Gulf Journal of Mathematics ISSN: 2309-4966
Vol 17, Issue 2 (2024) 73-90 https://doi.org/10.56947/gjom.v17i2.1918

A CLASS OF CONSTACYCLIC CODES OF LENGTH $2p^s$ OVER $\frac{\mathbb{F}_{p^m}[u,v]}{\langle u^2,v^2,uv-vu\rangle}$

YOUSSEF AHENDOUZ[1*] and ISMAIL AKHARRAZ[2]

Abstract. Let p be an odd prime number. This paper investigates λ-constacyclic codes of length $2p^s$ over the ring $R_{u,v} = \frac{\mathbb{F}_{p^m}[u,v]}{\langle u^2,v^2,uv-vu\rangle}$, where $\lambda = \psi + \rho u + \eta v + \tau uv$, with $\psi, \rho, \eta, \tau \in \mathbb{F}_{p^m}, \psi \in \mathbb{F}^*_{p^m}$, and ρ, η not both zero. When $\lambda = \mu^2$ for some $\mu \in R_{u,v}$ the structures of all λ-constacyclic codes of length $2p^s$ over $R_{u,v}$ are determined and can be expressed as the sum of a $(-\mu)$-constacyclic code and a μ-constacyclic code of length p^s. When λ is not a square, we classify these codes into four distinct types, provide the number of codewords for each type, and give the details of their dual codes.

1. Introduction

In error-correcting code theory, constacyclic codes play an important role because they can be efficiently encoded using simple shift registers. Their strong algebraic structures enable effective error correction and detection, making them valuable for both practical and theoretical purposes. However, classifying these codes remains a challenging task. So far, only certain classes of constacyclic codes of specific lengths over particular finite rings have been successfully classified.

Let R be a finite commutative ring with unity, and let λ be a unit of R. A λ-constacyclic code of length r over R is represented as an ideal of the quotient ring $\frac{R[x]}{\langle x^r-\lambda\rangle}$. When the code length r is coprime to the characteristic of the residue field of R, the codes are referred to as simple root codes; otherwise, they are called repeated root codes. In recent years, there has been significant interest in codes over finite rings, as certain good codes have been discovered as Gray images of codes over rings. Special classes of simple and repeated root constacyclic codes over various finite rings have been extensively studied by numerous authors; see, for example, [4, 16, 17, 1, 5, 2, 19, 3, 13].

Yildiz et al. in [18] have studied the ring $\frac{\mathbb{F}_2[u,v]}{\langle u^2,v^2,uv-vu\rangle}$, which is not a chain ring, and examined cyclic codes of odd length over it. They discovered some effective binary codes as the Gray images of these cyclic codes. A generalization of these codes was explored in [10], where the authors investigated the cyclic codes over $\frac{\mathbb{F}_2[u_1,u_2,\cdots,u_k]}{\left\langle u_i^2,u_j^2,u_iu_j-u_ju_i\right\rangle}$, as well as characterized the nontrivial one-generator cyclic codes.

Date: Received: Apr 20, 2024; Accepted: Aug 23, 2024.
* Corresponding author.
2020 *Mathematics Subject Classification.* Primary 11T71; Secondary 94B15 .
Key words and phrases. Constacyclic codes, codes over rings, dual code.

Subsequently, Sobhani and Molakarimi [15] extended these studies to cyclic codes over the ring $\frac{\mathbb{F}_{2^m}[u,v]}{\langle u^2,v^2,uv-vu\rangle}$. Additionally, in 2015, Kewat et al. [12] investigated cyclic codes over the ring $\frac{\mathbb{Z}_p[u,v]}{\langle u^2,v^2,uv-vu\rangle}$ and identified a unique set of generators for these codes.

In this article, we consider the ring $R_{u,v} = \frac{\mathbb{F}_{p^m}[u,v]}{\langle u^2,v^2,uv-vu\rangle}$, where p is an odd prime number. This ring is an important example of a finite local ring but not a chain ring. Its units have the form:

$$\psi + \rho u + \eta v + \tau uv,$$

where $\psi \in \mathbb{F}_{p^m}^*$ and $\rho, \eta, \tau \in \mathbb{F}_{p^m}$.

Dinh et al. [7] determined the algebraic structures of all constacyclic codes of length p^s over $R_{u,v}$, except for the $(\psi + \tau uv)$-constacyclic codes where $\tau \neq 0$, which are studied in [8]. In the case where $p = 2$, Dinh et al. [9] classified all self-dual λ-constacyclic codes of length 2^s over $R_{u,v}$ corresponding to units of the form

$$\lambda = \psi + \eta v + \tau uv, \quad \psi + \rho u + \tau uv, \quad \psi + \rho u + \eta v + \tau uv,$$

where $\psi, \rho, \eta \in \mathbb{F}_{2^m}^*$ and $\tau \in \mathbb{F}_{2^m}$. All these previous works were limited to the case of lengths p^s. In this article, we propose to study some cases of constacyclic codes of length $2p^s$ over $R_{u,v}$.

The remainder of this article is structured as follows: In Section 2, we present essential preliminary elements on constacyclic codes. Section 3 explores λ-constacyclic codes of length $2p^s$ over $R_{u,v}$, examining the number of elements in each constacyclic code and their duals when λ is a square. Section 4 continues this analysis for λ-constacyclic codes in the case where λ is not a square. Finally, Section 5 delves into the dual of the codes studied in Section 4.

2. Preliminaries

Let R be a finite commutative ring. The ring R is a local ring if it has a unique maximal ideal. Moreover, if this unique maximal ideal is principal, then R is known as a chain ring. If R satisfies the isomorphism $\frac{R}{\mathrm{J}(R)} \cong \mathrm{soc}(R)$, where $\mathrm{J}(R)$ denotes the Jacobson radical and $\mathrm{soc}(R)$ is the socle of the ring R, then R is called a Frobenius ring [14].

A linear code, denoted as C, of length r over R, is an R-submodule of R^r. Let λ be a unit in the ring R. A linear code C of length r over R is defined as a λ-constacyclic code if the following condition holds:

$$(\phi_0, \phi_1, \ldots, \phi_{r-1}) \in C \Rightarrow (\lambda\phi_{r-1}, \phi_0, \ldots, \phi_{r-2}) \in C.$$

Each $\phi = (\phi_0, \phi_1, \ldots, \phi_{r-1}) \in C$ can be represented as a polynomial $\phi(x) = \phi_0 + \phi_1 x + \cdots + \phi_{r-1}x^{r-1}$. This identification leads us to the following proposition.

Proposition 2.1. [11] *A subset C of R^r is a λ-constacyclic code if and only if C is an ideal of $\frac{R[x]}{\langle x^r-\lambda\rangle}$.*

The dual code $C^{\perp}$ of a linear code C of length r over a ring R is defined as

$$C^{\perp}=\left\{\phi=(\phi_0,\phi_1,\ldots,\phi_{r-1})\in R^r \mid \sum_{l=0}^{r-1}\phi_l\phi'_l=0,\ \text{for all } \phi'=\left(\phi'_0,\phi'_1,\ldots,\phi'_{r-1}\right)\in C\right\}.$$

Proposition 2.2. [7, Proposition 2.4] *Consider a linear code C of length r over a finite Frobenius ring R. Then,*

$$|C^{\perp}||C|=|R|^r.$$

The annihilator of an ideal I in the ring R, denoted as $\mathcal{A}(I)$, is defined as the set

$$\mathcal{A}(I)=\{a\in R \mid ab=0,\ \text{for all } b\in I\}.$$

For any polynomial $\phi(x)=\phi_0+\phi_1x+\ldots+\phi_lx^l\in R[x]$, where $\phi_l\neq 0$, we define the reciprocal polynomial $\phi^*(x)$ as $\phi^*(x)=x^l\phi(x^{-1})=\phi_l+\phi_{l-1}x+\ldots+\phi_0x^l$.

Proposition 2.3. [4] *Let C be a λ-constacyclic code of length r over R. Then*

$$C^{\perp}=\mathcal{A}(C)^*:=\{\phi^*(x)\mid \phi(x)\in\mathcal{A}(C)\}.$$

Throughout this paper, let p be an odd prime number and m a positive integer. We consider the following rings:

$$R_{u,v}=\frac{\mathbb{F}_{p^m}[u,v]}{\langle u^2,v^2,uv-vu\rangle}$$

and

$$T_v=\frac{\mathbb{F}_{p^m}[v]}{\langle v^2\rangle}.$$

It is straightforward to verify that $\mathrm{J}(R_{u,v})=\langle u,v\rangle$ and $\mathrm{Soc}(R_{u,v})=\langle uv\rangle$. As a result, we have the isomorphism

$$\frac{R_{u,v}}{\mathrm{J}(R_{u,v})}\cong\mathrm{Soc}(R_{u,v})$$

which implies that $R_{u,v}$ is a Frobenius ring. Additionally, T_v is a chain ring with maximal ideal $\langle v\rangle$. An element of $R_{u,v}$ of the form $\lambda=\psi+\rho u+\eta v+\tau uv$, where $\psi,\rho,\eta,\tau\in\mathbb{F}_{p^m}$, is a unit if and only if $\psi\neq 0$. Without loss of generality, we assume $\eta\neq 0$, ensuring that at least one of ρ or η is non-zero.

Let s be a positive integer. Applying the division algorithm, we can express s as $s=q_sm+r_s$, where q_s and r_s are non-negative integers satisfying $0\leq r_s\leq m-1$. Note that $\psi^{p^m}=\psi$. Define $\psi_0=\psi^{p^{m-r_s}}=\psi^{p^{(q_s+1)m-s}}$. It follows that

$$\psi_0^{p^s}=\psi^{p^{(q_s+1)m}}=\psi.$$

Now, let's define the following rings:

$$\mathcal{R}_\lambda=\frac{R_{u,v}[x]}{\langle x^{2p^s}-\lambda\rangle},$$

and

$$\mathcal{S}_{\psi+\eta v}=\frac{T_v[x]}{\langle x^{2p^s}-(\psi+\eta v)\rangle}.$$

Additionally, consider the homomorphism:

$$\Phi : \begin{array}{ccc} R_{u,v} & \rightarrow & T_v \\ a_1 + a_2u + a_3v + a_4uv & \mapsto & a_1 + a_3v \end{array}$$

where $a_i \in \mathbb{F}_{p^m}$. This homomorphism is the reduction modulo u and extends naturally to a homomorphism between polynomial rings:

$$\Phi : R_{u,v}[x] \rightarrow T_v[x].$$

Since

$$\Phi(x^{2p^s} - \lambda) = x^{2p^s} - (\psi + \eta v),$$

the universal property of quotient rings guarantees the existence of a unique homomorphism, also denoted by Φ, such that

$$\Phi : \mathcal{R}_\lambda \rightarrow \mathcal{S}_{\psi+\eta v}.$$

Proposition 2.4. *The following conditions are equivalent:*

(1) λ is a square in $R_{u,v}$.
(2) $\psi + \eta v$ is a square in T_v.
(3) ψ is a square in $\mathbb{F}_{p^m}$.

Proof. **(1) ⇒ (2):** Suppose λ is a square in $R_{u,v}$. Then there exists an element $\mu \in R_{u,v}$ such that $\lambda = \mu^2$. We can write $\mu = \psi' + \rho' u + \eta' v + \tau' uv$, where $\psi', \rho', \eta', \tau' \in \mathbb{F}_{p^m}$. Therefore,

$$\lambda = (\psi' + \rho' u + \eta' v + \tau' uv)^2.$$

Now, reducing modulo u, we have:

$$\psi + \eta v = (\psi' + \eta' v)^2.$$

This implies $\psi + \eta v$ is a square in T_v.

(2) ⇒ (3): Assume $\psi + \eta v$ is a square in T_v. Thus, there exists some $y \in T_v$ such that $\psi + \eta v = y^2$. Let $y = a + bv$, where $a, b \in \mathbb{F}_{p^m}$. Then:

$$\psi + \eta v = (a + bv)^2 = a^2 + 2abv + b^2v^2.$$

From this, we conclude that $\psi = a^2$, hence ψ is a square in $\mathbb{F}_{p^m}$.

(3) ⇒ (1): If ψ is a square in $\mathbb{F}_{p^m}$, then there exists an element $c \in \mathbb{F}_{p^m}$ such that $\psi = c^2$. Consider the element $\mu = c + \rho' u + \eta' v + \tau' uv \in R_{u,v}$, where $\rho', \eta', \tau' \in \mathbb{F}_{p^m}$ are chosen such that $\rho' = (2c)^{-1}\rho$, $\eta' = (2c)^{-1}\eta$, and $\tau' = c^{-1}(2^{-1}\tau - \rho'\eta')$. Then:

$$\lambda = \mu^2 = (c + \rho' u + \eta' v + \tau' uv)^2.$$

Thus, λ is a square in $R_{u,v}$. □

3. The case when λ is a square in $R_{u,v}$

In this section, we assume that λ is a square in the ring $R_{u,v}$, denoted by $\lambda = \mu^2$. Define two polynomials in $\mathcal{R}_{u,v}[x]$:

$$\ell_1(x) = (2\mu)^{-1}(x^{p^s} + \mu) \quad \text{and} \quad \ell_2(x) = -(2\mu)^{-1}(x^{p^s} - \mu).$$

Notably, in the ring $\mathcal{R}_\lambda$, the following equations hold:

$$\begin{cases} \ell_1(x) + \ell_2(x) = 1, \\ \ell_1(x) \cdot \ell_2(x) = 0, \\ \ell_1(x)^2 = \ell_1(x), \\ \ell_2(x)^2 = \ell_2(x). \end{cases} \tag{3.1}$$

Now, we state the following lemma:

Lemma 3.1. *(1)* $\mathcal{R}_\lambda = \ell_1(x)\mathcal{R}_\lambda \oplus \ell_2(x)\mathcal{R}_\lambda$;

(2) The ring homomorphisms

$$\begin{array}{rcl} \pi_{\ell_1} : \frac{R_{u,v}[x]}{\langle x^{p^s}-\mu\rangle} & \longrightarrow & \ell_1(x)\mathcal{R}_\lambda \\ z(x) & \mapsto & \ell_1(x)\cdot z(x) \end{array} \quad , \textit{and } \begin{array}{rcl} \pi_{\ell_2} : \frac{R_{u,v}[x]}{\langle x^{p^s}+\mu\rangle} & \longrightarrow & \ell_2(x)\mathcal{R}_\lambda \\ z(x) & \mapsto & \ell_2(x)\cdot z(x) \end{array}$$

are ring isomorphisms.

Proof. (1) For any $z(x) \in \mathcal{R}_\lambda$,

$$z(x) = z(x)(\ell_1(x) + \ell_2(x)) = \ell_1(x)z(x) + \ell_2(x)z(x) \ \subseteq \ell_1(x)\mathcal{R}_\lambda + \ell_2(x)\mathcal{R}_\lambda.$$

Thus, $\mathcal{R}_\lambda = \ell_1(x)\mathcal{R}_\lambda + \ell_2(x)\mathcal{R}_\lambda$. Additionally, if $\ell_1(x)z_1(x) + \ell_2(x)z_2(x) = 0$, then, by (3.1), we have

$$\begin{cases} \ell_1(x)z_1(x) = \ell_1(x)\left(\ell_1(x)z_1(x) + \ell_2(x)z_2(x)\right) = 0, \\ \ell_2(x)z_2(x) = \ell_1(x)\left(\ell_1(x)z_1(x) + \ell_2(x)z_2(x)\right) = 0. \end{cases}$$

Hence, $\mathcal{R}_\lambda = \ell_1(x)\mathcal{R}_\lambda \oplus \ell_2(x)\mathcal{R}_\lambda$.

(2) Let's demonstrate that π_{ℓ_1} is a ring isomorphism, and similarly for π_{ℓ_2}. If $\ell_1(x)\cdot z(x) = 0$ in $\ell_1(x)\mathcal{R}_\lambda$, then there exists $b(x) \in R_{u,v}[x]$ such that $\ell_1(x)\cdot z(x) = b(x)\cdot\left(x^{2p^s} - \lambda\right)$, i.e.,

$$(1 - \ell_2(x))\cdot z(x) = b(x)\cdot\left(x^{2p^s} - \lambda\right), \text{ in } R_{u,v}[x].$$

Since $\ell_2(x)$ and $\left(x^{2p^s} - \lambda\right)$ are both divisible by $x^{p^s} - \mu$, it follows that $z(x) = 0$ in $\frac{R_{u,v}[x]}{\langle x^{p^s}-\mu\rangle}$. Thus, we have shown that π_{ℓ_1} is injective. The surjection is obvious.

□

As a consequence of the preceding results, we can now present the following theorem.

Theorem 3.2. *A subset C of $\mathcal{R}_\lambda$ is a λ-constacyclic code of length $2p^s$ over $R_{u,v}$ if and only if $C = \ell_1(x)C_1 \oplus \ell_2(x)C_2$, where C_1 is a μ-constacyclic code of length p^s over $R_{u,v}$, and C_2 is a $(-\mu)$-constacyclic code of length p^s over $R_{u,v}$. Moreover, $\mid C \mid = \mid C_1 \mid\mid C_2 \mid$.*

Proof. By Lemma 3.1, we have $C = I \oplus J$, where I and J are ideals of $\ell_1(x)\mathcal{R}_\lambda$ and $\ell_2(x)\mathcal{R}_\lambda$, respectively. Since π_{ℓ_1} and π_{ℓ_2} are ring isomorphisms, $I = \ell_1(x)C_1$ and $J = \ell_2(x)C_2$, where C_1 and C_2 are ideals of $\frac{R_{u,v}[x]}{\langle x^{p^s}-\mu\rangle}$ and $\frac{R_{u,v}[x]}{\langle x^{p^s}+\mu\rangle}$, respectively. Moreover, we have

$$|C| = |I||J| = |C_1||C_2|.$$

□

Example 3.3. Let $R_{u,v} = \frac{\mathbb{F}_3[u,v]}{\langle u^2,v^2,uv-vu\rangle}$, $\lambda = 1+2v$, and $p^s = p^m = 3$. Here, $\lambda = \mu^2$ where $\mu = 1+v$. Consider the polynomials:

$$\ell_1(x) = (2\mu)^{-1}(x^3+\mu) \quad \text{and} \quad \ell_2(x) = -(2\mu)^{-1}(x^3-\mu).$$

Given that $(2\mu)^{-1} = 1+2v$, we have:

$$\ell_1(x) = (1+2v)(x^3+(1+v)),$$

$$\ell_2(x) = -(1+2v)(x^3-(1+v)).$$

Then, the $(1+2v)$-constacyclic code of length 6 over $R_{u,v}$ is given by:

$$C = \ell_1(x)C_1 \oplus \ell_2(x)C_2,$$

where C_1 is a $(1+v)$-constacyclic code of length 3 over $R_{u,v}$, and C_2 is a $(-(1+v))$-constacyclic code of length 3 over $R_{u,v}$.

Furthermore, the dual code $C^\perp$ of a code C is determined as follows:

Theorem 3.4. *Consider the λ-constacyclic code $C = \ell_1(x)C_1 \oplus \ell_2(x)C_2$ of length $2p^s$ over $R_{u,v}$, where C_1 is a μ-constacyclic code of length p^s over $R_{u,v}$, and C_2 is a $(-\mu)$-constacyclic code of length p^s over $R_{u,v}$. Then, $C^\perp = \ell_1(x)C_1^\perp \oplus \ell_2(x)C_2^\perp$.*

Proof. We have

$$\begin{aligned}
& t(x) = \ell_1(x)t_1(x) \oplus \ell_2(x)t_2(x) \in \mathcal{A}(C) \\
\Leftrightarrow\ & \forall z_1(x) \in C_1, \forall z_2(x) \in C_2, (\ell_1(x)t_1(x) \oplus \ell_2(x)t_2(x)) \cdot (\ell_1(x)z_1(x) \oplus \ell_2(x)z_2(x)) = 0 \\
\Leftrightarrow\ & \forall z_1(x) \in C_1, \forall z_2(x) \in C_2, \ell_1(x) \cdot t_1(x) \cdot z_1(x) = 0 \text{ and } \ell_2(x) \cdot t_2(x) \cdot z_2(x) = 0 \\
\Leftrightarrow\ & \forall z_1(x) \in C_1, t_1(x) \cdot z_1(x) = 0 \text{ in } \frac{R_{u,v}[x]}{\langle x^{p^s}-\mu\rangle} \text{ and } \forall z_2(x) \in C_2, t_2(x) \cdot z_2(x) = 0 \text{ in } \frac{R_{u,v}[x]}{\langle x^{p^s}+\mu\rangle} \\
\Leftrightarrow\ & t_1(x) \in \mathcal{A}(C_1) \text{ and } t_2(x) \in \mathcal{A}(C_2).
\end{aligned}$$

Therefore,

$$\mathcal{A}(C) = \ell_1(x)\mathcal{A}(C_1) \oplus \ell_2(x)\mathcal{A}(C_2).$$

Thus, by Proposition 2.3,

$$C^\perp = {\ell_1}^*(x)C_1^\perp \oplus {\ell_2}^*(x)C_2^\perp.$$

Since ${\ell_1}^*(x)$ is associated with $\ell_1(x)$ and ${\ell_2}^*(x)$ is associated with $\ell_2(x)$, we have

$$C^\perp = \ell_1(x)C_1^\perp \oplus \ell_2(x)C_2^\perp.$$

□

By Theorems 3.2 and 3.4, the structure of λ-constacyclic codes of length $2p^s$ over $R_{u,v}$, along with the cardinality and dual of each code, is entirely determined by the (μ) and $-\mu$-constacyclic codes of length p^s over $R_{u,v}$, which are studied in detail in [7].

4. The case when λ is not a square in $R_{u,v}$

In this section, we explore the structures of all λ-constacyclic codes of length $2p^s$ over $R_{u,v}$ when λ is not a square in $R_{u,v}$. Recall that $\lambda = \psi + \rho u + \eta v + \tau uv$, where $\psi, \eta \in \mathbb{F}_{p^m}^*$ and $\rho, \tau \in \mathbb{F}_{p^m}$. It is important to note that, by Proposition 2.4, $\psi + \eta v$ is not a square in T_v.

The following theorem presents some known results for $(\psi + \eta v)$-constacyclic codes of length p^s over the ring T_v, i.e., ideals of $\mathcal{S}_{\psi+\eta v}$, which are necessary in this section.

Theorem 4.1. [2]

(1) In the ring $\mathcal{S}_{\psi+\eta v}$, $(x^2-\psi_0)^{p^s} = \eta v$, and the polynomial $x^2-\psi_0$ is nilpotent, with a nilpotency index of $2p^s$.

(2) The ring $\mathcal{S}_{\psi+\eta v}$ forms a chain ring, and its ideals is expressed as follows:

$$\mathcal{S}_{\psi+\eta v} \supsetneq \langle x^2-\psi_0\rangle \supsetneq \cdots \supsetneq \left\langle \left(x^2-\psi_0\right)^{2p^s-1}\right\rangle \supsetneq \left\langle \left(x^2-\psi_0\right)^{2p^s}\right\rangle = \langle 0\rangle.$$

(3) For every $i = 0, \ldots, 2p^s$, the following relationship holds:

$$\left|\left\langle \left(x^2-\psi_0\right)^{i}\right\rangle\right| = p^{2m(2p^s-i)}. \tag{4.1}$$

Lemma 4.2. *In $\mathcal{R}_\lambda$,*

(1) $\forall i \in 0, \ldots, 2p^s-1$, $(x^2-\psi_0)^i \not\subseteq \langle u\rangle$.

(2) $(x^2-\psi_0)^{2p^s} = 2\rho u(x^2-\psi_0)^{p^s}$.

Proof. In $\mathcal{S}_{\psi+\eta v}$, by Theorem 4.1, we have the following:

$$\Phi\left((x^2-\psi_0)^{2p^s-1}\right) = \Phi((x^2-\psi_0))^{2p^s-1} = (x^2-\psi_0)^{2p^s-1} = (x^2-\psi_0)^{p^s}(x^2-\psi_0)^{p^s-1} = \eta v(x^2-\psi_0)^{p^s-1}.$$

Thus, if $(x^2-\psi_0)^{2p^s-1} \subseteq \langle u\rangle$, then $\Phi((x^2-\psi_0)^{2p^s-1}) = 0$. Consequently, $\eta v(x^2-\psi_0)^{p^s-1} = 0$ in $\mathcal{S}_{\psi+\eta v}$, leading to a contradiction.

For the second point, in $\mathcal{R}_\lambda$, for all $1 \le k \le p^s-1$, we have $p \mid \binom{p^s}{k}$. Then,

$$\left(x^2-\psi_0\right)^{p^s} = x^{2p^s} - \psi_0^{p^s} + \sum_{k=1}^{p^s-1}\binom{p^s}{k}x^{2k}(-\psi_0)^{p^s-k} = \rho u + \eta v + \tau uv.$$

So

$$\left(x^2-\psi_0\right)^{2p^s} - 2\rho u\left(x^2-\psi_0\right)^{p^s} = \left(\left(x^2-\psi_0\right)^{p^s} - \rho u\right)^2 = (\eta v + \tau uv)^2 = 0.$$

Then

$$\left(x^2-\psi_0\right)^{2p^s} = 2\rho u\left(x^2-\psi_0\right)^{p^s}.$$

$\square$

Lemma 4.3. *Let $z(x) \in \mathcal{R}_\lambda$. We can express it uniquely as:*

$$z(x) = \sum_{l=0}^{2p^s-1} (\sigma_{0l} + \varrho_{0l}x)(x^2-\psi_0)^l + u\sum_{l=0}^{2p^s-1} (\sigma_{1l} + \varrho_{1l}x)(x^2-\psi_0)^l, \tag{4.2}$$

where $\sigma_{0l}, \varrho_{0l}, \sigma_{1l}, \varrho_{1l} \in \mathbb{F}_{p^m}$.

Proof. In $\mathcal{S}_{\psi+\eta v}$, $\Phi(z(x))$ can be viewed as a polynomial over T_v of degree up to $2p^s - 1$. Thus $\Phi(z(x))$ can be uniquely expressed as

$$\begin{aligned}
\Phi(z(x)) &= \sum_{l=0}^{p^s-1} (\sigma_{0l} + \varrho_{0l}x)\left(x^2-\psi_0\right)^l + v\sum_{l=0}^{p^s-1} (\sigma'_{0l} + \varrho'_{0l}x)\left(x^2-\psi_0\right)^l \\
&= \sum_{l=0}^{p^s-1} (\sigma_{0l} + \varrho_{0l}x)\left(x^2-\psi_0\right)^l + \eta^{-1}\left(x^2-\psi_0\right)^{p^s}\sum_{l=0}^{p^s-1} (\sigma'_{0l} + \varrho'_{0l}x)\left(x^2-\psi_0\right)^l \\
&= \sum_{l=0}^{2p^s-1} (\sigma_{0l} + \varrho_{0l}x)\left(x^2-\psi_0\right)^l.
\end{aligned}$$

where for any $p^s \leq l \leq 2p^s - 1$, $\sigma_{0l} + \varrho_{0l}x = \eta^{-1}\left(\sigma'_{0,l-p^s} + \varrho'_{0,l-p^s}x\right)$. Then, in $\mathcal{R}_\lambda$,

$$z(x) = \sum_{l=0}^{2p^s-1} (\sigma_{0l} + \varrho_{0l}x)\left(x^2-\psi_0\right)^l + uy(x),$$

where $y(x) \in \mathcal{R}_\lambda$. Applying a similar process to $y(x)$, we obtain

$$y(x) = \sum_{l=0}^{2p^s-1} (\sigma_{1l} + \varrho_{1l}x)(x^2-\psi_0)^l + uw(x).$$

Thus, in $\mathcal{R}_\lambda$, we have

$$z(x) = \sum_{l=0}^{2p^s-1} (\sigma_{0l} + \varrho_{0l}x)(x^2-\psi_0)^l + u\sum_{l=0}^{2p^s-1} (\sigma_{1l} + \varrho_{1l}x)(x^2-\psi_0)^l.$$

$\square$

Lemma 4.4. *Any nonzero polynomial $\sigma + \varrho x \in \mathbb{F}_{p^m}[x]$ is invertible in $\mathcal{R}_\lambda$.*

Proof. If $\varrho = 0$, then $\sigma + \varrho x = \sigma \in \mathbb{F}^*_{p^m}$ is invertible. Now, suppose $\varrho \neq 0$. In the ring $\mathcal{R}_\lambda$, we have

$$(x+\varrho^{-1}\sigma)^{p^s}(x-\varrho^{-1}\sigma)^{p^s} = \left(x^2-(\varrho^{-1}\sigma)^2\right)^{p^s} = x^{2p^s}-(\varrho^{-1}\sigma)^{2p^s} = \left(\psi-(\varrho^{-1}\sigma)^{2p^s}\right)+\rho u+\eta v+\tau uv.$$

Because ψ is not a square (see Proposition 2.4), we have $\psi \neq (\varrho^{-1}\sigma)^{2p^s}$. Thus, $\psi - (\varrho^{-1}\sigma)^{2p^s} \in \mathbb{F}^*_{p^m}$.

On the other hand, since $\rho u + \eta v + \tau uv$ is nilpotent, the expression $(x + \varrho^{-1}\sigma)^{p^s}(x - \varrho^{-1}\sigma)^{p^s}$ is invertible. Consequently, $\sigma + \varrho x$ is also invertible.

$\square$

Theorem 4.5. *The ring $\mathcal{R}_\lambda$ is a local ring with the maximal ideal $\langle x^2-\psi_0, u\rangle$, but it is not a chain ring.*

Proof. First, it is evident that both u and $x^2-\psi_0$ are nilpotent elements in $\mathcal{R}_\lambda$. Consider a polynomial $z(x)$ in $\mathcal{R}_\lambda$. By Lemma 4.3, $z(x)$ can be uniquely expressed as:

$$z(x) = (\sigma_{00}+\varrho_{00}x) + \sum_{l=1}^{2p^s-1} (\sigma_{0l}+\varrho_{0l}x)\,(x^2-\psi_0)^l + u\sum_{l=0}^{2p^s-1} (\sigma_{1l}+\varrho_{1l}x)\,(x^2-\psi_0)^l,$$

where $\sigma_{0l},\varrho_{0l},\sigma_{1l},\varrho_{1l}\in\mathbb{F}_{p^m}$. According to Lemma 4.4, the polynomial $z(x)$ is non-invertible if $\sigma_{00}+\varrho_{00}x=0$, which implies that $z(x)\in\langle x^2-\psi_0,u\rangle$. Consequently, $\langle x^2-\psi_0,u\rangle$ represents the set of all non-invertible elements in $\mathcal{R}_\lambda$, thereby establishing that $\mathcal{R}_\lambda$ is a local ring with maximal ideal $\langle x^2-\psi_0,u\rangle$.

Next, we demonstrate that $u\notin\langle x^2-\psi_0\rangle$ in $\mathcal{R}_\lambda$. Suppose, for contradiction, that $u\in\langle x^2-\psi_0\rangle$. Then there exist polynomials $l(x)$ and $k(x)$ in $R_{u,v}$ such that

$$u = (x^2-\psi_0)k(x) + l(x)\left(x^{2p^s}-(\psi+\rho u+\eta v+\tau uv)\right).$$

Substituting $x=\psi_0$, yields

$$u = -l(\psi_0)\,(\rho u+\eta v+\tau uv)\,,$$

which leads to a contradiction because u cannot be expressed as a linear combination of v in $R_{u,v}[x]$. Hence, $u\notin\langle x^2-\psi_0\rangle$.

Furthermore, $x^2-\psi_0\notin\langle u\rangle$ because $(x^2-\psi_0)^2\neq 0$ in $\mathcal{R}_\lambda$. Therefore, $\mathcal{R}_\lambda$ cannot be a chain ring.

□

Lemma 4.6. *Let C be an ideal of the ring $\mathcal{R}_\lambda$. Then*

$$C = \langle (x^2-\psi_0)^\alpha + uz(x)\rangle + uD, \tag{4.3}$$

where $0\le\alpha\le 2p^s$, $\Phi(C)=\langle (x^2-\psi_0)^\alpha\rangle$, and $z(x)$ is a polynomial such that $(x^2-\psi_0)^\alpha+uz(x)\in C$. Additionally, $D=\{a(x)\in\mathcal{R}_\lambda \mid ua(x)\in C\}$.

Proof. Since $\Phi(C)$ is an ideal of $\mathcal{S}_{\psi+\eta v}$, by Theorem 4.1, there exists an integer $0\le\alpha\le 2p^s$ for which $\Phi(C)=\langle (x^2-\psi_0)^\alpha\rangle$. Given that Φ is surjective, we can find a polynomial $z(x)\in\mathcal{R}_\lambda$ with $(x^2-\psi_0)^\alpha+uz(x)\in C$.

For any polynomial $f(x)\in C$, there exists a polynomial $g(x)\in\mathcal{S}_{\psi+\eta v}$ satisfying $\Phi(f(x))=g(x)(x^2-\psi_0)^\alpha$. Let $h(x)\in\mathcal{R}_\lambda$ be such that $\Phi(h(x))=g(x)$. Thus:

$$\Phi(f(x)) = \Phi(h(x))\Phi((x^2-\psi_0)^\alpha+uz(x)).$$

Then,

$$f(x)-h(x)\left((x^2-\psi_0)^\alpha+uz(x)\right)\in\ker(\Phi)\cap C.$$

Therefore,

$$C\subseteq\langle (x^2-\psi_0)^\alpha+uz(x)\rangle+\ker(\Phi)\cap C.$$

Consequently,

$$\begin{aligned} C &= \langle (x^2-\psi_0)^\alpha + uz(x)\rangle + \ker(\Phi)\cap C \\ &= \langle (x^2-\psi_0)^\alpha + uz(x)\rangle + uD, \end{aligned}$$

where $D = \ker(\Phi)\cap C$.

□

Theorem 4.7. *λ-constacyclic codes of length $2p^s$ over $R_{u,v}$, i.e., ideals of the ring $\mathcal{R}_\lambda$, can be classified into the following types:*

i) Type 1: $\langle 0\rangle, \langle 1\rangle$.

ii) Type 2: $\langle u(x^2-\psi_0)^\alpha\rangle$, where $0 \le \alpha \le 2p^s-1$.

iii) Type 3: $\left\langle (x^2-\psi_0)^\alpha + u(x^2-\psi_0)^\beta t(x)\right\rangle$, where $1\le \alpha \le 2p^s-1$, $0 \le \beta < \Upsilon$, and $t(x)=0$ or $t(x)$ is a unit of the form

$$\sum_{l=0}^{2p^s-1} (\sigma_l + \varrho_l x)(x^2-\psi_0)^l,$$

with $\sigma_l, \varrho_l \in \mathbb{F}_{p^m}$ and $\sigma_0 + \varrho_0 x \neq 0$.

iv) Type 4: $\left\langle (x^2-\psi_0)^\alpha + u(x^2-\psi_0)^\beta t(x), u(x^2-\psi_0)^\delta\right\rangle$, where $1 \le \alpha \le 2p^s-1$, $0\le \beta<\delta<\Upsilon$, and $t(x)$ is as in Type 3. Here,

$$\Upsilon = \min\left\{w \mid u(x^2-\psi_0)^w \in \left\langle (x^2-\psi_0)^\alpha + u(x^2-\psi_0)^\beta t(x)\right\rangle\right\}.$$

Proof. The ideals of type 1 correspond to the trivial ideals. Let C be a non-trivial ideal of $\mathcal{R}_\lambda$.

- If $\Phi(C)=0$. Then, by Lemma 4.6 we can write $C = uD$, where $D = \{a(x)\in\mathcal{R}_\lambda \mid ua(x)\in C\}$. Furthermore, since $\Phi(D)$ is an ideal of $\mathcal{S}_{\psi+\eta v}$, we have $\Phi(D) = \langle (x^2-\psi_0)^\alpha\rangle$ with $0\le\alpha\le 2p^s-1$. Therefore, by applying Lemma 4.6 again, we obtain $D = \langle (x^2-\psi_0)^\alpha + uz(x)\rangle + uE$ with $E = \{a(x)\in\mathcal{R}_\lambda \mid ua(x)\in D\}$ and $z(x)\in\mathcal{R}_\lambda$. Hence, we can conclude that $C = \langle u(x^2-\psi_0)^\alpha\rangle$. This implies that C is of type 2.
- If $\Phi(C)\neq 0$. Since $\Phi(C)$ is a non-trivial ideal of $\mathcal{S}_{\psi+\eta v}$. Thus, we have $\Phi(D) = \langle (x^2-\psi_0)^\alpha\rangle$ with $1\le\alpha\le 2p^s-1$. By applying Lemma 4.6, we can write $C = \langle (x^2-\psi_0)^\alpha + uz(x)\rangle + uD$, where $z(x)$ is an element of $\mathcal{R}_\lambda$ and $D = \{a(x)\in\mathcal{R}_\lambda \mid ua(x)\in C\}$. Since $uD\subseteq\langle u\rangle$, then $uD = \left\langle u(x^2-\psi_0)^\delta\right\rangle$, where $0\le\delta\le 2p^s$. Next considering the expression of $z(x)$ given by Lemma 4.3, we have

$$uz(x) = u\sum_{l=0}^{2p^s-1}(\sigma_{0l}+\varrho_{0l}x)(x^2-\psi_0)^l = u(x^2-\psi_0)^\beta t(x),$$

where $t(x)=0$ or $t(x)$ is a unit of the form $\sum_{l=0}^{2p^s-1}(\sigma_l+\varrho_l x)(x^2-\psi_0)^l$, with $\sigma_l,\varrho_l\in\mathbb{F}_{p^m}$ and $\sigma_0+\varrho_0 x\neq 0$ is a nonzero polynomial. Consequently, we can write

$$C = \left\langle (x^2-\psi_0)^\alpha + u(x^2-\psi_0)^\beta t(x), u(x^2-\psi_0)^\delta\right\rangle.$$

Let $\Upsilon = \min\left\{w \mid u(x^2-\psi_0)^w \in \left\langle (x^2-\psi_0)^\alpha + u(x^2-\psi_0)^\beta t(x)\right\rangle\right\}$.

– If $\delta \geq \Upsilon$, then $C = \left\langle (x^2-\psi_0)^\alpha + u(x^2-\psi_0)^\beta t(x) \right\rangle$. This implies that C is of type 3.
– If $\delta < \Upsilon$, then $C = \left\langle (x^2-\psi_0)^\alpha + u(x^2-\psi_0)^\beta t(x), u(x^2-\psi_0)^\delta \right\rangle$. This implies that C is of type 4.

□

The value of Υ is crucial in the classification of λ-constacyclic codes of length $2p^s$ over $R_{u,v}$. Therefore, we propose to compute it in the following theorem.

Theorem 4.8. *Let Υ be defined as follows:*

$$\Upsilon = \min\left\{w \mid u(x^2-\psi_0)^w \in \left\langle (x^2-\psi_0)^\alpha + u(x^2-\psi_0)^\beta t(x) \right\rangle\right\}.$$

Then,

$$\Upsilon = \begin{cases} \alpha, & \text{if } z(x) = 0, \\ \min\{\alpha, \varepsilon\}, & \text{if } z(x) \neq 0, \end{cases}$$

with

$$\varepsilon = \max\left\{i \mid (x^2-\psi_0)^i \text{ divides } (x^2-\psi_0)^{2p^s+\beta-\alpha} t(x) + 2\rho(x^2-\psi_0)^{p^s}\right\},$$

and

$$(x^2-\psi_0)^{2p^s+\beta-\alpha} t(x) + 2\rho(x^2-\psi_0)^{p^s} = (x^2-\psi_0)^\varepsilon z(x),$$

where $z(x)$ is either zero or a unit of the form:

$$z(x) = \sum_{l=0}^{2p^s-1} c_l(x)(x^2-\psi_0)^l,$$

with $c_l(x)$ being linear polynomials over $\mathbb{F}_{p^m}$ and $c_0(x) \neq 0$.

Proof. Consider $u(x^2-\psi_0)^w \in \langle (x^2-\psi_0)^\alpha + u(x^2-\psi_0)^\beta t(x)\rangle$. This implies

$$u(x^2-\psi_0)^w = f(x)\left((x^2-\psi_0)^\alpha + u(x^2-\psi_0)^\beta t(x)\right),$$

for some $f(x) = \sum\limits_{l=0}^{2p^s-1} a_l(x)(x^2-\psi_0)^l + u\sum\limits_{l=0}^{2p^s-1} b_l(x)(x^2-\psi_0)^l \in \mathcal{R}_\lambda$. Let

$$f_{00}(x) = \sum_{l=0}^{2p^s-\alpha-1} a_l(x)(x^2-\psi_0)^l, \quad f_{01}(x) = \sum_{l=2p^s-\alpha}^{2p^s-1} a_l(x)(x^2-\psi_0)^{l-2p^s+\alpha},$$

and

$$f_1(x) = \sum_{l=0}^{2p^s-1} b_l(x)(x^2-\psi_0)^l.$$

Here, $a_l(x)$ and $b_l(x)$ are linear polynomials over $\mathbb{F}_{p^m}$. Thus,

$$f(x) = f_{00}(x) + (x^2-\psi_0)^{2p^s-\alpha} f_{01}(x) + u f_1(x).$$

Then,

$$\begin{array}{rcl} u(x^2-\psi_0)^w & = & (x^2-\psi_0)^\alpha f_{00}(x)+(x^2-\psi_0)^{2p^s}f_{01}(x) \\ & + & u\left((x^2-\psi_0)^\beta t(x)f_{00}(x)+(x^2-\psi_0)^\alpha f_1(x)+(x^2-\psi_0)^{2p^s+\beta-\alpha}t(x)f_{01}(x)\right) \\ & = & (x^2-\psi_0)^\alpha f_{00}(x)+u\left(2\rho(x^2-\psi_0)^{p^s}f_{01}(x)\right. \\ & + & \left.(x^2-\psi_0)^\beta t(x)f_{00}(x)+(x^2-\psi_0)^\alpha f_1(x)+(x^2-\psi_0)^{2p^s+\beta-\alpha}t(x)f_{01}(x)\right). \end{array}$$

The last equality holds by utilizing Lemma 4.2. Consequently,

$$(x^2-\psi_0)^\alpha f_{00}(x)=(x^2-\psi_0)^\alpha\sum_{l=0}^{2p^s-\alpha-1}a_l(x)(x^2-\psi_0)^l\in\langle u\rangle.$$

By applying Lemma 4.2 again, it follows that $f_{00}(x)=0$. Thus,

$$\begin{array}{rcl} u(x^2-\psi_0)^w & = & u\left(2\rho(x^2-\psi_0)^{p^s}f_{01}(x)+(x^2-\psi_0)^\alpha f_1(x)+(x^2-\psi_0)^{2p^s+\beta-\alpha}t(x)f_{01}(x)\right) \\ & = & u\left((x^2-\psi_0)^\alpha f_1(x)+(x^2-\psi_0)^\varepsilon z(x)f_{01}(x)\right). \end{array}$$

Now, we consider the following cases:

- If $z(x)=0$, then $\Upsilon\geq\alpha$. Since we have

$$u(x^2-\psi_0)^\alpha=u\left((x^2-\psi_0)^\alpha+u(x^2-\psi_0)^\beta t(x)\right)\in\langle(x^2-\psi_0)^\alpha+u(x^2-\psi_0)^\beta t(x)\rangle,$$

  it follows that $\Upsilon=\alpha$.
- If $z(x)\neq 0$, then $\Upsilon\geq\min\{\alpha,\varepsilon\}$. Conversely, we have

$$u(x^2-\psi_0)^\alpha=u\left((x^2-\psi_0)^\alpha+u(x^2-\psi_0)^\beta t(x)\right)\in\langle(x^2-\psi_0)^\alpha+u(x^2-\psi_0)^\beta t(x)\rangle,$$

  and

$$u(x^2-\psi_0)^\varepsilon=z(x)^{-1}(x^2-\psi_0)^{2p^s-\alpha}\left((x^2-\psi_0)^\alpha+u(x^2-\psi_0)^\beta t(x)\right)\in\langle(x^2-\psi_0)^\alpha+u(x^2-\psi_0)^\beta t(x)\rangle.$$

  Therefore, $\Upsilon=\min\{\alpha,\varepsilon\}$.

□

Remark 4.9. In the case where $\rho=0$, then

$$\Upsilon=\begin{cases}\alpha, & \text{if } z(x)=0,\\ \min\{\alpha,2p^s+\beta-\alpha\}, & \text{if } z(x)\neq 0.\end{cases}$$

We will now determine the count of codewords within each λ-constacyclic code of length $2p^s$ over $R_{u,v}$, denoted as C. To accomplish this, we introduce two concepts: the residue and torsion of C:

$$\begin{array}{l}\mathrm{Res}(C)=\Phi(C),\\ \mathrm{Tor}(C)=\{c(x)\in\mathcal{S}_{\psi+\eta v}\mid uc(x)\in C\}.\end{array}$$

It is clear that $\mathrm{Res}(C)$ and $\mathrm{Tor}(C)$ are ideals of $\mathcal{S}_{\psi+\eta v}$. Therefore, according to Theorem 4.1, they are of the form $\langle(x^2-\psi_0)^i\rangle$, where $0\leq i\leq 2p^s$. On the other hand, let's consider the ring homomorphism

$$\begin{array}{rccc} T: & C & \longrightarrow & \Phi(C) \\ & z(x) & \longmapsto & \Phi(z(x)) \end{array}.$$

We have $\operatorname{Im} T = \operatorname{Res}(C)$ and $\ker T \cong u\operatorname{Tor}(C)$, so the first isomorphism theorem implies

$$\mid C \mid = \mid\mid \operatorname{Tor}(C) \mid \operatorname{Res}(C) \mid . \qquad (4.4)$$

The following lemma, which can be easily proven, provides the expressions for $\operatorname{Res}(C)$ and $\operatorname{Tor}(C)$ for any ideal C in $\mathcal{R}_\lambda$.

Lemma 4.10. *With the notation of Theorem 4.7 :*

i) If $C = \langle 0\rangle$, then $\operatorname{Tor}(C) = \operatorname{Res}(C) = \langle 0\rangle$.
ii) If $C = \langle 1\rangle$, then $\operatorname{Tor}(C) = \operatorname{Res}(C) = \langle 1\rangle$.
iii) If $C = \langle u(x^2-\psi_0)^\alpha\rangle$ is of type 2, then $\operatorname{Tor}(C) = \langle (x^2-\psi_0)^\alpha\rangle$ and $\operatorname{Res}(C) = \langle 0\rangle$.
iv) If $C = \langle (x^2-\psi_0)^\alpha + u(x^2-\psi_0)^\beta t(x)\rangle$ is of type 3, then $\operatorname{Tor}(C) = \langle (x^2-\psi_0)^\Upsilon\rangle$ and $\operatorname{Res}(C) = \langle (x^2-\psi_0)^\alpha\rangle$.
v) If $C = \langle (x^2-\psi_0)^\alpha + u(x^2-\psi_0)^\beta t(x), u(x^2-\psi_0)^\delta\rangle$ is of type 4, then $\operatorname{Tor}(C) = \langle (x^2-\psi_0)^\delta\rangle$ and $\operatorname{Res}(C) = \langle (x^2-\psi_0)^\alpha\rangle$.

By determining $\operatorname{Res}(C)$ and $\operatorname{Tor}(C)$ in each case, we can calculate the cardinalities of all ideals in $\mathcal{R}_\lambda$. This can be accomplished by applying Equations (4.4) and (4.1).

5. Dual codes of λ-constacyclic codes over $R_{u,v}$

In this section, we focus on the dual codes of λ-constacyclic codes of length $2p^s$ over the ring $R_{u,v}$ when λ is not a square.

Lemma 5.1. *Let C be a λ-constacyclic code of length $2p^s$ over $R_{u,v}$, and let $0 \le a, b \le 2p^s$ such that $\operatorname{Res}(C) = \langle (x^2-\psi_0)^a\rangle$ and $\operatorname{Tor}(C) = \langle (x^2-\psi_0)^b\rangle$. Then,*

$$\operatorname{Res}(\mathcal{A}(C)) = \langle (x^2-\psi_0)^{2p^s-b}\rangle \text{ and } \operatorname{Tor}(\mathcal{A}(C)) = \langle (x^2-\psi_0)^{2p^s-a}\rangle.$$

Proof. Let $\operatorname{Res}(\mathcal{A}(C)) = \langle (x^2-\psi_0)^{a'}\rangle$ and $\operatorname{Tor}(\mathcal{A}(C)) = \langle (x^2-\psi_0)^{b'}\rangle$, where $0 \le a', b' \le 2p^s$. Then, $u(x^2-\psi_0)^b \in C$ and $u(x^2-\psi_0)^{b'} \in \mathcal{A}(C)$. Moreover, there exist polynomials $g(x)$ and $f(x)$ in $\mathcal{R}_\lambda$ such that $(x^2-\psi_0)^a + ug(x) \in C$ and $(x^2-\psi_0)^{a'} + uf(x) \in \mathcal{A}(C)$. The following equations hold:

$$\begin{cases} 0 &= u(x^2-\psi_0)^b((x^2-\psi_0)^{a'} + uf(x)) = u(x^2-\psi_0)^{b+a'}, \\ 0 &= u(x^2-\psi_0)^{b'}((x^2-\psi_0)^a + ug(x)) = u(x^2-\psi_0)^{b'+a}. \end{cases}$$

Thus, In light of lemma 4.2 we necessarily have $a' \ge 2p^s - b$ and $b' \ge 2p^s - a$. According to Proposition 2.2, $|C||\mathcal{A}(C)| = |\mathcal{R}_\lambda| = p^{8mp^s}$. From Equations (4.1) and (4.4), we deduce that $b' = 2p^s - a$ and $a' = 2p^s - b$. $\square$

Lemma 5.2. *With the previous notation, we have*

$$\mathcal{A}(C) = \langle (x^2-\psi_0)^{2p^s-b} + uf(x), u(x^2-\psi_0)^{2p^s-a}\rangle.$$

Proof. Firstly, it is clear that $u(x^2-\psi_0)^{2p^s-a} \in \mathcal{A}(C)$ and $(x^2-\psi_0)^{2p^s-b} + uf(x) \in \mathcal{A}(C)$. Now, let $c(x) \in \mathcal{A}(C)$. Then $\Phi(c(x)) \in \operatorname{Res}(\mathcal{A}(C))$, which implies that there exists $c_0(x) \in \mathcal{S}_{\psi+\eta v}$ such that

$$\Phi(c(x)) = c_0(x)(x^2-\psi_0)^{2p^s-b} = \Phi\left(c_0(x)\left((x^2-\psi_0)^{2p^s-b} + uf(x)\right)\right).$$

Therefore, we have

$$c(x) - c_0(x)\left((x^2-\psi_0)^{2p^s-b} + uf(x)\right) \in \ker \Phi.$$

This implies that

$$c(x) - c_0(x)\left((x^2-\psi_0)^{2p^s-b} + uf(x)\right) = uc_1(x) \in \mathcal{A}(C),$$

where $c_1(x) \in \mathcal{S}_{\psi+\eta v}$. Then $c_1(x) \in \mathrm{Tor}(\mathcal{A}(C)) = \langle (x^2-\psi_0)^{p^s-a}\rangle$. Then

$$c(x) \in \langle (x^2-\psi_0)^{2p^s-b} + uf(x), u(x^2-\psi_0)^{2p^s-a}\rangle.$$

It follows that

$$\mathcal{A}(C) = \langle (x^2-\psi_0)^{2p^s-b} + uf(x), u(x^2-\psi_0)^{2p^s-a}\rangle.$$

□

We will now proceed to determine the annihilator of each type of ideal in Theorem 4.7. For ideals of type 1, the annihilators are straightforward to determine. If $C = \langle 0\rangle$, then $\mathcal{A}(C) = \langle 1\rangle$. If $C = \langle 1\rangle$, then $\mathcal{A}(C) = \langle 0\rangle$.

For other types of ideals, we need to consider two integers a and b such that $\mathrm{Res}(C) = \langle (x^2-\psi_0)^a\rangle$ and $\mathrm{Tor}(C) = \langle (x^2-\psi_0)^b\rangle$. These integers are determined using Lemma 4.10. Next, we find a polynomial $f(x)$ such that $(x^2-\psi_0)^{2p^s-b} + uf(x) \in \mathcal{A}(C)$. Finally, we obtain $\mathcal{A}(C)$ using Lemma 5.2.

Proposition 5.3. *If $C = \langle u(x^2-\psi_0)^\alpha\rangle$ is an ideal of type 2, then $\mathcal{A}(C) = \langle (x^2-\psi_0)^{2p^s-\alpha}, u\rangle$.*

Proof. It is clear that $(x^2-\psi_0)^{2p^s-\alpha} \in \mathcal{A}(C)$. Therefore, we have $\mathcal{A}(C) = \langle (x^2-\psi_0)^{2p^s-\alpha}, u\rangle$.

□

We recall that

$$\varepsilon = \max\left\{i \mid (x^2-\psi_0)^i \text{ divides } (x^2-\psi_0)^{2p^s+\beta-\alpha}t(x) + 2\rho(x^2-\psi_0)^{p^s}\right\},$$

and $z(x)$ is either zero or a unit of the form

$$z(x) = \sum_{i=0}^{2p^s-1} c_i(x)(x^2-\psi_0)^i,$$

where $c_i(x)$ are linear polynomials over $\mathbb{F}_{p^m}$ with $c_0(x) \neq 0$, and

$$(x^2-\psi_0)^{2p^s+\beta-\alpha}t(x) + 2\rho(x^2-\psi_0)^{p^s} = (x^2-\psi_0)^\varepsilon z(x).$$

Proposition 5.4. *If $C = \langle (x^2-\psi_0)^\alpha + u(x^2-\psi_0)^\beta t(x)\rangle$ is an ideal of type 3, then:*

$$\mathcal{A}(C) = \begin{cases} \left\langle (x^2-\psi_0)^{2p^s-\alpha}\right\rangle, & \text{if } z(x) = 0, \\ \langle (x^2-\psi_0)^{2p^s-\varepsilon} - uz(x), u(x^2-\psi_0)^{2p^s-\alpha}\rangle, & \text{if } z(x) \neq 0 \text{ and } \alpha > \varepsilon, \\ \langle (x^2-\psi_0)^{2p^s-\alpha} - u(x^2-\psi_0)^{\varepsilon-\alpha}z(x)\rangle, & \text{if } z(x) \neq 0 \text{ and } \alpha \leq \varepsilon. \end{cases}$$

Proof. We will search for a polynomial $f(x) \in \mathcal{S}_{\psi+\eta v}$ that satisfies $(x^2-\psi_0)^{2p^s-\Upsilon} + uf(x) \in \mathcal{A}(C)$, i.e.,

$$\begin{aligned} 0 &= (x^2-\psi_0)^{2p^s-\Upsilon+\alpha} + u\left((x^2-\psi_0)^{2p^s-\Upsilon+\beta}t(x) + (x^2-\psi_0)^{\alpha}f(x)\right) \\ &= (x^2-\psi_0)^{\alpha-\Upsilon}(x^2-\psi_0)^{2p^s} + u\left((x^2-\psi_0)^{2p^s-\Upsilon+\beta}t(x) + (x^2-\psi_0)^{\alpha}f(x)\right) \\ &= u\left(2\rho(x^2-\psi_0)^{p^s+\alpha-\Upsilon} + (x^2-\psi_0)^{2p^s-\Upsilon+\beta}t(x) + (x^2-\psi_0)^{\alpha}f(x)\right) \\ &= u\left((x^2-\psi_0)^{\alpha-\Upsilon+\varepsilon}z(x) + (x^2-\psi_0)^{\alpha}f(x)\right). \end{aligned} \tag{5.1}$$

We consider two cases:

- If $z(x) = 0$, then $\Upsilon = \alpha$, and the equation (5.1) is equivalent to $0 = u(x^2-\psi_0)^{\alpha}f(x)$. In this case, we choose $f(x) = 0$, and we have
$$\mathcal{A}(C) = \langle (x^2-\psi_0)^{2p^s-\alpha}, u(x^2-\psi_0)^{2p^s-\alpha}\rangle = \langle (x^2-\psi_0)^{2p^s-\alpha}\rangle.$$
- If $z(x) \neq 0$, in this case, we choose $f(x) = -(x^2-\psi_0)^{\varepsilon-\Upsilon}z(x)$, and then
$$\mathcal{A}(C) = \langle (x^2-\psi_0)^{2p^s-\Upsilon} - u(x^2-\psi_0)^{\varepsilon-\Upsilon}z(x), u(x^2-\psi_0)^{2p^s-\alpha}\rangle.$$
More precisely,
  - If $\varepsilon < \alpha$, then $\Upsilon = \varepsilon$, and
$$\mathcal{A}(C) = \langle (x^2-\psi_0)^{2p^s-\varepsilon} - uz(x), u(x^2-\psi_0)^{2p^s-\alpha}\rangle.$$
  - If $\varepsilon \geq \alpha$, then $\Upsilon = \alpha$, and

$$\mathcal{A}(C) = \langle (x^2-\psi_0)^{2p^s-\alpha} - u(x^2-\psi_0)^{\varepsilon-\alpha}z(x), u(x^2-\psi_0)^{2p^s-\alpha}\rangle = \langle (x^2-\psi_0)^{2p^s-\alpha} - u(x^2-\psi_0)^{\varepsilon-\alpha}z(x)\rangle.$$

□

Proposition 5.5. *If $C = \langle (x^2-\psi_0)^{\alpha} + u(x^2-\psi_0)^{\beta}t(x), u(x^2-\psi_0)^{\delta}\rangle$, an ideal of type 4, then:*

$$\mathcal{A}(C) = \begin{cases} \left\langle (x^2-\psi_0)^{2p^s-\delta}, u(x^2-\psi_0)^{2p^s-\alpha}\right\rangle, & \text{if } z(x) = 0, \\ \left\langle (x^2-\psi_0)^{2p^s-\delta} - u(x^2-\psi_0)^{\varepsilon-\delta}z(x), u(x^2-\psi_0)^{2p^s-\alpha}\right\rangle, & \text{if } z(x) \neq 0. \end{cases}$$

Proof. It is sufficient to find a polynomial $f(x) \in \mathcal{S}_{\psi+\eta v}$ such that $(x^2-\psi_0)^{2p^s-\delta} + uf(x) \in \mathcal{A}(C)$. This can be expressed as follows:

$$\begin{aligned} 0 &= (x^2-\psi_0)^{2p^s-\delta+\alpha} + u\left((x^2-\psi_0)^{2p^s-\delta+\beta}t(x) + (x^2-\psi_0)^{\alpha}f(x)\right) \\ &= (x^2-\psi_0)^{\alpha-\delta}(x^2-\psi_0)^{2p^s} + u\left((x^2-\psi_0)^{2p^s-\delta+\beta}t(x) + (x^2-\psi_0)^{\alpha}f(x)\right) \\ &= u\left(2\rho(x^2-\psi_0)^{p^s+\alpha-\delta} + (x^2-\psi_0)^{2p^s-\delta+\beta}t(x) + (x^2-\psi_0)^{\alpha}f(x)\right) \\ &= u\left((x^2-\psi_0)^{\alpha-\delta+\varepsilon}z(x) + (x^2-\psi_0)^{\alpha}f(x)\right). \end{aligned} \tag{5.2}$$

Then, we choose $f(x) = -(x^2-\psi_0)^{\varepsilon-\delta}z(x)$ if $z(x) \neq 0$ and $f(x) = 0$ if $z(x) = 0$, resulting in:

- If $z(x) = 0$,
$$\mathcal{A}(C) = \left\langle (x^2-\psi_0)^{2p^s-\delta}, u(x^2-\psi_0)^{2p^s-\alpha}\right\rangle.$$
- If $z(x) \neq 0$,
$$\mathcal{A}(C) = \left\langle (x^2-\psi_0)^{2p^s-\delta} - u(x^2-\psi_0)^{\varepsilon-\delta}z(x), u(x^2-\psi_0)^{2p^s-\alpha}\right\rangle.$$

□

Let us now establish $C^{\perp} = \mathcal{A}(C)^{*}$ for any ideal in $\mathcal{R}_{\lambda}$. If C is an ideal of type 1, then $C^{\perp} = \langle 0 \rangle$ when $C = \langle 1 \rangle$, and $C^{\perp} = \langle 1 \rangle$ when $C = \langle 0 \rangle$. Let's investigate the other types. But before we proceed, let's recall the following lemma .

Lemma 5.6. [6] *Let $D = \langle t(x), uy(x) \rangle$ be an ideal of $\mathcal{R}_{\lambda}$. Then*

$$D^{*} = \langle t^{*}(x), uy^{*}(x) \rangle .$$

We use the following notation:

$$\vartheta = \max \left\{ i \mid (1-\psi_0 x^2)^i \text{ divides } x^{2(2p^s-\varepsilon)} z(x^{-1}) \right\},$$

then $x^{2(2p^s-\varepsilon)} z(x^{-1}) = (1-\psi_0 x^2)^{\vartheta} e(x)$, where $e(x)$ is either a unit or zero.

Corollary 5.7. *If $C = \langle u(x^2-\psi_0)^{\alpha} \rangle$ is an ideal of type 2, then $C^{\perp} = \langle (1-\psi_0 x^2)^{2p^s-\alpha}, u \rangle$.*

Corollary 5.8. *If $C = \langle (x^2-\psi_0)^{\alpha} + u(x^2-\psi_0)^{\beta} t(x) \rangle$ is an ideal of type 3, then:*

$$C^{\perp} = \begin{cases} \left\langle (1-\psi_0 x^2)^{2p^s-\alpha} \right\rangle, & \text{if } z(x)=0, \\ \langle (1-\psi_0 x^2)^{2p^s-\varepsilon} - u(1-\psi_0 x^2)^{\vartheta} e(x), u(1-\psi_0 x^2)^{2p^s-\alpha} \rangle, & \text{if } z(x) \neq 0 \text{ and } \alpha > \varepsilon, \\ \langle (1-\psi_0 x^2)^{2p^s-\alpha} - u(1-\psi_0 x^2)^{\varepsilon-\alpha+\vartheta} e(x) \rangle, & \text{if } z(x) \neq 0 \text{ and } \alpha \leq \varepsilon. \end{cases}$$

Proof. The result is evident in the case where $z(x)=0$. Now, suppose $z(x) \neq 0$.

- If $\alpha > \varepsilon$, then

$$\begin{aligned} C^{\perp} &= \langle (1-\psi_0 x^2)^{2p^s-\varepsilon} - ux^{2(2p^s-\varepsilon)} z(x^{-1}), u(1-\psi_0 x^2)^{2p^s-\alpha} \rangle \\ &= \langle (1-\psi_0 x^2)^{2p^s-\varepsilon} - u(1-\psi_0 x^2)^{\vartheta} e(x), u(1-\psi_0 x^2)^{2p^s-\alpha} \rangle. \end{aligned}$$

- If $\alpha \leq \varepsilon$, then

$$\begin{aligned} C^{\perp} &= \langle (1-\psi_0 x^2)^{2p^s-\alpha} - ux^{2(2p^s-\alpha)} \left((x^{-1})^2 - \psi_0 \right)^{\varepsilon-\alpha} z(x^{-1}) \rangle \\ &= \langle (1-\psi_0 x^2)^{2p^s-\alpha} - ux^{2(2p^s-\varepsilon)} (1-\psi_0 x^2)^{\varepsilon-\alpha} z(x^{-1}) \rangle \\ &= \langle (1-\psi_0 x^2)^{2p^s-\alpha} - u(1-\psi_0 x^2)^{\varepsilon-\alpha+\vartheta} e(x) \rangle. \end{aligned}$$

□

Corollary 5.9. *If $C = \langle (x^2-\psi_0)^{\alpha} + u(x^2-\psi_0)^{\beta} t(x), u(x^2-\psi_0)^{\delta} \rangle$, an ideal of type 4, then:*

$$C^{\perp} = \begin{cases} \left\langle (1-\psi_0 x^2)^{2p^s-\delta}, u(1-\psi_0 x^2)^{2p^s-\alpha} \right\rangle, & \text{if } z(x)=0, \\ \left\langle (1-\psi_0 x^2)^{2p^s-\delta} - u(1-\psi_0 x^2)^{\varepsilon-\delta+\vartheta} e(x), u(1-\psi_0 x^2)^{2p^s-\alpha} \right\rangle, & \text{if } z(x) \neq 0. \end{cases}$$

Proof. The result is immediate in the case where $z(x)=0$. For the case where $z(x) \neq 0$, we have

$$\begin{aligned} C^{\perp} &= \left\langle (1-\psi_0 x^2)^{2p^s-\delta} - ux^{2(2p^s-\delta)} \left((x^{-1})^2 - \psi_0 \right)^{\varepsilon-\delta} z(x^{-1}), u(1-\psi_0 x^2)^{2p^s-\alpha} \right\rangle \\ &= \left\langle (1-\psi_0 x^2)^{2p^s-\delta} - ux^{2(2p^s-\varepsilon)} (1-\psi_0 x^2)^{\varepsilon-\delta} z(x^{-1}), u(1-\psi_0 x^2)^{2p^s-\alpha} \right\rangle \\ &= \left\langle (1-\psi_0 x^2)^{2p^s-\delta} - u(1-\psi_0 x^2)^{\varepsilon-\delta+\vartheta} e(x), u(1-\psi_0 x^2)^{2p^s-\alpha} \right\rangle. \end{aligned}$$

□

References

1. Cao, Y. (2013). On constacyclic codes over finite chain rings. *Finite Fields and Their Applications*, 24, 124–135. https://doi.org/10.1016/j.ffa.2013.07.001
2. Chen, B., Dinh, H. Q., Liu, H., Wang, L. (2016). Constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *Finite Fields and Their Applications*, 37, 108-130. https://doi.org/10.1016/j.ffa.2015.09.006
3. Charkani, M., Kabore, J. (2020). Primitive idempotents and constacyclic codes over finite chain rings. *Gulf Journal of Mathematics*, 8(2), 55–67. https://doi.org/10.56947/gjom.v8i2.434
4. Dinh, H. Q., López-Permouth, S. R. (2004). Cyclic and negacyclic codes over finite chain rings. *IEEE Transactions on Information Theory*, 50(8), 1728-1744. DOI:10.1109/TIT.2004.831789
5. Dinh, H. Q. (2010). Constacyclic codes of length p^ℓ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *Journal of Algebra*, 324(5), 940-950. https://doi.org/10.1016/j.jalgebra.2010.05.027
6. Dinh, H. Q., Wang, L., Zhu, S. (2015). Negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *Finite Fields and Their Applications*, 31, https://doi.org/10.1016/j.ffa.2014.09.003
7. Dinh, H. Q., Kewat, P. K., Kushwaha, S., Yamaka, W. (2020). On constacyclic codes of length p^s over $\mathbb{F}_{p^m}[u,v]/ < u^2, v^2, uv - vu >$. *Discrete Mathematics*, 343(8), 111890. https://doi.org/10.1016/j.disc.2020.111890
8. Dinh, H. Q., Bag, T., Kewat, P. K., Pathak, S., Upadhyay, A. K., Chinnakum, W. (2021). Constacyclic codes of length (p^r, p^s) over mixed alphabets. *Journal of Applied Mathematics and Computing*, 1-26. https://doi.org/10.1007/s12190-021-01508-x
9. Dinh, H. Q., Kewat, P. K., Kushwaha, S., Yamaka, W. (2022). Self-dual constacyclic codes of length 2^s over the ring $\mathbb{F}_{2^m}[u,v]/ < u^2, v^2, uv - vu >$. *Journal of Applied Mathematics and Computing*, 1-29. https://doi.org/10.1007/s12190-021-01526-9
10. Dougherty, S. T., Karadeniz, S., Yildiz, B. (2012). Cyclic codes over R_k. *Designs, Codes and Cryptography*, 63, 113–126. https://doi.org/10.1007/s10623-011-9539-4
11. Huffman, W., Pless, V. (2003). *Fundamentals of Error-Correcting Codes*. Cambridge University Press.
12. Kewat, P., Ghosh, B., Pattanayak, S. (2015). Cyclic codes over the ring $\mathbb{Z}_p[u,v]/\langle u^2, v^2, uv- vu\rangle$. *Finite Fields and Their Applications*, 34, 161–175. https://doi.org/10.1007/s10623-013-9843-2
13. Ndiaye, O., Thiecoumb Gueye, C. (2016). On cyclic codes over $F_{p^k} + vF_{p^k} + v^2F_{p^k} + \ldots + v^kF_{p^k}$. *Gulf Journal of Mathematics*, 4(4). https://doi.org/10.56947/gjom.v4i4.272
14. Shi, M., Alahmadi, A., Sole, P. (2017). Chapter 2 - Rings. In M. Shi, A. Alahmadi, P. Sole (Eds.), *Codes and Rings* (pp. 11–20). Academic Press.
15. Sobhani, R., Molakarimi, M. (2013). Some results on cyclic codes over the ring $R_{2,m}$. *Turkish Journal of Mathematics*, 37(6), 1061–1074. https://doi.org/10.3906/mat-1211-20
16. Sobhani, R. (2015). Complete classification of $(\delta+\alpha u^2)$-constacyclic codes of length p^k over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$. *Finite Fields and Their Applications*, 34, 123-138. https://doi.org/10.1016/j.ffa.2015.01.008
17. Wood, J. A. (1999). Duality for modules over finite rings and applications to coding theory. *American Journal of Mathematics*, 121(3), 555-575. https://doi.org/10.1353/ajm.1999.0024
18. Yildiz, B., Karadeniz, S. (2011). Cyclic codes over R_k. *Designs, Codes and Cryptography*, 58(3), 221–234. https://doi.org/10.1007/s10623-010-9399-3
19. Zhao, W., Tang, X., Gu, Z. (2018). All $\alpha + u\beta$-constacyclic codes of length np^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *Finite Fields and Their Applications*, 50, 1-16. https://doi.org/10.1016/j.ffa.2017.10.006

[1] Ibn Zohr University - Morocco
Email address: youssef.ahendouz@gamil.com

[2] Ibn Zohr University - Morocco
Email address: i.akharraz@uiz.ac.ma