Repeated-root constacyclic codes over the chain ring \( \mathbb{F}_{p^m}[u]/\langle u^3 \rangle \)

Anuradha Sharma* and Tania Sidana

Department of Mathematics, IIIT-Delhi
New Delhi 110020, India

Abstract

Let \( R = \mathbb{F}_{p^m}[u]/\langle u^3 \rangle \) be the finite commutative chain ring with unity, where \( p \) is a prime, \( m \) is a positive integer and \( \mathbb{F}_{p^m} \) is the finite field with \( p^m \) elements. In this paper, we determine all repeated-root constacyclic codes of arbitrary lengths over \( R \), their sizes and their dual codes. As an application, we list some isodual constacyclic codes over \( R \). We also determine Hamming distances, RT distances, and RT weight distributions of some repeated-root constacyclic codes over \( R \).

Keywords: Cyclic codes; Negacyclic codes; Local rings.

1 Introduction

Berlekamp [4] first introduced and studied constacyclic codes over finite fields, which have a rich algebraic structure and are generalizations of cyclic and negacyclic codes. Calderbank et al. [6], Hammons et al. [14] and Nechaev [18] related binary non-linear codes (e.g. Kerdock and Preparata codes) to linear codes over the finite commutative chain ring \( \mathbb{Z}_4 \) of integers modulo 4, with the help of a Gray map. Since then, codes over finite commutative chain rings have received a great deal of attention. However, their algebraic structures are known only in a few cases.

Towards this, Dinh and López-Permouth [12] studied algebraic structures of simple-root cyclic and negacyclic codes of length \( n \) over a finite commutative chain ring \( R \) and their dual codes. In the same work, they determined all negacyclic codes of length \( 2^t \) over the ring \( \mathbb{Z}_{2^m} \) of integers modulo \( 2^m \) and their dual codes, where \( t \geq 1 \) and \( m \geq 2 \) are integers. In a related work, Batoul et al. [3] proved that when \( \lambda \) is an \( n \)th power of a unit in a finite chain ring \( R \), repeated-root \( \lambda \)-constacyclic codes of length \( n \) over \( R \) are equivalent to cyclic codes. Apart from this, many authors [1, 2, 5, 15, 22] investigated algebraic structures of linear and cyclic codes over the finite commutative chain ring \( \mathbb{F}_2[v]/\langle v^2 \rangle \).

To describe the recent work, let \( p \) be a prime, \( s, m \) be positive integers, \( \mathbb{F}_{p^m} \) be the finite field of order \( p^m \), and let \( \mathbb{F}_{p^m}[v]/\langle v^2 \rangle \) be the finite commutative chain ring with unity. Dinh [10] determined all constacyclic codes of length \( p^s \) over \( \mathbb{F}_{p^m}[v]/\langle v^2 \rangle \) and their Hamming distances. Later, Chen et al. [9], Dinh et al. [11] and Liu et al. [10] determined all constacyclic codes of length \( 2p^s \) over the ring \( \mathbb{F}_{p^m}[v]/\langle v^2 \rangle \), where \( p \) is an odd prime. Recently, Sharma and Rani [19] determined all constacyclic codes of length \( 4p^s \) over \( \mathbb{F}_{p^m}[v]/\langle v^2 \rangle \) and their dual codes, where \( p \) is an odd prime and \( s, m \) are positive integers. Using a technique different from that employed in [9,10,11,15,19], Cao et al. [8] determined all \( \alpha \)-constacyclic codes of length \( np^s \) over \( \mathbb{F}_{p^m}[v]/\langle v^2 \rangle \) and their dual codes by writing a canonical form decomposition for each code, where \( \alpha \) is a non-zero element of \( \mathbb{F}_{p^m} \) and \( n \) is a positive integer with \( \gcd(p,n) = 1 \). In a recent work, Zhao et al. [23] determined all \( (\alpha + \beta v) \)-constacyclic codes...
codes of length \( np^s \) over \( \mathbb{F}_{p^m}[v]/(v^3) \) and their dual codes, where \( n \) is a positive integer coprime to \( p \), and \( \alpha, \beta \) are non-zero elements of \( \mathbb{F}_{p^m} \). This completely solves the problem of determination of all constacyclic codes of length \( np^s \) over \( \mathbb{F}_{p^m}[v]/(v^3) \) and their dual codes, where \( n \) is a positive integer coprime to \( p \). In a subsequent work [20], we determined all repeated-root constacyclic codes of arbitrary lengths over finite commutative chain rings with nilpotency index 2 and their dual codes. In the same work, we also listed some isodual repeated-root constacyclic codes and obtained Hamming distances, RT distances and RT weight distributions of some repeated-root constacyclic codes over finite commutative chain rings with nilpotency index 2.

In a related work, Cao [14] established algebraic structures of all \((1 + aw)\)-constacyclic codes of arbitrary lengths over a finite commutative chain ring \( R \) with the maximal ideal as \( \langle w \rangle \), where \( a \) is a unit in \( R \). Later, Dinh et al. [13] studied repeated-root \((\alpha + aw)\)-constacyclic codes of length \( p^s \) over a finite commutative chain ring \( R \) with the maximal ideal as \( \langle w \rangle \), where \( p \) is a prime number, \( s \geq 1 \) is an integer and \( \alpha, a \) are units in \( R \). The results obtained in Dinh et al. [13] can also be obtained from the work of Cao [14] and by establishing a ring isomorphism from \( R[x]/(x^{p^s} − 1 − \alpha a^{-1} w) \) onto \( R[x]/(x^{p^s} − \alpha - aw) \) as \( A(x) \mapsto A(\alpha_0^{-1} x) \) for each \( A(x) \in R[x]/(x^{p^s} − 1 − \alpha a^{-1} w) \), where \( \alpha = \alpha_0^p \) (such an element \( \alpha_0 \) always exists in \( \mathbb{F}_{p^m} \)). The constraint that \( a \) is a unit in \( R \) restricts their study to only a few special classes of repeated-root constacyclic codes over \( R \). When \( a \) is a unit in \( R \), the codes belonging to these special classes are direct sums of (principal) ideals of certain finite commutative chain rings. However, when \( a \) is a non-unit in \( R \), repeated-root constacyclic codes over \( R \) can also be direct sums of non-principal ideals. In another related work, Sobhani [21] determined all \((\alpha + \gamma u^2)\)-constacyclic codes of length \( p^s \) over \( \mathbb{F}_{p^m}[u]/(u^3) \) and their dual codes, where \( \alpha, \gamma \) are non-zero elements of \( \mathbb{F}_{p^m} \).

The main goal of this paper is to determine all repeated-root constacyclic codes of arbitrary lengths over \( \mathbb{F}_{p^m}[u]/(u^3) \), their sizes and their dual codes, where \( p \) is a prime and \( m \) is a positive integer. The Hamming distances, RT distances, and RT weight distributions are also determined for some repeated-root constacyclic codes over \( \mathbb{F}_{p^m}[u]/(u^3) \). Some isodual repeated-root constacyclic codes over \( \mathbb{F}_{p^m}[u]/(u^3) \) are also listed.

This paper is organized as follows: In Section 2, we state some basic definitions and results that are needed to derive our main results. In Section 3, we determine all repeated-root constacyclic codes of arbitrary lengths over \( \mathbb{F}_{p^m}[u]/(u^3) \), their dual codes and their sizes (Theorems 3.1-3.3). As an application, we also determine some isodual repeated-root constacyclic codes over \( \mathbb{F}_{p^m}[u]/(u^3) \) (Corollaries 3.1-3.3). In Section 4, we determine Hamming distances, RT distances, and RT weight distributions of some repeated-root constacyclic codes over \( \mathbb{F}_{p^m}[u]/(u^3) \) (Theorems 4.1-4.3). In Section 5, we mention a brief conclusion and discuss some interesting open problems in this direction.

2 Some preliminaries

A commutative ring \( R \) with unity is said to be (i) a local ring if it has a unique maximal ideal (consisting of all the non-units of \( R \)), and (ii) a chain ring if all the ideals of \( R \) form a chain with respect to the inclusion relation. Then the following result is well-known.

**Proposition 2.1.** [12] For a finite commutative ring \( R \) with unity, the following statements are equivalent:

(a) \( R \) is a local ring whose maximal ideal \( M \) is principal, i.e., \( M = \langle w \rangle \) for some \( w \in R \).

(b) \( R \) is a local principal ideal ring.

(c) \( R \) is a chain ring and all its ideals are given by \( \langle w^i \rangle \), \( 0 \leq i \leq e \), where \( e \) is the nilpotency index of \( w \).

Furthermore, we have \( |\langle w^i \rangle| = |R/\langle w \rangle|^{e-1} \) for \( 0 \leq i \leq e \). (Throughout this paper, \( |A| \) denotes the cardinality of the set \( A \).)

Now let \( R \) be a finite commutative ring with unity and let \( N \) be a positive integer. Let \( R^N \) be the \( R \)-module consisting of all \( N \)-tuples over \( R \). For a unit \( \lambda \in R \), a \( \lambda \)-constacyclic code \( C \) of length \( N \) over \( R \) is defined as an \( R \)-submodule of \( R^N \) satisfying the following property: \( (a_0, a_1, \cdots, a_{N-1}) \in C \) implies that
(\lambda a_{N-1}, a_0, a_1, \cdots, a_{N-2}) \in \mathcal{C}. The Hamming distance of \mathcal{C}, denoted by \textit{d}_H(\mathcal{C}), is defined as \textit{d}_H(\mathcal{C}) = \min \{w_H(c) : c \in \mathcal{C} \setminus \{0\}\}, where \textit{w}_H(c) is the number of non-zero components of \(c\) and is called the Hamming weight of \(c\). The Rosenbloom-Tsfasman (RT) distance of the code \(\mathcal{C}\), denoted by \textit{d}_RT(\mathcal{C}), is defined as \textit{d}_RT(\mathcal{C}) = \min \{w_{RT}(c) : c \in \mathcal{C} \setminus \{0\}\}, where \textit{w}_{RT}(\mathcal{C}) is the RT weight of \(c\) and is defined as
\[
\textit{w}_{RT}(c) = \begin{cases} 
1 + \max \{j | c_j \neq 0\} & \text{if } c = (c_0, c_1, \cdots, c_{N-1}) \neq 0; \\
0 & \text{if } c = 0.
\end{cases}
\]
The Rosenbloom-Tsfasman (RT) weight distribution of \(\mathcal{C}\) is defined as the list \(A_0, A_1, \cdots, A_N\), where for \(0 \leq \rho \leq N\), \(A_\rho\) denotes the number of codewords in \(\mathcal{C}\) having the RT weight as \(\rho\). The Hamming distance of a code is a measure of its error-detecting and error-correcting capabilities, while RT distances and RT weight distributions have applications in uniform distributions.

The dual code of \(\mathcal{C}\), denoted by \(\mathcal{C}^\perp\), is defined as \(\mathcal{C}^\perp = \{u \in R^N : u.c = 0 \text{ for all } c \in R^N\}\), where \(u.c = u_0c_0 + u_1c_1 + \cdots + u_{N-1}c_{N-1}\) for \(u = (u_0, u_1, \cdots, u_{N-1})\) and \(c = (c_0, c_1, \cdots, c_{N-1})\) in \(R^N\). It is easy to observe that \(\mathcal{C}^\perp\) is a \(\lambda^{-1}\)-constacyclic code of length \(N\) over \(R\). The code \(\mathcal{C}\) is said to be isodual if it is \(R\)-linearly equivalent to its dual code \(\mathcal{C}^\perp\). Under the standard \(R\)-module isomorphism \(\psi : R^N \rightarrow R[x]/\langle x^N - \lambda \rangle\), defined as \(\psi(a_0, a_1, \cdots, a_{N-1}) = a_0 + a_1x + \cdots + a_{N-1}x^{N-1} + \langle x^N - \lambda \rangle\) for each \((a_0, a_1, \cdots, a_{N-1}) \in R^N\), the code \(\mathcal{C}\) can be identified as an ideal of the ring \(R[x]/\langle x^N - \lambda \rangle\). Thus the study of \(\lambda\)-constacyclic codes of length \(N\) over \(R\) is equivalent to the study of ideals of the quotient ring \(R[x]/\langle x^N - \lambda \rangle\). From this point on, we shall represent elements of \(R[x]/\langle x^N - \lambda \rangle\) by their representatives in \(R[x]\) of degree less than \(N\), and we shall perform their addition and multiplication modulo \(x^N - \lambda\). Further, it is easy to see that the Hamming weight \(w_H(c(x))\) of \(c(x) \in R[x]/\langle x^N - \lambda \rangle\) is defined as the number of non-zero coefficients of \(c(x)\) and the RT weight \(w_{RT}(c(x))\) of \(c(x) \in R[x]/\langle x^N - \lambda \rangle\) is defined as \(w_{RT}(c(x)) = \begin{cases} 1 + \deg f(x) & \text{if } c(x) \neq 0; \\
0 & \text{if } c(x) = 0.
\end{cases}\) (throughout this paper, \(\deg f(x)\) denotes the degree of a non-zero polynomial \(f(x) \in R[x]\)). The dual code \(\mathcal{C}^\perp\) of \(\mathcal{C}\) is given by \(\mathcal{C}^\perp = \{u(x)c^*(x) = 0 \text{ in } R[x]/\langle x^N - \lambda \rangle\} \text{ for all } c(x) \in \mathcal{C}\}, where \(c^*(x) = x^{\deg c(x)}c(x^{-1})\) for all \(c(x) \in \mathcal{C} \setminus \{0\}\) and \(c^*(x) = 0\) if \(c(x) = 0\). The annihilator of \(\mathcal{C}\) is defined as \(\text{ann}(\mathcal{C}) = \{f(x) \in R[x]/\langle x^N - \lambda \rangle : f(x)c(x) = 0 \text{ in } R[x]/\langle x^N - \lambda \rangle\} \text{ for all } c(x) \in \mathcal{C}\}. One can easily observe that \(\text{ann}(\mathcal{C})\) is an ideal of \(R[x]/\langle x^N - \lambda \rangle\). Further, for any ideal \(I\) of \(R[x]/\langle x^N - \lambda \rangle\), we define \(I^* = \{f^*(x) : f(x) \in I\}\), where \(f^*(x) = x^{\deg f(x)}f(x^{-1})\) if \(f(x) \neq 0\) and \(f^*(x) = 0\) if \(f(x) = 0\). It is easy to see that \(I^*\) is an ideal of the ring \(R[x]/\langle x^N - \lambda \rangle\). Now the following holds.

**Lemma 2.1.** [4] If \(\mathcal{C} \subseteq R[x]/\langle x^N - \lambda \rangle\) is a \(\lambda\)-constacyclic code of length \(N\) over \(R\), then we have \(\mathcal{C}^\perp = \text{ann}(\mathcal{C})^*\).

From this point on, throughout this paper, let \(R\) be the ring \(\mathcal{R} = \mathbb{F}_{p^m}[u]/(u^3)\). It is easy to observe that \(\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}\) with \(u^3 = 0\), and that any element \(\lambda \in \mathcal{R}\) can be uniquely expressed as \(\lambda = \alpha + u\beta + u^2\gamma\), where \(\alpha, \beta, \gamma \in \mathbb{F}_{p^m}\). Now we make the following observation.

**Lemma 2.2.** [9] Let \(\lambda = \alpha + u\beta + u^2\gamma \in \mathcal{R}\), where \(\alpha, \beta, \gamma \in \mathbb{F}_{p^m}\). Then the following hold.

(a) \(\lambda\) is a unit in \(\mathcal{R}\) if and only if \(\alpha \neq 0\).

(b) There exists \(\alpha_0 \in \mathbb{F}_{p^m}\) satisfying \(\alpha_0^{p^m} = \alpha\).

The following theorem is useful in the determination of Hamming distances of repeated-root constacyclic codes over \(\mathcal{R}\) and is an extension of Theorem 3.4 of Dinh [10].

**Theorem 2.1.** For \(\eta \in \mathbb{F}_{p^m} \setminus \{0\}\), there exists \(\eta_0 \in \mathbb{F}_{p^m}\) satisfying \(\eta = \eta_0^{p^m}\). Suppose that the polynomial \(x^n - \eta_0\) is irreducible over \(\mathbb{F}_{p^m}\). Let \(\mathcal{C}\) be an \(\eta\)-constacyclic code of length \(np^m\) over \(\mathbb{F}_{p^m}\). Then we have \(\mathcal{C} = ((x^n - \eta_0)^v)^o\), where \(0 \leq v \leq p^m\). Moreover, the Hamming distance \(d_H(\mathcal{C})\) of the code \(\mathcal{C}\) is given by
Moreover, the polynomials $f$ into pairwise coprime polynomials in $R$.

Next we observe that for $1 \leq 1 \leq p - 1$ and $1 \leq k \leq s - 1$; we have $\lambda \cdot x^{p}$.

3 Constacyclic codes of length $np^s$ over $R$

Throughout this paper, let $p$ be a prime and let $n, s, m$ be positive integers with $\gcd(n, p) = 1$. Let $\mathbb{F}_{p^m}$ be the finite field of order $p^m$, and let $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3 \rangle$ be the finite commutative chain ring with unity. Let $\lambda = \alpha + \beta u + \gamma u^2$, where $\alpha, \beta, \gamma \in \mathbb{F}_{p^m}$ and $\alpha$ is non-zero. In this section, we will determine all $\lambda$-constacyclic codes of length $np^s$ over $\mathcal{R}$ and their dual codes. We will also determine the number of codewords in each code. Apart from this, we shall list some isodual constacyclic codes of length $np^s$ over $\mathcal{R}$.

To do this, we recall that a $\lambda$-constacyclic code of length $np^s$ over $\mathcal{R}$ is an ideal of the quotient ring $\mathcal{R}_\lambda = \mathcal{R}[x]/\langle x^{np^s} - \lambda \rangle$. Further, by Lemma 2.2(b), there exists $\alpha_0 \in \mathbb{F}_{p^m}$ satisfying $\alpha_0^{p^s} = \alpha$. Now let $x^n - \alpha_0 = f_1(x)f_2(x) \cdots f_r(x)$ be the irreducible factorization of $x^n - \alpha_0$ over $\mathbb{F}_{p^m}$, where $f_1(x), f_2(x), \ldots, f_r(x)$ are pairwise coprime monic (irreducible) polynomials over $\mathbb{F}_{p^m}$. In the following lemma, we factorize the polynomial $x^{np^s} - \lambda$ into pairwise coprime polynomials in $\mathcal{R}[x]$.

**Lemma 3.1.** We have $x^{np^s} - \lambda = \prod_{j=1}^{r} \left( f_j(x)^{p^s} + ug_j(x) + u^2 h_j(x) \right)$, where the polynomials $g_1(x), g_2(x), \ldots, g_r(x), h_1(x), h_2(x), \ldots, h_r(x) \in \mathbb{F}_{p^m}[x]$ satisfy the following for $1 \leq j \leq r$:

- $\gcd(f_j(x), g_j(x)) = 1$ when $\beta \neq 0$.
- $g_j(x) = h_j(x) = 0$ when $\beta = \gamma = 0$.
- $g_j(x) = 0$ and $\gcd(f_j(x), h_j(x)) = 1$ in $\mathbb{F}_{p^m}[x]$ when $\beta = 0$ and $\gamma$ is non-zero.

Moreover, the polynomials $f_1(x)^{p^s} + ug_1(x) + u^2 h_1(x), f_2(x)^{p^s} + ug_2(x) + u^2 h_2(x), \ldots, f_r(x)^{p^s} + ug_r(x) + u^2 h_r(x)$ are pairwise coprime in $\mathcal{R}[x]$.

**Proof.** To prove the result, we see that

$$x^{np^s} - \lambda = (x^n - \alpha_0)^{p^s} - \beta u + \gamma u^2 = f_1(x)^{p^s} f_2(x)^{p^s} \cdots f_r(x)^{p^s} - \beta u - u^2 \gamma. \quad (1)$$

Next we observe that for $1 \leq j \leq r - 1$, the polynomials $f_j(x)^{p^s}$ and $\prod_{i=j+1}^{r} f_i(x)^{p^s}$ are coprime in $\mathbb{F}_{p^m}[x]$, which implies that there exist $v_j(x), w_j(x) \in \mathbb{F}_{p^m}[x]$ satisfying $\deg w_j(x) < \deg f_j(x)^{p^s}$ and

$$v_j(x)f_j(x)^{p^s} + w_j(x) \prod_{i=j+1}^{r} f_i(x)^{p^s} = 1. \quad (2)$$

Now by (1) and (2), we obtain

$$x^{np^s} - \lambda = \left\{ f_1(x)^{p^s} - \beta u w_1(x) - u^2 w_1(x)(\gamma + \beta^2 v_1(x)w_1(x)) \right\} \left( \prod_{i=2}^{r} f_i(x)^{p^s} - u\beta v_1(x) - u^2 v_1(x)(\gamma + \beta^2 v_1(x)w_1(x)) \right).$$

Further, using (2) again, we get

$$\prod_{i=2}^{r} f_i(x)^{p^s} - u\beta v_1(x) - u^2 v_1(x)(\gamma + \beta^2 v_1(x)w_1(x)) = \left\{ f_2(x)^{p^s} - u\beta v_1(x)w_2(x) - u^2 v_1(x)w_2(x)(\gamma + \beta^2 v_1(x)w_1(x)) \right\}. $$
Lemma 3.2. \[ \text{more explicitly, we observe that} \quad g_j(x) = -\beta w_j(x) \prod_{i=1}^{j-1} v_i(x) \quad \text{and} \quad h_j(x) = -w_j(x) \prod_{i=1}^{j-1} v_i(x) \left( \gamma + \beta^2 \sum_{i=1}^{j} v_1(x)v_2(x) \cdots v_i(x)w_i(x) \right) \]

for \( 1 \leq j \leq r \) when \( r \geq 2 \). From this, the desired result follows. \( \Box \)

From now on, we define \( k_j(x) = f_j(x)p^r + ug_j(x) + u^2h_j(x) \) for \( 1 \leq j \leq r \). Then we have \( x^{np^r} - \lambda = \prod_{j=1}^{r} k_j(x) \).

Further, if \( \deg f_j(x) = d_j \), then we observe that \( \deg k_j(x) = d_jp^r \) for each \( j \). By Lemma 3.1 we see that \( k_1(x), k_2(x), \ldots, k_r(x) \) are pairwise coprime in \( \mathcal{R}[x] \). This, by Chinese Remainder Theorem, implies that

\[ \mathcal{R}_\lambda \cong \bigoplus_{j=1}^{r} \mathcal{K}_j, \]

where \( \mathcal{K}_j = \mathcal{R}[x]/\langle k_j(x) \rangle \) for \( 1 \leq j \leq r \). Then we observe the following:

**Proposition 3.1.** (a) Let \( C \) be a \( \lambda \)-constacyclic code of length \( np^s \) over \( \mathcal{R} \), i.e., an ideal of the ring \( \mathcal{R}_\lambda \). Then \( C = C_1 \oplus C_2 \oplus \cdots \oplus C_r \), where \( C_j \) is an ideal of \( \mathcal{K}_j \) for \( 1 \leq j \leq r \).

(b) If \( I_j \) is an ideal of \( \mathcal{K}_j \) for \( 1 \leq j \leq r \), then \( I = I_1 \oplus I_2 \oplus \cdots \oplus I_r \) is an ideal of \( \mathcal{R}_\lambda \) (i.e., \( I \) is a \( \lambda \)-constacyclic code of length \( np^s \) over \( \mathcal{R} \)). Moreover, we have \( |I| = |I_1||I_2| \cdots |I_r| \).

**Proof.** Proof is trivial. \( \Box \)

Next if \( C \) is a \( \lambda \)-constacyclic code of length \( np^s \) over \( \mathcal{R} \), then its dual code \( C^\perp \) is a \( \lambda^{-1} \)-constacyclic code of length \( np^s \) over \( \mathcal{R} \). This implies that \( C^\perp \) is an ideal of the ring \( \mathcal{R}_{\lambda^{-1}} = \mathcal{R}[x]/\langle x^{np^r} - \lambda^{-1} \rangle \). In order to determine \( C^\perp \) more explicitly, we observe that \( x^{np^r} - \lambda^{-1} = -\alpha^{-1}k_1(x)k_2^*(x) \cdots k_r^*(x) \). By applying Chinese Remainder Theorem again, we get \( \mathcal{R}_{\lambda^{-1}} \cong \bigoplus_{j=1}^{r} \widehat{\mathcal{K}}_j \), where \( \widehat{\mathcal{K}}_j = \mathcal{R}[x]/\langle k_j^*(x) \rangle \) for \( 1 \leq j \leq r \). Then we have the following:

**Proposition 3.2.** Let \( C \) be a \( \lambda \)-constacyclic code of length \( np^s \) over \( \mathcal{R} \), i.e., an ideal of the ring \( \mathcal{R}_\lambda \). If \( C = C_1 \oplus C_2 \oplus \cdots \oplus C_r \) with \( C_j \) an ideal of \( \mathcal{K}_j \) for each \( j \), then the dual code \( C^\perp \) of \( C \) is given by \( C^\perp = C_1^\perp \oplus C_2^\perp \oplus \cdots \oplus C_r^\perp \), where \( C_j^\perp = \{ a_j(x) \in \widehat{\mathcal{K}}_j : a_j(x)c_j^*(x) = 0 \text{ in } \widehat{\mathcal{K}}_j \text{ for all } c_j(x) \in C_j \} \) is the orthogonal complement of \( C_j \) for each \( j \).

Furthermore, \( C_j^\perp \) is an ideal of \( \mathcal{K}_j = \mathcal{R}[x]/\langle k_j^*(x) \rangle \) for each \( j \).

**Proof.** Its proof is straightforward. \( \Box \)

In view of Propositions 3.1 and 3.2, we see that to determine all \( \lambda \)-constacyclic codes of length \( np^s \) over \( \mathcal{R} \), their sizes and their dual codes, we need to determine all ideals of the ring \( \mathcal{K}_j \), their cardinalities and their orthogonal complements in \( \widehat{\mathcal{K}}_j \) for \( 1 \leq j \leq r \). To do so, throughout this paper, let \( 1 \leq j \leq r \) be a fixed integer. From now onwards, we shall represent elements of the rings \( \mathcal{K}_j \) and \( \widehat{\mathcal{K}}_j \) (resp. \( \mathbb{F}_{p^m}[x]/\langle f_j(x)p^r \rangle \)) by their representatives in \( \mathcal{R}[x] \) (resp. \( \mathbb{F}_{p^m}[x] \)) of degree less than \( d_jp^r \) (resp. \( d_jp^s \)) and we shall perform their addition and multiplication modulo \( k_j(x) \) and \( k_j^*(x) \) (resp. \( f_j(x)p^r \)), respectively. To determine all ideals of the ring \( \mathcal{K}_j \), we need to prove the following lemma.

**Lemma 3.2.** Let \( 1 \leq j \leq r \) be fixed. In the ring \( \mathcal{K}_j \), the following hold.

(a) Any non-zero polynomial \( g(x) \in \mathbb{F}_{p^m}[x] \) satisfying \( \gcd(g(x), f_j(x)) = 1 \) is a unit in \( \mathcal{K}_j \). As a consequence, any non-zero polynomial in \( \mathbb{F}_{p^m}[x] \) of degree less than \( d_j \) is a unit in \( \mathcal{K}_j \).

(b) \( \langle f_j(x)p^r \rangle = \begin{cases} \langle u \rangle & \text{if } \beta \neq 0; \\ \langle u^2 \rangle & \text{if } \beta = 0 \text{ and } \gamma \neq 0; \\ \{0\} & \text{if } \beta = \gamma = 0. \end{cases} \)

As a consequence, \( f_j(x) \) is a nilpotent element of \( \mathcal{K}_j \) with the nilpotency index as \( 3p^s \) when \( \beta \neq 0 \), the nilpotency index of \( f_j(x) \) is \( 2p^s \) when \( \beta = 0 \) and \( \gamma \neq 0 \), while the nilpotency index of \( f_j(x) \) is \( p^s \) when \( \beta = \gamma = 0 \).
Proof. (a) As \( f_j(x) \) is irreducible over \( \mathbb{F}_{p^m} \) and \( \gcd(g(x), f_j(x)) = 1 \), we have \( \gcd(g(x), f_j(x)^p) = 1 \) in \( \mathbb{F}_{p^m}[x] \), which implies that there exist polynomials \( a(x), b(x) \in \mathbb{F}_{p^m}[x] \) such that \( a(x)g(x) + b(x)f_j(x)^p = 1 \). This implies that \( a(x)g(x) + b(x)f_j(x)^p + ug_j(x) + u^2h_j(x) = 1 + ub(x)(g_j(x) + uh_j(x)) \). From this, we get \( a(x)g(x) = 1 + ub(x)(g_j(x) + uh_j(x)) \) in \( K_j \). As \( u^3 = 0 \) in \( K_j \), we see that \( 1 + ub(x)(g_j(x) + uh_j(x)) \) is a unit in \( K_j \), which implies that \( g(x) \) is a unit in \( K_j \).

(b) It follows immediately from Lemma 3.1 and part (a).

Next for a positive integer \( k \), let \( \mathcal{P}_k(\mathbb{F}_{p^m}) = \{ g(x) \in \mathbb{F}_{p^m}[x] : \text{ either } g(x) = 0 \text{ or } \deg g(x) < k \} \). Note that every element \( a(x) \in K_j \) can be uniquely expressed as \( a(x) = a_0(x) + ua_1(x) + u^2a_2(x) \), where \( a_0(x), a_1(x), a_2(x) \in \mathcal{P}_d, p^e(\mathbb{F}_{p^m}) \). Further, by repeatedly applying division algorithm in \( \mathbb{F}_{p^m}[x] \), for \( d \in \{ 0, 1, 2 \} \), we can write \( a(x) = \sum_{i=0}^{p^{d-1}} A_i(x)f_j(x)^i \), where \( A_i(x) \in \mathcal{P}_d, p^e(\mathbb{F}_{p^m}) \) for \( 0 \leq i \leq p^d - 1 \). That is, each element \( a(x) \in K_j \) can be uniquely expressed as \( a(x) = \sum_{i=0}^{p^{d-1}} A_i(x)f_j(x)^i + u \sum_{i=0}^{p^{d-1}} A_i(x)f_j(x)^{i+1} + u^2 \sum_{i=0}^{p^{d-1}} A_i(x)f_j(x)^{i+2} \), where \( A_i(x) \in \mathcal{P}_d, p^e(\mathbb{F}_{p^m}) \) for each \( i \) and \( d \). Now to determine cardinalities of all ideals of \( K_j \), we prove the following lemma.

**Lemma 3.3.** Let \( 1 \leq j \leq r \) be a fixed integer. If \( \mathcal{I} \) is an ideal of \( K_j \), then \( \text{Res}_u(\mathcal{I}) = \{ a_0(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^p \rangle : a_0(x) + u a_1(x) + u^2 a_2(x) \in \mathcal{I} \text{ for some } a_0(x), a_1(x), a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^p \rangle \} \), \( \text{Tor}_u(\mathcal{I}) = \{ a_1(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^p \rangle : a_1(x) + u^2 a_2(x) \in \mathcal{I} \text{ for some } a_0(x), a_1(x), a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^p \rangle \} \) and \( \text{Tor}_{u^2}(\mathcal{I}) = \{ a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^p \rangle : a_2(x) \in \mathcal{I} \} \) are ideals of \( \mathbb{F}_{p^m}[x]/\langle f_j(x)^p \rangle \). Moreover, we have \( |\mathcal{I}| = |\text{Res}_u(\mathcal{I})||\text{Tor}_u(\mathcal{I})||\text{Tor}_{u^2}(\mathcal{I})| \).

**Proof.** One can easily observe that \( \text{Res}_u(\mathcal{I}), \text{Tor}_u(\mathcal{I}) \) and \( \text{Tor}_{u^2}(\mathcal{I}) \) are ideals of \( \mathbb{F}_{p^m}[x]/\langle f_j(x)^p \rangle \). In order to prove the second part, we define a map

\[
\phi : \mathcal{I} \rightarrow \text{Res}_u(\mathcal{I})
\]

as \( \phi(a(x)) = a_0(x) \) for each \( a(x) = a_0(x) + u a_1(x) + u^2 a_2(x) \in \mathcal{I} \) with \( a_0(x), a_1(x), a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^p \rangle \).

We observe that \( \phi \) is a surjective \( \mathbb{F}_{p^m}[x]/\langle f_j(x)^p \rangle \)-module homomorphism and its kernel is given by \( K_\mathcal{I} = \{ u a_1(x) + u^2 a_2(x) \in \mathcal{I} : a_1(x), a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^p \rangle \} \). This implies that

\[
|\mathcal{I}| = |\text{Res}_u(\mathcal{I})||K_\mathcal{I}|. \tag{3}
\]

We further define a map

\[
\psi : K_\mathcal{I} \rightarrow \text{Tor}_u(\mathcal{I})
\]

as \( \psi(u a_1(x) + u^2 a_2(x)) = a_1(x) \) for each \( a_1(x), a_2(x) \in K_\mathcal{I} \), where \( a_1(x), a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^p \rangle \). We see that \( \psi \) is also a surjective \( \mathbb{F}_{p^m}[x]/\langle f_j(x)^p \rangle \)-module homomorphism with the kernel as \( \ker \psi = \{ u^2 a_2(x) \in K_\mathcal{I} : a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^p \rangle \} \). From this, it follows that

\[
|K_\mathcal{I}| = |\text{Tor}_u(\mathcal{I})||\ker \psi| = |\text{Tor}_u(\mathcal{I})||\text{Tor}_{u^2}(\mathcal{I})|,
\]

which, by (3), implies that

\[
|\mathcal{I}| = |\text{Res}_u(\mathcal{I})||\text{Tor}_u(\mathcal{I})||\text{Tor}_{u^2}(\mathcal{I})|.
\]

To determine orthogonal complements of all ideals of \( K_j \), we need the following lemma.

**Lemma 3.4.** Let \( 1 \leq j \leq r \) be a fixed integer. Let \( \mathcal{I} \) be an ideal of the ring \( K_j \) with the orthogonal complement as \( \mathcal{I}^\perp \). Then the following hold.

(a) \( \mathcal{I}^\perp \) is an ideal of \( K_j \).

(b) \( \mathcal{I}^\perp = \{ a^*(x) \in K_j^* : a^*(x) \in \text{ann}(\mathcal{I}) \} = \text{ann}(\mathcal{I})^* \).

(c) If \( \mathcal{I} = \langle f(x), ug(x), u^2h(x) \rangle \), then we have \( \mathcal{I}^\perp = \langle f^*(x), ug^*(x), u^2h^*(x) \rangle \).

(d) For non-zero \( f(x), g(x) \in K_j \), let us define \( \langle fg(x) \rangle = f(x)g(x) \) and \( \langle f + g(x) \rangle = f(x) + g(x) \). If \( (fg)(x) \neq 0 \), then we have \( f^*(x)g^*(x) = x^{\deg f(x) + \deg g(x)} f(x)^*(x)g(x)^*(x) \). If \( (f + g)(x) \neq 0 \), then we have

\[
(f + g)^*(x) = \begin{cases} 
  f^*(x) + x^{\deg f(x) + \deg g(x)} g^*(x) & \text{if } \deg f(x) > \deg g(x); \\
  x^{\deg (f + g)(x)} f(x)^*(x) + g(x)^*(x) & \text{if } \deg f(x) = \deg g(x).
\end{cases}
\]
Proof. Its proof is straightforward. □

By the above lemma, we see that to determine $\mathcal{I}^\perp$, it is enough to determine $\text{ann}(\mathcal{I})$ for each ideal $\mathcal{I}$ of $K_j$. Further, to write down all ideals of $K_j$, we see, by Lemma 5.3, that for each ideal $\mathcal{I}$ of $K_j$, $\text{Res}_u(\mathcal{I})$, $\text{Tor}_u(\mathcal{I})$ and $\text{Tor}_u(\mathcal{I})$ all are ideals of the ring $\mathbb{F}_{p^n}[x]/(f_j(x)p^s)$, which is a finite commutative chain ring with the maximal ideal as $(f_j(x))$. Next by Proposition 2.1, we see that all the ideals of $\mathbb{F}_{p^n}[x]/(f_j(x)p^s)$ are given by $\langle f_j(x)^i \rangle$ with $0 \leq i \leq p^s$ and that $|\langle f_j(x)^i \rangle| = p^{md_j(3p^s - i)}$ for each $i$. This implies that $\text{Res}_u(\mathcal{I}) = \langle f_j(x)^a \rangle$, $\text{Tor}_u(\mathcal{I}) = \langle f_j(x)^b \rangle$ and $\text{Tor}_u(\mathcal{I}) = \langle f_j(x)^c \rangle$ for some integers $a, b, c$ satisfying $0 \leq c \leq b \leq a \leq p^s$.

First of all, we shall consider the case $\beta \neq 0$. Here we see that when $\alpha_0 = \mu^n$ for some $\mu \in \mathbb{F}_{p^m}$, each $\lambda$-constacyclic code of length $np^s$ over $R$ is equivalent to a cyclic code of length $np^s$ over $R$ and can be determined by using the results derived in Cao [7] via the map $\Psi : R[x]/(x^{np^s} - 1 - \alpha x - \alpha^{-1}u - \alpha^{-1}u^2) \rightarrow R[x]/(x^{np^s} - 1 - \alpha x - \alpha^{-1}u - \alpha^{-1}u^2)$, defined as $a(x) \rightarrow a(\mu^{-1}x)$ for each $a(x) \in R[x]/(x^{np^s} - 1 - \alpha x - \alpha^{-1}u - \alpha^{-1}u^2)$. However, when $\alpha_0$ (and hence $\alpha$) is not an $n$th power of an element in $\mathbb{F}_{p^m}$, this method cannot be employed to determine all $(\alpha + \beta u + \gamma u^2)$-constacyclic codes of length $np^s$ over $R$. In fact, the problem of determination of all $(\alpha + \beta u + \gamma u^2)$-constacyclic codes of length $np^s$ over $R$ and their dual codes is not yet completely solved. Propositions 5.1 & 3.2 and the following theorem completely solves this problem when $\beta$ is non-zero.

**Theorem 3.1.** When $\beta \neq 0$, all ideals of the ring $K_j$ are given by $\langle f_j(x)^i \rangle$, where $0 \leq i \leq 3p^s$. Furthermore, for $0 \leq i \leq 3p^s$, we have $|\langle f_j(x)^i \rangle| = p^{md_j(3p^s - i)}$ and $\text{ann}(\langle f_j(x)^i \rangle) = \langle f_j(x)^{3p^s - i} \rangle$.

**Proof.** To prove this, we first observe that an element $a(x) \in K_j$ can be uniquely expressed as $a(x) = a_0(x) + u_1(x) + u_1^2(x)$, where $a_0(x), a_1(x), a_2(x) \in P_{d_j,p}(\mathbb{F}_{p^n})$. By division algorithm in $\mathbb{F}_{p^n}[x]$, there exist unique polynomials $q(x), r(x) \in \mathbb{F}_{p^n}[x]$ such that $a(x) = f_j(x)q(x) + r(x)$, where either $r(x) = 0$ or $\deg r(x) < d_j$. This implies that $a(x) = f_j(x)q(x) + r(x) + u_1(x) + u_1^2(x)$. Now in view of Lemma 5.2(b), we see that $a(x)$ is a unit in $K_j$ if and only if $r(x)$ is a unit in $K_j$. Further, by Lemma 5.2(a), we see that $r(x) \in \mathbb{F}_{p^n}[x]$ is a unit in $K_j$ if and only if $r(x) \neq 0$. This shows that $a(x)$ is a non-unit in $K_j$ if and only if $r(x) = 0$ if and only if $a(x) = (f_j(x))$. That is, all the non-units of $K_j$ are given by $\langle f_j(x) \rangle$. Now using Proposition 2.1 and Lemma 5.2(b), we see that $K_j$ is a chain ring and all its ideals are given by $\langle f_j(x)^i \rangle$ with $0 \leq i \leq 3p^s$. Furthermore, we observe that the residue field of $K_j$ is given by $\overline{K_j} = K_j/(f_j(x))$, and that $|\overline{K_j}| = p^{md_j}$. Now using Proposition 2.1 and Lemma 5.2(b) again, we obtain $|\langle f_j(x)^i \rangle| = p^{md_j(3p^s - i)}$ for $0 \leq i \leq 3p^s$. Further, it is easy to observe that $\text{ann}(\langle f_j(x)^i \rangle) = (f_j(x)^{3p^s - i})$, which completes the proof of the theorem. □

As a consequence of the above theorem, we deduce the following:

**Corollary 3.1.** Let $n \geq 1$ be an integer and $\alpha_0 \in \mathbb{F}_{p^n}$ be such that the binomial $x^n - \alpha_0$ is irreducible over $\mathbb{F}_{p^n}$. Let $\alpha = \alpha_0^p$, and $\beta(\neq 0), \gamma \in \mathbb{F}_{p^n}$. Then there exists an isodual $(\alpha + \beta u + u^2\gamma)$-constacyclic code of length $np^s$ over $R$ if and only if $p = 2$. Moreover, when $p = 2$, the ideal $\langle (x^n - \alpha_0)^{3 \cdot 2^{s-1}} \rangle$ is the only isodual $(\alpha + \beta u + u^2\gamma)$-constacyclic code of length $n2^s$ over $R$.

**Proof.** On taking $f_j(x) = x^n - \alpha_0$ in Theorem 3.1, we see that all $(\alpha + \beta u + u^2\gamma)$-constacyclic codes of length $np^s$ over $R$ are given by $\langle (x^n - \alpha_0)^{3p^s} \rangle$, where $0 \leq l \leq 3p^s$. Furthermore, for $0 \leq l \leq 3p^s$, the ideal $\langle (x^n - \alpha_0)^{3p^s} \rangle$ has $p^{mn(3p^s - l)}$ elements and the annihilator $\langle (x^n - \alpha_0)^{3p^s} \rangle$ is given by $\langle (x^n - \alpha_0)^{3p^s - l} \rangle$. Next we see that if a code $C = \langle (x^n - \alpha_0)^{3p^s} \rangle$ is isodual, then we must have $|C| = |C^\perp|$. This gives $p^{mn(3p^s - l)} = p^{mn l}$. This implies that $3p^s = 2l$, which holds if and only if $p = 2$. So when $p$ is an odd prime, there does not exist any isodual $(\alpha + \beta u + u^2\gamma)$-constacyclic code of length $np^s$ over $R$. When $p = 2$, we get $l = 3 \cdot 2^{s-1}$. On the other hand, when $p = 2$, we observe that $(x^n - \alpha_0)^{3 \cdot 2^{s-1}}$ is an isodual $(\alpha + \beta u + u^2\gamma)$-constacyclic code of length $n2^s$ over $R$, which completes the proof.

**Remark 3.1.** By Theorem 3.75 of [17], we see that the binomial $x^n - \alpha_0$ is irreducible over $\mathbb{F}_{p^n}$ if and only if the following two conditions are satisfied: (i) each prime divisor of $n$ divides the multiplicative order $e$ of $\alpha_0$, but not $(p^m - 1)/e$ and (ii) $p^m \equiv 1 (mod 4)$ if $n \equiv 0 (mod 4)$.
In the following theorem, we consider the case $\beta = \gamma = 0$, and we determine all non-trivial ideals of the ring $K_j$, their cardinalities and their annihilators.

**Theorem 3.2.** Let $\beta = \gamma = 0$, and let $I$ be a non-trivial ideal of the ring $K_j$ with $Res_u(I) = \langle f_j(x)^a \rangle$, $Tor_n(I) = \langle f_j(x)^b \rangle$ and $Tor_{n,2}(I) = \langle f_j(x)^c \rangle$ for some integers $a, b, c$ satisfying $0 \leq c \leq b \leq a \leq p^s$. Suppose that $B_i(x), C_k(x), Q_k(x), W_s(x)$ run over $P_d_j(\mathbb{F}_{p^m})$ for each relevant $i, k, \ell$ and $e$. Then the following hold.

*Type I:* When $a = b = p^s$, we have

$$I = \langle u^2 f_j(x)^c \rangle,$$

where $c < p^s$. Moreover, we have

$$|I| = p^{md_j(p^s - c)} \text{ and } \text{ann}(I) = \langle f_j(x)^{p^s - c}, u \rangle.$$

*Type II:* When $a = p^s$ and $b < p^s$, we have

$$I = \langle uf_j(x)^b + u^2 f_j(x)^d G(x), u^2 f_j(x)^c \rangle,$$

where $c + b - p^s \leq t < c$ if $G(x) \neq 0$ and $G(x)$ is either 0 or a unit in $K_j$ of the form $\sum_{k=0}^{c-1} B_i(x) f_j(x)^i$. Moreover, we have

$$|I| = p^{md_j(2p^s - b - c)} \text{ and } \text{ann}(I) = \langle f_j(x)^{p^s - c - t} - u f_j(x)^{p^s - t - b} G(x), u f_j(x)^{p^s - b}, u^2 \rangle.$$

*Type III:* When $a < p^s$, we have

$$I = \langle f_j(x)^a + uf_j(x)^{t_1} D_1(x) + u^2 f_j(x)^{t_2} D_2(x), uf_j(x)^b + u^2 f_j(x)^d G(x), u^2 f_j(x)^c \rangle,$$

where $a + b - p^s \leq t_1 < b$ if $D_1(x) \neq 0$, $0 \leq t_2 < c$ if $D_2(x) \neq 0$, $b + c - p^s \leq \theta < c$ if $V(x) \neq 0$, $D_1(x)$ is either 0 or a unit in $K_j$ of the form $\sum_{k=0}^{c-1} C_k(x) f_j(x)^k$, $D_2(x)$ is either 0 or a unit in $K_j$ of the form $\sum_{k=0}^{c-1} Q_k(x) f_j(x)^k$. Furthermore, we have $u^2 (f_j(x)^{p^s - a + t_1 - b} V(x) D_1(x) - f_j(x)^{p^s - a + t_2} D_2(x)) \in \langle u^2 f_j(x)^c \rangle$, i.e., there exists $A(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s} \rangle$ such that $u^2 (f_j(x)^{p^s - a + t_1 - b} V(x) D_1(x) - f_j(x)^{p^s - a + t_2} D_2(x)) = u^2 f_j(x)^c A(x)$. Moreover, we have

$$|I| = p^{md_j(3p^s - a - b - c)}$$

and the annihilator of $I$ is given by

$$\text{ann}(I) = \langle f_j(x)^{p^s - c} - uf_j(x)^{p^s - c - t - b} V(x) + u^2 A(x), uf_j(x)^{p^s - b} - u^2 f_j(x)^{p^s - a + t_1 - b} D_1(x), u^2 f_j(x)^{p^s - a} \rangle.$$

Proof. As $I$ is a non-trivial ideal of $K_j$, we note that neither $a = 0$ nor $a = b = c = p^s$ hold. Further, by Lemma 3.3, we have $|I| = p^{md_j(3p^s - a - b - c)}$. Now to write down all such non-trivial ideals of $K_j$ and to determine their annihilators, we shall distinguish the following three cases: (i) $a = p^s$, (ii) $a = p^s$ and $b < p^s$, and (iii) $a < p^s$.

1. **(i) When $a = b = p^s$, we have $I \subseteq \langle u^2 \rangle.$** In this case, we have $0 \leq c < p^s$. Here we observe that $I = \langle u^2 f_j(x)^c \rangle$. Now to find $\text{ann}(I)$, we consider the ideal $B_1 = \langle f_j(x)^{p^s - c}, u, u^2 \rangle$, and we see that $B_1 \subseteq \text{ann}(I)$ and that $|B_1| = p^{md_j(2p^s + c)}$. As

$$p^{md_j(p^s - c)} = |I| = \frac{|K_j|}{|\text{ann}(I)|} \leq \frac{p^{md_j(p^s)}}{|B_1|} = p^{md_j(p^s - c)},$$

we obtain $\text{ann}(I) = B_1 = \langle f_j(x)^{p^s - c}, u, u^2 \rangle$.
(ii) When \( a = p^s \) and \( b < p^s \), we have \( \mathcal{I} \subseteq \langle u \rangle \) and \( \mathcal{I} \nsubseteq \langle u^2 \rangle \). Here we observe that

\[
I = \langle uf_j(x)^b + u^2r(x), u^2f_j(x)^c \rangle
\]

for some \( r(x) \in \mathcal{K}_j \). Let us write \( u^2r(x) = u^2 \sum_{i=0}^{c-1} G_i(x)f_j(x)^i \), where \( G_i(x) \in \mathcal{P}_j(\mathbb{F}_p^n) \) for \( 0 \leq i \leq p^s - 1 \). Note that for all \( i \geq c \), we have \( u^2f_j(x)^i = u^2f_j(x)^{c}f_j(x)^{i-c} \in \mathcal{I} \), which implies that \( \mathcal{I} = \langle uf_j(x)^b + u^2 \sum_{i=0}^{c-1} G_i(x)f_j(x)^i, u^2f_j(x)^c \rangle \). If \( u^2 \sum_{i=0}^{c-1} G_i(x)f_j(x)^i \neq 0 \) in \( \mathcal{K}_j \), then choose the smallest integer \( t \) with \( 0 \leq t < c \) satisfying \( G_t(x) \neq 0 \), which gives \( u^2 \sum_{i=0}^{c-1} G_i(x)f_j(x)^i = u^2f_j(x)^tG(x) \), where \( G(x) = \sum_{i=0}^{c-1} G_i(x)f_j(x)^{i-t} \) is a unit in \( \mathcal{K}_j \). On the other hand, when \( u^2 \sum_{i=0}^{c-1} G_i(x)f_j(x)^i = 0 \) in \( \mathcal{K}_j \), let us choose \( G(x) = 0 \). From this, it follows that

\[
\mathcal{I} = \langle uf_j(x)^b + u^2f_j(x)^tG(x), u^2f_j(x)^c \rangle,
\]

where \( G(x) \) is either 0 or a unit in \( \mathcal{K}_j \) of the form \( \sum_{i=0}^{c-t-1} a_i(x)f_j(x)^i \) with \( a_i(x) \in \mathcal{P}_j(\mathbb{F}_p^n) \) for \( 0 \leq i \leq c-t-1 \).

Further, as \( f_j(x)^{p^s-b} \{ uf_j(x)^b + u^2f_j(x)^tG(x) \} = u^2f_j(x)^{t-b+t}G(x) \in \mathcal{I} \), we have \( p^s - b + t \geq c \) when \( G(x) \neq 0 \).

Moreover, let \( B_2 = \langle f_j(x)^{p^s-c} - uf_j(x)^{p^s-c+t-b}G(x), uf_j(x)^{p^s-b}, u^2 \rangle \). We observe that \( B_2 \subseteq \langle u \rangle \) and \( |B_2| \geq p^{md_j(p^s+b+c)} \).

Since

\[
p^{md_j(2p^s-b-c)} = |\mathcal{I}| = \frac{|\mathcal{K}_j|}{|\langle u \rangle|} \leq \frac{p^{md_j(p^s)}}{|B_2|} \leq p^{md_j(2p^s-b-c)},
\]

we obtain \( |\langle u \rangle| = |B_2| = p^{md_j(p^s+b+c)} \) and \( |\langle u \rangle| = B_2 = \langle f_j(x)^{p^s-c} - uf_j(x)^{p^s-c+t-b}G(x), uf_j(x)^{p^s-b}, u^2 \rangle \).

(iii) When \( a < p^s \), we have \( \mathcal{I} \nsubseteq \langle u \rangle \). In this case, we see that \( a > 0 \). Here we observe that

\[
\mathcal{I} = \langle f_j(x)^a + ur_1(x) + u^2r_2(x), uf_j(x)^b + u^2q(x), u^2f_j(x)^c \rangle
\]

for some \( r_1(x), r_2(x), q(x) \in \mathcal{K}_j \). Let us write \( ur_1(x) = u \sum_{\ell=0}^{p^s-1} A_{\ell}(x)f_j(x)^{\ell} \), where \( A_{\ell}(x) \in \mathcal{P}_j(\mathbb{F}_p^n) \) for \( 0 \leq \ell \leq p^s - 1 \). Now for all \( \ell \geq b \), we observe that \( uf_j(x)^{\ell} = f_j(x)^{\ell-b} \{ uf_j(x)^b + u^2q(x) \} = u^2f_j(x)^{\ell-b}q(x) \). This implies that

\[
\mathcal{I} = \langle f_j(x)^a + u \sum_{\ell=0}^{b-1} A_{\ell}(x)f_j(x)^{\ell} + u^2 \{ r_2(x) - q(x) \sum_{\ell=0}^{p^s-1} A_{\ell}(x)f_j(x)^{\ell-a} \}, uf_j(x)^b + u^2q(x), u^2f_j(x)^c \rangle.
\]

Next we write \( u^2 \{ r_2(x) - q(x) \sum_{\ell=0}^{p^s-1} A_{\ell}(x)f_j(x)^{\ell-a} \} = u^2 \sum_{k=0}^{p^s-1} B_k(x)f_j(x)^k \), where \( B_k(x) \in \mathcal{P}_j(\mathbb{F}_p^n) \) for \( 0 \leq k \leq p^s - 1 \). Further, for all \( k \geq c \), we see that \( u^2f_j(x)^k = u^2f_j(x)^c f_j(x)^{k-c} \in \mathcal{I} \), which implies that

\[
\mathcal{I} = \langle f_j(x)^a + u \sum_{\ell=0}^{b-1} A_{\ell}(x)f_j(x)^{\ell} + u^2 \sum_{k=0}^{p^s-1} B_k(x)f_j(x)^k, uf_j(x)^b + u^2q(x), u^2f_j(x)^c \rangle.
\]

Next we write \( u^2q(x) = u^2 \sum_{i=0}^{p^s-1} W_i(x)f_j(x)^i \). We further observe that \( \mathcal{I} = \langle f_j(x)^a + u \sum_{\ell=0}^{b-1} A_{\ell}(x)f_j(x)^{\ell} + u^2 \sum_{k=0}^{p^s-1} B_k(x)f_j(x)^k, uf_j(x)^b + u^2 \sum_{i=0}^{p^s-1} W_i(x)f_j(x)^i, u^2f_j(x)^c \rangle \). If \( u \sum_{\ell=0}^{b-1} A_{\ell}(x)f_j(x)^{\ell} \neq 0 \), then there exists a smallest integer \( t_1 \) satisfying \( 0 \leq t_1 < b \) and \( A_{t_1}(x) \neq 0 \), and we can write \( u \sum_{\ell=0}^{b-1} A_{\ell}(x)f_j(x)^{\ell} = uf_j(x)^{t_1}D_1(x) \), where \( D_1(x) = \sum_{\ell=t_1}^{b-1} A_{\ell}(x)f_j(x)^{\ell-t_1} \) is a unit in \( \mathcal{K}_j \). Moreover, if \( u^2 \sum_{k=0}^{p^s-1} B_k(x)f_j(x)^k \neq 0 \), then there exists a smallest integer \( t_2 \) satisfying \( 0 \leq t_2 < c \) and \( B_{t_2}(x) \neq 0 \), and we can write \( u^2 \sum_{k=0}^{p^s-1} B_k(x)f_j(x)^k =
$u^2 f_j(x)^{t_2} D_2(x)$, where $D_2(x) = \sum_{k=t_2}^{c-1} B_k(x) f_j(x)^{k-t_2}$ is a unit in $K_j$. Further, if $u^2 \sum_{i=0}^{c-1} W_i(x) f_j(x)^i \neq 0$, then there exists a smallest integer $\theta$ satisfying $0 \leq \theta < c$ and $W_\theta(x) \neq 0$, and we can write $u^2 \sum_{i=0}^{c-1} W_i(x) f_j(x)^i = u^2 f_j(x)^\theta V(x)$, where $V(x) = \sum_{i=0}^{c-1} W_i(x) f_j(x)^{i-\theta}$ is a unit in $K_j$. From this, it follows that

$$I = \langle f_j(x)^a + u f_j(x)^{t_1} D_1(x) + u^2 f_j(x)^{t_2} D_2(x), u f_j(x)^b + u^2 f_j(x)^\theta V(x), u^2 f_j(x)^c \rangle,$$

where $D_1(x)$ is either 0 or a unit in $K_j$ of the form $\sum_{k=t_1}^{b-1} A_k(x) f_j(x)^{k-t_1}$. $D_2(x)$ is either 0 or a unit in $K_j$ of the form $\sum_{k=t_2}^{c-1} B_k(x) f_j(x)^{k-t_2}$ and $V(x)$ is either 0 or a unit in $K_j$ of the form $\sum_{i=0}^{c-1} W_i(x) f_j(x)^{i-\theta}$ with $A_k(x), B_k(x), W_i(x) \in K_j$ for each $\ell, k$ and $i$.

In order to determine $\text{ann}(I)$, we first observe that $u f_j(x)^{p^\ell-a+t_1} D_1(x) + u^2 f_j(x)^{p^\ell-a+t_2} D_2(x) \in I$, which implies that $p^\ell - a + t_1 \geq b$ when $D_1(x) \neq 0$. Next we see that $f_j(x)^{p^\ell-b} \{ u f_j(x)^b + u^2 f_j(x)^\theta V(x) \} \in I$, which gives $p^\ell - b + \theta \geq c$ when $V(x) \neq 0$. Moreover, as $u f_j(x)^a + u^2 f_j(x)^{t_1} D_1(x) \in I$ and $f_j(x)^{p^\ell-b} \{ u f_j(x)^b + u^2 f_j(x)^\theta V(x) \} \in I$, we note that $u^2 \{ f_j(x)^{t_1} D_1(x) - f_j(x)^{a-b+\theta} V(x) \} \in I$, which implies that $u^2 \{ f_j(x)^{t_1} D_1(x) - f_j(x)^{a-b+\theta} V(x) \} \in (u^2 f_j(x)^c)$. From this, we obtain $u^2 f_j(x)^{p^\ell-c} \{ f_j(x)^{t_1} D_1(x) - f_j(x)^{a-b+\theta} V(x) \} = 0$.

Further, we see that $u f_j(x)^{p^\ell-a+t_1} D_1(x) + u^2 f_j(x)^{p^\ell-a+t_2} D_2(x) \in I$ can be rewritten as $f_j(x)^{p^\ell-a+t_1-b} D_1(x) \{ u f_j(x)^{b} + u^2 f_j(x)^{p^\ell-b} D_2(x) \} = u^2 f_j(x)^c A(x)$, where $A(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x) \rangle$. Now consider the ideal

$\mathcal{B}_3 = \langle f_j(x)^{p^\ell-c} - u f_j(x)^{p^\ell-c-b} A(x), u f_j(x)^{p^\ell-b} - u^2 f_j(x)^{p^\ell-a+t_1-b} D_1(x), u^2 f_j(x)^{p^\ell-a} \rangle$. Here we note that $|\mathcal{B}_3| \geq p^{md_j(a+b+c)}$ and $\mathcal{B}_3 \subseteq \text{ann}(I)$. Further, as

$$p^{md_j(3p^\ell-a-b-c)} = |I| = \frac{|K_j|}{|\text{ann}(I)|} \leq \frac{p^{3md_j p^\ell}}{|\mathcal{B}_3|} \leq p^{md_j(3p^\ell-a-b-c)},$$

we get $|\text{ann}(I)| = |\mathcal{B}_3| = p^{md_j(a+b+c)}$ and $\text{ann}(I) = \mathcal{B}_3$.

This completes the proof of the theorem.

In the following corollary, we obtain some isodual $\alpha$-constacyclic codes of length $np^s$ over $\mathcal{R}$ when the binomial $x^a - \alpha_0$ is irreducible over $\mathbb{F}_{p^m}$.

**Corollary 3.2.** Let $n \geq 1$ be an integer and $\alpha_0 \in \mathbb{F}_{p^m} \setminus \{0\}$ be such that the binomial $x^a - \alpha_0$ is irreducible over $\mathbb{F}_{p^m}$. Let $\alpha = \alpha_0^{p^s} \in \mathbb{F}_{p^m}$. Following the same notations as in Theorem 3.2, we have the following:

(a) There does not exist any isodual $\alpha$-constacyclic code of Type I over $\mathcal{R}$.

(b) There exists an isodual $\alpha$-constacyclic code of Type II over $\mathcal{R}$ if and only if $p = 2$. In fact, when $p = 2$, the code $\langle x^{a_0} - \alpha_0 \rangle^{2^{s-1}} \langle u \rangle$ is the only isodual $\alpha$-constacyclic code of Type II over $\mathcal{R}$.

(c) There exists an isodual $\alpha$-constacyclic code of Type III over $\mathcal{R}$ if and only if $p = 2$. Moreover, when $p = 2$, the codes $\mathcal{C} \subseteq \langle x^{a_0} - \alpha_0 \rangle^{2^{s-1}}, u^2 (x^{10} - \alpha_0^{2^{s-1}}), 2^{s-1} \leq a < 2^s$, are isodual $\alpha$-constacyclic codes of Type III over $\mathcal{R}$.

**Proof.** Let $\mathcal{C}$ be an $\alpha$-constacyclic code of length $np^s$ over $\mathcal{R}$. For the code $\mathcal{C}$ to be isodual, we must have $|\mathcal{C}| = |\mathcal{C}^\perp| = |\text{ann}(\mathcal{C})|$. 

10
(a) Let $C$ be of Type I, i.e., $C = \langle u^2(x^n - \alpha_0)^c \rangle$ for some integer $c$ satisfying $0 \leq c < p^s$. By Theorem 3.2, we see that $|C| = p^{mn(p^s-c)}$ and $|\text{ann}(C)| = p^{mn(2p^s+c)}$. Now if the code $C$ is isodual, then we must have $|C| = |\text{ann}(C)|$. This implies that $p^s + 2c = 0$, which is a contradiction. Hence there does not exist any isodual $\alpha$-constacyclic code of Type I over $R$.

(b) If the code $C$ is of Type II, then $C = \langle u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^t G(x) \rangle$, where $0 \leq c \leq b < p^s$ and $0 \leq t < c$ if $G(x) \neq 0$. By Theorem 3.2 we have $|C| = p^{mn(2p^s-b-c)}$, $|\text{ann}(C)| = (|C| - n)^{(t+1)} = p^{mn(p^s+c)}$. Now if the code $C$ is isodual, then we must have $|C| = |\text{ann}(C)|$, which gives $p = 2$ and $c = 2s - b$. Further, if the code $C$ is $R$-linearly equivalent to $\text{ann}(C)$, then $\text{Res}_u(\text{ann}(C)) = \langle (x^n - \alpha_0)^{2s} \rangle$, which implies that $c = 0$. This gives $b = 2s - 2s = 2s - 1$.

On the other hand, when $p = 2$, $c = 0$ and $b = 2s - 1$, by Theorem 3.2 again, we see that $C = \text{ann}(C)$ holds, which implies that the codes $C(\subseteq R_n)$ and $C(\subseteq R_n)$ are $R$-linearly equivalent.

(c) If the code $C$ is of Type III, then $C = \langle (x^n - \alpha_0)^a + u(x^n - \alpha_0)^t D_1(x) + u^2(x^n - \alpha_0)^t D_2(x), u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^t V(x), u^2(x^n - \alpha_0)^c \rangle$, where $0 \leq b \leq a < p^s$, $0 \leq t_1 < b$ if $D_1(x) \neq 0$, $0 \leq t_2 < c$ if $D_2(x) \neq 0$ and $0 \leq \theta < c$ if $V(x) \neq 0$.

Here by Theorem 3.2 we have $|C| = p^{mn(3p^s-a-b-c)}$ and $|\text{ann}(C)| = p^{mn(a+b+c)}$. From this, we see that if the code $C$ is isodual, then we must have $3p^s = 2(a + b + c)$, which implies that $p = 2$.

On the other hand, when $p = 2$, we see, by Theorem 3.2 again, that for $2s - 1 \leq a < 2s$, the code $C = \langle (x^n - \alpha_0)^a + u^2(x^n - \alpha_0)^t D_2(x), u(x^n - \alpha_0)^{2s-m} - u^2(x^n - \alpha_0)^c \rangle$ satisfies $C = \text{ann}(C)$, from which part (c) follows.

In the following theorem, we consider the case $\beta = 0$ and $\gamma \neq 0$, and we determine all non-trivial ideals of the ring $K_j$, their orthogonal complements and their cardinalities.

**Theorem 3.3.** Let $\beta = 0$ and $\gamma$ be a non-zero element of $\mathbb{F}_{p^s}$. Let $I$ be a non-trivial ideal of the ring $K_j$ with $\text{Res}_u(I) = \langle f_j(x)^a \rangle$, $\text{Tor}_n(I) = \langle f_j(x)^b \rangle$ and $\text{Tor}_2(I) = \langle f_j(x)^c \rangle$ for some integers $a, b, c$ satisfying $0 \leq c \leq b \leq a < p^s$. Suppose that $B_i(x), C_k(x), Q_\ell(x), W_e(x)$ run over $\mathcal{P}_{d_j}(\mathbb{F}_{p^s})$ for each relevant $i, k, \ell$ and $e$. Then the following hold.

**Type I:** When $a = b = p^s$, we have

$$I = \langle a^2 f_j(x)^c \rangle,$$

where $0 \leq c < p^s$. Moreover, we have

$$|I| = p^{md_j(p^s-c)} \quad \text{and} \quad \text{ann}(I) = \langle f_j(x)^{p^s-c}, u \rangle.$$

**Type II:** When $a = p^s$ and $b < p^s$, we have

$$I = \langle u f_j(x)^b + u^2 f_j(x)^t G(x), u^2 f_j(x)^c \rangle,$$

where $c + b - p^s \leq t < c$ if $G(x) \neq 0$ and $G(x)$ is either 0 or a unit in $K_j$ of the form $\sum_{i=0}^{c-1} B_i(x) f_j(x)^i$. Moreover, we have

$$|I| = p^{md_j(2p^s-b-c)} \quad \text{and} \quad \text{ann}(I) = \langle f_j(x)^{p^s-c} - u f_j(x)^{p^s-c+t-b} G(x), u f_j(x)^{p^s-b}, u^2 \rangle.$$

**Type III:** When $a < p^s$, we have

$$I = \langle f_j(x)^a + u f_j(x)^t D_1(x) + u^2 f_j(x)^t D_2(x), u f_j(x)^b + u^2 f_j(x)^c \rangle,$$

where $0 \leq c < p^s$ and $G(x) \neq 0$.
where \( a + b - p^s \leq t_1 < b \) if \( D_1(x) \neq 0 \), \( 0 \leq t_2 < c \) if \( D_2(x) \neq 0 \), \( b + c - p^s \leq \theta < c \) if \( V(x) \neq 0 \), \( D_1(x) \) is either 0 or a unit in \( K_j \) of the form \( \sum_{k=0}^{c-t_2-1} C_k(x) f_j(x)^k \), \( D_2(x) \) is either 0 or a unit in \( K_j \) of the form \( \sum_{k=0}^{c-\theta-1} W_k(x) f_j(x)^k \). Furthermore, we have \( u^2(h_j(x) + f_j(x)^{p^s-a+t_1-b+\theta} V(x) D_1(x) - f_j(x)^{p^s-a+t_2} D_2(x)) \in \langle u^2 f_j(x)^c \rangle \), i.e., there exists \( B(x) \in F_{p^m}[x]/\langle f_j(x)^p \rangle \) such that \( u^2 (h_j(x) + f_j(x)^{p^s-a+t_1-b+\theta} V(x) D_1(x) - f_j(x)^{p^s-a+t_2} D_2(x)) = u^2 f_j(x)^c B(x) \). Moreover, we have
\[
|\mathcal{I}| = p^{md_1}(3p^s-a-b-c)
\]
and the annihilator of \( \mathcal{I} \) is given by
\[
\text{ann}(\mathcal{I}) = \langle f_j(x)^{p^s-c} - u f_j(x)^{p^s-c+\theta} V(x) + u^2 B(x), u f_j(x)^{p^s-b} - u^2 f_j(x)^{p^s-a+\theta} D_1(x), u^2 f_j(x)^{p^s-a} \rangle.
\]

Proof. Working as in Theorem 3.2 and by applying Lemmas 3.2(c) and 3.3 the desired result follows. □

In the following corollary, we list some isodual \((\alpha + \gamma u^2)\)-constacyclic codes of length \( np^s \) over \( \mathcal{R} \) when \( \beta = 0, \gamma \neq 0 \) and the binomial \( x^n - \alpha_0 \) is irreducible over \( F_{p^m} \).

Corollary 3.3. Let \( n \geq 1 \) be an integer and \( \alpha_0 \in F_{p^m} \setminus \{0\} \) be such that the binomial \( x^n - \alpha_0 \) is irreducible over \( F_{p^m} \). Let \( \alpha = \alpha_0^\gamma \in F_{p^m} \), and let \( \gamma \) be a non-zero element of \( F_{p^m} \). Following the same notations as in Theorem 3.3, we have the following:

(a) There does not exist any isodual \((\alpha + \gamma u^2)\)-constacyclic code of Type I over \( \mathcal{R} \).

(b) There exists an isodual \((\alpha + \gamma u^2)\)-constacyclic code of Type II over \( \mathcal{R} \) if and only if \( p = 2 \). Furthermore, when \( p = 2 \), the code \( \langle u(x^n - \alpha_0)^{2r-1}, u^2 \rangle \) is the only isodual \((\alpha + \gamma u^2)\)-constacyclic code of Type II over \( \mathcal{R} \).

(c) There exists an isodual \((\alpha + \gamma u^2)\)-constacyclic code of Type III over \( \mathcal{R} \) if and only if \( p = 2 \). Furthermore, when \( p = 2 \), the codes \( \mathcal{C} = \langle (x^n - \alpha_0)^a + u(x^n - \alpha_0)^{a-2^{r-1}} \gamma x^{2^{r-1}}, u^2(x^n - \alpha_0)^{2s-1} + u^2 \gamma x^{2^{r-1}}, u^2(x^n - \alpha_0)^{2s-1} \rangle, 2s-1 \leq a < 2^r \), are isodual \((\alpha + \gamma u^2)\)-constacyclic codes of Type III over \( \mathcal{R} \).

Proof. Working in a similar manner as in Corollary 3.2 and by applying Theorem 3.3 the desired result follows. □

4 Hamming distances, RT distances and RT weight distributions

Throughout this section, let \( n \geq 1 \) be an integer and \( \alpha_0 \in F_{p^m} \setminus \{0\} \) be such that the binomial \( x^n - \alpha_0 \) is irreducible over \( F_{p^m} \). Let \( \alpha = \alpha_0^\gamma \) and \( \beta, \gamma \in F_{p^m} \). When \( \beta \neq 0 \), Sharma & Sidana [20] explicitly determined Hamming distances, RT distances and RT weight distributions of all repeated-root \((\alpha + \beta u + \gamma u^2)\)-constacyclic codes over \( \mathcal{R} \). In this section, we shall consider the case \( \beta = 0 \), and we shall determine Hamming distances, RT distances and RT weight distributions of all non-trivial \((\alpha + \gamma u^2)\)-constacyclic codes of length \( np^s \) over \( \mathcal{R} \).

Now let \( \mathcal{C} \) be an \((\alpha + \gamma u^2)\)-constacyclic code of length \( np^s \) over \( \mathcal{R} \). It is easy to see that \( d_H(\mathcal{C}) = d_{RT}(\mathcal{C}) = 0 \) when \( \mathcal{C} = 0 \), while \( d_H(\mathcal{C}) = d_{RT}(\mathcal{C}) = 1 \) when \( \mathcal{C} = \langle 1 \rangle \). In the following theorem, we determine Hamming distances of all non-trivial \((\alpha + \gamma u^2)\)-constacyclic codes of length \( np^s \) over \( \mathcal{R} \).

Theorem 4.1. Let \( \mathcal{C} \) be a non-trivial \((\alpha + \gamma u^2)\)-constacyclic code of length \( np^s \) over \( \mathcal{R} \) with \( \text{Tor}_{\gamma}(\mathcal{C}) = \langle (x^n - \alpha_0)^c \rangle \) for some integer \( c \) satisfying \( 0 \leq c < p^s \) (as determined in Theorems 3.2 and 3.3). Then the Hamming distance \( d_H(\mathcal{C}) \) of the code \( \mathcal{C} \) is given by
\[
d_H(\mathcal{C}) = \begin{cases} 
1 & \text{if } c = 0; \\
\ell + 2 & \text{if } \ell p^{s-1} + 1 \leq c \leq (\ell + 1) p^{s-1} \text{ with } 0 \leq \ell \leq p - 2; \\
(i + 1) p^k & \text{if } p^{s-k} + (i - 1) p^{s-k-1} + 1 \leq c \leq p^{s-k} + i p^{s-k-1} \text{ with } 1 \leq i \leq p - 1 \text{ and } 1 \leq k \leq s - 1.
\end{cases}
\]
Proof. To prove the result, we assert that

$$d_H(C) = d_H(\text{Torr}_{u^2}(C)).$$

To prove this assertion, we note that \( \langle u^2(x^n - \alpha_0)^c \rangle \subseteq C \), which implies that

$$d_H(\langle u^2(x^n - \alpha_0)^c \rangle) \geq d_H(C).$$

Next we observe that

$$w_H(Q(x)) \geq w_H(uQ(x))$$

for each \( Q(x) \in \mathcal{R}_{\alpha+\gamma u^2} \).

When \( C \) is of Type I, we have \( C = \langle u^2(x^n - \alpha_0)^c \rangle \). Here we have \( d_H(C) = d_H(\langle u^2(x^n - \alpha_0)^c \rangle) \).

When \( C \) is of Type II, we have \( C = \langle u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^4G(x), u^2(x^n - \alpha_0)^c \rangle \), where \( c \leq b < p^s \), \( c + b - p^s \leq t < c \) if \( G(x) \neq 0 \) and \( G(x) \) is either 0 or a unit in \( \mathbb{F}_{p^n}[x]/(f_j(x)^{p^s}) \). Here for each codeword \( Q(x) \in C \setminus \langle u^2(x^n - \alpha_0)^c \rangle \), we see, by (i), that \( w_H(Q(x)) \geq w_H(uQ(x)) \geq d_H(\langle u^2(x^n - \alpha_0)^c \rangle) \). From this, we obtain \( d_H(C) \geq d_H(\langle u^2(x^n - \alpha_0)^c \rangle) \).

When \( C \) is of Type III, we have \( C = \langle (x^n - \alpha_0)^a + u(x^n - \alpha_0)^t D_1(x) + u^2(x^n - \alpha_0)^t D_2(x), u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^6V(x), u^2(x^n - \alpha_0)^c \rangle \), where \( c \leq b < p^s \), \( a + b - p^s \leq t_1 < b \) if \( D_1(x) \neq 0 \), \( 0 \leq t_2 < c \) if \( D_2(x) \neq 0 \), \( b + c - p^s \leq \theta < c \) if \( V(x) \neq 0 \) and \( D_1(x), D_2(x), V(x) \) are either 0 or a units in \( \mathbb{F}_{p^n}[x]/(f_j(x)^{p^s}) \). Here for each codeword \( Q(x) \in C \setminus \langle u^2(x^n - \alpha_0)^c \rangle \) and \( Q(x) \in \langle u \rangle \), by (ii), we see that \( w_H(Q(x)) \geq w_H(uQ(x)) \geq d_H(\langle u^2(x^n - \alpha_0)^c \rangle) \). Further, for a codeword \( Q(x) \in C \setminus \langle u \rangle \), by (iii) again, we note that \( w_H(Q(x)) \geq w_H(u^2Q(x)) \geq d_H(\langle u^2(x^n - \alpha_0)^c \rangle) \). This implies that \( d_H(C) \geq d_H(\langle u^2(x^n - \alpha_0)^c \rangle) \).

From this and by (iii), we get \( d_H(C) = d_H(\langle u^2(x^n - \alpha_0)^c \rangle) \). Further, we observe that \( d_H(\langle u^2(x^n - \alpha_0)^c \rangle) = d_H(\text{Torr}_{u^2}(C)) \), from which the assertion (ii) follows. Now by applying Theorem 2.1 we get the desired result.

In the following theorem, we determine RT distances of all non-trivial \( (\alpha+\gamma u^2) \)-constacyclic codes of length \( np^s \) over \( \mathcal{R} \).

**Theorem 4.2.** Let \( C \) be a non-trivial \( (\alpha+\gamma u^2) \)-constacyclic code of length \( np^s \) over \( \mathcal{R} \) with \( \text{Torr}_{u^2}(C) = \langle (x^n - \alpha_0)^c \rangle \) for some integer \( c \) satisfying \( 0 \leq c < p^s \) (as determined in Theorems 2.2 and 2.3). Then the RT distance \( d_{RT}(C) \) of the code \( C \) is given by

$$d_{RT}(C) = nc + 1.$$

**Proof.** To prove the result, we first observe that

$$w_{RT}(Q(x)) \geq w_{RT}(uQ(x))$$

for each \( Q(x) \in \mathcal{R}_{\alpha+\gamma u^2} \).

(i) When \( C \) is of Type I, we have \( C = \langle u^2(x^n - \alpha_0)^c \rangle \). Here we note that \( C = \langle u^2(x^n - \alpha_0)^c \rangle = \{ u^2(x^n - \alpha_0)^c f(x) \mid f(x) \in \mathbb{F}_{p^n}[x] \} \). Now for each non-zero \( Q(x) \in C \), by (7), we see that \( w_{RT}(Q(x)) \geq w_{RT}(u^2(x^n - \alpha_0)^c) = nc + 1 \), which implies that \( d_{RT}(C) \geq nc + 1 \). Since \( u^2(x^n - \alpha_0)^c \in C \), we obtain \( d_{RT}(C) = nc + 1 \).

(ii) When \( C \) is of Type II, we have \( C = \langle u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^4G(x), u^2(x^n - \alpha_0)^c \rangle \), where \( c \leq b < p^s \), \( c + b - p^s \leq t < c \) if \( G(x) \neq 0 \) and \( G(x) \) is either 0 or a unit in \( \mathbb{F}_{p^n}[x]/(f_j(x)^{p^s}) \). Here by (7), we note that \( w_{RT}(Q(x)) \geq w_{RT}(uQ(x)) \) for each \( Q(x) \in C \setminus \langle u \rangle \), which implies that \( w_{RT}(Q(x)) \geq d_{RT}(u^2(x^n - \alpha_0)^c) \) for each \( Q(x) \in C \setminus \langle u^2 \rangle \). From this, we get \( d_{RT}(C) \geq d_{RT}(u^2(x^n - \alpha_0)^c) \). Since \( u^2(x^n - \alpha_0)^c \subseteq C \), we have \( d_{RT}(u^2(x^n - \alpha_0)^c) \geq d_{RT}(C) \). This implies that \( d_{RT}(C) = d_{RT}(u^2(x^n - \alpha_0)^c) \). From this and by case (i), we get \( d_{RT}(C) = nc + 1 \).

(iii) When \( C \) is of Type III, we have \( C = \langle (x^n - \alpha_0)^a + u(x^n - \alpha_0)^t D_1(x) + u^2(x^n - \alpha_0)^t D_2(x), u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^6V(x), u^2(x^n - \alpha_0)^c \rangle \), where \( c \leq b \leq a < p^s \), \( a + b - p^s \leq t_1 < b \) if \( D_1(x) \neq 0 \), \( 0 \leq t_2 < c \) if \( D_2(x) \neq 0 \), \( b + c - p^s \leq \theta < c \) if \( V(x) \neq 0 \) and \( D_1(x), D_2(x), V(x) \) are either 0 or a units in \( \mathbb{F}_{p^n}[x]/(f_j(x)^{p^s}) \). For each \( Q(x) \in C \setminus \langle u \rangle \), by (7), we see that \( w_{RT}(Q(x)) \geq w_{RT}(u^2Q(x)) \). From this, we get
$w_{RT}(Q(x)) \geq d_{RT}(u^2(x^n - \alpha_0)^c)$ for each $Q(x) \in \mathcal{C} \setminus \langle u \rangle$. Further, for a codeword $Q(x) \in \mathcal{C} \setminus \langle u^2(x^n - \alpha_0)^c \rangle$ with $Q(x) \notin \langle u \rangle$, by (17) again, we see that $w_{RT}(Q(x)) \geq w_{RT}(uQ(x)) \geq d_{RT}(u^2(x^n - \alpha_0)^c)$. This implies that $d_{RT}(\mathcal{C}) \geq d_{RT}(u^2(x^n - \alpha_0)^c)$. On the other hand, as $\langle u^2(x^n - \alpha_0)^c \rangle \subseteq \mathcal{C}$, we have $d_{RT}(u^2(x^n - \alpha_0)^c) \geq d_{RT}(\mathcal{C})$, which implies that $d_{RT}(\mathcal{C}) = d_{RT}(u^2(x^n - \alpha_0)^c)$. From this and by case (i), we get $d_{RT}(\mathcal{C}) = nc + 1$.

This completes the proof of the theorem. □

In the following theorem, we determine RT weight distributions of all $(\alpha + \gamma u^2)$-constacyclic codes of length $np^s$ over $\mathcal{R}$.

**Theorem 4.3.** Let $\mathcal{C}$ be an $(\alpha + \gamma u^2)$-constacyclic code of length $np^s$ over $\mathcal{R}$ with Res$_u(\mathcal{C}) = \langle (x^n - \alpha_0)^a \rangle$, Tor$_u(\mathcal{C}) = \langle (x^n - \alpha_0)^b \rangle$ and Tor$_a(\mathcal{C}) = \langle (x^n - \alpha_0)^c \rangle$ for some integers $a, b, c$ satisfying $0 \leq c \leq b \leq a \leq p^s$ (as determined in Theorems 3.2 and 3.3). For $0 \leq \rho \leq np^s$, let $A_\rho$ denote the number of codewords in $\mathcal{C}$ having the RT weight as $\rho$.

(a) If $\mathcal{C} = \langle \emptyset \rangle$, then we have $A_0 = 1$ and $A_\rho = 0$ for $1 \leq \rho \leq np^s$.

(b) If $\mathcal{C} = \langle 1 \rangle$, then we have $A_0 = 1$ and $A_\rho = (p^{\rho m} - 1)p^{\rho n(n-1)}$ for $1 \leq \rho \leq np^s$.

(c) If $\mathcal{C} = \langle u^2(x^n - \alpha_0)^c \rangle$ is of Type I, then we have

$$A_\rho = \begin{cases} 1 & \text{if } \rho = 0; \\ 0 & \text{if } 1 \leq \rho \leq nc; \\ (p^m - 1)p^{\rho(n-nc-1)} & \text{if } nc + 1 \leq \rho \leq np^s. \end{cases}$$

(d) If $\mathcal{C} = \langle u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^c \rangle$ is of Type II, then we have

$$A_\rho = \begin{cases} 1 & \text{if } \rho = 0; \\ 0 & \text{if } 1 \leq \rho \leq nc; \\ (p^m - 1)p^{\rho(n-nc-1)} & \text{if } nc + 1 \leq \rho \leq nb; \\ (p^{2m} - 1)p^{\rho(2n-nb-nc-2)} & \text{if } nb + 1 \leq \rho \leq np^s. \end{cases}$$

(e) If $\mathcal{C} = \langle (x^n - \alpha_0)^a + u(x^n - \alpha_0)^b D_1(x) + u^2(x^n - \alpha_0)^c D_2(x), u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^b V(x), u^2(x^n - \alpha_0)^c \rangle$ is of Type III, then we have

$$A_\rho = \begin{cases} 1 & \text{if } \rho = 0; \\ 0 & \text{if } 1 \leq \rho \leq nc; \\ (p^m - 1)p^{\rho(n-nc-1)} & \text{if } nc + 1 \leq \rho \leq nb; \\ (p^{2m} - 1)p^{\rho(2n-nb-nc-2)} & \text{if } nb + 1 \leq \rho \leq na; \\ (p^{3m} - 1)p^{\rho(3n-na-nb-nc-3)} & \text{if } na + 1 \leq \rho \leq np^s. \end{cases}$$

**Proof.** Proofs of parts (a) and (b) are trivial. To prove parts (c)-(e), by Theorem 4.2(c), we see that $d_{RT}(\mathcal{C}) = nc + 1$, which implies that $A_\rho = 0$ for $1 \leq \rho \leq nc$. So from now on, we assume that $nc + 1 \leq \rho \leq np^s$.

To prove (c), let $\mathcal{C} = \langle u^2(x^n - \alpha_0)^c \rangle$. Here we see that $\mathcal{C} = \langle u^2(x^n - \alpha_0)^c \rangle = \{u^2(x^n - \alpha_0)^c F(x) \mid F(x) \in F_{p^m}[x]\}$. This implies that the codeword $u^2(x^n - \alpha_0)^c F(x) \in \mathcal{C}$ has RT weight $\rho$ if and only if $\deg F(x) = \rho - nc - 1$. From this, we obtain $A_\rho = (p^m - 1)p^{\rho(n-nc-1)}$.

To prove (d), let $\mathcal{C} = \langle u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^b G(x), u^2(x^n - \alpha_0)^c \rangle$. Here we observe that each codeword $Q(x) \in \mathcal{C}$ can be uniquely expressed as $Q(x) = (u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^b G(x)) A_Q(x) + u^2(x^n - \alpha_0)^b B_Q(x)$, where $A_Q(x), B_Q(x) \in F_{p^m}[x]$ satisfy $\deg A_Q(x) \leq n(p^s - b) - 1$ if $A_Q(x) \neq 0$ and $\deg B_Q(x) \leq n(p^s - c) - 1$ if $B_Q(x) \neq 0$. From this, we see that if $nc + 1 \leq \rho \leq nb$, then the RT weight of the codeword $Q(x) \in \mathcal{C}$ is $\rho$ if and only if $A_Q(x) = 0$ and $\deg B_Q(x) = \rho - nc - 1$. This implies that $A_\rho = (p^m - 1)p^{\rho(n-nc-1)}$ for $nc + 1 \leq \rho \leq nb$. Further, if $nb + 1 \leq \rho \leq np^s$, then the RT weight of the codeword $Q(x) \in \mathcal{C}$ is $\rho$ if and only if one of the following two conditions are satisfied: (i) $\deg A_Q(x) = \rho - nb - 1$ and $B_Q(x)$ is either 0 or $\deg B_Q(x) \leq \rho - nc - 1$ and (ii) $A_Q(x)$
is either 0 or \(\deg A_\theta(x) \leq p - nb - 2\) and \(\deg B_\theta(x) = p - nc - 1\). From this, we get \(A_\rho = (p^{2m} - 1)p^{m(2p - nb - nc - 2)}\) for \(nb + 1 \leq \rho \leq np^s\).

To prove (e), let \(C = \langle (x^n - \alpha^n)^a + u(x^n - \alpha^n)^{ib}D_1(x) + u^2(x^n - \alpha^n)^{ib}D_2(x), u(x^n - \alpha^n)^b + u^2(x^n - \alpha^n)^9V(x), u^2(x^n - \alpha^n)^c \rangle\). Here, we see that each codeword \(Q(x) \in C\) can be uniquely expressed as \(Q(x) = ((x^n - \alpha^n)^a + u(x^n - \alpha^n)^{ib}D_1(x) + u^2(x^n - \alpha^n)^{ib}D_2(x))M_Q(x) + (u(x^n - \alpha^n)^b + u^2(x^n - \alpha^n)^9V(x))N_Q(x) + u^2(x^n - \alpha^n)^cW_Q(x)\), where \(M_Q(x), N_Q(x), W_Q(x) \in \mathbb{F}^{pm}\) satisfy \(\deg M_Q(x) \leq n(p^s - a) - 1\) if \(M_Q(x) \neq 0\), \(\deg N_Q(x) \leq n(p^s - b) - 1\) if \(N_Q(x) \neq 0\), and \(\deg W_Q(x) \leq n(p^s - c) - 1\) if \(W_Q(x) \neq 0\). From this, we see that if \(nc + 1 \leq \rho \leq na\), then the codeword \(Q(x) \in C\) has RT weight \(\rho\) if and only if \(M_Q(x) = N_Q(x) = 0\) and \(\deg W_Q(x) = p - nc - 1\). This implies that \(A_\rho = (p^{2m} - 1)p^{m(p - nc - 1)}\) for \(nc + 1 \leq \rho \leq na\). Further, if \(nb + 1 \leq \rho \leq na\), then the RT weight of the codeword \(Q(x) \in C\) is \(\rho\) if and only if \(M_Q(x) = 0\) and one of the following two conditions are satisfied: (i) \(\deg N_Q(x) = p - nb - 1\) and \(\deg W_Q(x) = p - 1 - nc\); and (ii) \(N_Q(x) = 0\) or \(\deg N_Q(x) \leq p - nb - 2\) and \(\deg W_Q(x) = p - nc - 1\). This implies that \(A_\rho = (p^{2m} - 1)p^{m(2p - na - nb - 2)}\) for \(nb + 1 \leq \rho \leq np^s\). Here the RT weight of the codeword \(Q(x) \in C\) is \(\rho\) if and only if one of the following three conditions are satisfied: (i) \(\deg M_Q(x) = p - na - 1\), \(N_Q(x) = 0\), and \(\deg W_Q(x) = p - nb - 1\); and \(\deg M_Q(x) = 0\) or \(\deg M_Q(x) \leq p - na - 2\), \(\deg N_Q(x) = p - nb - 1\), and \(\deg W_Q(x) = p - nc - 1\); and (iii) \(M_Q(x) = 0\), \(\deg M_Q(x) \leq p - na - 2\), \(\deg N_Q(x) = 0\), and \(\deg W_Q(x) = p - nb - 2\). This implies that \(A_\rho = (p^{3m} - 1)p^{m(3p - na - nb - nc - 3)}\) for \(na + 1 \leq \rho \leq np^s\).

This completes the proof of the theorem. \(\square\)

5 Conclusion and Future work

Let \(p\) be a prime, \(n, s, m\) be positive integers with \(\gcd(n, p) = 1\), \(\mathbb{F}_{pm}\) be the finite field of order \(p^m\), and let \(R = \mathbb{F}_{pm}[u]/(u^3)\) be the finite commutative ring chain ring with unity. Let \(\alpha, \beta, \gamma \in \mathbb{F}_{pm}\) and \(\alpha \neq 0\). When \(\alpha\) is an \(n\)th power of an element in \(\mathbb{F}_{pm}\) and \(\beta \neq 0\), one can determine all \((\alpha + \beta u + \gamma u^2)\)-constacyclic codes of length \(np^s\) over \(R\) by applying the results derived in Cao [7] and by establishing a ring isomorphism from \(R[x]/(x^{np^s} - 1 - \alpha^{-1}\beta u - \alpha^{-1}\gamma u^2)\) onto \(R[x]/(x^{np^s} - \alpha - \beta u - \gamma u^2)\). However, when \(\alpha\) is not an \(n\)th power of an element in \(\mathbb{F}_{pm}\) and \(\beta \neq 0\), algebraic structures of all \((\alpha + \beta u + \gamma u^2)\)-constacyclic codes of length \(np^s\) over \(R\) and their dual codes were not established. In this paper, we determined all \((\alpha + \beta u + \gamma u^2)\)-constacyclic codes of length \(np^s\) over \(R\) and their dual codes when \(\beta \neq 0\). We also considered the case \(\beta = 0\) in this paper, and we determined all \((\alpha + \gamma u^2)\)-constacyclic codes of length \(np^s\) over \(R\) and their dual codes. We also listed some isodual \((\alpha + \beta u + \gamma u^2)\)-constacyclic codes of length \(np^s\) over \(R\) when the binomial \(x^n - \alpha_0\) is irreducible over \(\mathbb{F}_{pm}\).

In another work [20], we obtained Hamming distances, RT distances and RT weight distributions of \((\alpha + \beta u + \gamma u^2)\)-constacyclic codes of length \(np^s\) over \(R\) when the binomial \(x^n - \alpha_0\) is irreducible over \(\mathbb{F}_{pm}\) and \(\beta\) is non-zero. In this case, we considered the case \(\beta = 0\) and we explicitly determined these parameters for all \((\alpha + \gamma u^2)\)-constacyclic codes of length \(np^s\) over \(R\), provided the binomial \(x^n - \alpha_0\) is irreducible over \(\mathbb{F}_{pm}\). Another interesting problem would be to study their duality properties and to determine their homogeneous distances.

References
[1] M. M. Al-Ashker, Simplex codes over the ring \(\mathbb{F}_2 + u\mathbb{F}_2\), Arab. J. Sci. Eng. Sect. A Sci. 30(2), pp. 277-285 (2005).
[2] E. Bannai, M. Harada, T. Ibukiyama, A. Munemasa and M. Oura, Type II codes over \(\mathbb{F}_2 + u\mathbb{F}_2\) and applications to Hermitian modular forms, Abh. Math. Semin. Univ. Hambg. 73(1), pp. 13-42 (2003).
[3] A. Batoul, K. Guenda and T. A. Gulliver, Some constacyclic codes over finite chain rings, arXiv:1212.3704v1 [cs.IT].

[4] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill Book Company, New York (1968).

[5] A. Bonnecaze and P. Udaya, Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory 45(4), pp. 1250-1255 (1999).

[6] A. R. Calderbank, A. R. Hammons Jr., P. V. Kumar, N. J. A. Sloane and P. Solé, A linear construction for certain Kerdock and Preparata codes, Bull. Amer. Math. Soc. 29, pp. 218-222 (1993).

[7] Y. Cao, On constacyclic codes over finite chain rings, Finite Fields Appl. 24, pp. 124-135 (2013).

[8] Y. Cao, Y. Cao, J. Gao and F. Fu, Constacyclic codes of length $p^n$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, arXiv:1512.0140v1 [cs.IT] (2015).

[9] 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, pp. 108-130 (2016).

[10] H. Q. Dinh, Constacyclic codes of length $p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, J. Algebra 324(5), pp. 940-950 (2010).

[11] 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, pp. 178-201 (2015).

[12] H. Dinh and S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory 50(8), pp. 1728-1744 (2004).

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

[14] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory 40(2), pp. 301-319 (1994).

[15] W. C. Huffman, On the decomposition of self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ with an automorphism of odd prime order, Finite Fields Appl. 13(3), pp. 681-712 (2007).

[16] 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. 34B(3), pp. 829-839 (2014).

[17] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press (2000).

[18] A. A. Nechaev, Kerdock code in a cyclic form, Discrete Math. Appl. 1, pp. 365-384 (1991).

[19] A. Sharma and S. Rani, Constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, arXiv:1707.06133 [cs.IT].

[20] A. Sharma and T. Sidana, Repeated-root constacyclic codes over finite commutative chain rings and their distances, submitted.

[21] R. Sobhani, Complete classification of $(\delta + au^2)$-constacyclic codes of length $p^k$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$, Finite Fields Appl. 34, pp. 123-138 (2015).

[22] P. Udaya and A. Bonnecaze, Decoding of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory 45(6), pp. 2148-2157 (1999).

[23] W. Zhao, X. Tang and Z. Gu, All $(\alpha + \beta u)$-constacyclic codes of length $np^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, arXiv:1606.06428v1 [cs.IT].