||C_7^\perp||C_9^\perp||C_{11}^\perp||C_{11}^\perp||C_{13}^\perp||C_{15}^\perp| \\
&= \frac{|R|^{p^s}}{|C_1|}\frac{|R|^{p^s}}{|C_3|}\frac{|R|^{p^s}}{|C_5|}\frac{|R|^{p^s}}{|C_7|}\frac{|R|^{p^s}}{|C_9|}\frac{|R|^{p^s}}{|C_{11}|}\frac{|R|^{p^s}}{|C_{13}|}\frac{|R|^{p^s}}{|C_{15}|} \\
&= \frac{|R|^{8p^s}}{|C_1||C_3||C_5||C_7||C_9||C_{11}||C_{13}||C_{15}|} \\
&= \frac{|R|^{8p^s}}{|C|} \\
&= |C^\perp|.
\end{aligned}$$

Hence, $C^\perp = C_1^\perp \oplus C_3^\perp \oplus C_5^\perp \oplus C_7^\perp \oplus C_9^\perp \oplus C_{11}^\perp \oplus C_{13}^\perp \oplus C_{15}^\perp$. Using Proposition 2.4, the dual code $C_i^\perp$ is a γ^{jp^s}-constacyclic code of length p^s over R where $i+j = 16$. Therefore, the dual code $C^\perp = C_{15} \oplus C_{13} \oplus C_{11} \oplus C_9 \oplus C_7 \oplus C_5 \oplus C_3 \oplus C_1$. □

From Theorem 3.3, we see that the dual code of negacyclic codes of length $8p^s$ over R is an isodual code.

The following result can be found in [10, Section 5], and will apply to determine self-dual of negacyclic codes of length $8p^s$ over $\mathcal{R}$:

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, $\langle u\rangle$ is the unique self-dual γ^{ip^s}-constacyclic codes of length p^s over R because $\gamma^{ip^s} \neq \gamma^{jp^s} = \left(\gamma^{ip^s}\right)^{-1}$ for each $i = 1, 3, 5, 7, 9, 11, 13, 15$ and $i+j = 16$. Now, we obtain that the following result for self-dual negacyclic codes of length $8p^s$ over R as follows:

Corollary 3.4. *Let $C = C_1 \oplus C_3 \oplus C_5 \oplus C_7 \oplus C_9 \oplus C_{11} \oplus C_{13} \oplus C_{15}$ be a negacyclic code of length $8p^s$ over R where C_i is a γ^{ip^s}-constacyclic code of length p^s over R for $i = 1, 3, 5, 7, 9, 11, 13, 15$. Then $C = \langle u \rangle$ is the unique self-dual negacyclic codes of length $8p^s$ over R.*

4. The cases $p^m \equiv 3 \pmod{16}$ or $p^m \equiv 11 \pmod{16}$

In this section, we assume that $p^m \equiv 3 \pmod{16}$ or $p^m \equiv 11 \pmod{16}$, and then $p^m \equiv 3 \pmod 8$. This implies that $p \equiv 3 \pmod 8$. Thus, -2 is a square element in $\mathbb{F}_{p^m}$, i.e., there exists $\delta \in \mathbb{F}_{p^m}$ such that $\delta^2 = -2$. We now consider

$$\begin{aligned} x^{8p^s} + 1 &= (x^8 + 1)^{p^s} \\ &= (x^8 - 2x^4 + 1 + 2x^4)^{p^s} \\ &= ((x^4 - 1)^2 - \delta^2 x^4)^{p^s} \\ &= (x^4 - \delta x^2 - 1)^{p^s} (x^4 + \delta x^2 - 1)^{p^s}. \end{aligned}$$

Next, we give the properties for investigating the algebraic structures of such negacyclic codes as the following lemma.

Lemma 4.1.

(i) *The polynomial $x^2 + 1$ is irreducible over $\mathbb{F}_{p^m}$.*
(ii) *The polynomial $x^2 + 1$ is irreducible over R.*
(iii) *The polynomials $x^2 + a\delta x - a^2$ and $x^2 - a\delta x - a^2$ are irreducible over $\mathbb{F}_{p^m}$ where $a \in \mathbb{F}_{p^m} \setminus \{0\}$.*
(iv) *The polynomials $x^4 - \delta x^2 - 1$ and $x^4 + \delta x^2 - 1$ are irreducible over $\mathbb{F}_{p^m}$.*
(v) *The polynomials $x^4 - \delta x^2 - 1$ and $x^4 + \delta x^2 - 1$ are irreducible over R.*
(vi) *$x^4 - \delta x^2 - 1$ and $x^4 + \delta x^2 - 1$ are coprimes in $R[x]$.*

Proof. (i) Suppose that x^2+1 is reducible over $\mathbb{F}_{p^m}$. There exists $\beta \in \mathbb{F}_{p^m}$ such that $\beta^2+1 = 0$, implying that $\beta^4 = 1$. If $ord(\beta) = 1$ or 2, then $\beta^2+1 = 1+1 \neq 0$. It is a contradiction. Thus, $ord(\beta) = 4$. This implies that $4 \mid (p^m - 1)$ and, then $p^m \equiv 1 \pmod 4$. It is a contradiction. Hence, $x^2 + 1$ is irreducible over $\mathbb{F}_{p^m}$.

(ii) Suppose that $x^2 + 1$ is reducible over R. There exists $\beta_0 + u\beta_1 \in R$ such that $(\beta_0 + u\beta_1)^2 + 1 = 0$. We consider that

$$\begin{aligned} 0 &= (\beta_0 + u\beta_1)^2 + 1 \\ &= \beta_0^2 + u(2\beta_0\beta_1) + 1. \end{aligned}$$

This implies that $0 = \beta_0^2 + 1$ and $0 = 2\beta_0\beta_1$. It is a contradiction by Lemma 4.1(i).

(iii) We will show that $x^2 + a\delta x - a^2$ is irreducible over $\mathbb{F}_{p^m}$. Suppose that $x^2 + a\delta x - a^2$ is reducible over $\mathbb{F}_{p^m}$. There exists $\beta \in \mathbb{F}_{p^m}$ such that $\beta^2 + a\delta\beta - a^2 = 0$. So, β is a root of x^4+a^4 because $x^4+a^4 = (x^2+a\delta x-a^2)(x^2-a\delta x-a^2)$. Thus, $\beta^4 + a^4 = 0$, implying $(\beta a^{-1})^4 = -1$. This means that $(\beta a^{-1})^8 = 1$. So, $ord(\beta a^{-1}) \mid 8$, i.e., $ord(\beta a^{-1}) = 1$ or 2 or 4 or 8. If $ord(\beta a^{-1}) = 1$ or 2

or 4, then $0 = \beta^4 + a^4 = 1 + a^4$, and thus $a^4 = -1 = \xi^{\frac{p^m-1}{2}}$. Now, we have $a = \xi^{\frac{p^m-1}{8}}$. Thus, $p^m \equiv 1 \pmod 8$. It is a contraction. Hence, $ord(\beta a^{-1}) = 8$. This implies that $8 \mid (p^m - 1)$, and then $p^m \equiv 1 \pmod 8$. It is a contradiction. Therefore, $x^2 + a\delta x - a^2$ is irreducible over $\mathbb{F}_{p^m}$. Similarly, $x^2 - a\delta x - a^2$ is irreducible over $\mathbb{F}_{p^m}$.

(iv) We will show that $x^4 - \delta x^2 - 1$ is irreducible over $\mathbb{F}_{p^m}$. Suppose that $x^4 - \delta x^2 - 1$ is reducible over $\mathbb{F}_{p^m}$. There exist $f(x), g(x) \in \mathbb{F}_{p^m}[x]$ such that $x^4 - \delta x^2 - 1 = f(x)g(x)$.

If $\deg f(x) = 1$, then $\deg g(x) = 3$. So, there exists $\beta \in \mathbb{F}_{p^m}$ such that $f(\beta) = 0$. Since

$$\begin{aligned} x^8 + 1 &= (x^4 - \delta x^2 - 1)(x^4 + \delta x^2 - 1) \\ &= f(x)g(x)(x^4 + \delta x^2 - 1), \end{aligned}$$

we have β is a root of $x^8 + 1$, implying that $\beta^{16} = 1$. Thus, $ord(\beta) \mid 16$. If $ord(\beta) = 1$ or 2 or 4 or 8, then $\beta^8 + 1 = 1 + 1 \neq 0$. This means that $ord(\beta) = 16$. So, $16 \mid (p^m - 1)$, i.e., $p^m \equiv 1 \pmod{16}$. It is a contradiction.

If $\deg f(x) = 2$, then $\deg g(x) = 2$. Let $f(x) = x^2 + ax + b$ and $g(x) = x^2 + cx + d$ for some $a, b, c, d \in \mathbb{F}_{p^m}$. Then

$$\begin{aligned} x^4 - \delta x^2 - 1 &= f(x)g(x) \\ &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (c + a)x^3 + (d + ac + b)x^2 + (ad + bc)x + bd. \end{aligned}$$

Thus,

$$c + a = 0, \tag{4.1}$$

$$d + ac + b = -\delta, \tag{4.2}$$

$$ad + bc = 0, \tag{4.3}$$

$$bd = -1. \tag{4.4}$$

From (4.1) and (4.4), we get that $c = -a$ and $b = -d^{-1}$. This implies that $0 = ad + bc = ad + d^{-1}a = a(d + d^{-1})$. So, $a = 0$ or $d + d^{-1} = 0$. If $a = 0$, then $c = 0$. Thus, $-\delta = d + ac + b = d - d^{-1}$. We consider that

$$\begin{aligned} -2 &= (-\delta)^2 \\ &= (d - d^{-1})^2 \\ &= d^2 - 2 + d^{-2}. \end{aligned}$$

This means that $d^2 = -d^{-2}$, implying $d^4 = -1$. So, $d^8 = 1$. Now, we see that $ord(d) = 8$. Thus, $8 \mid (p^m - 1)$. That is $p^m \equiv 1 \pmod 8$. It is a contradiction. If $d + d^{-1} = 0$, then $d^4 = 1$. So, $4 \mid (p^m - 1)$. Now, we see that $p^m \equiv 1 \pmod 4$. It is a contradiction. Similarly, $x^4 + \delta x^2 - 1$ is irreducible over $\mathbb{F}_{p^m}$.

(v) Suppose that $x^4 - \delta x^2 - 1$ is reducible over R. Then $x^4 - \delta x^2 - 1 = f(x)g(x)$ for some $f(x), g(x) \in R[x]$.

If $\deg f(x) = 1$, then $\deg g(x) = 3$. There exists $\beta_0 + u\beta_1 \in R$ such that $f(\beta_0 + u\beta_1) = 0$. Since $x^8 + 1 = (x^4 - \delta x^2 - 1)(x^4 + \delta x^2 - 1)$, $\beta_0 + u\beta_1$ is a root of $x^8 + 1$. Thus, $-1 = (\beta_0 + u\beta_1)^8 = \beta_0^8 + 8u\beta_0^7\beta_1$, implying $-1 = \beta_0^8$ and $8\beta_0^7\beta_1 = 0$. Now, we have $\beta_0^{16} = 1$. So, $ord(\beta_0) \mid 16$, i.e., $ord(\beta_0) = 1$ or 2 or 4 or 8 or 16. If $ord(\beta_0) = 1$ or 2 or 4 or 8, then $\beta_0^8 + 1 = 1 + 1 \neq 0$. It is a contradiction. Thus, $ord(\beta_0) = 16$. This implies that $16 \mid (p^m - 1)$, i.e., $p^m \equiv 1 \pmod{16}$. It is a contradiction.

If $\deg f(x) = 2$, then $\deg g(x) = 2$. Let $f(x) = x^2 + (a_0 + ua_1)x + (b_0 + ub_1)$ and $g(x) = x^2 + (c_0 + uc_1)x + (d_0 + ud_1)$ where $a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 \in \mathbb{F}_{p^m}$. We consider

$$\begin{aligned}
&x^4 - \delta x^2 - 1 \\
&= f(x)g(x) \\
&= (x^2 + (a_0 + ua_1)x + (b_0 + ub_1))(x^2 + (c_0 + uc_1)x + (d_0 + ud_1)) \\
&= x^4 + (c_0 + a_0 + u(c_1 + a_1))x^3 + (d_0 + a_0c_0 + b_0 + u(d_1 + a_1c_0 + a_0c_1 + b_1))x^2 \\
&\quad + (a_0d_0 + b_0c_0 + u(a_1d_0 + a_0d_1 + b_1c_0 + c_1b_0))x + b_0d_0 + u(b_1d_0 + b_0d_1).
\end{aligned}$$

Thus, we have

$$\begin{aligned}
c_0 + a_0 + u(c_1 + a_1) &= 0, \\
d_0 + a_0c_0 + b_0 + u(d_1 + a_1c_0 + a_0c_1 + b_1) &= -\delta, \\
a_0d_0 + b_0c_0 + u(a_1d_0 + a_0d_1 + b_1c_0 + c_1b_0) &= 0, \\
b_0d_0 + u(b_1d_0 + b_0d_1) &= -1.
\end{aligned}$$

This implies that

$$c_0 + a_0 = 0, \tag{4.5}$$

$$c_1 + a_1 = 0, \tag{4.6}$$

$$d_0 + a_0c_0 + b_0 = -\delta, \tag{4.7}$$

$$d_1 + a_1c_0 + a_0c_1 + b_1 = 0, \tag{4.8}$$

$$a_0d_0 + b_0c_0 = 0, \tag{4.9}$$

$$a_1d_0 + a_0d_1 + b_1c_0 + c_1b_0 = 0, \tag{4.10}$$

$$b_0d_0 = -1, \tag{4.11}$$

$$b_1d_0 + b_0d_1 = 0. \tag{4.12}$$

By Lemma 4.1(iv) and equations (4.5), (4.7), (4.9) and (4.11), it is impossible to find a_0, b_0, c_0, d_0. So, it is a contradiction. Hence, $x^4 - \delta x^2 - 1$ is irreducible over R.

(vi) Suppose that $x^4 - \delta x^2 - 1$ and $x^4 + \delta x^2 - 1$ are not coprime. By Lemma 4.1(v), $\gcd(x^4 - \delta x^2 - 1, x^4 + \delta x^2 - 1) = x^4 - \delta x^2 - 1$ or $x^4 + \delta x^2 - 1$. This means that $-\delta = \delta$. It is a contradiction. Hence, $x^4 - \delta x^2 - 1$ and $x^4 + \delta x^2 - 1$ are coprimes. □

Using Chinese Remainder Theorem, we obtain that the algebraic structures of negacyclic codes of length $8p^s$ over R as follows:

Theorem 4.2. *Let C be a negacyclic code of length $8p^s$ over R. Then*

(i) $C = I_{-\delta} \oplus I_\delta$ *where* $I_{-\delta}$ *and* I_δ *are ideals of* $\frac{R[x]}{\langle (x^4-\delta x^2-1)^{p^s}\rangle}$, $\frac{R[x]}{(x^4+\delta x^2-1)^{p^s}\rangle}$, *respectively.*

(ii) $|C| = |I_{-\delta}||I_\delta|$.

(iii) *The dual code* $C^\perp$ *of* C *is given by* $C^\perp = \mathcal{A}(I_{-\delta})^* \oplus \mathcal{A}(I_\delta)^*$.

(iv) $|C^\perp| = |\mathcal{A}(I_{-\delta})^*||\mathcal{A}(I_\delta)^*|$.

Now, we determine the ideals of the quotient ring $\frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s}\rangle}$ where $\eta \in \{-1, 1\}$.

Proposition 4.3. *Each nonzero polynomial* $f(x) = ax^3 + bx^2 + cx + d$ *is invertible in* $\frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s}\rangle}$ *where* $a, b, c, d \in \mathbb{F}_{p^m}$.

Proof. If $a = b = c = 0$, then $f(x) = d \neq 0$ is invetible.

If $a = b = 0$ and $c \neq 0$, then $f(x) = cx + d$.

$$\begin{aligned}
f(x)^{-1} &= (cx+d)^{-1} \\
&= c^{-1}(x + c^{-1}d)^{-1} \\
&= c^{-1}(x + c^{-1}d)^{p^s-1}(x + c^{-1}d)^{-p^s}(x^3 - c^{-1}dx^2 + ((c^{-1}d)^2 + \eta\delta)x \\
&\quad - (c^{-1}d)((c^{-1}d)^2 + \eta\delta))^{-p^s} \\
&\quad (x^3 - c^{-1}dx^2 + ((c^1d)^2 + \eta\delta)x - (c^{-1}d)((c^{-1}d)^2 + \eta\delta))^{p^s} \\
&= c^{-1}(x + c^{-1}d)^{p^s-1}(x^3 - c^{-1}dx^2 + ((c^1d)^2 + \eta\delta)x \\
&\quad - (c^{-1}d)((c^{-1}d)^2 + \eta\delta))^{p^s} \\
&\quad (x^4 + \eta\delta x^2 - (c^{-1}d)^2((c^{-1}d)^2 + \eta\delta))^{-p^s} \\
&= c^{-1}(x + c^{-1}d)^{p^s-1}(x^3 - c^{-1}dx^2 + ((c^{-1}d)^2 + \eta\delta)x \\
&\quad - (c^{-1}d)((c^{-1}d)^2 + \eta\delta))^{p^s} \\
&\quad ((x^4 + \eta\delta x^2)^{p^s} - ((c^{-1}d)^2((c^{-1}d)^2 + \eta\delta))^{p^s})^{-1} \\
&= c^{-1}(x + c^{-1}d)^{p^s-1}(x^3 - c^{-1}dx^2 + ((c^{-1}d)^2 + \eta\delta)x \\
&\quad - (c^{-1}d)((c^{-1}d)^2 + \eta\delta))^{p^s}((1)^{p^s} - (c^{-1}d)^2((c^{-1}d)^2 + \eta\delta))^{p^s})^{-1} \\
&= -c^{-1}(x + c^{-1}d)^{p^s-1}(x^3 - c^{-1}dx^2 + ((c^{-1}d)^2 + \eta\delta)x \\
&\quad - (c^{-1}d)((c^1d)^2 + \eta\delta))^{p^s}((c^{-1}d)^4 + \eta\delta(c^{-1}d)^2 - 1)^{-p^s}.
\end{aligned}$$

Thus, $f(x)$ is invertible if and only if $(c^{-1}d)^4 + \eta\delta(c^{-1}d)^2 - 1 \neq 0$. By Lemma 4.1(iv), we get that $(c^{-1}d)^4 + \eta\delta(c^{-1}d)^2 - 1 \neq 0$. Hence, $f(x)$ is invertible.

If $a = 0$ and $b \neq 0$, then $f(x) = bx^2 + cx + d$. First of all, we will show that $x^2 + e$ is invertible over $\frac{R[x]}{(x^4+\eta\delta x^2-1)^{p^s}\rangle}$ where $e \in \mathbb{F}_{p^m}$. We consider that

$$(x^2+e)^{-1} = (x^2+e)^{p^s-1}(x^2 - e + \eta\delta)^{p^s}(x^2+e)^{-p^s}(x^2 - e + \eta\delta)^{-p^s}$$

$$\begin{aligned}
&= (x^2+e)^{p^s-1}(x^2-e+\eta\delta)^{p^s}(x^4+\eta\delta x^2-e^2+\eta\delta e)^{-p^s}\\
&= (x^2+e)^{p^s-1}(x^2-e+\eta\delta)^{p^s}((x^4+\eta\delta x^2)^{p^s}-(e^2+\eta\delta e)^{-p^s})^{-1}\\
&= (x^2+e)^{p^s-1}(x^2-e+\eta\delta)^{p^s}((1)^{p^s}-(e^2+\eta\delta e)^{-p^s})^{-1}\\
&= -(x^2+e)^{p^s-1}(x^2-e+\eta\delta)^{p^s}(e^2+\eta\delta e-1)^{-p^s}.
\end{aligned}$$

Thus, x^2+e is invertible if and only if $e^2+\eta\delta e-1\neq 0$. By Lemma 4.1(iv), we have $e^2+\eta\delta e-1\neq 0$. This implies that x^2+e is invertible. Now, we consider that

$$\begin{aligned}
f(x)^{-1} &= b^{-1}(x^2+b^{-1}cx+b^{-1}d)^{-1}\\
&= b^{-1}(x^2+b^{-1}cx+b^{-1}d)^{p^s-1}(x^2-b^{-1}cx+b^{-1}d)^{p^s}\\
&\quad (x^2+b^{-1}cx+b^{-1}d)^{-p^s}(x^2-b^{-1}cx+b^{-1}d)^{-p^s}\\
&= b^{-1}(x^2+b^{-1}cx+b^{-1}d)^{p^s-1}(x^2-b^{-1}cx+b^{-1}d)^{p^s}\\
&\quad (x^4+(2b^{-1}d-(b^{-1}c)^2)x^2+(b^{-1}d)^2)^{-p^s}\\
&= b^{-1}(x^2+b^{-1}cx+b^{-1}d)^{p^s-1}(x^2-b^{-1}cx+b^{-1}d)^{p^s}\\
&\quad (x^{4p^s}+((2b^{-1}d-(b^{-1}c)^2)x^2+(b^{-1}d)^2)^{p^s})^{-1}\\
&= b^{-1}(x^2+b^{-1}cx+b^{-1}d)^{p^s-1}(x^2-b^{-1}cx+b^{-1}d)^{p^s}\\
&\quad ((-\eta\delta x^2+1)^{p^s}+((2b^{-1}d-(b^{-1}c)^2)x^2+(b^{-1}d)^2)^{p^s})^{-1}\\
&= b^{-1}(x^2+b^{-1}cx+b^{-1}d)^{p^s-1}(x^2-b^{-1}cx+b^{-1}d)^{p^s}\\
&\quad ((2b^{-1}d-(b^{-1}c)^2-\eta\delta)x^2+(b^{-1}d)^2+1)^{-p^s}.
\end{aligned}$$

Thus, $f(x)$ is invertible if and only if $(2b^{-1}d-(b^{-1}c)^2-\eta\delta)x^2+(b^{-1}d)^2+1\neq 0$.

If $(2b^{-1}d-(b^{-1}c)^2-\eta\delta)=0$, then $(2b^{-1}d-(b^{-1}c)^2-\eta\delta)x^2+(b^{-1}c)^2+1=(b^{-1}d)^2+1$. By Lemma 4.1(i), $(2b^{-1}d-(b^{-1}c)^2-\eta\delta)x^2+(b^{-1}d)^2+1\neq 0$.

If $(2b^{-1}d-(b^{-1}c)^2-\eta\delta)\neq 0$, then $(2b^{-1}d-(b^{-1}c)^2-\eta\delta)x^2+(b^{-1}c)^2+1=(2b^{-1}d-(b^{-1}c)^2-\eta\delta)(x^2+((b^{-1}d)^2+1)(2b^{-1}d-(b^{-1}c)^2-\eta\delta)^{-1})$. So, $(2b^{-1}d-(b^{-1}c)^2-\eta\delta)x^2+(b^{-1}c)^2+1$ is invertible because $x^2+((b^{-1}d)^2+1)(2b^{-1}d-(b^{-1}c)^2-\eta\delta)^{-1}$ is invertible.

If $a\neq 0$, then $f(x)=ax^3+bx^2+cx+d$. We now consider

$$\begin{aligned}
f(x)^{-1} &= a^{-1}(x^3+a^{-1}bx^2+a^{-1}cx+a^{-1}d)^{-1}\\
&= a^{-1}(x^3+a^{-1}bx^2+a^{-1}cx+a^{-1}d)^{p^s-1}(x-a^{-1}b)^{p^s}\\
&\quad \times (x^3+a^{-1}bx^2+a^{-1}cx+a^{-1}d)^{-p^s}(x-a^{-1}b)^{-p^s}\\
&= a^{-1}(x^3+a^{-1}bx^2+a^{-1}cx+a^{-1}d)^{p^s-1}(x-a^{-1}b)^{p^s}\\
&\quad \times (x^4+(a^{-1}c-(a^{-1}b)^2)x^2+(a^{-1}d-a^{-2}bc)x-a^{-2}bd)^{-p^s}\\
&= a^{-1}(x^3+a^{-1}bx^2+a^{-1}cx+a^{-1}d)^{p^s-1}(x-a^{-1}b)^{p^s}\\
&\quad \times (x^{4p^s}+((a^{-1}c-(a^{-1}b)^2)x^2+(a^{-1}d-a^{-2}bc)x-a^{-2}bd)^{p^s})^{-1}
\end{aligned}$$

$$\begin{aligned}
&= a^{-1}(x^3+a^{-1}bx^2+a^{-1}cx+a^{-1}d)^{p^s-1}(x-a^{-1}b)^{p^s}\\
&\quad\times((-\eta\delta x^2+1)^{p^s}+(((a^{-1}c-(a^{-1}b)^2)x^2+(a^{-1}d-a^{-2}bc)x\\
&\qquad-a^{-2}bd)^{p^s})^{-1}\\
&= a^{-1}(x^3+a^{-1}bx^2+a^{-1}cx+a^{-1}d)^{p^s-1}(x-a^{-1}b)^{p^s}\\
&\quad\times((a^{-1}c-(a^{-1}b)^2-\eta\delta)x^2+(a^{-1}d-a^{-2}bc)x-a^{-2}bd+1)^{-p^s}.
\end{aligned}$$

Thus, $f(x)$ is invertible if and only if $(a^{-1}c-(a^{-1}b)^2-\eta\delta)x^2+(a^{-1}d-a^{-2}bc)x-a^{-2}bd+1\neq 0$. Assume that $(a^{-1}c-(a^{-1}b)^2-\eta\delta)x^2+(a^{-1}d-a^{-2}bc)x-a^{-2}bd+1=0$. So,

$$a^{-1}c-(a^{-1}b)^2-\eta\delta=0, \tag{4.13}$$

$$a^{-1}d-a^{-2}bc=0, \tag{4.14}$$

$$-a^{-2}bd+1=0. \tag{4.15}$$

By (4.13), (4.14) and (4.15), we have $c-a\eta\delta=a^{-1}b^2$, $d=a^{-1}bc$ and $bd=a^2$, respectively. This implies that

$$a^2=bd=ba^{-1}bc=a^{-1}b^2c=(c-a\eta\delta)c=c^2-a\eta\delta c.$$

So, $a^2+a\eta\delta c-c^2=0$. By Lemma 4.1(iii), $a^2+a\eta\delta c-c^2\neq 0$. It is a contradiction. Thus, $(a^{-1}c-(a^{-1}b)^2-\eta\delta)x^2+(a^{-1}d-a^{-2}bc)x-a^{-2}bd+1\neq 0$. This implies that $f(x)$ is invertible. □

Lemma 4.4. *Let $f(x)\in\frac{R[x]}{\langle(x^4+\eta\delta x^2-1)^{p^s}\rangle}$. Then $f(x)$ can be unique expressed as*

$$\begin{aligned}
f(x)=&\sum_{i=0}^{p^s-1}(a_{0i}x^3+b_{0i}x^2+c_{0i}x+d_{0i})(x^4+\eta\delta x^2-1)^i\\
&+u\sum_{i=0}^{p^s-1}(a_{1i}x^3+b_{1i}x^2+c_{1i}x+d_{1i})(x^4+\eta\delta x^2-1)^i\\
=\ &a_{00}x^3+b_{00}x^2+c_{00}x+d_{00}\\
&+\sum_{i=1}^{p^s-1}(a_{0i}x^3+b_{0i}x^2+c_{0i}x+d_{0i})(x^4+\eta\delta x^2-1)^i\\
&+u\sum_{i=0}^{p^s-1}(a_{1i}x^3+b_{1i}x^2+c_{1i}x+d_{1i})(x^4+\eta\delta x^2-1)^i,
\end{aligned}$$

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

Proof. Let $f(x)\in\frac{R[x]}{\langle(x^4+\eta\delta x^2-1)^{p^s}\rangle}$. Then $f(x)$ can be viewed as a polynomial of degree up to $4p^s-1$ of $R[x]$, and so $f(x)=f_1(x)+uf_2(x)$, where $f_1(x),f_2(x)$

are polynomials of degrees up to $4p^s-1$ of $\mathbb{F}_{p^m}[x]$. Thus, $f(x)$ can be uniquely expressed as

$$\begin{aligned} f(x) = &\sum_{i=0}^{p^s-1}(a_{0i}x^3+b_{0i}x^2+c_{0i}x+d_{0i})(x^4+\eta\delta x^2-1)^i \\ &+u\sum_{i=0}^{p^s-1}(a_{1i}x^3+b_{1i}x^2+c_{1i}x+d_{1i})(x^4+\eta\delta x^2-1)^i \\ =\ &a_{00}x^3+b_{00}x^2+c_{00}x+d_{00} \\ &+(x^4+\eta\delta x^2-1)\sum_{i=1}^{p^s-1}(a_{0i}x^3+b_{0i}x^2+c_{0i}x+d_{0i})(x^4+\eta\delta x^2-1)^{i-1} \\ &+u\sum_{i=0}^{p^s-1}(a_{1i}x^3+b_{1i}x^2+c_{1i}x+d_{1i})(x^4+\eta\delta x^2-1)^i, \end{aligned}$$

where $a_{0i},a_{1i},b_{0i},b_{1i},c_{0i},c_{1i},d_{0i},d_{1i}\in\mathbb{F}_{p^m}$ for $0\le i\le p^s-1$. Since $x^4+\eta\delta x^2-1$ and u are nilpotent elements in $\frac{R[x]}{\langle(x^4+\eta\delta x^2-1)^{p^s}\rangle}$, $f(x)$ is non-invertible if and only if $a_{00}=b_{00}=c_{00}=d_{00}=0$. □

Theorem 4.5. *The ring $\frac{R[x]}{\langle(x^4+\eta\delta x^2-1)^{p^s}\rangle}$ is a local ring with the maximal ideal $\langle u,x^4+\eta\delta x^2-1\rangle$, and it is not a chain ring.*

Proof. By Proposition 4.4, we have the set of all non-invertible elements of $\frac{R[x]}{\langle(x^4+\eta\delta x^2-1)^{p^s}\rangle}$ forms as $\langle u,x^4+\eta\delta x^2-1\rangle$. Thus, $\frac{R[x]}{\langle(x^4+\eta\delta x^2-1)^{p^s}\rangle}$ is a local ring with the maximal ideal $\langle u,x^4+\eta\delta x^2-1\rangle$. Next, we will show that a local ring $\frac{R[x]}{\langle(x^4+\eta\delta x^2-1)^{p^s}\rangle}$ is not a chain ring. If $u\in\langle x^4+\eta\delta x^2-1\rangle$, then

$$\begin{aligned} u = &(x^4+\eta\delta x^2-1)(\sum_{i=0}^{p^s-1}(a_{0i}x^3+b_{0i}x^2+c_{0i}x+d_{0i})(x^4+\eta\delta x^2-1)^i \\ &+u\sum_{i=0}^{p^s-1}(a_{1i}x^3+b_{1i}x^2+c_{1i}x+d_{1i})(x^4+\eta\delta x^2-1)^i) \\ =\ &\sum_{i=0}^{p^s-1}(a_{0i}x^3+b_{0i}x^2+c_{0i}x+d_{0i})(x^4+\eta\delta x^2-1)^{i+1} \\ &+u\sum_{i=0}^{p^s-1}(a_{1i}x^3+b_{1i}x^2+c_{1i}x+d_{1i})(x^4+\eta\delta x^2-1)^{i+1}, \end{aligned}$$

where $a_{0i},a_{1i},b_{0i},b_{1i},c_{0i},c_{1i},d_{0i},d_{1i}\in\mathbb{F}_{p^m}$ for $0\le i\le p^s-1$. This implies that $\sum_{i=0}^{p^s-1}(a_{0i}x^3+b_{0i}x^2+c_{0i}x+d_{0i})(x^4+\eta\delta x^2-1)^{i+1}=0$ and $(x^4+\eta\delta x^2-1)(\sum_{i=0}^{p^s-1}(a_{1i}x^3+b_{1i}x^2+c_{1i}x+d_{1i})(x^4+\eta\delta x^2-1)^i)=\sum_{i=0}^{p^s-1}(a_{1i}x^3+b_{1i}x^2+c_{1i}x+d_{1i})(x^4+\eta\delta x^2-1)^{i+1}=1$. Thus, $x^4+\eta\delta x^2-1$ is invertible. It is

a contradiction. Clearly, $x^4 + \eta\delta x^2 - 1 \notin \langle u \rangle$ because u and $x^4 + \eta\delta x^2 - 1$ are nilpotent elements with nilpotent index 2 and p^s, respectively. Thus, the quotient ring $\frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s} \rangle}$ is not a chain ring. □

Proposition 4.6.

(i) *Each nonzero polynomial* $f(x) = ax^3 + bx^2 + cx + d$ *is invertible in* $\frac{\mathbb{F}_{p^m}[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s} \rangle}$ *where* $a, b, c, d \in \mathbb{F}_{p^m}$.

(ii) *The ring* $\frac{\mathbb{F}_{p^m}[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s} \rangle}$ *is a finite chain ring whose each ideal forms as* $\langle (x^4 + \eta\delta x^2 - 1)^i \rangle$ *for* $0 \le i \le p^s$ *and*

$$\begin{aligned}\langle 0 \rangle &= \langle (x^4 + \eta\delta x^2 - 1)^{p^s} \rangle \subsetneq \cdots \subsetneq \langle (x^4 + \eta\delta x^2 - 1)^i \rangle \subsetneq \cdots \subsetneq \langle (x^4 + \eta\delta x^2 - 1)^0 \rangle \\ &= \langle 1 \rangle.\end{aligned}$$

Proof. (i) It follows from Theorem 4.3.

(ii) Let $f(x) \in \frac{\mathbb{F}_{p^m}[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s} \rangle}$. Then $f(x)$ is a polynomial degree up $4p^s$ and thus, $f(x)$ can be expressed as

$$f(x) = \sum_{i=0}^{p^s-1} (a_{0i}x^3 + b_{0i}x^2 + c_{0i}x + d_{0i})(x^4 + \eta\delta x^2 - 1)^i,$$

where $a_{0i}, b_{0i}, c_{0i}, d_{0i} \in \mathbb{F}_{p^m}$. We now consider that

$$\begin{aligned}f(x) &= \sum_{i=0}^{p^s-1} (a_{0i}x^3 + b_{0i}x^2 + c_{0i}x + d_{0i})(x^4 + \eta\delta x^2 - 1)^i \\ &= a_{00}x^3 + b_{00}x^2 + c_{00}x + d_{00} \\ &\quad + \sum_{i=1}^{p^s-1} (a_{0i}x^3 + b_{0i}x^2 + c_{0i}x + d_{0i})(x^4 + \eta\delta x^2 - 1)^i \\ &= a_{00}x^3 + b_{00}x^2 + c_{00}x + d_{00} \\ &\quad + (x^4 + \eta\delta x^2 - 1) \sum_{i=1}^{p^s-1} (a_{0i}x^3 + b_{0i}x^2 + c_{0i}x + d_{0i})(x^4 + \eta\delta x^2 - 1)^{i-1}.\end{aligned}$$

This implies that $f(x)$ is non-invertible if and only if $a_{00} = b_{00} = c_{00} = d_{00} = 0$. Moreover, the set of all non-invertible elements of $\frac{\mathbb{F}_{p^m}[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s} \rangle}$ forms as $\langle x^4 + \eta\delta x^2 - 1 \rangle$. By Proposition 2.1, the quotient ring $\frac{\mathbb{F}_{p^m}[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s} \rangle}$ is a chain ring with each ideal forms as $\langle (x^4 + \eta\delta x^2 - 1)^i \rangle$ for $0 \le i \le p^s$.

The proof is complete. □

Thus, we characterize all ideals of $\frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s} \rangle}$ as the following theorem.

Theorem 4.7. *All ideals of* $\frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s} \rangle}$ *are*

- *Type 1*: (*trivial ideals*)
$$\langle 0\rangle \text{ and } \langle 1\rangle.$$
- *Type 2*: (*principal ideals with nonmonic polynomial generators*)
$$\langle u(x^4+\eta\delta x^2-1)^i\rangle,$$
where $0<i\leq p^s-1$.
- *Type 3*: (*principal ideals with monic polynomial generators*)
$$\langle (x^4+\eta\delta x^2-1)^i+u(x^4+\eta\delta x^2-1)^t h(x)\rangle,$$
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* $h(x)=\sum_j(h_{3j}x^3+h_{2j}x^2+h_{1j}x+h_{0j})(x^4+\eta\delta x^2-1)^j$ *with* $h_{0j},h_{1j},h_{2j},h_{3j}\in\mathbb{F}_{p^m}$ *and* $h_{30}x^3+h_{20}x^2+h_{10}x+h_{00}\neq 0$.
- *Type 4*: (*non-principal ideals*)
$$\langle (x^4+\eta\delta x^2-1)^i+u\sum_{j=0}^{\omega-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j, u(x^4+\eta\delta x^2-1)^\omega\rangle$$
for $1\leq i\leq p^s-1$, $a_{0j},b_{0j},c_{0j},d_{0j}\in\mathbb{F}_{p^m}$, *and* $\omega<T$ *where* T *is the smallest integers such that* $u(x^4+\eta\delta x^2-1)^T\in\langle (x^4+\eta\delta x^2-1)^i+u\sum_{j=0}^{\omega-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j\rangle$ *or equivalently,* $\langle (x^4+\eta\delta x^2-1)^i+u(x^4+\eta\delta x^2-1)^t h(x), u(x^4+\eta\delta x^2-1)^\omega\rangle$ *with* $h(x)$ *as in Type 3, and* $\deg h(x)\leq \omega-t-1$.

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 $\frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s}\rangle}$. 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 $u\sum_{i=0}^{p^s-1}(a_{0i}x^3+b_{0i}x^2+c_{0i}x+d_{0i})(x^4+\eta\delta x^2-1)^i$ where $a_{0i},b_{0i},c_{0i},d_{0i}\in\mathbb{F}_{p^m}$. This implies that there exists an element $a(x)\in I$ that has the smallest k such that $a_{0k}x^3+b_{0k}x^2+c_{0k}x+d_{0k}\neq 0$. Hence each element $c(x)\in I$ have the form $c(x)=u(x^4+\eta\delta x^2-1)^k\sum_{i=k}^{p^s-1}(e_{0i}x^3+f_{0i}x^2+g_{0i}x+h_{0i})(x^4+\eta\delta x^2-1)^{i-k}$, implying that $I\subseteq\langle u(x^4+\eta\delta x^2-1)^k\rangle$. However, we have $a(x)\in I$ with

$$\begin{aligned}a(x)&=u(x^4+\eta\delta x^2-1)^k\sum_{i=k}^{p^s-1}(a_{0i}x^3+b_{0i}x^2+c_{0i}x+d_{0i})(x^4+\eta\delta x^2-1)^{i-k}\\&=u(x^4+\eta\delta x^2-1)^k\Bigg(a_{0k}x^3+b_{0k}x^2+c_{0k}x+d_{0k}\\&\qquad+\sum_{i=k+1}^{p^s-1}(a_{0i}x^3+b_{0i}x^2+c_{0i}x+d_{0i})(x^4+\eta\delta x^2-1)^{i-k}\Bigg).\end{aligned}$$

From $a_{0k}x^3+b_{0k}x^2+c_{0k}x+d_{0k}\neq 0$, we can see that $a_{0k}x^3+b_{0k}x^2+c_{0k}x+d_{0k}+\sum_{i=k+1}^{p^s-1}(a_{0i}x^2+b_{0i}x+c_{0i})(x^4+\eta\delta x^2-1)^{i-k}$ is invertible, proving that

$u(x^4+\eta\delta x^2-1)^k \in I$. Therefore, $I=\langle u(x^4+\eta\delta x^2-1)^k\rangle$, which means that the nontrivial ideals of $\frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s}\rangle}$ contained in $\langle u\rangle$ are $\langle u(x^4+\eta\delta x^2-1)^k\rangle$, $0\le k\le p^s-1$, 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. Note that I_u is a nonzero ideal of the ring $\frac{\mathbb{F}_{p^m}[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s}\rangle}$, which is a finite chain ring with ideals $\langle (x^4+\eta\delta x^2-1)^j\rangle$ where $0\le j\le p^s$. Then there is an integer $i\in\{0,1,\ldots,p^s-1\}$ such that $I_u=\langle (x^4+\eta\delta x^2-1)^i\rangle\subseteq\frac{\mathbb{F}_{p^m}[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s}\rangle}$. This follows that there exists an element

$$\begin{aligned} c(x) = &\sum_{j=0}^{p^s-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j \\ &+u\sum_{j=0}^{p^s-1}(a_{1j}x^3+b_{1j}x^2+c_{1j}x+d_{1j})(x^4+\eta\delta x^2-1)^j \\ &\in \frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s}\rangle}, \end{aligned}$$

where $a_{0j},a_{1j},b_{0j},b_{1j},c_{0j},c_{1j},d_{0j},d_{1j}\in\mathbb{F}_{p^m}$ such that $(x^4+\eta\delta x^2-1)^i+uc(x)\in I$. Since

$$\begin{aligned} &(x^4+\eta\delta x^2-1)^i+uc(x) \\ &=(x^4+\eta\delta x^2-1)^i+u\sum_{j=0}^{p^s-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j\in I, \end{aligned}$$

and $u(x^4+\eta\delta x^2-1)^k=u\big((x^4+\eta\delta x^2-1)^i+uc(x)\big)(x^4+\eta\delta x^2-1)^{k-i}\in I$ with $i\le k\le p^s-1$, we have $(x^4+\eta\delta x^2-1)^i+u\sum_{j=0}^{i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j\in I$. We now consider two subcases.

Case 2a. $I=\langle (x^4+\eta\delta x^2-1)^i+u\sum_{j=0}^{i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j\rangle$, then I can be expressed as

$$I=\langle (x^4+\eta\delta x^2-1)^i+u(x^4+\eta\delta x^2-1)^t h(x)\rangle,$$

where $h(x)$ is 0 or a unit. If $h(x)$ is a unit, then $h(x)$ can be represented as $h(x)=\sum_{j=0}^{i-t-1}(h_{3j}x^3+h_{2j}x^2+h_{1j}x+h_{0j})(x^4+\eta\delta x^2-1)^j$ with $h_{0j},h_{1j},h_{2j},h_{3j}\in\mathbb{F}_{p^m}$ and $h_{20}x^2+h_{10}x+h_{00}\neq 0$. it follows that I is of Type 3.

Case 2b. $\langle (x^4+\eta\delta x^2-1)^i+u\sum_{j=0}^{i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j\rangle\subsetneq I$. Then, there exists $f(x)\in I\backslash\langle (x^4+\eta\delta x^2-1)^i+u\sum_{j=0}^{i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j\rangle$. By Division Algorithm, there exist polynomials $r(x),q(x)\in\frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s}\rangle}$ such that

$$0\neq r(x)=f(x)-q(x)\Bigg((x^4+\eta\delta x^2-1)^i$$

$$+ u\sum_{j=0}^{i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(x^4 + \eta\delta x^2 - 1)^j\Bigg) \in I,$$

where $\deg r(x) < \deg((x^4+\eta\delta x^2-1)^i + u\sum_{j=0}^{i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j)$. This implies that $r(x)$ can be expressed as

$$\begin{aligned} r(x) = &\sum_{j=0}^{i-1}(r_{3j}x^3 + r_{2j}x^2 + r_{1j}x + r_{0j})(x^4 + \eta\delta x^2 - 1)^j \\ &+ u\sum_{j=0}^{i-1}(r'_{3j}x^3 + r'_{2j}x^2 + r'_{1j}x + r'_{0j})(x^4 + \eta\delta x^2 - 1)^j, \end{aligned}$$

where $r_{0j}, r_{1j}, r_{2j}, r_{3j}, r'_{0j}, r'_{1j}, r'_{2j}, r'_{3j} \in \mathbb{F}_{p^m}$. Hence, $r(x)$ reduced modulo u is in $I_u = \langle(x^4 + \eta\delta x^2 - 1)^i\rangle$, and thus, $r_{3j} = r_{2j} = r_{1j} = r_{0j} = 0$ for all $0 \le j \le i-1$, i.e., $r(x) = u\sum_{j=0}^{i-1}(r'_{3j}x^3 + r'_{2j}x^2 + r'_{1j}x + r'_{0j})(x^4 + \eta\delta x^2 - 1)^j$. Since $r(x) \neq 0$, there exists the smallest integer k, $0 \le k \le i-1$, such that $r'_{3k}x^3 + r'_{2k}x^2 + r'_{1k}x + r'_{0k} \neq 0$. Then

$$\begin{aligned} r(x) &= u\sum_{j=k}^{i-1}(r'_{3j}x^3 + r'_{2j}x^2 + r'_{1j}x + r'_{0j})(x^4 + \eta\delta x^2 - 1)^j \\ &= u(x^4 + \eta\delta x^2 - 1)^k\Bigg(r'_{3k}x^3 + r'_{2k}x^2 + r'_{1k}x + r'_{0k} \\ &\qquad + \sum_{j=k+1}^{i-1}(r'_{3j}x^3 + r'_{2j}x^2 + r'_{1j}x + r'_{0j})(x^4 + \eta\delta x^2 - 1)^{j-k}\Bigg). \end{aligned}$$

As $r'_{3k}x^3 + r'_{2k}x^2 + r'_{1k}x + r'_{0k} \neq 0$, $r'_{3k}x^3 + r'_{2k}x^2 + r'_{1k}x + r'_{0k} + \sum_{j=k+1}^{i-1}(r'_{3j}x^3 + r'_{2j}x^2 + r'_{1j}x + r'_{0j})(x^4 + \eta\delta x^2 - 1)^{j-k}$ is an invertible element in $\frac{R[x]}{\langle(x^4+\eta\delta x^2-1)^{p^s}\rangle}$. Hence,

$$\begin{aligned} &u(x^4 + \eta\delta x^2 - 1)^k \\ &= (r'_{3k}x^3 + r'_{2k}x^2 + r'_{1k}x + r'_{0k} \\ &\quad + \sum_{j=k+1}^{i-1}(r'_{3j}x^3 + r'_{2j}x^2 + r'_{1j}x + h'_{0j})(x^4 + \eta\delta x^2 - 1)^{j-k})^{-1}r(x) \in I. \end{aligned}$$

It has been shown that for any $f(x) \in I\backslash\langle(x^4 + \eta\delta x^2 - 1)^i + u\sum_{j=0}^{i-1}(a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(x^4 + \eta\delta x^2 - 1)^j\rangle$, there is an integer k_f with $0 \le k_f \le i-1$ such that $u(x^4+\eta\delta x^2-1)^{k_f} \in I$. Let $\omega = \min\{k_f : f(x) \in I\backslash\langle(x^4+\eta\delta x^2-1)^i + u\sum_{j=0}^{i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j\rangle\}$. Then $\langle(x^4+\eta\delta x^2-1)^i + u\sum_{j=0}^{i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j, u(x^4+\eta\delta x^2-1)^\omega\rangle \subseteq I$. In addition, by the above construction, for any $f(x) \in I$, there exists a polynomial

$q(x) \in \frac{R[x]}{\langle x^4+\eta\delta x^2-1\rangle}$ satisfying

$$\begin{aligned} & f(x) - q(x)[(x^4+\eta\delta x^2-1)^i \\ & + u\sum_{j=0}^{i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j] \\ & \in \langle u(x^4+\eta\delta x^2-1)^\omega\rangle, \end{aligned}$$

implying that

$$\begin{aligned} f(x) \in \langle & (x^4+\eta\delta x^2-1)^i + u\sum_{j=0}^{i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j, \\ & u(x^4+\eta\delta x^2-1)^\omega\rangle. \end{aligned}$$

Thus,

$$\begin{aligned} I = \langle & (x^4+\eta\delta x^2-1)^i + u\sum_{j=0}^{i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j, \\ & u(x^4+\eta\delta x^2-1)^\omega\rangle \\ = \langle & (x^4+\eta\delta x^2-1)^i + u\sum_{j=0}^{\omega-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j, \\ & u(x^4+\eta\delta x^2-1)^\omega\rangle. \end{aligned}$$

Let T be the smallest integer such that $u(x^4+\eta\delta x^2-1)^T \in \langle (x^4+\eta\delta x^2-1)^i + u\sum_{j=0}^{i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d)(x^4+\eta\delta x^2-1)^j\rangle$. If $\omega \geq T$, then

$$\begin{aligned} I = \langle & (x^4+\eta\delta x^2-1)^i + u\sum_{j=0}^{\omega-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j, \\ & u(x^4+\eta\delta x^2-1)^\omega\rangle \\ = \langle & (x^4+\eta\delta x^2-1)^i + u\sum_{j=0}^{i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j\rangle. \end{aligned}$$

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

Next, we obtain that the properties of the integer T in Type 4 as following proposition.

Proposition 4.8. *Let T be the smallest integer such that $u(x^4+\eta\delta x^2-1)^T \in I = \langle (x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)\rangle$, 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 $u(x^4+\eta\delta x^2-1)^i = u\big((x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)\big) \in I$. If $h(x)=0$, then $I = \langle (x^4+\eta\delta x^2-1)^i \rangle$, implying that $T = i$. Now we consider that the case $h(x)$ is a unit. Since $u(x^4+\eta\delta x^2-1)^T \in \langle (x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)\rangle$, there is a polynomial $f(x) \in \frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s}\rangle}$ satisfying $u(x^4+\eta\delta x^2-1)^T = f(x)\big((x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)\big)$. So, $f(x)$ can be written as

$$\begin{aligned} f(x) = &\sum_{j=0}^{p^s-1} (a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(x^4+\eta\delta x^2-1)^j \\ &+ u\sum_{j=0}^{p^s-1} (a_{1j}x^3 + b_{1j}x^2 + c_{0j}x + d_{0j})(x^4+\eta\delta x^2-1)^j, \end{aligned}$$

where $a_{0j}, a_{1j}, b_{0j}, b_{1j}, c_{0j}, c_{1j}, d_{0j}, d_{1j} \in \mathbb{F}_{p^m}$. Then $u(x^4+\eta\delta x^2-1)^T$ can be expressed as follows:

$$\begin{aligned} &\Bigg(\sum_{j=0}^{p^s-1} (a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(x^4+\eta\delta x^2-1)^j \\ &\quad + u\sum_{j=0}^{p^s-1} (a_{1j}x^3 + b_{1j}x^2 + c_{1j}x + d_{1j})(x^4+\eta\delta x^2-1)^j\Bigg) \\ &\quad \times \big((x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)\big) \\ &= (x^4+\eta\delta x^2-1)^i \sum_{j=0}^{p^s-1} (a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(x^4+\eta\delta x^2-1)^j \\ &\quad + u(x^4+\eta\delta x^2-1)^i \sum_{j=0}^{p^s-1} (a_{1j}x^3 + b_{1j}x^2 + c_{1j}x + d_{1j})(x^4+\eta\delta x^2-1)^j \\ &\quad + u(x^4+\eta\delta x^2-1)^t h(x) \sum_{j=0}^{p^s-1} (a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(x^4+\eta\delta x^2-1)^j \\ &= (x^4+\eta\delta x^2-1)^i \sum_{j=0}^{p^s-i-1} (a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(x^4+\eta\delta x^2-1)^j \\ &\quad + (x^4+\eta\delta x^2-1)^{p^s} \sum_{j=p^s-i}^{p^s-1} (a_{0j}x^3 + b_{0j}x^2 + c_{0j}x + d_{0j})(x^4+\eta\delta x^2-1)^{i+j-p^s} \\ &\quad + u(x^4+\eta\delta x^2-1)^i \sum_{j=0}^{p^s-i-1} (a_{1j}x^3 + b_{1j}x^2 + c_{1j}x + d_{1j})(x^4+\eta\delta x^2-1)^j \end{aligned}$$

$$
\begin{aligned}
&+ u(x^4+\eta\delta x^2-1)^{p^s}\sum_{j=p^s-i}^{p^s-1}(a_{1j}x^3+b_{1j}x^2+c_{1j}x+d_{1j})(x^4+\eta\delta x^2-1)^{i+j-p^s}\\
&+ u(x^4+\eta\delta x^2-1)^t h(x)\sum_{j=0}^{p^s-i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j\\
&+ u(x^4+\eta\delta x^2-1)^t h(x)\sum_{j=p^s-i}^{p^s-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j\\
&= (x^4+\eta\delta x^2-1)^i\sum_{j=0}^{p^s-i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j\\
&+ u(x^4+\eta\delta x^2-1)^i\sum_{j=0}^{p^s-i-1}(a_{1j}x^3+b_{1j}x^2+c_{1j}x+d_{1j})(x^4+\eta\delta x^2-1)^j\\
&+ u(x^4+\eta\delta x^2-1)^t h(x)\sum_{j=0}^{p^s-i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j\\
&+ u(x^4+\eta\delta x^2-1)^t h(x)\sum_{j=p^s-i}^{p^s-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j.
\end{aligned}
$$

We see that $(x^4+\eta\delta x^2-1)^i\sum_{j=0}^{p^s-i-1}(a_{0j}x^3+b_{0j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j = 0$, implying that $a_{0j} = b_{0j} = c_{0j} = d_{0j} = 0$ for all $j = 0, 1, 2, \ldots, p^s - i - 1$. Thus,

$$
\begin{aligned}
&u(x^4+\eta\delta x^2-1)^T\\
&= u(x^4+\eta\delta x^2-1)^i\sum_{j=0}^{p^s-i-1}(a_{1j}x^3+b_{1j}x^2+c_{0j}x+d_{0j})(x^4+\eta\delta x^2-1)^j\\
&\quad + u(x^4+\eta\delta x^2-1)^{p^s-i+t}h(x)\\
&\quad \times\sum_{j=0}^{i-1}(a_{0,p^s-i+j}x^3+b_{0,p^s-i+j}x^2+c_{0,p^s-i+j}x+d_{0,p^s-i+j})\\
&\quad \times(x^4+\eta\delta x^2-1)^j.
\end{aligned}
$$

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

$$
\begin{aligned}
&[(x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)](x^4+\eta\delta x^2-1)^{p^s-1}\\
&= u(x^4+\eta\delta x^2-1)^{p^s-i+t}h(x).
\end{aligned}
$$

Hence,

$$
\begin{aligned}
&u(x^4+\eta\delta x^2-1)^{p^s-i+t}\\
&= [(x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)](x^4+\eta\delta x^2-1)^{p^s-i}h(x)^{-1} \in I.
\end{aligned}
$$

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

Now, we determine the number of codewords of ideals of $\frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s}\rangle}$ as following theorem.

Theorem 4.9. *Let I be an ideal of the ring $\frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s}\rangle}$. Then the number of elements of I, denoted by n_I is determined as follows.*

- *If $I = \langle 0\rangle$ and $I = \langle 1\rangle$, then $n_I = 1$ and $n_I = p^{8mp^s}$, respectively.*
- *If $I = \langle u(x^4 + \eta\delta x^2 - 1)^i\rangle$ where $0 \leq i \leq p^s - 1$, then $n_I = p^{4m(p^s-i)}$.*
- *If $I = \langle (x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)\rangle$ where $1 \leq i \leq p^s-1, 0 \leq t < i$, and $h(x)$ is 0 or a unit, then*

$$n_I = \begin{cases} p^{8m(p^s-i)}, & \text{if } h(x) \text{ is } 0,\ 1 \leq i \leq p^s - 1 \text{ or } h(x) \text{ is a unit, } 1 \leq i \leq \frac{p^s+t}{2}, \\ p^{4m(p^s-t)}, & \text{if } h(x) \text{ is a unit, } \frac{p^s+t}{2} < i \leq p^s - 1. \end{cases}$$

- *If $I = \langle (x^4 + \eta\delta x^2 - 1)^i + u(x^4 + \eta\delta x^2 - 1)^t h(x),\ u(x^4 + \eta\delta x^2 - 1)^\omega\rangle$, where $1 \leq i \leq p^s - 1$, $0 \leq t < i$, either $h(x)$ is 0 or $h(x)$ is a unit, and*

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

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

Proof. We apply Proposition 2.8 for computing the number of elements of I and separate this proof into following types in Theorem 4.7.

(i) Type 1:

- If $I = \langle 0\rangle$, then $\mathrm{Res}(I) = \mathrm{Tor}(I) = \langle 0\rangle$. Thus, $n_I = |\mathrm{Res}(I)||\mathrm{Tor}(I)| = 1 \cdot 1 = 1$.
- If $I = \langle 1\rangle$, then $\mathrm{Res}(I) = \mathrm{Tor}(I) = \langle 1\rangle$, implying that

$$n_I = |\mathrm{Res}(I)||\mathrm{Tor}(I)| = p^{4mp^s} \cdot p^{4mp^s} = p^{8mp^s}.$$

(ii) Type 2: $I = \langle u(x^4 + \eta\delta x^2 - 1)^i\rangle$ where $0 < i \leq p^s - 1$, then $\mathrm{Res}(I) = \langle 0\rangle$ and $\mathrm{Tor}(I) = \langle (x^4 + \eta\delta x^2 - 1)^i\rangle$. Hence, we get that $n_I = |\mathrm{Res}(I)||\mathrm{Tor}(I)| = 1 \cdot p^{4m(p^s-i)} = p^{4m(p^s-i)}$.

(iii) Type 3: $I = \langle (x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)\rangle$ where $0 \leq i \leq p^s-1$, $0 \leq t < i$, and $h(x)$ is 0 or a unit. If $h(x) = 0$, then $\mathrm{Res}(I) = \langle (x^4 + \eta\delta x^2 - 1)^i\rangle$ and $\mathrm{Tor}(I) = \langle (x^4 + \eta\delta x^2 - 1)^i\rangle$, implying that $n_I = |\mathrm{Res}(I)||\mathrm{Tor}(I)| = p^{4m(p^s-i)} \cdot p^{4m(p^s-i)} = p^{8m(p^s-i)}$.

If $h(x)$ is a unit, then $\mathrm{Res}(I) = \langle (x^4+\eta\delta x^2-1)^i\rangle$ and $\mathrm{Tor}(I) = \langle (x^4+\eta\delta x^2-1)^T\rangle$, where T is the smallest integer such that

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

For $1 \leq i \leq \frac{p^s+t}{2}$, we see that $\mathrm{Tor}(I) = \langle (x^4 + \eta\delta x^2 - 1)^i\rangle$, implying that $n_I = |\mathrm{Res}(I)||\mathrm{Tor}(I)| = p^{4m(p^s-i)} \cdot p^{4m(p^s-i)} = p^{8m(p^s-i)}$. Moreover, $\mathrm{Tor}(I) =$

$\langle (x^4+\eta\delta x^2-1)^{p^s-i+t}\rangle$ for $\frac{p^s+t}{2} < i \le p^s-1$. Thus, $n_I = |\operatorname{Res}(I)||\operatorname{Tor}(I)| = p^{4m(p^s-i)} \cdot p^{4m(i-t)} = p^{4m(p^s-t)}$.

(iv) Type 4: If $I = \langle (x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x), u(x^4+\eta\delta x^2-1)^\omega\rangle$, where $1 \le i \le p^s-1$, $0 \le t < i$, either $h(x)$ is 0 or $h(x)$ is a unit, and $\omega < T$, then $\operatorname{Res}(I) = \langle (x^4+\eta\delta x^2-1)^i\rangle$ and $\operatorname{Tor}(I) = \langle (x^4+\eta\delta x^2-1)^\omega\rangle$. Thus, $n_I = |\operatorname{Res}(I)||\operatorname{Tor}(I)| = p^{4m(p^s-i)} \cdot p^{4m(p^s-\omega)} = p^{4m(2p^s-i-\omega)}$.

The proof is complete. □

We now investigate the dual codes and determine the annihilator of I where I is an ideal of the ring $\frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s}\rangle}$. We need to give the following lemma.

Lemma 4.10. *Let I be an ideal of the ring $\frac{R[x]}{\langle (x^4+\eta\delta x^2-1)^{p^s}\rangle}$. If $I = \langle (x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x), u(x^4+\eta\delta x^2-1)^\omega\rangle$ where $h(x)$ is 0 or a unit, then p^s-i is the smallest positive integer r such that $u(x^4+\eta\delta x^2-1)^r \in \mathcal{A}(I)$.*

Proof. Since $(x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x) \in I$ and $u(x^4+\eta\delta x^2-1)^r \in \mathcal{A}(I)$, we have

$$\begin{aligned} 0 &= \big((x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)\big) u(x^4+\eta\delta x^2-1)^r \\ &= u(x^4+\eta\delta x^2-1)^{i+r}. \end{aligned}$$

We see that $i+r \ge p^s$. So, we have the smallest value of r is p^s-i. Hence, $u(x^4+\eta\delta x^2-1)^{p^s-i} \in \mathcal{A}(I)$. □

Lemma 4.11. *Let $f(x) = (x^4+\eta\delta x^2-1)^i - u\sum_{j=0}^{t}(a_j x^3 + b_j x^2 + c_j x + d_j)(x^4+\eta\delta x^2-1)^j$ be a polynomial over R where $a_j, b_j, c_j, d_j \in \mathbb{F}_{p^m}$ and $t < i$. Then*

$$\begin{aligned} f^*(x) = {} & (-1)^i (x^4-\eta\delta x^2-1)^i \\ & - u\sum_{j=0}^{t}(d_j x^3 + c_j x^2 + b_j x + a_j)(-1)^j (x^4-\eta\delta x^2-1) x^{4i-4j-3}. \end{aligned}$$

Proof. By Lemma 2.7, we see that

$$\begin{aligned} \big((x^4+\eta\delta x^2-1)^k\big)^* &= \big((x^4+\eta\delta x^2-1)^*\big)^k \\ &= (-x^4+\eta\delta x^2+1)^k \\ &= (-1)^k (x^4-\eta\delta x^2-1)^k. \end{aligned}$$

Applying Lemma 2.7 again, we have

$$\begin{aligned} f^*(x) = {} & (-1)^i (x^4-\eta\delta x^2-1)^i \\ & - u\sum_{j=0}^{t}(a_j x^3 + b_j x^2 + c_j x + d_j)^* (-1)^j (x^4-\eta\delta x^2-1)^j x^{4i-4j-3} \\ = {} & (-1)^i (x^4-\eta\delta x^2-1)^i \end{aligned}$$

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

Now, we obtain that the form of $f^*(x)$. □

Theorem 4.12. *Let $I = \langle u(x^4 + \eta\delta x^2 - 1)^i\rangle$ be an ideal of the ring*

$$\frac{R[x]}{\langle (x^4 + \eta\delta x^2 - 1)^{p^s}\rangle}.$$

Then $\mathcal{A}(I)^* = \langle (x^4 - \eta\delta x^2 - 1)^{p^s-i}, u\rangle$.

Proof. Since $I \subseteq \langle u\rangle$ and $I \subseteq \langle (x^4 + \eta\delta x^2 - 1)^i\rangle$, we have $\langle (x^4 + \eta\delta x^2 - 1)^{p^s-i}\rangle = \mathcal{A}(\langle (x^4 + \eta\delta x^2 - 1)^i\rangle) \subseteq \mathcal{A}(I)$ and $\langle u\rangle = \mathcal{A}(\langle u\rangle) \subseteq \mathcal{A}(I)$. This implies that $\langle (x^4 + \eta\delta x^2 - 1)^{p^s-i}, u\rangle \subseteq \mathcal{A}(I)$. The other inclusion follows from the fact that the coefficient vector of $(x^4 + \eta\delta x^2 - 1)^{p^s-i}$ is orthogonal to the coefficient vector of $u(x^4 + \eta\delta x^2 - 1)^i$ and all its constacyclic shift. Thus, $\mathcal{A}(I) = \langle (x^4 + \eta\delta x^2 - 1)^{p^s-i}, u\rangle$. By Lemma 2.7, we have

$$\mathcal{A}(I)^* = \langle (x^4 - \eta\delta x^2 - 1)^{p^s-i}, u\rangle.$$ □

Theorem 4.13. *Let $I = \langle (x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)\rangle$ where $h(x)$ is 0 or a unit. Then*

(i) *If $h(x) = 0$, then $\mathcal{A}(I)^* = \langle (x^4 - \eta\delta x^2 - 1)^{p^s-i}\rangle$.*

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

$$\begin{aligned}\mathcal{A}(I)^* = \langle &(-1)^{i-t}(x^4 - \eta\delta x^2 - 1)^{p^s-i}\\ &- u(x^4 - \eta\delta x^2 - 1)^{p^s-2i+t}\sum_{j=0}^{i-t-1}(d_jx^3 + c_jx^2 + b_jx + a_j)\\ &\times (-1)^j(x^4 - \eta\delta x^2 - 1)^j\rangle.\end{aligned}$$

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

$$\begin{aligned}\mathcal{A}(I)^* = \langle &(-1)^{i-t}(x^4 - \eta\delta x^2 - 1)^{i-t}\\ &- u\sum_{j=0}^{p^s-i-1}(d_jx^3+c_jx^2+b_jx+a_j)(-1)^j(x^4-\eta\delta x^2-1)^j x^{4i-4t-4j-3},\\ &u(x^4 - \eta\delta x^2 - 1)^{p^s-i}\rangle.\end{aligned}$$

Proof. (i) Suppose that $h(x) = 0$. So, we have $I = \langle (x^4 + \eta\delta x^2 - 1)^i\rangle$. Now, it is obvious to see that $\mathcal{A}(I) = \langle (x^4 + \eta\delta x^2 - 1)^{p^s-i}\rangle$. Since

$$\begin{aligned}\left((x^4 + \eta\delta x^2 - 1)^{p^s-i}\right)^* &= [(x^4 + \eta\delta x^2 - 1)^*]^{p^s-i}\\ &= (-x^4 + \eta\delta x^2 + 1)^{p^s-i}\\ &= (-1)^{p^s-i}(x^4 - \eta\delta x^2 - 1)^{p^s-i},\end{aligned}$$

we have $\mathcal{A}(I)^* = \langle (x^4 - \eta\delta x^2 - 1)^{p^s-i}\rangle$.

(ii) Suppose that $h(x)$ is a unit and $1 \leq i \leq \frac{p^s+t}{2}$. Since

$$0 = \Big((x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)\Big) \Big((x^4+\eta\delta x^2-1)^{p^s-i} - u(x^4+\eta\delta x^2-1)^{p^s-2i+t}h(x)\Big),$$

we have

$$(x^4+\eta\delta x^2-1)^{p^s-i} - u(x^4+\eta\delta x^2-1)^{p^s-2i+t}h(x) \in \mathcal{A}(I).$$

Note that $0 = \Big((x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)\Big)\Big(u(x^4+\eta\delta x^2-1)^{p^s-i}\Big)$ and, thus $u(x^4+\eta\delta x^2-1)^{p^s-i} \in \mathcal{A}(I)$. This implies that

$$\langle (x^4+\eta\delta x^2-1)^{p^s-i} - u(x^4+\eta\delta x^2-1)^{p^s-2i+t}h(x), u(x^4+\eta\delta x^2-1)^{p^s-i}\rangle \subseteq \mathcal{A}(I).$$

Writing,

$$\mathcal{A}(I) = \langle (x^4+\eta\delta x^2-1)^a + u(x^4+\eta\delta x^2-1)^b g(x), u(x^4+\eta\delta x^2-1)^c\rangle$$

and by Lemma 4.10, we have $p^s - i$ is the smallest positive integer such that $u(x^4+\eta\delta x^2-1)^{p^s-i} \in \mathcal{A}(I)$. Thus, $c = p^s - i$. Now, we consider that

$$\begin{aligned} 0 &= \Big((x^4+\eta\delta x^2-1)^a + u(x^4+\eta\delta x^2-1)^b g(x)\Big) \\ &\quad \Big((x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)\Big) \\ &= (x^4+\eta\delta x^2-1)^{a+i} + u(x^4+\eta\delta x^2-1)^{b+i}g(x) + u(x^4+\eta\delta x^2-1)^{a+t}h(x). \end{aligned}$$

This means that $a + i \geq p^s$, i.e., $a \geq p^s - i$. Since $a \geq p^s - i$, we can choose $a = p^s - i$. Then, we can set $b = p^s - 2i + t$ and $g(x) = -h(x)$. Therefore,

$$\begin{aligned} \mathcal{A}(I) = \langle &(x^4+\eta\delta x^2-1)^{p^s-i} - u(x^4+\eta\delta x^2-1)^{p^s-2i+t}h(x), \\ &u(x^4+\eta\delta x^2-1)^{p^s-i}\rangle. \end{aligned}$$

Noting that

$$\begin{aligned} u(x^4+\eta\delta x^2-1)^{p^s-i} &= u\big((x^4+\eta\delta x^2-1)^{p^s-i} - u(x^4+\eta\delta x^2-1)^t h(x)\big) \\ &\in \langle (x^4+\eta\delta x^2-1)^{p^s-i} - u(x^4+\eta\delta x^2-1)^t h(x)\rangle, \end{aligned}$$

we have $\mathcal{A}(I) = \langle (x^4+\eta\delta x^2-1)^{p^s-i} - u(x^4+\eta\delta x^2-1)^t h(x)\rangle$. Let $h(x) = \sum_j (a_j x^3 + b_j x^2 + c_j x + d_j)(x^4+\eta\delta x^2-1)^j$ where $a_0x^3 + b_0x^2 + c_0x + d_0 \neq 0$ and $a_j, b_j, c_j, d_j \in \mathbb{F}_{p^m}$. Since $1 \leq i \leq \frac{p^s+t}{2}$, we have $t + j < T = \min\{i, p^s - i + t\} = i$. So, $j \leq i - t - 1$. Thus,

$$h(x) = \sum_j (a_j x^3 + b_j x^2 + c_j x + d_j)(x^4+\eta\delta x^2-1)^j.$$

Hence,

$$\mathcal{A}(I)^* = \langle (-1)^{i-t}(x^4-\eta\delta x^2-1)^{p^s-i}$$

$$- u(x^4-\eta\delta x^2-1)^t \sum_{j=0}^{i-t-1}(d_jx^3+c_jx^2+b_jx+a_j)(-1)^j \times (x^4-\eta\delta x^2-1)^j x^{4i-4j-3}\rangle$$

because

$$\begin{aligned}&[(x^4+\eta\delta x^2-1)^{p^s-i}\\ &- u(x^4+\eta\delta x^2-1)^t \sum_{j=0}^{i-t-1}(a_jx^3+b_jx^2+c_jx+d_j)(x^4+\eta\delta x^2-1)^j]^*\\ &= (-1)^{p^s-i}(x^4-\eta\delta x^2-1)^{p^s-i}\\ &- u(-1)^{p^s-2i+t}(x^4-\eta\delta x^2-1)^t \sum_{j=0}^{i-t-1}(d_jx^3+c_jx^2+b_jx+a_j)(-1)^j\\ &\times (x^4-\eta\delta x^2-1)^j x^{4i-4j-3}.\end{aligned}$$

(iii) Suppose that $h(x)$ is a unit and $\frac{p^s+t}{2} < i \le p^s - i$. By the above process, we have

$$\mathcal{A}(I) = \langle (x^4+\eta\delta x^2-1)^a + u(x^4+\eta\delta x^2-1)^b g(x), u(x^4+\eta\delta x^2-1)^{p^s-i}\rangle.$$

Since

$$\begin{aligned}0 &= \Big((x^4+\eta\delta x^2-1)^a + u(x^4+\eta\delta x^2-1)^b g(x)\Big)\\ &\quad \Big((x^4+\eta\delta x^2-1)^i + u(x^4+\eta\delta x^2-1)^t h(x)\Big)\\ &= (x^4+\eta\delta x^2-1)^{a+i} + u(x^4+\eta\delta x^2-1)^{b+i} g(x) + u(x^4+\eta\delta x^2-1)^{a+t} h(x),\end{aligned}$$

we have $a+i \ge p^s$, i.e., $a \ge p^s - i$. Since $\frac{p^s+t}{2} < i$, we have $p^s - i < i - t$ and choose $a = i - t$. Thus, $b = 0$ and $g(x) = -h(x)$. This implies that

$$\mathcal{A}(I) = \langle (x^4+\eta\delta x^2-1)^{i-t} - uh(x), u(x^4+\eta\delta x^2-1)^{p^s-i}\rangle.$$

Let $h(x) = \sum_j (a_jx^3+b_jx^2+c_jx+d_j)(x^4+\eta\delta x^2-1)^j$ where $a_0x^3+b_0x^2+c_0x+d_0 \ne 0$ and $a_j, b_j, c_j, d_j \in \mathbb{F}_{p^m}$. By assumption and $t+j < T = \min\{i, p^s - i + t\} = p^s - i + t$, we have $j \le p^s - i - 1$. Thus,

$$h(x) = \sum_{j=0}^{p^s-i-1}(a_jx^3+b_jx^2+c_jx+d_j)(x^4+\eta\delta x^2-1)^j.$$

By Lemma 4.11, we get that

$$\begin{aligned}\mathcal{A}(I)^* = \langle &(-1)^{i-t}(x^4-\eta\delta x^2-1)^{i-t}\\ &- u\sum_{j=0}^{p^s-i-1}(d_jx^3+c_jx^2+b_jx+a_j)(-1)^j(x^4-\eta\delta x^2-1)^j x^{4i-4t-4j-3},\\ &u(x^4-\eta\delta x^2-1)^{p^s-i}\rangle.\end{aligned}$$

This completes the proof of (i)-(iii). □

Theorem 4.14. *Let* $I = \langle (x^4 + \eta\delta x^2 - 1)^i + u(x^4 + \eta\delta x^2 - 1)^t h(x), u(x^4 + \eta\delta x^2 - 1)^\omega \rangle$, *where* $h(x)$ *is* 0 *or a unit.*

(i) *If* $h(x) = 0$, *then*

$$\mathcal{A}(I)^* = \langle (x^4 - \eta\delta x^2 - 1)^{p^s-\omega}, u(x^4 - \eta\delta x^2 - 1)^{p^s-i} \rangle.$$

(ii) *If* $h(x)$ *is a unit, then*

$$\begin{aligned}\mathcal{A}(I)^* = \langle &(-1)^{i-t}(x^4 - \eta\delta x^2 - 1)^{p^s-\omega} - u(x^4 - \eta\delta x^2 - 1)^{p^s-i-\omega+t} \\ &\times \sum_{j=0}^{\omega-t-1} (d_j x^3 + c_j x^2 + b_j x + a_j)(-1)^j (x^4 - \eta\delta x^2 - 1)^j, \\ &u(x^4 - \eta\delta x^2 - 1)^{p^s-i} \rangle.\end{aligned}$$

Proof. (i) Suppose that $h(x) = 0$. So, $I = \langle (x^4 + \eta\delta x^2 - 1)^i, u(x^4 + \eta\delta x^2 - 1)^\omega \rangle$. It is obvious to see that

$$\mathcal{A}(I) = \langle (x^4 + \eta\delta x^2 - 1)^{p^s-\omega}, u(x^4 + \eta\delta x^2 - 1)^{p^s-i} \rangle.$$

This implies that

$$\mathcal{A}(I)^* = \langle (x^4 - \eta\delta x^2 - 1)^{p^s-\omega}, u(x^4 - \eta\delta x^2 - 1)^{p^s-i} \rangle.$$

(ii) Suppose that $h(x)$ is a unit. We consider that

$$\begin{aligned}0 = &u(x^4 + \eta\delta x^2 - 1)^{p^s-i} \\ &\times \Big(((x^4 + \eta\delta x^2 - 1)^i + u(x^4 + \eta\delta x^2 - 1)^t h(x)) + u(x^4 + \eta\delta x^2 - 1)^\omega \Big)\end{aligned}$$

and

$$\begin{aligned}0 = &\Big((x^4 + \eta\delta x^2 - 1)^{p^s-\omega} - u(x^4 + \eta\delta x^2 - 1)^{p^s-i-\omega+t} h(x) \Big) \\ &\times \Big(((x^4 + \eta\delta x^2 - 1)^i + u(x^4 + \eta\delta x^2 - 1)^t h(x)) + u(x^4 + \eta\delta x^2 - 1)^\omega \Big).\end{aligned}$$

Thus,

$$\begin{aligned}D = &\langle (x^4+\eta\delta x^2-1)^{p^s-\omega} - u(x^4+\eta\delta x^2-1)^{p^s-i-\omega+t} h(x), u(x^4+\eta\delta x^2-1)^{p^s-i} \rangle \\ &\subseteq \mathcal{A}(I),\end{aligned}$$

and $|D| = p^{4m(i+\omega)}$. Then, we have

$$\begin{aligned}p^{4m(i+\omega)} = |D| \le |\mathcal{A}(I)| &= |\mathcal{A}(I)^*| \\ &\le |I^\perp| = \frac{p^{8mp^s}}{|I|} = \frac{p^{8mp^s}}{p^{4m(2p^s-i-\omega)}} = p^{4m(i+\omega)}.\end{aligned}$$

Therefore,

$$\begin{aligned}&\langle (x^4 + \eta\delta x^2 - 1)^{p^s-\omega} - u(x^4+\eta\delta x^2 - 1)^{p^s-i-\omega+t} h(x), u(x^4 + \eta\delta x^2 - 1)^{p^s-i} \rangle \\ &= \mathcal{A}(I).\end{aligned}$$

Let $h(x) = \sum_{j=0}^{\omega-t-1}(a_jx^3 + b_jx^2 + c_jx + d_j)(x^4 + \eta\delta x^2 - 1)^j$, where $a_0x^3 + b_0x^2 + c_0x + d_0 \neq 0$ and $a_j, b_j, c_j, d_j \in \mathbb{F}_{p^m}$. By Lemma 4.11, we obtain that

$$\begin{aligned}\mathcal{A}(I)^* = \langle (-1)^{i-t}(x^4 - \eta\delta x^2 - 1)^{p^s-\omega} - u(x^4 - \eta\delta x^2 - 1)^{p^s-i-\omega+t} \\ \times \sum_{j=0}^{\omega-t-1}(d_jx^3 + c_jx^2 + b_jx + a_j)(-1)^j(x^4 - \eta\delta x^2 - 1)^j, \\ u(x^4 - \eta\delta x^2 - 1)^{p^s-i}\rangle.\end{aligned}$$

This completes the proof of (i) and (ii). □

5. The case $p^m \equiv 5 \pmod{16}$ or $p^m \equiv 13 \pmod{16}$

In this section, using Chinese Remainder Theorem, we obtain the algebraic structures of the negacyclic codes of length $8p^s$ over R with $p^m \equiv 5 \pmod{16}$ or $p^m \equiv 13 \pmod{16}$. Since $p^m \equiv 5, 13 \pmod{16}$, we have $p^m \equiv 1 \pmod 4$. Then $x^2 + 1 = (x - \gamma)(x - \gamma^3)$ where $\gamma = \xi^{\frac{p^m-1}{4}}$. So,

$$\begin{aligned}x^{8p^s} + 1 &= (x^8 + 1)^{p^s} \\ &= (x^4 - \gamma)^{p^s}(x^4 - \gamma^3)^{p^s} \\ &= (x^{4p^s} - \gamma^{p^s})(x^{4p^s} - \gamma^{3p^s}).\end{aligned}$$

Remark 5.1. $\gamma\gamma^3 = 1$.

Next, we give the properties about the polynomials $x^4 - \gamma$ and $x^4 - \gamma^3$.

Lemma 5.2.

(i) *The polynomials $x^4 - \gamma$ and $x^4 - \gamma^3$ are irreducible over $\mathbb{F}_{p^m}$.*
(ii) *The polynomials $x^4 - \gamma$ and $x^4 - \gamma^3$ are irreducible over R.*
(iii) *$x^4 - \gamma$ and $x^4 - \gamma^3$ are coprimes of $R[x]$.*

Proof. (i) We will show that $x^4 - \gamma$ is irreducible over $\mathbb{F}_{p^m}$. Suppose that $x^4 - \gamma$ is reducible over $\mathbb{F}_{p^m}$. There exist $f(x), g(x) \in \mathbb{F}_{p^m}[x]$ such that $x^4 - \gamma = f(x)g(x)$.

If $\deg f(x) = 1$, then $\deg g(x) = 3$. So, there exists $\beta \in \mathbb{F}_{p^m}$ such that $f(\beta) = 0$. Since $x^8 + 1 = (x^4 - \gamma)(x^4 - \gamma^3) = f(x)g(x)(x^4 - \gamma^3)$, we have β is a root of $x^8 + 1$, i.e., $\beta^8 + 1 = 0$. This implies that $\beta^16 = 1$. Thus, $ord(\beta) \mid 16$, i.e., $ord(\beta) = 1$ or 2 or 4 or 8 or 16. If $ord(\beta) = 1$ or 2 or 4 or 8, then $\beta^8 + 1 = 1 + 1 = 2 \neq 0$. It is a contradiction. So, $ord(\beta) = 16$. This means that $16 \mid (p^m - 1)$, i.e., $p^m \equiv 1 \pmod{16}$. It is a contradiction. Hence, $x^4 - \gamma$ is irreducible over $\mathbb{F}_{p^m}$.

If $f(x) = 2$, then $g(x) = 2$. Let $f(x) = x^2 + ax + b$ and $g(x) = x^2 + cx + d$ for some $a, b, c, d \in \mathbb{F}_{p^m}$. Then

$$\begin{aligned}x^4 - \gamma = f(x)g(x) &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (c + a)x^3 + (d + ac + b)x^2 + (ad + bc)x + bd.\end{aligned}$$

This means that

$$c + a = 0, \tag{5.1}$$

$$d + ac + b = 0, \tag{5.2}$$

$$ad + bc = 0, \tag{5.3}$$

$$bd = -\gamma. \tag{5.4}$$

From equations (5.1), we have $a = -c$ and, implying $0 = ad+bc = (-c)d+bc = c(b-d)$. So, $c = 0$ or $b - d = 0$.

If $c = 0$, then $a = 0$ and $d = -b$. This implies that $-\xi^{\frac{p^m-1}{4}} = -\gamma = bd = -b^2$. Thus, $b = \xi^{\frac{p^m-1}{8}}$. That is $p^m \equiv 1 \pmod 8$. It is a contradiction.

If, $b - d = 0$, i.e., $b = d$, then $\xi^{\frac{3(p^m-1)}{4}} = -\xi^{\frac{(p^m-1)}{4}} = -\gamma = bd = b^2$. This implies that $b = \xi^{\frac{3(p^m-1)}{8}}$. So, $8 \mid (p^m - 1)$, i.e., $p^m \equiv 1 \pmod 8$. It is a contradiction. Hence, $x^4 - \gamma$ is irreducible over $\mathbb{F}_{p^m}$. Similarly, $x^4 - \gamma^3$ is irreducible over $\mathbb{F}_{p^m}$.

(ii) We will show that $x^4 - \gamma$ is irreducible over R. Suppose that $x^4 - \gamma$ is reducible over R. There exist $f(x), g(x) \in R[x]$ such that $x^4 - \gamma = f(x)g(x)$.

If $\deg f(x) = 1$, then $\deg g(x) = 3$. So, there exists $\beta_0 + u\beta_1 \in R$ such that $f(\beta_0 + u\beta_1) = 0$. Thus,

$$\begin{aligned} 0 &= f(\beta_0 + u\beta_1)g(\beta_0 + u\beta_1) \\ &= (\beta_0 + u\beta_1)^4 - \gamma \\ &= \beta_0^4 - \gamma + (2^2\beta_0^3\beta_1)u. \end{aligned}$$

This implies that $\beta_0^4 - \gamma = 0$ and $2^2\beta_0^3\beta_1 = 0$. By Lemma 5.2(i), we have $\beta_0^4 - \gamma \neq 0$ for any $\alpha \in \mathbb{F}_{p^m}$. It is a contradiction. Thus, $x^4 - \gamma$ is irreducible over R.

If $\deg f(x) = 2$, then $\deg g(x) = 2$. Let $f(x) = x^2 + (a_0 + a_1u)x + (b_0 + b_1u)$ and $g(x) = x^2+(c_0+c_1u)x+(d_0+ud_1)$ for some $a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 \in \mathbb{F}_{p^m}$. Then

$$\begin{aligned} x^4 - \gamma &= f(x)g(x) \\ &= \big(x^2 + (a_0 + a_1u)x + (b_0 + b_1u)\big)\big(x^2 + (c_0 + c_1u)x + (d_0 + ud_1)\big) \\ &= x^4 + \big(c_0 + a_0 + (c_1 + a_1)u\big)x^3 \\ &\quad + \big((d_0 + a_0b_0 + b_0) + (d_1 + 2a_1b_1 + b_1)u\big)x^2 \\ &\quad + \big(a_0d_0 + b_0c_0 + 2(a_1d_1 + b_1c_1)u\big)x + b_0d_0 + 2b_1d_1u. \end{aligned}$$

This implies that

$$\begin{aligned} c_0 + a_0 + (c_1 + a_1)u &= 0, \\ (d_0 + a_0b_0 + b_0) + (d_1 + 2a_1b_1 + b_1)u &= 0, \\ a_0d_0 + b_0c_0 + 2(a_1d_1 + b_1c_1)u &= 0, \\ b_0d_0 + 2b_1d_1u &= \gamma, \end{aligned}$$

and thus,

$$c_0 + a_0 = 0, \tag{5.5}$$

$$c_1 + a_1 = 0, \tag{5.6}$$

$$d_0 + a_0 b_0 + b_0 = 0, \tag{5.7}$$

$$d_1 + 2a_1 b_1 + b_1 = 0, \tag{5.8}$$

$$a_0 d_0 + b_0 c_0 = 0, \tag{5.9}$$

$$a_1 d_1 + b_1 c_1 = 0, \tag{5.10}$$

$$b_0 d_0 = \gamma, \tag{5.11}$$

$$2b_1 d_1 = 0. \tag{5.12}$$

From equations (5.5), (5.7), (5.9) and (5.11), it is a contradiction. (It is similar to Lemma 5.2(i).) Hence $x^4 - \gamma$ is irreducible over R. Similarly, $x^4 - \gamma^3$ is irreducible over R.

(iii) Suppose that $x^4 - \gamma$ and $x^4 - \gamma^3$ are not coprimes of $R[x]$. By Lemma 5.2(ii), we have $x^4 - \gamma$ and $x^4 - \gamma^3$ are irreducible over R. So, $\gcd(x^4 - \gamma, x^4 - \gamma^3) = x^4 - \gamma$ or $x^4 - \gamma^3$. This means that $\gamma = \gamma^3$. It is a contradiction. Hence, $x^4 - \gamma$ and $x^4 - \gamma^3$ are coprimes of $R[x]$. □

By Lemma 5.2, we have the algebraic structures of negacyclic codes of length $8p^s$ over R as following theorem.

Theorem 5.3. *Let C be a negacyclic code of length $8p^s$ over R. Then $C = C_1 \oplus C_3$ where C_i is a γ^{ip^s}-constacyclic code of length $4p^s$ over R for $i = 1, 3$. In particular, $|C| = |C_1||C_3|$.*

Thus, every negacyclic codes C of length $8p^s$ over R can be represented as direct sum of C_i, which are a γ^{ip^s}-constacyclic codes of length $4p^s$ over R for $i = 1, 3$. Moreover, the algebraic structures of all constacyclic codes of length $4p^s$ over R have been determined in [9] and [13].

Next, the dual code of a negacyclic code of length $8p^s$ over R is also a direct sum of the dual codes of the direct summands $C_i^\perp$ where $i = 1, 3$ as following theorem.

Theorem 5.4. *Let $C = C_1 \oplus C_3$ be a negacyclic code of length $8p^s$ over R where C_i is a γ^{ip^s}-constacyclic code of length $4p^s$ over R for $i = 1, 3$. Then $C^\perp = C_3 \oplus C_1$. In particular, $|C^\perp| = |C_1||C_3|$.*

From Theorem 5.4, we see that the dual of negacyclic codes of length $8p^s$ over R is isodual. Moreover, we obtain property for self-dual negacyclic codes of length $8p^s$ over R.

Proposition 5.5. *Let $C = C_1 \oplus C_3$ be a negacyclic code of length $8p^s$ over R where C_i is a γ^{ip^s}-constacyclic code of length $4p^s$ over R for $i = 1, 3$. Then the following hold*:

(i) $C_i = \langle u \rangle$ *is a self-dual* γ^{ip^s}*-constacyclic code of length* $4p^s$ *over* R *for* $i = 1, 3$.
(ii) $C = \langle u \rangle$ *is a self-dual negacyclic code of length* $8p^s$ *over* R.

Proof. (i) By [13, Theorem 3.7], we can see that $C_i = \langle u \rangle$ is a self-dual γ^{ip^s}-constacyclic code of length $4p^s$ over R for $i = 1, 3$.

(ii) By Theorem 5.4, we have $C^\perp = C_3 \oplus C_1$. Form Proposition 5.5(ii), we obtain $C = \langle u \rangle = C^\perp$. Thus, $C = \langle u \rangle$ is a self-dual negacyclic code of length $8p^s$ over R. □

6. The cases $p^m \equiv 7 \pmod{16}$ or $p^m \equiv 15 \pmod{16}$

In this case that $p^m \equiv 7 \pmod{16}$ or $p^m \equiv 15 \pmod{16}$, we have $p^m \equiv 7 \pmod 8$, implying $p \equiv 7 \pmod 8$. Thus, 2 is a square element under modulo p. This means that, there exists $\nu \in \mathbb{F}_{p^m}$ such that $\nu^2 = 2$. First of all, we give the properties as follows:

Proposition 6.1. *Let* $\nu^2 = 2$. *Then either* $2 - \nu$, $2 + \nu$ *or* $\nu - 2$, $-\nu - 2$ *are square elements in* $\mathbb{F}_{p^m}$.

Proof. Let $2 - \nu = \xi^k$ for some $k \in \{1, 2, \ldots, p^m - 2\}$.

Case 1: k is even. So, $2 - \nu$ is a square element. Note that $(2 - \nu)(2 + \nu) = 2 = \nu^2$. This implies that

$$2 + \nu = \frac{\nu^2}{2 - \nu}.$$

Thus, $2 + \nu$ is also a square element.

Case 2: k is odd. Clearly, $-1 = \xi^l$ for some l is odd. So, $\nu - 2 = \xi^{k+l}$. This means that $\nu - 2$ is a square element. Note that $(\nu - 2)(-\nu - 2) = 2 = \nu^2$. We consider that

$$-\nu - 2 = \frac{\nu^2}{\nu - 2}.$$

Thus, $-\nu - 2$ is also a square element. □

We now consider

$$\begin{aligned} x^{8p^s} + 1 &= (x^8 + 1)^{p^s} \\ &= (x^8 + 2x^4 + 1 - 2x^4)^{p^s} \\ &= (x^4 + 1)^2 - \nu^2 x^4)^{p^s} \\ &= (x^4 + \nu x^2 + 1)^{p^s} (x^4 - \nu x^2 + 1)^{p^s}. \end{aligned}$$

Case 1: $2 - \nu$ and $2 + \nu$ are square elements, i.e., $\delta_1^2 = 2 - \nu$ and $\delta_2^2 = 2 + \nu$ for some $\delta_1, \delta_2 \in \mathbb{F}_{p^m}$. So,

$$\begin{aligned} x^{8p^s} + 1 &= (x^4 + \nu x^2 + 1)^{p^s} (x^4 - \nu x^2 + 1)^{p^s} \\ &= (x^4 + 2x^2 + 1 + \nu x^2 - 2x^2)^{p^s} (x^4 + 2x^2 + 1 - \nu x^2 - 2x^2)^{p^s} \\ &= ((x^2 + 1)^2 - (2 - \nu)x^2)^{p^s} ((x^2 + 1)^2 - (2 + \nu)x^2)^{p^s} \end{aligned}$$

$$\begin{aligned}
&= ((x^2+1)^2 - \delta_1^2 x^2)^{p^s}((x^2+1)^2 - \delta_2^2 x^2)^{p^s} \\
&= (x^2+\delta_1 x+1)^{p^s}(x^2-\delta_1 x+1)^{p^s}(x^2+\delta_2 x+1)^{p^s}(x^2-\delta_2 x+1)^{p^s}.
\end{aligned}$$

Case 2: $\nu-2$ and $-\nu-2$ are square elements, i.e., $\delta_1^2 = \nu-2$ and $\delta_2^2 = -\nu-2$ for some $\delta_1, \delta_2 \in \mathbb{F}_{p^m}$. So,

$$\begin{aligned}
x^{8p^s}+1 &= (x^4+\nu x^2+1)^{p^s}(x^4-\nu x^2+1)^{p^s} \\
&= (x^4-2x^2+1+\nu x^2+2x^2)^{p^s}(x^4-2x^2+1-\nu x^2+2x^2)^{p^s} \\
&= ((x^2-1)^2-(-\nu-2)x^2)^{p^s}((x^2-1)^2-(\nu-2)x^2)^{p^s} \\
&= ((x^2-1)^2-\delta_1^2 x^2)^{p^s}((x^2-1)^2-\delta_2^2 x^2)^{p^s} \\
&= (x^2+\delta_1 x-1)^{p^s}(x^2-\delta_1 x-1)^{p^s}(x^2+\delta_2 x-1)^{p^s}(x^2-\delta_2 x-1)^{p^s}.
\end{aligned}$$

Remark 6.2. The polynomial $x^{8p^s}+1$ can be expressed as

$$x^{8p^s}+1 = (x^2+\delta_1 x+\eta)^{p^s}(x^2-\delta_1 x+\eta)^{p^s}(x^2+\delta_2 x+\eta)^{p^s}(x^2-\delta_2 x+\eta)^{p^s},$$

where $\eta \in \{-1,1\}$ such that

$$\delta_1^2 = \begin{cases} 2-\nu, & \text{if } \eta = 1 \\ \nu-2, & \text{if } \eta = -1 \end{cases}$$

and

$$\delta_2^2 = \begin{cases} 2+\nu, & \text{if } \eta = 1 \\ -\nu-2, & \text{if } \eta = -1. \end{cases}$$

Let the notation be as in Remark 6.2, the properties of $x^2+\mu\delta_i x+\eta$ where $i \in \{1,2\}$ and $\mu \in \{-1,1\}$ are obtained as following lemma.

Lemma 6.3.

(i) *The polynomial x^2+1 is irreducible over $\mathbb{F}_{p^m}$.*
(ii) *The polynomial $x^2+\mu\delta_i x+\eta$ is irreducible over $\mathbb{F}_{p^m}$.*
(iii) *The polynomial $x^2+\mu\delta_i x+\eta$ is irreducible over R.*
(iv) *$x^2+\delta_1 x+\eta$, $x^2-\delta_1 x+\eta$, $x^2+\delta_2 x+\eta$ and $x^2-\delta_2 x+\eta$ are coprimes in $R[x]$.*

Proof. Proofs of (i), (ii) and (iv), they follow from Lemma 4.1. Suppose that $x^2+\mu\delta_i x+\eta$ is reducible over $\mathbb{F}_{p^m}$. There exists $\beta \in \mathbb{F}_{p^m}$ such that

$$\beta^2+\mu\delta_i\beta+\eta = 0.$$

Since $x^2+\mu\delta_i x+\eta$ is a factor of x^8+1, we have β is a root of x^8+1. This implies that $\beta^8 = -1$. Thus, $ord(\beta) \mid 16$ because $\beta^{16} = 1$. If $ord(\beta) = 1, 2, 4$ and 8, we have

$$0 = \beta^8+1 = 1+1 = 2.$$

It is a contradiction. Thus, $ord(\beta) = 16$. This means that $16 \mid (p^m-1)$ and then, $p^m \equiv 1 \pmod 8$. It is a contradiction. Hence, $x^2+\mu\delta_i x+\eta$ is irreducible over $\mathbb{F}_{p^m}$. □

By Chinese Remainder Theorem, we investigate the algebraic structure of negacyclic codes of length $8p^s$ over R.

Theorem 6.4. *Let C be a negacyclic code of length $8p^s$ over R. Then*

(i) $C = I_{\delta_1} \oplus I_{-\delta_1} \oplus I_{\delta_2} \oplus I_{-\delta_2}$ *where* I_{δ_1}, $I_{-\delta_1}$, I_{δ_2} *and* $I_{-\delta_2}$ *are ideals of* $\frac{R[x]}{\langle (x^2+\delta_1 x+\eta)^{p^s}\rangle}$, $\frac{R[x]}{\langle (x^2-\delta_1 x+\eta)^{p^s}}$, $\frac{R[x]}{\langle (x^2+\delta_2 x+\eta)^{p^s}\rangle}$ *and* $\frac{R[x]}{\langle (x^2-\delta_2 x+\eta)^{p^s}\rangle}$, *respectively.*

(ii) $|C| = |I_{\delta_1}||I_{-\delta_1}||I_{\delta_2}||I_{-\delta_2}|$.

(iii) *The dual code $C^\perp$ of C is given by* $C^\perp = \mathcal{A}(I_{\delta_1})^* \oplus \mathcal{A}(I_{-\delta_1})^* \oplus \mathcal{A}(I_{\delta_2})^* \oplus \mathcal{A}(I_{-\delta_2})^*$.

(iv) $|C^\perp| = |\mathcal{A}(I_{\delta_1})^*||\mathcal{A}(I_{-\delta_1})^*||\mathcal{A}(I_{\delta_2})^*||\mathcal{A}(I_{-\delta_2})^*|$.

From Remark 6.2, we can determine the algebraic structure of ideals of the quotient ring $\frac{R[x]}{\langle (x^2+\mu\delta_i x+\eta)^{p^s}\rangle}$ where $i \in \{1,2\}$ and $\mu \in \{-1,1\}$. Moreover, we obtain that the number of elements of each ideal of $\frac{R[x]}{\langle (x^2+\mu\delta_i x+\eta)^{p^s}\rangle}$ as in Section 5.

Proposition 6.5. *Each nonzero polynomial $f(x) = ax + b$ is invertible in $\frac{R[x]}{\langle (x^2+\mu\delta_i x+\eta)^{p^s}\rangle}$ where $a, b \in \mathbb{F}_{p^m}$.*

Theorem 6.6. *The ring $\frac{R[x]}{\langle (x^2+\mu\delta_i x+\eta)^{p^s}\rangle}$ is a local ring with the maximal ideal $\langle u, x^2 + \mu\delta_i x + \eta\rangle$, and it is not a chain ring.*

Furthermore, we obtain that all forms of all ideals of $\frac{R[x]}{\langle (x^2+\mu\delta_i x+\eta)^{p^s}\rangle}$ as following theorem.

Theorem 6.7. *All ideals of $\frac{R[x]}{\langle (x^2+\mu\delta_i x+\eta)^{p^s}\rangle}$ are*

- *Type 1*: (*trivial ideals*)
$$\langle 0\rangle \text{ and } \langle 1\rangle.$$
- *Type 2*: (*principal ideals with nonmonic polynomial generators*)
$$\langle u(x^2 + \mu\delta_i x + \eta)^i\rangle,$$
where $0 < i \leq p^s - 1$.
- *Type 3*: (*principal ideals with monic polynomial generators*)
$$\langle (x^2 + \mu\delta_i x + \eta)^i + u(x^2 + \mu\delta_i x + \eta)^t h(x)\rangle,$$
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* $h(x) = \sum_j (h_{1j}x + h_{0j})(x^2 + \mu\delta_i x + \eta)^j$ *with* $h_{0j}, h_{1j} \in \mathbb{F}_{p^m}$ *and* $h_{10}x + h_{00} \neq 0$.
- *Type 4*: (*non-principal ideals*)

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

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

Next, we compute the number of elements of each type of ideals of the quotient ring $\frac{R[x]}{\langle (x^2+\mu\delta_i x+\eta)^{p^s}\rangle}$.

Theorem 6.8. *Let* I *be an ideal of the ring* $\frac{R[x]}{\langle (x^2+\mu\delta_i x+\eta)^{p^s}\rangle}$. *Then the number of elements of* I, *denoted by* n_I, *is determined as follows.*

- *If* $I = \langle 0\rangle$ *and* $I = \langle 1\rangle$, *then* $n_I = 1$ *and* $n_I = p^{4mp^s}$, *respectively.*
- *If* $I = \langle u(x^2+\mu\delta_i x+\eta)^i\rangle$ *where* $0 \le i \le p^s - 1$, *then* $n_I = p^{2m(p^s-i)}$.
- *If* $I = \langle (x^2+\mu\delta_i x+\eta)^i + u(x^2+\mu\delta_i x+\eta)^t h(x)\rangle$ *where* $1 \le i \le p^s - 1$, $0 \le t < i$, *and* $h(x)$ *is* 0 *or a unit, then*

$$n_I = \begin{cases} p^{4m(p^s-i)}, & \text{if } h(x) \text{ is } 0,\ 1 \le i \le p^s-1 \text{ or } h(x) \text{ is a unit},\ 1 \le i \le \frac{p^s+t}{2}, \\ p^{2m(p^s-t)}, & \text{if } h(x) \text{ is a unit},\ \frac{p^s+t}{2} < i \le p^s - 1. \end{cases}$$

- *If* $I = \langle (x^2+\mu\delta_i x+\eta)^i + u(x^2+\mu\delta_i x+\eta)^t h(x), u(x^2+\mu\delta_i x+\eta)^\omega\rangle$, *where* $1 \le i \le p^s - 1$, $0 \le t < i$, *either* $h(x)$ *is* 0 *or* $h(x)$ *is a unit, and*

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

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

Finally, we get that the dual code of such ideal of $\frac{R[x]}{\langle (x^2+\mu\delta_i x+\eta)^{p^s}\rangle}$ as follows:

Theorem 6.9. *Let* $I = \langle u(x^2+\mu\delta_i x+\eta)^i\rangle$ *be an ideal of the ring* $\frac{R[x]}{\langle (x^2+\mu\delta_i x+\eta)^{p^s}\rangle}$. *Then* $\mathcal{A}(I)^* = \langle (x^2+\mu\delta_i x+\eta)^{p^s-i}, u\rangle$.

Theorem 6.10. *Let* $I = \langle (x^2+\mu\delta_i x+\eta)^i + u(x^2+\mu\delta_i x+\eta)^t h(x)\rangle$ *where* $h(x)$ *is* 0 *or a unit. Then*

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

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

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

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

$$\mathcal{A}(I)^* = \langle (-1)^{i-t}(x^2+\mu\delta_i x+\eta)^{i-t}$$

$$- u \sum_{j=0}^{p^s-i-1} (b_j x + a_j)(-1)^j (x^2 + \mu\delta_i x + \eta)^j x^{2i-2t-2j-1},$$
$$u(x^2 + \mu\delta_i x + \eta)^{p^s-i}\rangle.$$

Theorem 6.11. *Let* $I = \langle (x^2 + \mu\delta_i x + \eta)^i + u(x^2 + \mu\delta_i x + \eta)^t h(x), u(x^2 + \mu\delta_i x + \eta)^\omega \rangle$, *where* $h(x)$ *is* 0 *or a unit.*

(i) *If* $h(x) = 0$, *then*

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

(ii) *If* $h(x)$ *is a unit, then*

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

7. The case $p^m \equiv 9 \pmod{16}$

In this section, we focus on the algebraic structures of the negacyclic codes of length $8p^s$ over R with $p^m \equiv 9 \pmod{16}$. Since $p^m \equiv 9 \pmod{16}$, we have $p^m \equiv 1 \pmod 8$. Then $x^4 + 1 = (x - \gamma)(x - \gamma^3)(x - \gamma^5)(x - \gamma^7)$ where $\gamma = \xi^{\frac{p^m-1}{8}}$. So,

$$\begin{aligned} x^{8p^s} + 1 &= (x^8 + 1)^{p^s} \\ &= (x^2 - \gamma)^{p^s}(x^2 - \gamma^3)^{p^s}(x^2 - \gamma^5)^{p^s}(x^2 - \gamma^7)^{p^s} \\ &= (x^{2p^s} - \gamma^{p^s})(x^{2p^s} - \gamma^{3p^s})(x^{2p^s} - \gamma^{5p^s})(x^{2p^s} - \gamma^{7p^s}). \end{aligned}$$

Remark 7.1. $\gamma^i\gamma^j = 1$ with $i + j = 8$.

Lemma 7.2.

(i) *The polynomial* $x^2 - \gamma^i$ *is irreducible over* $\mathbb{F}_{p^m}$ *where* $i = 1, 3, 5, 7$.
(ii) *The polynomial* $x^2 - \gamma^i$ *is irreducible over* R *where* $i = 1, 3, 5, 7$.
(iii) $x^2 - \gamma^i$ *and* $x^2 - \gamma^j$ *are coprimes of* $R[x]$ *where* $i, j = 1, 3, 5, 7$ *and* $i \neq j$.

Proof. (i) Suppose that $x^2 - \gamma^i$ is reducible over $\mathbb{F}_{p^m}$ for all $i = 1, 3, 5, 7$. There exists $\beta \in \mathbb{F}_{p^m}$ such that $\beta^2 - \gamma^i = 0$. Since $x^8 + 1 = (x^2 - \gamma)(x^2 - \gamma^3)(x^2 - \gamma^5)(x^2 - \gamma^7)$, we have β is a root of $x^8 + 1$ over $\mathbb{F}_{p^m}$. So, $\beta^8 + 1 = 0$, implying $\beta^{16} = 1$. This means that $ord(\beta) \mid 16$, i.e., $ord(\beta) = 1$ or 2 or 8 or 16. If $ord(\beta) = 1$ or 2 or 8, then $\beta^8 + 1 = 1 + 1 \neq 0$. It is a contraction. Thus $ord(\beta) = 16$. This implies that $16 \mid (p^m - 1)$. That is $p^m \equiv 1 \pmod{16}$. It is a contradiction. Hence, $x^2 - \gamma^i$ is irreducible over $\mathbb{F}_{p^m}$ for all $i = 1, 3, 5, 7$.

(ii) Suppose that $x^2 - \gamma^i$ is reducible over R for each $i = 1, 3, 5, 7$. There exists $\beta_0 + u\beta_1 \in R$ such that $(\beta_0 + u\beta_1)^2 - \gamma^i = 0$. So,

$$0 = (\beta_0 + u\beta_1)^2 - \gamma^i = \beta_0^2 + (2\beta_0\beta_1)u - \gamma^i.$$

This implies that $\beta_0^2 - \gamma^i = 0$ and $2\beta_0\beta_1 = 0$. By Lemma 7.2(i), $\beta_0^2 - \gamma^i \neq 0$. It is a contradiction. Hence, $x^2 - \gamma^i$ is irreducible over R for all $i = 1, 3, 5, 7$.

(iii) Suppose that $x^2 - \gamma^i$ and $x^2 - \gamma^j$ are not coprimes of $R[x]$ with $i \neq j$. By Lemma Lemma 7.2(ii), $\gcd(x^2 - \gamma^i, x^2 - \gamma^j) = x^2 - \gamma^i$ or $x^2 - \gamma^j$. This means that $\gamma^i = \gamma^j$, implying that $i = j$. It is a contradiction. Hence, $x^2 - \gamma^i$ and $x^2 - \gamma^j$ are coprimes of $R[x]$. □

Similarly, by Chinese Remainder Theorem, we obtain that algebraic structures of such negacyclic code as follow:

Theorem 7.3. *Let C be a negacyclic code of length $8p^s$ over R. Then $C = C_1 \oplus C_3 \oplus C_5 \oplus C_7$ where C_i is a γ^{ip^s}-constacyclic code of length $2p^s$ over R for $i = 1, 3, 5, 7$. In particular, $|C| = |C_1||C_3||C_5||C_7|$.*

Theorem 7.4. *Let $C = C_1 \oplus C_3 \oplus C_5 \oplus C_7$ be a negacyclic code of length $8p^s$ over R where C_i is a γ^{ip^s}-constacyclic code of length $2p^s$ over R for all $i = 1, 3, 5, 7$. Then $C^\perp = C_7 \oplus C_5 \oplus C_3 \oplus C_1$. In particular, $|C^\perp| = |C_1||C_3||C_5||C_7|$.*

From above theorem, we see that the dual code of negacyclic codes of length $8p^s$ over R is a isodual code.

Finally, we determine the self-dual negacyclic codes of length $8p^s$ over R.

Proposition 7.5. *Let $C = C_1 \oplus C_3 \oplus C_5 \oplus C_7$ be a negacyclic code of length $8p^s$ over R where C_i is a γ^{ip^s}-constacyclic code of length $4p^s$ over R for $i = 1, 3, 5, 7$. Then the following hold*

(i) *$C_i = \langle u \rangle$ is a self-dual γ^{ip^s}-constacyclic code of length $4p^s$ over R for $i = 1, 3$.*
(ii) *$C = \langle u \rangle$ is a self-dual negacyclic code of length $8p^s$ over R.*

8. Conclusions

We obtain that the algebraic structures of the negacyclic codes of length $8p^s$ over R in the below table.

Furthermore, we characterize the ideals of the quotient rings $\frac{R[x]}{\langle (x^4+\mu\delta x^2-1)^{p^s} \rangle}$ into 4 types; trivial ideals, principal ideals with nonmonic polynomial generators, principal ideals with monic polynomial generators and non-principal ideals; in Theorem 4.7 where $\mu \in \{-1, 1\}$. Next, the number of elements for each ideals of $\frac{R[x]}{\langle (x^4+\mu\delta x^2-1)^{p^s} \rangle}$ is mentioned in Theorem 4.9. In addition, the structures of dual codes are determined in Theorem 4.12, Theorem 4.13 and Theorem 4.14. For the quotient rings $\frac{R[x]}{\langle (x^2+\mu\delta_i x+\eta)^{p^s} \rangle}$ where $i \in \{1, 2\}$ and $\mu \in \{-1, 1\}$, it follows from the quotient ring $\frac{R[x]}{\langle (x^4+\mu\delta x^2-1)^{p^s} \rangle}$. Finally, we summarize some self-dual negacyclic code of length $8p^s$ over R in Table 2.

Acknowledgement. The authors would like to thank Naresuan University and Science Achievement Scholarship of Thailand, which provides supporting for research. We are also thank the referees for careful reading and useful comments and suggestions.

TABLE 1. The algebraic structures of each negacyclic code C of length $8p^s$ over R

Cases	Algebraic structures
$p^m \equiv 1 \pmod{16}$	$C = C_1 \oplus C_3 \oplus C_5 \oplus C_7 \oplus C_9 \oplus C_{11} \oplus C_{13} \oplus C_{15}$, where C_i is a $\xi^{\frac{i(p^m-1)}{16}}$-constacyclic code of length p^s over R for all $i = 1, 3, 5, 7, 9, 11, 13, 15$ (see Theorem 3.2).
$p^m \equiv 3, 11 \pmod{16}$	$C = I_\delta \oplus I_{-\delta}$, where I_δ and $I_{-\delta}$ are ideals of $\frac{R[x]}{\langle (x^4+\delta x^2-1)^{p^s} \rangle}$ and $\frac{R[x]}{\langle (x^4-\delta x^2-1)^{p^s} \rangle}$, respectively (see Theorem 4.2).
$p^m \equiv 5, 13 \pmod{16}$	$C = C_1 \oplus C_3$, where C_i is a $\xi^{\frac{i(p^m-1)}{4}}$-constacyclic code of length $4p^s$ over R for all $i = 1, 3$ (see Theorem 5.3).
$p^m \equiv 7, 15 \pmod{16}$	$C = I_{\delta_1} \oplus I_{-\delta_1} \oplus I_{\delta_2} \oplus I_{-\delta_2}$ where $I_{\delta_1}, I_{-\delta_1}, I_{\delta_2}$ and $I_{-\delta_2}$ are ideals of $\frac{R[x]}{\langle (x^2+\delta_1 x+\eta)^{p^s} \rangle}$, $\frac{R[x]}{\langle (x^2-\delta_1 x+\eta)^{p^s} \rangle}$, $\frac{R[x]}{\langle (x^2+\delta_2 x+\eta)^{p^s} \rangle}$ and $\frac{R[x]}{\langle (x^2-\delta_2 x+\eta)^{p^s} \rangle}$, respectively (see Theorem 6.4).
$p^m \equiv 9 \pmod{16}$	$C = C_1 \oplus C_3 \oplus C_5 \oplus C_7$, where C_i is a $\xi^{\frac{i(p^m-1)}{8}}$-constacyclic code of length $2p^s$ over R for all $i = 1, 3, 5, 7$ (see Theorem 7.3)

TABLE 2. Some self-dual negacyclic codes of length $8p^s$ over R

Cases	Self-dual negacyclic codes of length $8p^s$ over R
$p^m \equiv 1 \pmod{16}$	$\langle u \rangle$ is the unique self-dual negacyclic codes of length $8p^s$ over R (see Corollary 3.4).
$p^m \equiv 5, 9, 13 \pmod{16}$	$\langle u \rangle$ (see Proposition 5.5 and Proposition 7.5).

References

[1] T. Abualrub and I. Siap, *Constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$*, J. Franklin Inst. **346** (2009), no. 5, 520–529. https://doi.org/10.1016/j.jfranklin.2009.02.001

[2] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seemann, *On repeated-root cyclic codes*, IEEE Trans. Inform. Theory **37** (1991), no. 2, 337–342. https://doi.org/10.1109/18.75249

[3] 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.

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

[5] ———, *Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$*, IEEE Trans. Inform. Theory **55** (2009), no. 4, 1730–1740. https://doi.org/10.1109/TIT.2009.2013015

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

[7] ———, *Repeated-root constacyclic codes of length $2p^s$*, Finite Fields Appl. **18** (2012), no. 1, 133–143. https://doi.org/10.1016/j.ffa.2011.07.003

[8] ———, *Structure of repeated-root constacyclic codes of length $3p^s$ and their duals*, Discrete Math. **313** (2013), no. 9, 983–991. https://doi.org/10.1016/j.disc.2013.01.024

[9] 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), no. 4, 832–849. https://doi.org/10.1016/j.disc.2016.11.014

[10] 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), no. 2, 324–335.

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

[12] H. Q. Dinh, B. T. Nguyen, and S. Sriboonchitta, *Negacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ and their duals*, Discrete Math. **341** (2018), no. 4, 1055–1071. https://doi.org/10.1016/j.disc.2017.12.019

[13] H. Q. Dinh, B. T. Nguyen, S. Sriboonchitta, and T. M. Vo, *On $(\alpha+u\beta)$-constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$**, J. Algebra Appl. **18** (2019), no. 2, 1950023, 16 pp. https://doi.org/10.1142/S0219498819500233

[14] 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. https://doi.org/10.1016/j.ffa.2014.09.003

[15] G. Falkner, B. Kowol, W. Heise, and E. Zehendner, *On the existence of cyclic optimal codes*, Atti Sem. Mat. Fis. Univ. Modena **28** (1979), no. 2, 326–341.

[16] K. Guenda and T. A. Gulliver, *Construction of cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$ for DNA computing*, Appl. Algebra Engrg. Comm. Comput. **24** (2013), no. 6, 445–459. https://doi.org/10.1007/s00200-013-0188-x

[17] J. H. van Lint, *Repeated-root cyclic codes*, IEEE Trans. Inform. Theory **37** (1991), no. 2, 343–345. https://doi.org/10.1109/18.75250

[18] X. Liu and X. Xu, *Cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$*, Acta Math. Sci. Ser. B (Engl. Ed.) **34** (2014), no. 3, 829–839. https://doi.org/10.1016/S0252-9602(14)60053-9

[19] R. M. Roth and G. Seroussi, *On cyclic MDS codes of length q over* GF(q), IEEE Trans. Inform. Theory **32** (1986), no. 2, 284–285. https://doi.org/10.1109/TIT.1986.1057151

Chakkrid Klin-eam
Department of Mathematics
Faculty of Science
Naresuan University
Phitsanulok 65000, Thailand
and
Research Center for Academic Excellence in Mathematics
Naresuan University
Phitsanulok 65000, Thailand
Email address: chakkridk@nu.ac.th

Jirayu Phuto
Department of Mathematics
Faculty of Science
Naresuan University
Phitsanulok 65000, Thailand
Email address: jirayup60@email.nu.ac.th