IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received May 8, 2020, accepted May 28, 2020, date of publication June 1, 2020, date of current version June 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2998836

Repeated-Root Constacyclic Codes Over the Chain Ring $\mathbb{F}_{p^m}[u]/\langle u^3 \rangle$

TANIA SIDANA AND ANURADHA SHARMA
Department of Mathematics, IIIT-Delhi, New Delhi 110020, India
Corresponding author: Anuradha Sharma (anuradha@iiitd.ac.in)

This work was supported by the Science and Engineering Research Board (SERB), India, under Grant EMR/2017/000662.

ABSTRACT Let $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3 \rangle$ be the finite commutative chain ring, 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 $\mathcal{R}$ and their dual codes. We also determine the number of codewords in each repeated-root constacyclic code over $\mathcal{R}$. We also obtain Hamming distances, RT distances, RT weight distributions and ranks (i.e., cardinalities of minimal generating sets) of some repeated-root constacyclic codes over $\mathcal{R}$. Using these results, we also identify some isodual and maximum distance separable (MDS) constacyclic codes over $\mathcal{R}$ with respect to the Hamming and RT metrics.

INDEX TERMS Cyclic codes, local rings, negacyclic codes, optimal codes.

I. INTRODUCTION

Constructing codes that are easy to encode and decode, can detect and correct many errors and have a sufficiently large number of codewords is the primary aim of coding theory. Several metrics (e.g. Hamming metric, Lee metric, RT metric, etc.) have been introduced to study error-detecting and error-correcting properties of a code with respect to various communication channels. Among the prevalent metrics in coding theory, the Hamming metric is the most studied metric and it is suitable for orthogonal modulated channels. The Singleton bound [31] is an upper bound on the size M of an arbitrary block code with respect to the Hamming metric:

$$M \leq q^{n-d+1}, \tag{1}$$

where q is the cardinality of the code alphabet, n is the block length and d is the Hamming distance of the code. Linear codes that attain the Singleton bound are called maximum distance separable (MDS) codes with respect to the Hamming metric. Later, motivated by the problem to transmit messages over several parallel communication channels with some channels not available for transmission, a non-Hamming metric, called the Rosenbloom-Tsfasman metric (or RT metric), was introduced by Rosenbloom and Tsfasman [30]; they also derived Singleton bound for the RT metric. Linear codes that attain the Singleton bound for the RT metric are called MDS codes with respect to the RT metric. MDS codes have the highest possible error-detecting and error-correcting capabilities for given code length, code size and alphabet size, hence they are considered optimal codes in that sense. This has encouraged many coding theorists to further study and construct MDS codes with respect to various metrics (see [20], [23], [39]). Recently, Li and Yue [24] determined Hamming distances of all repeated-root cyclic codes of length $5p^s$ over $\mathbb{F}_{p^m}$ and identified all MDS codes within this class of codes, where p is a prime, s, m are positive integers and $\mathbb{F}_{p^m}$ is the finite field of order p^m. In this paper, we shall also find MDS codes with respect to Hamming and RT metrics within the family of constacyclic codes over $\mathbb{F}_{p^m}[u]/\langle u^3 \rangle$.

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. For recent works on constacyclic codes over finite fields, please refer to [32], [33], [37]. Calderbank *et al.* [6], Hammons *et al.* [21] and Nechaev [28] 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 [17] studied algebraic structures of simple-root cyclic and negacyclic codes over finite commutative chain rings and their dual codes. In the same work, they also determined all

The associate editor coordinating the review of this manuscript and approving it for publication was Zesong Fei.

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 λ is an nth power of a unit in a finite commutative chain ring R, repeated-root λ-constacyclic codes of length n over R are equivalent to cyclic codes of the same length over R. Apart from this, many authors [1], [2], [5], [22], [36] 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 [15] 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.* [14] and Liu and Xu [25] 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. Using a technique different from that employed in [14], [15], [25], Cao *et al.* [8] determined all α-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 α 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.* [38] determined all $(\alpha+\beta v)$-constacyclic codes of length np^s over $\mathbb{F}_{p^m}[v]/\langle v^2\rangle$ and their dual codes, where n is a positive integer coprime to p, and α, β are non-zero elements of $\mathbb{F}_{p^m}$. This completely solved the problem of determination of all constacyclic codes of length np^s over $\mathbb{F}_{p^m}[v]/\langle v^2\rangle$ and their dual codes, where n is a positive integer coprime to p. In a recent work [34], we determined all repeated-root constacyclic codes of arbitrary lengths over the Galois ring $GR(p^2, m)$ of characteristic p^2 and cardinality p^{2m}, their sizes and their dual codes. In the same work, we also listed some isodual repeated-root constacyclic codes over $GR(p^2, m)$.

In a related work, Cao [7] 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.* [18] 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 α, a are units in R. The results obtained in Dinh *et al.* [18] can also be obtained from the work of Cao [7] via the ring isomorphism from $R[x]/\langle x^{p^s} - 1 - a\alpha^{-1}w\rangle$ onto $R[x]/\langle x^{p^s} - textalpha - aw\rangle$, defined as $A(x) \mapsto A(\alpha_0^{-1}x)$ for each $A(x) \in R[x]/\langle x^{p^s} - 1 - a\alpha^{-1}w\rangle$, where $\alpha = \alpha_0^{p^s}$ (such an element α_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, 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, there are repeated-root constacyclic codes over R, which are direct sums of non-principal ideals. In another related work, Sobhani [35] determined all $(\alpha + \gamma u^2)$-constacyclic codes of length p^s over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ and their dual codes, where α, γ are non-zero elements of $\mathbb{F}_{p^m}$. For more related works, readers may refer to [9]–[13].

The main goal of this paper is to determine all repeated-root constacyclic codes of arbitrary lengths over the finite commutative chain ring $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$, their sizes and their dual codes, where p is a prime and m is a positive integer. Hamming distances, RT distances, RT weight distributions and ranks (i.e., cardinalities of minimal generating sets) are also determined for some repeated-root constacyclic codes over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$. Some isodual and MDS codes over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ with respect to Hamming and RT metrics are also identified within this class of constacyclic codes.

This paper is organized as follows: In Section II, we state some basic definitions and results that are needed to derive our main results. In Section III, we determine all repeated-root constacyclic codes of arbitrary lengths over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$, their dual codes and their sizes (Theorems 13-18). As an application, we also determine some isodual repeated-root constacyclic codes over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ (Corollaries 14-19). In Section IV, we determine Hamming distances, RT distances, RT weight distributions and ranks (i.e., cardinalities of minimal generating sets) of some repeated-root constacyclic codes over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ (Theorems 21, 23, 25, 26, 28, 30). We also list some MDS constacyclic codes over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ with respect to Hamming and RT metrics (Theorems 22, 24, 27 and 29). In Section V, we determine Hamming distances of all repeated-root constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ (Theorem 33). We also list all MDS repeated-root constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ with respect to the Hamming metric (Theorem 35). In Section VI, we mention a brief conclusion and discuss some interesting open problems in this direction.

II. SOME PRELIMINARIES

A commutative ring R with unity is called (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 its ideals form a chain with respect to the inclusion relation. Then the following result is well-known.

Proposition 1 [17]: 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 $|\langle w^i\rangle| = |R/\langle w\rangle|^{e-i}$ 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 λ-constacyclic code $\mathcal{C}$ of length N over R is defined as an R-submodule of

R^N satisfying the following property: $(a_0, a_1, \cdots, a_{N-1}) \in \mathcal{C}$ implies that $(\lambda a_{N-1}, a_0, a_1, \cdots, a_{N-2}) \in \mathcal{C}$. The Hamming distance $d_H(\mathcal{C})$ of the code $\mathcal{C}$ is given by $d_H(\mathcal{C}) = \min\{w_H(c) : c(\neq 0) \in \mathcal{C}\}$, where $w_H(c)$ is the number of non-zero components of c and is called the Hamming weight of c. The Rosenbloom-Tsfasman (RT) distance $d_{RT}(\mathcal{C})$ of the code $\mathcal{C}$ is given by $d_{RT}(\mathcal{C}) = \min\{w_{RT}(c) : c(\neq 0) \in \mathcal{C}\}$, where $w_{RT}(c)$ is the RT weight of c and is defined as

$$w_{RT}(c) = \begin{cases} 1 + \max\{j : c_j \neq 0\} \\ \quad \text{if } c = (c_0, c_1, \cdots, \cdots, c_{N-1}) \neq 0; \\ 0 \quad \text{if } c = 0. \end{cases}$$

Note that each R-submodule of R^N need not be free. The cardinality of a minimal generating set of the code $\mathcal{C}$ is called the rank of $\mathcal{C}$ and is denoted by rank$(\mathcal{C})$. The code $\mathcal{C}$ of length N and rank k over R is referred to as an $[N, k, d_H(\mathcal{C})]$-code with respect to the Hamming metric, while the code $\mathcal{C}$ is referred to as an $[N, k, d_{RT}(\mathcal{C})]$-code with respect to the RT metric.

The Rosenbloom-Tsfasman (RT) weight distribution of the code $\mathcal{C}$ is defined as the list $\mathcal{A}_0, \mathcal{A}_1, \cdots, \mathcal{A}_N$, where for $0 \leq \rho \leq N$, $\mathcal{A}_\rho$ is the number of codewords in $\mathcal{C}$ having the RT weight as ρ. Further, the code $\mathcal{C}$ is called (i) an MDS code with respect to the Hamming metric if it satisfies $|\mathcal{C}| = |R|^{N-d_H(\mathcal{C})+1}$, and (ii) an MDS code with respect to the RT metric if it satisfies $|\mathcal{C}| = |R|^{N-d_{RT}(\mathcal{C})+1}$. Note that an MDS code has to be non-zero. The dual code of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined as $\mathcal{C}^\perp = \{u \in R^N : u.c = 0 \text{ for all } c \in \mathcal{C}\}$, where $u.c = u_0c_0 + u_1c_1 + \cdots + u_{N-1}c_{N-1}$ for $u = (u_0, u_1, \cdots, u_{N-1}) \in R^N$ and $c = (c_0, c_1, \cdots, c_{N-1}) \in \mathcal{C}$. It is easy to observe that the dual code $\mathcal{C}^\perp$ is a λ^{-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 $\psi : R^N \to R[x]/\langle x^N - \lambda\rangle$, 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 λ-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 $x^N - \lambda$. Under this identification, the Hamming weight $w_H(c(x))$ of $c(x) \in R[x]/\langle x^N - \lambda\rangle$ is 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 given by

$$w_{RT}(c(x)) = \begin{cases} 1 + \deg c(x) & \text{if } c(x) \neq 0; \\ 0 & \text{if } c(x) = 0, \end{cases}$$

(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 $\mathcal{C}^\perp = \{u(x) \in R[x]/\langle x^N - \lambda^{-1}\rangle : u(x)c^*(x) = 0 \text{ in } R[x]/\langle x^N - \lambda^{-1}\rangle \text{ for all } c(x) \in \mathcal{C}\}$, 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 ann$(\mathcal{C})$ is an ideal of $R[x]/\langle x^N - \lambda\rangle$. Furthermore, 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 $R[x]/\langle x^N - \lambda^{-1}\rangle$. Now the following holds.

Lemma 2 [14]: If $\mathcal{C} \subseteq R[x]/\langle x^N - \lambda\rangle$ is a λ-constacyclic code of length N over R, then we have $\mathcal{C}^\perp = ann(\mathcal{C})^*$.

From this point on, throughout this paper, let R be the ring $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3\rangle$. 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 $\lambda = \alpha + \beta u + \gamma u^2$, where $\alpha, \beta, \gamma \in \mathbb{F}_{p^m}$. Now we make the following observation.

Lemma 3 [14]: Let $\lambda = \alpha + \beta u + \gamma u^2 \in \mathcal{R}$, where $\alpha, \beta, \gamma \in \mathbb{F}_{p^m}$. Then the following hold.

(a) *λ is a unit in $\mathcal{R}$ if and only if $\alpha \neq 0$.*
(b) *There exists $\alpha_0 \in \mathbb{F}_{p^m}$ satisfying $\alpha_0^{p^s} = \alpha$.*

The following three theorems are useful in the determination of Hamming distances of some repeated-root constacyclic codes over $\mathcal{R}$. In fact, the following theorem is an extension of Theorem 3.4 of Dinh [15].

Theorem 4: For $\eta \in \mathbb{F}_{p^m} \setminus \{0\}$, there exists $\eta_0 \in \mathbb{F}_{p^m}$ satisfying $\eta = \eta_0^{p^s}$. Suppose that the polynomial $x^n - \eta_0$ is irreducible over $\mathbb{F}_{p^m}$. Let $\mathcal{C}$ be an η-constacyclic code of length np^s over $\mathbb{F}_{p^m}$. Then we have $\mathcal{C} = \langle (x^n - \eta_0)^\upsilon\rangle$, where $0 \leq \upsilon \leq p^s$. Further, the Hamming distance $d_H(\mathcal{C})$ of the code $\mathcal{C}$ is given by

$$d_H(\mathcal{C}) = \begin{cases} 1 & \text{if } \upsilon = 0; \\ \ell + 2 & \text{if } \ell p^{s-1} + 1 \leq \upsilon \leq (\ell+1)p^{s-1} \\ & \text{with } 0 \leq \ell \leq p-2; \\ (i+1)p^k & \text{if } p^s - p^{s-k} + (i-1)p^{s-k-1} + 1 \\ & \leq \upsilon \leq p^s - p^{s-k} + ip^{s-k-1} \text{ with} \\ & 1 \leq i \leq p-1 \text{ and } 1 \leq k \leq s-1; \\ 0 & \text{if } \upsilon = p^s. \end{cases}$$

Moreover, the code $\mathcal{C}$ is an MDS code if and only if exactly one of the following conditions is satisfied:

- *$0 \leq \upsilon \leq p - 1$ when $n = s = 1$;*
- *$\upsilon \in \{0, 1, p^s - 1\}$ when $n = 1$ and $s \geq 2$;*
- *$\upsilon = 0$ when $n \geq 2$.*

Proof: Working in a similar manner as in Theorem 3.4 of Dinh [15], the desired result follows. □

Theorem 5 [27]: Let p be an odd prime, and let ω be a non-zero square in $\mathbb{F}_{p^m}$. Then there exists $\omega_0 \in \mathbb{F}_{p^m}$ satisfying $\omega = \omega_0^{p^s}$. Further, ω_0 is a square in $\mathbb{F}_{p^m}$, i.e., there exists $\zeta \in \mathbb{F}_{p^m}$ such that $\omega_0 = \zeta^2$.

Now let $\mathcal{C}$ be a non-zero ω-constacyclic code of length $2p^s$ over $\mathbb{F}_{p^m}$. Then we have $\mathcal{C} = \langle (x+\zeta)^{\upsilon_1}(x-\zeta)^{\upsilon_2}\rangle$, where $0 \leq \upsilon_1, \upsilon_2 \leq p^s$.

When $\upsilon_1 \geq \upsilon_2$, the Hamming distance $d_H(\mathcal{C})$ of the code $\mathcal{C}$ over $\mathbb{F}_{p^m}$ is given by

$$d_H(\mathcal{C}) = \begin{cases} 1 & \text{if } \upsilon_1 = \upsilon_2 = 0; \\ 2 & \text{if } \upsilon_2 = 0 \text{ and } 0 < \upsilon_1 \leq p^s; \\ \min\{(\ell+2)p^k, 2(\ell_1+2)p^{k'}\} \text{ if} \\ \quad p^s - p^{s-k} + \ell p^{s-k-1} + 1 \leq \upsilon_1 \leq p^s - p^{s-k} \\ \quad + (\ell+1)p^{s-k-1} \text{ and } p^s - p^{s-k'} \\ \quad + \ell_1 p^{s-k'-1} + 1 \leq \upsilon_2 \leq p^s - p^{s-k'} \\ \quad + (\ell_1+1)p^{s-k'-1} \text{ with } 0 \leq \ell, \ell_1 \leq p-2, \\ \quad \text{and } 0 \leq k' \leq k \leq s-1; \\ 2(\ell_1+2)p^{k'} \text{ if } \upsilon_1 = p^s \text{ and } p^s - p^{s-k'} \\ \quad + \ell_1 p^{s-k'-1} + 1 \leq \upsilon_2 \leq p^s - p^{s-k'} \\ \quad + (\ell_1+1)p^{s-k'-1} \text{ with } 0 \leq \ell_1 \leq p-2 \\ \quad \text{and } 0 \leq k' \leq s-1. \end{cases}$$

When $\upsilon_2 \geq \upsilon_1$, the Hamming distance $d_H(\mathcal{C})$ of the code $\mathcal{C}$ over $\mathbb{F}_{p^m}$ is given by

$$d_H(\mathcal{C}) = \begin{cases} 1 & \text{if } \upsilon_1 = \upsilon_2 = 0; \\ 2 & \text{if } \upsilon_1 = 0 \text{ and } 0 < \upsilon_2 \leq p^s; \\ \min\{(\ell+2)p^k, 2(\ell_1+2)p^{k'}\} \text{ if} \\ \quad p^s - p^{s-k} + \ell p^{s-k-1} + 1 \leq \upsilon_2 \leq p^s - p^{s-k} \\ \quad + (\ell+1)p^{s-k-1} \text{ and } p^s - p^{s-k'} \\ \quad + \ell_1 p^{s-k'-1} + 1 \leq \upsilon_1 \leq p^s - p^{s-k'} \\ \quad + (\ell_1+1)p^{s-k'-1} \text{ with } 0 \leq \ell, \ell_1 \leq p-2, \\ \quad \text{and } 0 \leq k' \leq k \leq s-1; \\ 2(\ell_1+2)p^{k'} \text{ if } \upsilon_2 = p^s \text{ and } p^s - p^{s-k'} \\ \quad + \ell_1 p^{s-k'-1} + 1 \leq \upsilon_1 \leq p^s - p^{s-k'} \\ \quad + (\ell_1+1)p^{s-k'-1} \text{ with } 0 \leq \ell_1 \leq p-2 \\ \quad \text{and } 0 \leq k' \leq s-1. \end{cases}$$

Moreover, the code $\mathcal{C}$ is an MDS code if and only if exactly one of the following conditions is satisfied:

- $\upsilon_1 = \upsilon_2 = 0$;
- $\upsilon_1 = 1$ *and* $\upsilon_2 = 0$;
- $\upsilon_1 = 0$ *and* $\upsilon_2 = 0$;
- $\upsilon_1 = p^s$ *and* $\upsilon_2 = p^s - 1$;
- $\upsilon_1 = p^s - 1$ *and* $\upsilon_2 = p^s$.

Theorem 6 [29]: Let $\mathcal{C}$ be a linear code of length N over $\mathcal{R}$. Then $Tor_2(\mathcal{C}) = \{a \in \mathbb{F}_{p^m}^N : u^2 a \in \mathcal{C}\}$ is a linear code of length N over $\mathbb{F}_{p^m}$. Furthermore, we have $d_H(\mathcal{C}) = d_H(Tor_2(\mathcal{C}))$.

Next we proceed to study algebraic structures of all constacyclic codes of length $N = np^s$ over the ring $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$, where $u^3 = 0$, p is a prime and n, s, m are positive integers with $\gcd(n, p) = 1$.

III. CONSTACYCLIC CODES OF LENGTH np^s OVER $\mathcal{R}$

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 α is non-zero. In this section, we shall provide a method to construct all λ-constacyclic codes of length np^s over $\mathcal{R}$ for the purpose of error-detection and error-correction. We shall also determine their dual codes and the number of codewords in each code. Apart from this, we shall list some isodual constacyclic codes of length np^s over $\mathcal{R}$. These results are useful in encoding and decoding these codes and in studying their error-detecting and error-correcting capabilities with respect to various communication channels.

To do this, we recall that a λ-constacyclic code of length np^s over $\mathcal{R}$ is an ideal of the quotient ring $\mathcal{R}_\lambda = \mathcal{R}[x]/\langle x^{np^s} - \lambda\rangle$. Furthermore, by Lemma 3(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 $f_1(x), f_2(x), \cdots, f_r(x)$ are monic pairwise coprime 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 7: There exist polynomials $g_1(x), g_2(x), \cdots, g_r(x)$, $h_1(x), h_2(x), \cdots, h_r(x) \in \mathbb{F}_{p^m}[x]$ such that

$$x^{np^s} - \lambda = \prod_{j=1}^{r} \left(f_j(x)^{p^s} + ug_j(x) + u^2 h_j(x)\right),$$

where 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* γ *is non-zero.*

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

Proof: Working in a similar manner as in Lemma 3.1 of Sharma and Sidana [34], the desired result follows. □

From now on, we define $k_j(x) = f_j(x)^{p^s} + ug_j(x) + u^2h_j(x)$ for $1 \leq j \leq r$. Then we have $x^{np^s} - \lambda = \prod_{j=1}^{r} k_j(x)$. Furthermore, if $\deg f_j(x) = d_j$, then we observe that $\deg k_j(x) = d_jp^s$ for each j. By Lemma 7, we see that $k_1(x), k_2(x), \cdots, k_r(x)$ are pairwise coprime in $\mathcal{R}[x]$. This, by Chinese Remainder Theorem, implies that

$$\mathcal{R}_\lambda \simeq \bigoplus_{j=1}^{r} \mathcal{K}_j,$$

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

Proposition 8: (a) *Let $\mathcal{C}$ be a λ-constacyclic code of length np^s over $\mathcal{R}$, i.e., an ideal of the ring $\mathcal{R}_\lambda$. Then $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \cdots \oplus \mathcal{C}_r$, where $\mathcal{C}_j$ 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*

λ-constacyclic code of length np^s over $\mathcal{R}$). Moreover, we have $|I| = |I_1||I_2|\cdots|I_r|$.

Proof: Proof is trivial. □

Next if $\mathcal{C}$ is a λ-constacyclic code of length np^s over $\mathcal{R}$, then its dual code $\mathcal{C}^\perp$ is a λ^{-1}-constacyclic code of length np^s over $\mathcal{R}$. This implies that $\mathcal{C}^\perp$ is an ideal of the ring $\mathcal{R}_{\lambda^{-1}} = \mathcal{R}[x]/\langle x^{np^s} - \lambda^{-1}\rangle$. In order to determine $\mathcal{C}^\perp$ more explicitly, we observe that $x^{np^s} - \lambda^{-1} = -\alpha^{-1}k_1^*(x)k_2^*(x)\cdots k_r^*(x)$. By applying Chinese Remainder Theorem again, we get $\mathcal{R}_{\lambda^{-1}} \simeq \bigoplus_{j=1}^{r}\widehat{\mathcal{K}}_j$, 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 9: Let $\mathcal{C}$ be a λ-constacyclic code of length np^s over $\mathcal{R}$, i.e., an ideal of the ring $\mathcal{R}_\lambda$. If $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \cdots \oplus \mathcal{C}_r$ with $\mathcal{C}_j$ an ideal of $\mathcal{K}_j$ for each j, then the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ is given by $\mathcal{C}^\perp = \mathcal{C}_1^\perp \oplus \mathcal{C}_2^\perp \oplus \cdots \oplus \mathcal{C}_r^\perp$, where $\mathcal{C}_j^\perp = \{a_j(x) \in \widehat{\mathcal{K}}_j : a_j(x)c_j^*(x) = 0 \text{ in } \widehat{\mathcal{K}}_j \text{ for all } c_j(x) \in \mathcal{C}_j\}$ is the orthogonal complement of $\mathcal{C}_j$ for each j. Furthermore, $\mathcal{C}_j^\perp$ is an ideal of $\widehat{\mathcal{K}}_j = \mathcal{R}[x]/\langle k_j^*(x)\rangle$ for each j.

Proof: Its proof is straightforward. □

In view of Propositions 8 and 9, we see that to determine all λ-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 on, we shall represent elements of the rings $\mathcal{K}_j$ and $\widehat{\mathcal{K}}_j$ (resp. $\mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$) by their representatives in $\mathcal{R}[x]$ (resp. $\mathbb{F}_{p^m}[x]$) of degree less than d_jp^s, and we shall perform their addition and multiplication modulo $k_j(x)$ and $k_j^*(x)$ (resp. $f_j(x)^{p^s}$), respectively. To determine all ideals of the ring $\mathcal{K}_j$, we make the following observation.

Lemma 10: 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) $$\langle f_j(x)^{p^s}\rangle = \begin{cases} \langle u\rangle & \text{if } \beta \neq 0; \\ \langle u^2\rangle & \text{if } \beta = 0 \text{ and } \gamma \neq 0; \\ \{0\} & \text{if } \beta = \gamma = 0. \end{cases}$$
As a consequence, $f_j(x)$ is a nilpotent element of $\mathcal{K}_j$. The nilpotency index of $f_j(x)$ is $3p^s$ 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: Proof is trivial. □

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 $a(x) \in \mathcal{K}_j$ can be uniquely expressed as $a(x) = a_0(x) + ua_1(x) + u^2\, a_2(x)$, where $a_0(x), a_1(x), a_2(x) \in \mathcal{P}_{d_jp^s}(\mathbb{F}_{p^m})$. Further, by repeatedly applying the division algorithm in $\mathbb{F}_{p^m}[x]$, for $\ell \in \{0, 1, 2\}$, we can write $a_\ell(x) = \sum_{i=0}^{p^s-1} A_i^{(a_\ell)}(x)f_j(x)^i$, where $A_i^{(a_\ell)}(x) \in \mathcal{P}_{d_j}(\mathbb{F}_{p^m})$ for $0 \leq i \leq p^s - 1$. That is, each element $a(x) \in \mathcal{K}_j$ can be uniquely expressed as $a(x) = \sum_{i=0}^{p^s-1} A_i^{(a_0)}(x)f_j(x)^i + u\sum_{i=0}^{p^s-1} A_i^{(a_1)}(x)f_j(x)^i + u^2\sum_{i=0}^{p^s-1} A_i^{(a_2)}(x)f_j(x)^i$, where $A_i^{(a_\ell)}(x) \in \mathcal{P}_{d_j}(\mathbb{F}_{p^m})$ for each i and ℓ. Now to determine cardinalities of all ideals of $\mathcal{K}_j$, we observe the following:

Lemma 11: Let $1 \leq j \leq r$ be a fixed integer. For an ideal $\mathcal{I}$ of $\mathcal{K}_j$, let us define $Tor_0(\mathcal{I}) = \{a_0(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle : a_0(x) + ua_1(x) + u^2\, a_2(x) \in \mathcal{I}$ for some $a_1(x), a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle\}$, $Tor_1(\mathcal{I}) = \{a_1(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle : ua_1(x) + u^2\, a_2(x) \in \mathcal{I}$ for some $a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle\}$ and $Tor_2(\mathcal{I}) = \{a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle : u^2\, a_2(x) \in \mathcal{I}\}$. Then $Tor_0(\mathcal{I})$, $Tor_1(\mathcal{I})$ and $Tor_2(\mathcal{I})$ are ideals of $\mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$. Moreover, we have
$$|\mathcal{I}| = |Tor_0(\mathcal{I})||Tor_1(\mathcal{I})||Tor_2(\mathcal{I})|.$$

Proof: Proof is trivial. □

To determine orthogonal complements of all ideals of $\mathcal{K}_j$, we need the following lemma.

Lemma 12: Let $1 \leq j \leq r$ be a fixed integer. Let $\mathcal{I}$ be an ideal of the ring $\mathcal{K}_j$ with the orthogonal complement as $\mathcal{I}^\perp$. Then the following hold.

(a) *$\mathcal{I}^\perp$ is an ideal of $\widehat{\mathcal{K}}_j$.*

(b) *$\mathcal{I}^\perp = \{a^*(x) \in \widehat{\mathcal{K}}_j : a(x) \in ann(\mathcal{I})\} = ann(\mathcal{I})^*$.*

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

(d) *For non-zero $f(x), g(x) \in \mathcal{K}_j$, let us define $(fg)(x) = f(x)g(x)$ and $(f+g)(x) = f(x) + g(x)$. If $(fg)(x) \neq 0$, then we have $f^*(x)g^*(x) = x^{\deg f(x) + \deg g(x) - \deg (fg)(x)}(fg)^*(x)$. If $(f+g)(x) \neq 0$, then we have*
$$(f+g)^*(x) = \begin{cases} f^*(x) + x^{\deg f(x) - \deg g(x)}g^*(x) \text{ if} \\ \quad \deg f(x) > \deg g(x); \\ x^{\deg (f+g)(x) - \deg f(x)}(f^*(x) + g^*(x)) \\ \quad \text{if } \deg f(x) = \deg g(x). \end{cases}$$

Proof: Its proof is straightforward. □

From the above lemma, we see that to determine $\mathcal{I}^\perp$, it is enough to determine ann$(\mathcal{I})$ for each ideal $\mathcal{I}$ of $\mathcal{K}_j$. Further, to write down all ideals of $\mathcal{K}_j$, we see, by Lemma 11, that for each ideal $\mathcal{I}$ of $\mathcal{K}_j$, $\text{Tor}_0(\mathcal{I})$, $\text{Tor}_1(\mathcal{I})$ and $\text{Tor}_2(\mathcal{I})$ all are ideals of the ring $\mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$, which is a finite commutative chain ring with the maximal ideal as $\langle f_j(x)\rangle$. Next by Proposition 1, we see that all the ideals of $\mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$ are given by $\langle f_j(x)^i\rangle$ with $0 \leq i \leq p^s$ and that $|\langle f_j(x)^i\rangle| = p^{md_j(p^s-i)}$ for each i. This implies that $\text{Tor}_0(\mathcal{I}) = \langle f_j(x)^a\rangle$, $\text{Tor}_1(\mathcal{I}) = \langle f_j(x)^b\rangle$ and $\text{Tor}_2(\mathcal{I}) = \langle f_j(x)^c\rangle$ 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 λ-constacyclic code of length np^s over $\mathcal{R}$ can be determined by using the results derived in Cao [7] and by applying the ring isomorphism from $\mathcal{R}[x]/\langle x^{np^s} - 1 - \alpha^{-1}\beta u - \alpha^{-1}\gamma u^2\rangle$ onto $\mathcal{R}[x]/\langle x^{np^s} - \alpha - \beta u - \gamma u^2\rangle$, defined as $a(x) \mapsto a(\mu^{-1}x)$ for each $a(x) \in \mathcal{R}[x]/\langle x^{np^s} - 1 - \alpha^{-1}\beta u - \alpha^{-1}\gamma u^2\rangle$.

However, when α_0 (and hence α) is not an nth power of an element in $\mathbb{F}_{p^m}$, the same technique can not be employed to determine all $(\alpha+\beta u+\gamma u^2)$-constacyclic codes of length np^s over $\mathcal{R}$. In fact, the problem of determination of all $(\alpha+\beta u+\gamma u^2)$-constacyclic codes of length np^s over $\mathcal{R}$ and their dual codes is not yet completely solved. Propositions 8 and 9 and the following theorem completely solves this problem when β is non-zero.

Theorem 13: When $\beta \neq 0$, the following hold.

(a) *All ideals of the ring $\mathcal{K}_j$ are given by $\langle f_j(x)^\ell\rangle$, where $0 \leq \ell \leq 3p^s$. Furthermore, for $0 \leq \ell \leq 3p^s$, we have $|\langle f_j(x)^\ell\rangle| = p^{md_j(3p^s-\ell)}$ and $ann(\langle f_j(x)^\ell\rangle) = \langle f_j(x)^{3p^s-\ell}\rangle$.*

(b) *When $kp^s \leq \ell \leq (k+1)p^s$ with $k \in \{0,1,2\}$, the set $\{u^k f_j(x)^{\ell-kp^s}, u^k x f_j(x)^{\ell-kp^s}, \cdots, u^k x^{d_j((k+1)p^s-\ell)-1} f_j(x)^{\ell-kp^s}\} \cup \{u^{k+1}, u^{k+1}x, \cdots, u^{k+1}x^{d_j(\ell-kp^s)-1}\}$ is a minimal generating set of the ideal $\langle f_j(x)^\ell\rangle$ when viewed as an $\mathcal{R}$-module.*

Proof: Proof of part (a) is similar to that of Theorem 3.3 and Corollary 3.5 of Chen *et al.* [14], while part (b) is an easy exercise. □

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

Corollary 14: Let $n \geq 1$ be an integer and $\alpha_0 \in \mathbb{F}_{p^m}$ be such that the binomial $x^n - \alpha_0$ is irreducible over $\mathbb{F}_{p^m}$. Let $\alpha = \alpha_0^{p^s}$, and $\beta(\neq 0), \gamma \in \mathbb{F}_{p^m}$. Then there exists an isodual $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$ 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 $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length $n2^s$ over $\mathcal{R}$.

Proof: On taking $f_j(x) = x^n - \alpha_0$ in Theorem 13, we see that all $(\alpha+\beta u+\gamma u^2)$-constacyclic codes of length np^s over $\mathcal{R}$ are given by $\langle (x^n-\alpha_0)^\ell\rangle$, where $0 \leq \ell \leq 3p^s$. Furthermore, for $0 \leq \ell \leq 3p^s$, the code $\langle (x^n-\alpha_0)^\ell\rangle$ has $p^{mn(3p^s-\ell)}$ elements and the annihilator of $\langle (x^n-\alpha_0)^\ell\rangle$ is given by $\langle (x^n-\alpha_0)^{3p^s-\ell}\rangle$. Next we see that if the code $\mathcal{C} = \langle (x^n-\alpha_0)^\ell\rangle$ is isodual, then we must have $|\mathcal{C}| = |\mathcal{C}^\perp|$. This gives $p^{mn(3p^s-\ell)} = p^{mn\ell}$. This implies that $3p^s = 2\ell$, which holds if and only if $p = 2$. So when p is an odd prime, there does not exist any isodual $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$. When $p = 2$, we get $\ell = 3\cdot 2^{s-1}$. On the other hand, when $p = 2$, we observe that $\langle (x^n-\alpha_0)^{3\cdot 2^{s-1}}\rangle$ is an isodual $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length $n2^s$ over $\mathcal{R}$, which completes the proof. □

Remark 15: By Theorem 3.75 of [26], we see that the binomial $x^n - \alpha_0$ is irreducible over $\mathbb{F}_{p^m}$ if and only if the following two conditions are satisfied: (i) each prime divisor of n divides the multiplicative order e of α_0, but not $(p^m-1)/e$ and (ii) $p^m \equiv 1 \pmod 4$ if $n \equiv 0 \pmod 4$.

In the following theorem, we consider the case $\beta = \gamma = 0$, and we determine all non-trivial ideals of the ring $\mathcal{K}_j$, their cardinalities, their annihilators and their minimal generating sets.

Theorem 16: Let $\beta = \gamma = 0$, and let $\mathcal{I}$ be a non-trivial ideal of the ring $\mathcal{K}_j$ with $Tor_0(\mathcal{I}) = \langle f_j(x)^a\rangle$, $Tor_1(\mathcal{I}) = \langle f_j(x)^b\rangle$ and $Tor_2(\mathcal{I}) = \langle f_j(x)^c\rangle$ for some integers a, b, c satisfying $0 \leq c \leq b \leq a \leq p^s$. Suppose that $B_i(x), C_k(x), Q_\ell(x), W_e(x)$ run over $\mathcal{P}_{d_j}(\mathbb{F}_{p^m})$ for each relevant i, k, ℓ and e. Then the following hold.

- ***Type I:*** *When $a = b = p^s$, we have*
$$\mathcal{I} = \langle u^2 f_j(x)^c\rangle,$$
where $c < p^s$. Moreover, we have
$$|\mathcal{I}| = p^{md_j(p^s-c)}, \quad ann(\mathcal{I}) = \langle f_j(x)^{p^s-c}, u\rangle,$$
and the set
$$\{u^2 f_j(x)^c, u^2 x f_j(x)^c, \cdots, u^2 x^{d_jp^s-d_jc-1} f_j(x)^c\}$$
is a minimal generating set of the ideal $\mathcal{I}$ when viewed as an $\mathcal{R}$-module.
- ***Type II:*** *When $a = p^s$ and $b < p^s$, we have*
$$\mathcal{I} = \langle uf_j(x)^b + u^2 f_j(x)^t G(x), u^2 f_j(x)^c\rangle,$$
where $\max\{0, c+b-p^s\} \leq t < c$ if $G(x) \neq 0$ and $G(x)$ is either 0 or a unit in $\mathcal{K}_j$ of the form $\sum_{i=0}^{c-t-1} B_i(x) f_j(x)^i$. Moreover, we have
$$|\mathcal{I}| = p^{md_j(2p^s-b-c)}, \quad ann(\mathcal{I}) = \langle f_j(x)^{p^s-c} - uf_j(x)^{p^s-c+t-b}G(x), uf_j(x)^{p^s-b}, u^2\rangle$$
and the set
$$\{uf_j(x)^b + u^2 f_j(x)^t G(x), x(uf_j(x)^b + u^2 f_j(x)^t G(x)), \cdots, x^{d_jp^s-d_jb-1}(uf_j(x)^b + u^2 f_j(x)^t G(x))\} \cup \{u^2 f_j(x)^c, u^2 x f_j(x)^c, \cdots, u^2 x^{d_jb-d_jc-1} f_j(x)^c\}$$
is a minimal generating set of the ideal $\mathcal{I}$ when viewed as an $\mathcal{R}$-module.
- ***Type III:*** *When $a < p^s$, we have*
$$\mathcal{I} = \langle f_j(x)^a + uf_j(x)^{t_1} D_1(x) + u^2 f_j(x)^{t_2} D_2(x), uf_j(x)^b + u^2 f_j(x)^\theta V(x), u^2 f_j(x)^c\rangle,$$
where $\max\{0, a+b-p^s\} \leq t_1 < b$ if $D_1(x) \neq 0$, $0 \leq t_2 < c$ if $D_2(x) \neq 0$, $\max\{0, b+c-p^s\} \leq \theta < c$ if $V(x) \neq 0$, $D_1(x)$ is either 0 or a unit in $\mathcal{K}_j$ of the form $\sum_{k=0}^{b-t_1-1} C_k(x) f_j(x)^k$, $D_2(x)$ is either 0 or a unit in $\mathcal{K}_j$ of the form $\sum_{\ell=0}^{c-t_2-1} Q_\ell(x) f_j(x)^\ell$ and $V(x)$ is either 0 or a unit in $\mathcal{K}_j$ of the form $\sum_{i=0}^{c-\theta-1} W_i(x) f_j(x)^i$. Furthermore, we have
$$u^2\big(f_j(x)^{p^s-a+t_1-b+\theta} V(x) D_1(x) - f_j(x)^{p^s-a+t_2} D_2(x)\big) \in \langle u^2 f_j(x)^c\rangle,$$
i.e., there exists $A(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$ such that
$$u^2\big(f_j(x)^{p^s-a+t_1-b+\theta} V(x) D_1(x) - f_j(x)^{p^s-a+t_2} D_2(x)\big) = u^2 f_j(x)^c A(x).$$

Moreover, we have

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

the annihilator of $\mathcal{I}$ is given by

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

and the set

$$\{F_1(x), xF_1(x), \cdots, x^{d_jp^s-d_ja-1}F_1(x)\} \cup \{F_2(x), xF_2(x), \cdots, x^{d_ja-d_jb-1}F_2(x)\} \cup \{u^2 f_j(x)^c, u^2 xf_j(x)^c, \cdots, u^2 x^{d_jb-d_jc-1}f_j(x)^c\}$$

is a minimal generating set of the ideal $\mathcal{I}$ when viewed as an $\mathcal{R}$-module, where $F_1(x) = f_j(x)^a + uf_j(x)^{t_1}D_1(x) + u^2 f_j(x)^{t_2}D_2(x)$ and $F_2(x) = uf_j(x)^b + u^2 f_j(x)^{\theta}V(x)$.

Proof: As $\mathcal{I}$ is a non-trivial ideal of $\mathcal{K}_j$, we note that neither $a = 0$ nor $a = b = c = p^s$ hold. Further, by Lemma 11, we have $|\mathcal{I}| = p^{md_j(3p^s-a-b-c)}$. Now to write down all such non-trivial ideals of $\mathcal{K}_j$ and to determine their annihilators, we shall distinguish the following three cases: **(i)** $a = b = p^s$, **(ii)** $a = p^s$ and $b < p^s$, and **(iii)** $a < p^s$.

(i) When $a = b = p^s$, we have $\mathcal{I} \subseteq \langle u^2\rangle$. In this case, we have $0 \le c < p^s$. Here we observe that $\mathcal{I} = \langle u^2 f_j(x)^c\rangle$. Now to find ann$(\mathcal{I})$, we consider the ideal $\mathcal{B}_1 = \langle f_j(x)^{p^s-c}, u, u^2\rangle$, and we see that $\mathcal{B}_1 \subseteq \text{ann}(\mathcal{I})$ and that $|\mathcal{B}_1| = p^{md_j(2p^s+c)}$. As

$$p^{md_j(p^s-c)} = |\mathcal{I}| = \frac{|\mathcal{K}_j|}{|\text{ann}(\mathcal{I})|} \le \frac{p^{3md_jp^s}}{|\mathcal{B}_1|} = p^{md_j(p^s-c)},$$

we get $\text{ann}(\mathcal{I}) = \mathcal{B}_1 = \langle f_j(x)^{p^s-c}, u, u^2\rangle$.

(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

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

for some $r(x) \in \mathcal{K}_j$. Let us write $u^2 r(x) = u^2 \sum_{i=0}^{p^s-1} \mathcal{G}_i(x)f_j(x)^i$, where $\mathcal{G}_i(x) \in \mathcal{P}_{d_j}(\mathbb{F}_{p^m})$ for $0 \le i \le p^s - 1$. Note that for all $i \ge c$, we have $u^2 f_j(x)^i = u^2 f_j(x)^c f_j(x)^{i-c} \in \mathcal{I}$, which implies that

$$\mathcal{I} =< uf_j(x)^b + u^2 \sum_{i=0}^{c-1} \mathcal{G}_i(x)f_j(x)^i, u^2 f_j(x)^c > .$$

If $u^2 \sum_{i=0}^{c-1} \mathcal{G}_i(x)f_j(x)^i \neq 0$ in $\mathcal{K}_j$, then choose the smallest integer t $(0 \le t < c)$ satisfying $\mathcal{G}_t(x) \neq 0$, which gives $u^2 \sum_{i=0}^{c-1} \mathcal{G}_i(x)f_j(x)^i = u^2 f_j(x)^t G(x)$, where $G(x) = \sum_{i=t}^{c-1} \mathcal{G}_i(x)f_j(x)^{i-t}$ is a unit in $\mathcal{K}_j$. On the other hand, when $u^2 \sum_{i=0}^{c-1} \mathcal{G}_i(x)f_j(x)^i = 0$ in $\mathcal{K}_j$, let us choose $G(x) = 0$. From this, it follows that

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

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 $a_i(x) \in \mathcal{P}_{d_j}(\mathbb{F}_{p^m})$ for $0 \le i \le c - t - 1$.
Further, as $f_j(x)^{p^s-b}\{uf_j(x)^b + u^2 f_j(x)^t G(x)\} = u^2 f_j(x)^{p^s-b+t}G(x) \in \mathcal{I}$, we must have $p^s - b + t \ge c$ when $G(x) \neq 0$. Moreover, let $\mathcal{B}_2 = \langle f_j(x)^{p^s-c} - uf_j(x)^{p^s-c+t-b}G(x), uf_j(x)^{p^s-b}, u^2\rangle$. We observe that $\mathcal{B}_2 \subseteq \text{ann}(\mathcal{I})$ and $|\mathcal{B}_2| \ge p^{md_j(p^s+b+c)}$. Since

$$p^{md_j(2p^s-b-c)} = |\mathcal{I}| = \frac{|\mathcal{K}_j|}{|\text{ann}(\mathcal{I})|} \le \frac{p^{3md_jp^s}}{|\mathcal{B}_2|} \le p^{md_j(2p^s-b-c)},$$

we obtain $|\text{ann}(\mathcal{I})| = |\mathcal{B}_2| = p^{md_j(p^s+b+c)}$. This implies that

$$\text{ann}(\mathcal{I}) = \mathcal{B}_2 = \langle f_j(x)^{p^s-c} - uf_j(x)^{p^s-c+t-b}G(x), uf_j(x)^{p^s-b}, u^2\rangle.$$

(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

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

for some $r_1(x), r_2(x), q(x) \in \mathcal{K}_j$. Further, working as in the previous case, one can show that

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

where $D_1(x)$ is either 0 or a unit in $\mathcal{K}_j$ of the form $\sum_{\ell=t_1}^{b-1} A_\ell(x)f_j(x)^{\ell-t_1}$, $D_2(x)$ is either 0 or a unit in $\mathcal{K}_j$ 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 $\mathcal{K}_j$ of the form $\sum_{i=\theta}^{c-1} W_i(x)f_j(x)^{i-\theta}$ with $A_\ell(x), B_k(x), W_i(x) \in \mathcal{K}_j$ for each ℓ, k and i.
In order to determine ann$(\mathcal{I})$, we first observe that $uf_j(x)^{p^s-a+t_1}D_1(x) + u^2 f_j(x)^{p^s-a+t_2}D_2(x) \in \mathcal{I}$, which implies that $p^s - a + t_1 \ge b$ when $D_1(x) \neq 0$. Next we see that $f_j(x)^{p^s-b}\{uf_j(x)^b + u^2 f_j(x)^{\theta}V(x)\} \in \mathcal{I}$, which gives $p^s - b + \theta \ge c$ when $V(x) \neq 0$. Moreover, as $uf_j(x)^a + u^2 f_j(x)^{t_1}D_1(x) \in \mathcal{I}$and $f_j(x)^{a-b}\{uf_j(x)^b + u^2 f_j(x)^{\theta}V(x)\} \in \mathcal{I}$, we note that $u^2\{f_j(x)^{t_1}D_1(x) - f_j(x)^{a-b+\theta}V(x)\} \in \mathcal{I}$, which implies that

$$u^2\{f_j(x)^{t_1}D_1(x) - f_j(x)^{a-b+\theta}V(x)\} \in \langle u^2 f_j(x)^c\rangle.$$

From this, we obtain $u^2 f_j(x)^{p^s-c}\{f_j(x)^{t_1}D_1(x) - f_j(x)^{a-b+\theta}V(x)\} = 0$. Further, we see that

$$uf_j(x)^{p^s-a+t_1}D_1(x) + u^2 f_j(x)^{p^s-a+t_2}D_2(x) \in \mathcal{I}$$

can be rewritten as

$$f_j(x)^{p^s-a+t_1-b}D_1(x)\{uf_j(x)^b + u^2 f_j(x)^{\theta}V(x)\} - u^2 f_j(x)^{p^s-a+t_1-b+\theta}D_1(x)V(x) + u^2 f_j(x)^{p^s-a+t_2}D_2(x),$$

which implies that

$$u^2\{f_j(x)^{p^s-a+t_1-b+\theta}D_1(x)V(x) - f_j(x)^{p^s-a+t_2}D_2(x)\} \in \mathcal{I}.$$

This further implies that

$$u^2\{f_j(x)^{p^s-a+t_1-b+\theta}D_1(x)V(x) - f_j(x)^{p^s-a+t_2}D_2(x)\} \in \langle u^2 f_j(x)^c\rangle.$$

Let us write $u^2\{f_j(x)^{p^s-a+t_1-b+\theta}D_1(x)V(x) - f_j(x)^{p^s-a+t_2}D_2(x)\} = u^2 f_j(x)^c A(x)$, where $A(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$.

Next consider the ideal

$$\mathcal{B}_3 = \langle f_j(x)^{p^s-c} - uf_j(x)^{p^s-c+\theta-b}V(x) + u^2 A(x), uf_j(x)^{p^s-b} - u^2 f_j(x)^{p^s-a+t_1-b}D_1(x), u^2 f_j(x)^{p^s-a}\rangle.$$

Here we note that $|\mathcal{B}_3| \geq p^{md_j(a+b+c)}$ and $\mathcal{B}_3 \subseteq \text{ann}(\mathcal{I})$. Further, as

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

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

The determination of minimal generating sets of non-trivial ideals of $\mathcal{K}_j$ is a straightforward exercise. □

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

Corollary 17: Let $n \geq 1$ be an integer and $\alpha_0 \in \mathbb{F}_{p^m} \setminus \{0\}$ be such that the binomial $x^n - \alpha_0$ is irreducible over $\mathbb{F}_{p^m}$. Let $\alpha = \alpha_0^{p^s}$. Following the same notations as in Theorem 16, we have the following:

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

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

(c) *There exists an isodual α-constacyclic code of Type III over $\mathcal{R}$ if and only if $p = 2$. Moreover, when $p = 2$, the codes $\mathcal{C} = \langle (x^n - \alpha_0)^a + u^2(x^n - \alpha_0)^{t_2}D_2(x), u(x^n - \alpha_0)^{2^{s-1}}, u^2(x^n - \alpha_0)^{2^s-a}\rangle$, $2^{s-1} \leq a < 2^s$, are isodual α-constacyclic codes of Type III over $\mathcal{R}$.*

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

(a) Let $\mathcal{C}$ be of Type I, i.e., $\mathcal{C} = \langle u^2(x^n - \alpha_0)^c\rangle$ for some integer c satisfying $0 \leq c < p^s$. By Theorem 16, we see that $|\mathcal{C}| = p^{mn(p^s-c)}$ and $|\text{ann}(\mathcal{C})| = p^{mn(2p^s+c)}$. Now if the code $\mathcal{C}$ is isodual, then we must have $|\mathcal{C}| = |\text{ann}(\mathcal{C})|$. This implies that $p^s + 2c = 0$, which is a contradiction. Hence there does not exist any isodual α-constacyclic code of Type I over $\mathcal{R}$.

(b) Suppose that the code $\mathcal{C}$ is of Type II, i.e., $\mathcal{C} = \langle u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^t G(x), u^2(x^n - \alpha_0)^c\rangle$, where $0 \leq c \leq b < p^s$ and $0 \leq t < c$ if $G(x) \neq 0$. By Theorem 16, we have $|\mathcal{C}| = p^{mn(2p^s-b-c)}$, $\text{ann}(\mathcal{C}) = \langle (x^n - \alpha_0)^{p^s-c} - u(x^n - \alpha_0)^{p^s-c+t-b}G(x), u(x^n - \alpha_0)^{p^s-b}, u^2\rangle$ and $|\text{ann}(\mathcal{C})| = p^{mn(p^s+b+c)}$. Now if the code $\mathcal{C}$ is isodual, then we must have $|\mathcal{C}| = |\text{ann}(\mathcal{C})|$, which gives $p = 2$ and $c = 2^{s-1} - b$. Further, if the code $\mathcal{C}$ is $\mathcal{R}$-linearly equivalent to $\text{ann}(\mathcal{C})$, then $\text{Tor}_0(\mathcal{C}) = \{0\}$ must be $\mathbb{F}_{2^m}$-linearly equivalent to $\text{Tor}_0(\text{ann}(\mathcal{C})) = \langle (x^n - \alpha_0)^{2^s-c}\rangle$, which implies that $c = 0$. This gives $b = 2^{s-1} - c = 2^{s-1}$.
On the other hand, when $p = 2$, $c = 0$ and $b = 2^{s-1}$, by Theorem 16 again, we see that $\mathcal{C} = \text{ann}(\mathcal{C})$ holds, which implies that the codes $\mathcal{C}(\subseteq \mathcal{R}_\alpha)$ and $\mathcal{C}^{\perp}(\subseteq \widehat{\mathcal{R}_\alpha})$ are $\mathcal{R}$-linearly equivalent.

(c) Suppose that the code $\mathcal{C}$ is of Type III, i.e., $\mathcal{C} = \langle (x^n - \alpha_0)^a + u(x^n - \alpha_0)^{t_1}D_1(x) + u^2(x^n - \alpha_0)^{t_2}D_2(x), u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^{\theta}V(x), u^2(x^n - \alpha_0)^c\rangle$, where $0 \leq c \leq b \leq a < p^s$, $0 \leq t_1 < b$ 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 16, we have $|\mathcal{C}| = p^{mn(3p^s-a-b-c)}$ and $|\text{ann}(\mathcal{C})| = p^{mn(a+b+c)}$. From this, we see that if the code $\mathcal{C}$ 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 16 again, that for $2^{s-1} \leq a < 2^s$, the code $\mathcal{C} = \langle (x^n - \alpha_0)^a + u^2(x^n - \alpha_0)^{t_2}D_2(x), u(x^n - \alpha_0)^{2^{s-1}}, u^2(x^n - \alpha_0)^{2^s-a}\rangle$ satisfies $\mathcal{C} = \text{ann}(\mathcal{C})$, 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 $\mathcal{K}_j$, their orthogonal complements, their cardinalities and their minimal generating sets.

Theorem 18: Let $\beta = 0$ and γ be a non-zero element of $\mathbb{F}_{p^m}$. Let $\mathcal{I}$ be a non-trivial ideal of the ring $\mathcal{K}_j$ with $Tor_0(\mathcal{I}) = \langle f_j(x)^a\rangle$, $Tor_1(\mathcal{I}) = \langle f_j(x)^b\rangle$ and $Tor_2(\mathcal{I}) = \langle f_j(x)^c\rangle$ for some integers a, b, c satisfying $0 \leq c \leq b \leq a \leq p^s$. Suppose that $B_i(x), C_k(x), Q_\ell(x), W_e(x)$ run over $\mathcal{P}_{d_j}(\mathbb{F}_{p^m})$ for each relevant i, k, ℓ and e. Then the following hold.

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

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

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

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

and the set

$$\left\{u^2 f_j(x)^c, u^2 xf_j(x)^c, \cdots, u^2 x^{d_jp^s-d_jc-1}f_j(x)^c\right\}$$

is a minimal generating set of the ideal $\mathcal{I}$ *when viewed as an* $\mathcal{R}$*-module.*

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

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

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

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

and the set

$$\{uf_j(x)^b + u^2f_j(x)^tG(x), x(uf_j(x)^b + u^2f_j(x)^tG(x)), \cdots, x^{d_jp^s-d_jb-1}(uf_j(x)^b + u^2f_j(x)^tG(x))\} \cup \{u^2 f_j(x)^c, u^2 xf_j(x)^c, \cdots, u^2 x^{d_jb-d_jc-1}f_j(x)^c\}$$

is a minimal generating set of the ideal $\mathcal{I}$ *when viewed as an* $\mathcal{R}$*-module.*

- ***Type III:*** *When* $a < p^s$, *we have* $\mathcal{I} = \langle f_j(x)^a + uf_j(x)^{t_1}D_1(x) + u^2 f_j(x)^{t_2}D_2(x), uf_j(x)^b + u^2 f_j(x)^\theta V(x), u^2 f_j(x)^c\rangle$, *where* $\max\{0, a+b-p^s\} \leq t_1 < b$ *if* $D_1(x) \neq 0$, $0 \leq t_2 < c$ *if* $D_2(x) \neq 0$, $\max\{0, b+c-p^s\} \leq \theta < c$ *if* $V(x) \neq 0$, $D_1(x)$ *is either* 0 *or a unit in* $\mathcal{K}_j$ *of the form* $\sum_{k=0}^{b-t_1-1} C_k(x)f_j(x)^k$, $D_2(x)$ *is either* 0 *or a unit in* $\mathcal{K}_j$ *of the form* $\sum_{\ell=0}^{c-t_2-1} Q_\ell(x)f_j(x)^\ell$ *and* $V(x)$ *is either* 0 *or a unit in* $\mathcal{K}_j$ *of the form* $\sum_{i=0}^{c-\theta-1} W_i(x)f_j(x)^i$. *Furthermore, we have*

$$u^2\big(h_j(x) + f_j(x)^{p^s-a+t_1-b+\theta}V(x)D_1(x) - f_j(x)^{p^s-a+t_2}D_2(x)\big) \in \langle u^2f_j(x)^c\rangle,$$

i.e., there exists $B(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$ *such that* $u^2\big(h_j(x) + f_j(x)^{p^s-a+t_1-b+\theta}V(x)D_1(x) - f_j(x)^{p^s-a+t_2}D_2(x)\big) = u^2f_j(x)^cB(x)$. *Moreover, we have*

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

the annihilator of $\mathcal{I}$ *is given by*

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

and the set

$$\{F_1(x), xF_2(x), \cdots, x^{d_jp^s-d_ja-1}F_1(x)\} \cup \{F_2(x), xF_2(x), \cdots, x^{d_ja-d_jb-1}F_2(x)\} \cup \{u^2 f_j(x)^c, u^2 xf_j(x)^c, \cdots, u^2 x^{d_jb-d_jc-1}f_j(x)^c\}$$

is a minimal generating set of the ideal $\mathcal{I}$ *when viewed as an* $\mathcal{R}$*-module, where* $F_1(x) = f_j(x)^a + uf_j(x)^{t_1}D_1(x) + u^2 f_j(x)^{t_2}D_2(x)$ *and* $F_2(x) = uf_j(x)^b + u^2 f_j(x)^\theta V(x)$.

Proof: Working as in Theorem 16 and by applying Lemmas 10(c) and 11, 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 $\gamma \neq 0$ and the binomial $x^n - \alpha_0$ is irreducible over $\mathbb{F}_{p^m}$.

Corollary 19: Let $n \geq 1$ *be an integer and* $\alpha_0 \in \mathbb{F}_{p^m} \setminus \{0\}$ *be such that the binomial* $x^n - \alpha_0$ *is irreducible over* $\mathbb{F}_{p^m}$. *Let* $\alpha = \alpha_0^{p^s} \in \mathbb{F}_{p^m}$, *and let* γ *be a non-zero element of* $\mathbb{F}_{p^m}$. *Following the same notations as in Theorem 18, 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* $\langle u(x^n - \alpha_0)^{2^{s-1}}, u^2\rangle$ *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* $\mathcal{C} = \langle (x^n - \alpha_0)^a + u(x^n - \alpha_0)^{a-2^{s-1}}\gamma^{2^{m-1}} + u^2(x^n - \alpha_0)^{t_2}D_2(x), u(x^n - \alpha_0)^{2^{s-1}} + u^2\gamma^{2^{m-1}}, u^2(x^n - \alpha_0)^{2^s-a}\rangle$, $2^{s-1} \leq a < 2^s$, *are isodual* $(\alpha + \gamma u^2)$*-constacyclic codes of Type III over* $\mathcal{R}$.

Proof: Working in a similar manner as in Corollary 17 and by applying Theorem 18, the desired result follows. □

IV. RANKS, HAMMING DISTANCES, RT DISTANCES AND RT WEIGHT DISTRIBUTIONS

Let $\alpha, \beta, \gamma \in \mathbb{F}_{p^m}$ be such that α is non-zero. By Lemma 3(b), we see that there exists $\alpha_0 \in \mathbb{F}_{p^m}$ such that $\alpha = \alpha_0^{p^s}$. Throughout this section, we assume that $n \geq 1$ is an integer and $\alpha_0 \in \mathbb{F}_{p^m} \setminus \{0\}$ is such that the binomial $x^n - \alpha_0$ is irreducible over $\mathbb{F}_{p^m}$. In this section, we shall determine ranks, Hamming distances, RT distances and RT weight distributions of all $(\alpha + \beta u + \gamma u^2)$-constacyclic codes of length np^s over $\mathcal{R}$. We shall also list all MDS $(\alpha + \beta u + \gamma u^2)$-constacyclic codes of length np^s over $\mathcal{R}$ with respect to the Hamming and RT metrics.

In the following theorem, ranks of all non-zero $(\alpha + \beta u + \gamma u^2)$-constacyclic codes of length np^s over $\mathcal{R}$ are determined.

Theorem 20: The following hold.

(a) *Let* $\beta \in \mathbb{F}_{p^m} \setminus \{0\}$, *and let* $\mathcal{C} = \langle (x^n - \alpha_0)^\nu\rangle$ *be an* $(\alpha + \beta u + \gamma u^2)$*-constacyclic code of length* np^s *over* $\mathcal{R}$, *where* $0 \leq \nu \leq 3p^s - 1$. *Then the rank of* $\mathcal{C}$ *is given by*

$$rank(\mathcal{C}) = \begin{cases} np^s & \text{if } 0 \leq \nu \leq 2p^s - 1; \\ n(3p^s - \nu) & \text{if } 2p^s \leq \nu \leq 3p^s - 1. \end{cases}$$

(b) *Let $\mathcal{C}$ be an $(\alpha+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$ with $Tor_2(\mathcal{C}) = \langle (x^n-\alpha_0)^c\rangle$, where $0 \le c \le p^s-1$. Then we have $rank(\mathcal{C}) = np^s - nc$.*

Proof: It follows immediately from Theorems 13(b), 16 and 18. □

In the following theorem, Hamming distances of all non-zero $(\alpha+\beta u+\gamma u^2)$-constacyclic codes of length np^s over $\mathcal{R}$ are determined when β is non-zero.

Theorem 21: Let $\beta \in \mathbb{F}_{p^m}\setminus\{0\}$, and let $\mathcal{C} = \langle (x^n-\alpha_0)^\nu\rangle$ be an $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$, where $0 \le \nu \le 3p^s-1$. Then with respect to the Hamming metric, the following hold.

(a) *When $0 \le \nu \le 2p^s$, the code $\mathcal{C}$ is an $[np^s, np^s, 1]$-code over $\mathcal{R}$.*

(b) *When $2p^s+1 \le \nu \le 3p^s-1$, the code $\mathcal{C}$ is an $[np^s, n(3p^s-\nu), d_H(\mathcal{C})]$-code over $\mathcal{R}$, where*

$$d_H(\mathcal{C}) = \begin{cases} \ell+2 & \text{if } 2p^s+\ell p^{s-1}+1 \le \nu \le 2p^s \\ & \quad +(\ell+1)p^{s-1} \text{ with } 0 \le \ell \le p-2; \\ (i+1)p^k & \text{if } 3p^s-p^{s-k}+(i-1)p^{s-k-1} \\ & \quad +1 \le \nu \le 3p^s-p^{s-k}+ip^{s-k-1} \text{ with} \\ & \quad 1 \le i \le p-1 \text{ and } 1 \le k \le s-1. \end{cases}$$

Proof: The Hamming distance of the code $\mathcal{C}$ can be determined by applying Theorems 4 and 6, while Theorem 20(a) gives the rank of the code $\mathcal{C}$. □

In the following theorem, we show that there does not exist any non-trivial MDS $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$ when $\beta \neq 0$.

Theorem 22: Let $\beta \in \mathbb{F}_{p^m}\setminus\{0\}$. With respect to the Hamming metric, the code $\mathcal{C} = \langle 1\rangle$ is the only MDS $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$.

Proof: Let $\mathcal{C}$ be a non-zero $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$. Then by Theorem 13, we see that $\mathcal{C} = \langle (x^n-\alpha_0)^\nu\rangle$, where $0 \le \nu \le 3p^s-1$. By Theorem 13 again, we see that $|\mathcal{C}| = p^{mn(3p^s-\nu)}$.

Now by (1), the code $\mathcal{C}$ is MDS if and only if $p^{mn(3p^s-\nu)} = |\mathcal{C}| = p^{3m(np^s-d_H(\mathcal{C})+1)}$, which holds if and only if

$$n\nu = 3\{d_H(\mathcal{C})-1\}. \quad (2)$$

When $0 \le \nu \le 2p^s$, we see, by Theorem 21, that $d_H(\mathcal{C}) = 1$. This, by (2), implies that the code $\mathcal{C}$ is MDS if and only if $\nu = 0$.

Next let $2p^s+1 \le \nu \le 3p^s-1$. Here working as in Theorem 21, we see that $d_H(\mathcal{C})$ is equal to the Hamming distance of the α-constacyclic code $\mathcal{D} = \langle (x^n-\alpha_0)^{\nu-2p^s}\rangle$ of length np^s over $\mathbb{F}_{p^m}$. By Proposition 1, we see that $|\mathcal{D}| = p^{mn(p^s-\nu+2p^s)}$. By (1), we have $|\mathcal{D}| \le p^{m(np^s-d_H(\mathcal{D})+1)}$. This implies that $n\nu-2np^s \ge d_H(\mathcal{D})-1 = d_H(\mathcal{C})-1$. From this and using the fact that $np^s \ge d_H(\mathcal{C}) > d_H(\mathcal{C})-1$, we get $n\nu > 3\{d_H(\mathcal{C})-1\}$. This, by (2), implies that the code $\mathcal{C}$ is not MDS when $2p^s+1 \le \nu \le 3p^s-1$.

This shows that $\mathcal{C} = \langle 1\rangle$ is the only MDS $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$ with respect to the Hamming metric. □

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

Theorem 23: Let $\beta \in \mathbb{F}_{p^m}\setminus\{0\}$, and let $\mathcal{C} = \langle (x^n-\alpha_0)^\nu\rangle$ be an $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$, where $0 \le \nu \le 3p^s-1$. With respect to the RT metric, the following hold.

(a) *When $0 \le \nu \le 2p^s$, the code $\mathcal{C}$ is an $[np^s, np^s, 1]$-code over $\mathcal{R}$.*

(b) *When $2p^s+1 \le \nu \le 3p^s-1$, the code $\mathcal{C}$ is an $[np^s, n(3p^s-\nu), n\nu-2np^s+1]$-code over $\mathcal{R}$.*

Proof: By Lemma 10(b), we have $\langle (x^n-\alpha_0)^{p^s}\rangle = \langle u\rangle$, which implies that $u^2 \in \langle (x^n-\alpha_0)^\nu\rangle$ for $1 \le \nu \le 2p^s$. This implies that $d_{RT}(\mathcal{C}) = 1$ for $1 \le \nu \le 2p^s$.

Next for $2p^s+1 \le \nu \le 3p^s-1$, we note that $\mathcal{C} = \langle (x^n-\alpha_0)^\nu\rangle = \langle u^2(x^n-\alpha_0)^{\nu-2p^s}\rangle = \{u^2(x^n-\alpha_0)^{\nu-2p^s}f(x) : f(x) \in \mathbb{F}_{p^m}[x]\}$. From this, it follows that $w_{RT}(Q(x)) \ge w_{RT}(u^2(x^n-\alpha_0)^{\nu-2p^s}) = n\nu-2np^s+1$ for each $Q(x) \in \mathcal{C}\setminus\{0\}$. Moreover, we see that $w_{RT}((x^n-\alpha_0)^\nu) = w_{RT}(u^2(x^n-\alpha_0)^{\nu-2p^s}) = n\nu-2np^s+1$, which gives $d_{RT}(\mathcal{C}) = n\nu-2np^s+1$.

From this and by Theorem 20(a), we get the desired result. □

In the following theorem, we show that there does not exist any non-trivial MDS $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$ with respect to the RT metric when $\beta \neq 0$.

Theorem 24: Let $\beta \in \mathbb{F}_{p^m}\setminus\{0\}$. Then the code $\mathcal{C} = \langle 1\rangle$ is the only MDS $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$ with respect to the RT metric.

Proof: Let $\mathcal{C}$ be a non-zero $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$. Then by Theorem 13, we have $\mathcal{C} = \langle (x^n-\alpha_0)^\nu\rangle$, where $0 \le \nu \le 3p^s-1$. By Theorem 13 again, we see that $|\mathcal{C}| = p^{mn(3p^s-\nu)}$. Further, the code $\mathcal{C}$ is MDS with respect to the RT metric if and only if $p^{mn(3p^s-\nu)} = |\mathcal{C}| = p^{3m(np^s-d_{RT}(\mathcal{C})+1)}$, which holds if and only if

$$n\nu = 3\{d_{RT}(\mathcal{C})-1\}. \quad (3)$$

Now for $0 \le \nu \le 2p^s$, by Theorem 23, we see that $d_{RT}(\mathcal{C}) = 1$. By (3), we note that the code $\mathcal{C}$ is MDS if and only if $\nu = 0$.

On the other hand, when $2p^s+1 \le \nu \le 3p^s-1$, by Theorem 23, we see that $d_{RT}(\mathcal{C}) = n\nu-2np^s+1$. One can easily verify that (3) does not hold in this case. This shows that the code $\mathcal{C}$ is not MDS when $2p^s+1 \le \nu \le 3p^s-1$. □

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

Theorem 25: Let $\beta \in \mathbb{F}_{p^m}\setminus\{0\}$, and let $\mathcal{C} = \langle (x^n-\alpha_0)^\nu\rangle$ be an $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$, where $0 \le \nu \le 3p^s$. For $0 \le \rho \le np^s$, let $\mathcal{A}_\rho$ denote the number of codewords in $\mathcal{C}$ having the RT weight as ρ.

(a) *For $\nu = 3p^s$, we have*

$$\mathcal{A}_\rho = \begin{cases} 1 & \text{if } \rho = 0; \\ 0 & \text{otherwise.} \end{cases}$$

(b) *For $2p^s+1 \le \nu \le 3p^s-1$, we have*

$$\mathcal{A}_\rho = \begin{cases} 1 & \text{if } \rho = 0; \\ 0 & \text{if } 1 \le \rho \le n\nu - 2np^s; \\ (p^m-1) \quad p^{m(\rho-n\nu+2np^s-1)} & \\ \quad \text{if } n\nu - 2np^s + 1 \le \rho \le np^s. \end{cases}$$

(c) *For $\nu = yp^s$ with $y \in \{0,1,2\}$, we have*

$$\mathcal{A}_\rho = \begin{cases} 1 & \text{if } \rho = 0; \\ (p^{m(3-y)}-1)p^{m(3-y)(\rho-1)} & \text{if } 1 \le \rho \le np^s. \end{cases}$$

(d) *For $(k-1)p^s+1 \le \nu \le kp^s-1$ with $k \in \{1,2\}$, we have*

$$\mathcal{A}_\rho = \begin{cases} 1 \quad \text{if } \rho = 0; \\ (p^{m(3-k)}-1)p^{m(3-k)(\rho-1)} \\ \quad \text{if } 1 \le \rho \le \\ \ n\nu - (k-1)np^s; \\ p^{m((k-1)np^s-n\nu-4+k)}(p^{m(4-k)}-1)p^{m(4-k)\rho} \\ \quad \text{if } n\nu-(k-1)np^s+1 \le \rho \le np^s. \end{cases}$$

Proof: It is easy to see that $\mathcal{A}_0 = 1$. So from now onwards, throughout the proof, we assume that $1 \le \rho \le np^s$.

(a) When $\nu = 3p^s$, we have $\mathcal{C} = \{0\}$. This gives $\mathcal{A}_\rho = 0$ for $1 \le \rho \le np^s$.

(b) Let $2p^s+1 \le \nu \le 3p^s-1$. Here by Theorem 23, we see that $d_{RT}(\mathcal{C}) = n\nu - 2np^s + 1$, which gives $\mathcal{A}_\rho = 0$ for $1 \le \rho \le n\nu - 2np^s$. Next let $n\nu - 2np^s + 1 \le \rho \le np^s$. Here by Lemma 10(b), we see that $\langle (x^n-\alpha_0)^{p^s}\rangle = \langle u\rangle$. This implies that $\mathcal{C} = \langle u^2(x^n-\alpha_0)^{\nu-2p^s}\rangle = \{u^2(x^n-\alpha_0)^{\nu-2p^s}F(x) : F(x) \in \mathbb{F}_{p^m}[x]\}$. From this, we observe that the RT weight of the codeword $u^2(x^n-\alpha_0)^{\nu-2p^s}F(x) \in \mathcal{C}$ is ρ if and only if $\deg F(x) = \rho - n\nu + 2np^s - 1$. This gives $\mathcal{A}_\rho = (p^m-1)p^{m(\rho-n\nu+2np^s-1)}$.

(c) Next let $\nu = yp^s$, where $y \in \{0,1,2\}$. Here by Lemma 10(b), we see that $\mathcal{C} = \langle (x^n-\lambda_0)^{yp^s}\rangle = \langle u^y\rangle = \{u^yF(x) : F(x) \in \mathcal{P}_{np^s}(\mathcal{R})\}$. From this, we see that $\mathcal{A}_\rho = (p^{m(3-y)}-1)p^{m(3-y)(\rho-1)}$ for $1 \le \rho \le np^s$.

(d) Next let $(k-1)p^s+1 \le \nu \le kp^s-1$, where $k \in \{1,2\}$. Here also, by Lemma 10(b), we have $\langle (x^n-\alpha_0)^{p^s}\rangle = \langle u\rangle$, which implies that $u^k \in \mathcal{C}$ and $\mathcal{C} = \langle u^{k-1}(x^n-\alpha_0)^{\nu-(k-1)p^s}\rangle$. Further, we observe that any codeword $Q(x) \in \mathcal{C}$ can be uniquely written as $Q(x) = u^{k-1}(x^n-\alpha_0)^{\nu-(k-1)p^s}F_Q(x) + u^kH_Q(x)$, where $H_Q(x) \in \mathcal{P}_{np^s}(\mathcal{R})$ and $F_Q(x) \in \mathcal{P}_{knp^s-n\nu}(\mathbb{F}_{p^m})$.
When $1 \le \rho \le n\nu - (k-1)np^s$, we see that the RT weight of the codeword $Q(x) \in \mathcal{C}$ is ρ if and only if $F_Q(x) = 0$ and $\deg H_Q(x) = \rho - 1$. From this, we obtain $\mathcal{A}_\rho = (p^{m(3-k)}-1)p^{m(3-k)(\rho-1)}$ for $1 \le \rho \le n\nu$.
Next let $n\nu - (k-1)np^s + 1 \le \rho \le np^s$. In this case, we see that the RT weight of the codeword $Q(x) \in \mathcal{C}$ is ρ if and only if exactly one of the following two conditions is satisfied: (i) $\deg F_Q(x) = \rho - n\nu + (k-1)np^s - 1$ and $H_Q(x) \in \mathcal{P}_\rho(\mathcal{R})$, and (ii) $F_Q(x) \in \mathcal{P}_{\rho-n\nu+(k-1)np^s-1}(\mathbb{F}_{p^m})$ and $\deg H_Q(x) = \rho - 1$. From this, we obtain

$$\begin{aligned}\mathcal{A}_\rho &= (p^m-1)p^{m(\rho-n\nu+(k-1)np^s-1)}p^{m(3-k)\rho} \\ &\quad + p^{m(\rho-n\nu+(k-1)np^s-1)}(p^{m(3-k)}-1)p^{m(3-k)(\rho-1)} \\ &= p^{m((k-1)np^s-n\nu-4+k)}(p^{m(4-k)}-1)p^{m(4-k)\rho}.\end{aligned}$$

This completes the proof of the theorem. □

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

Theorem 26: Let $\mathcal{C}$ be a non-trivial $(\alpha+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$ with $Tor_2(\mathcal{C}) = \langle (x^n-\alpha_0)^c\rangle$ for some integer c satisfying $0 \le c < p^s$ (as determined in Theorems 16 and 18). Then with respect to the Hamming metric, the code $\mathcal{C}$ is an $[np^s, n(p^s-c), d_H(\mathcal{C})]$-code over $\mathcal{R}$, where

$$d_H(\mathcal{C}) = \begin{cases} 1 \text{ if } c = 0; \\ \ell+2 \text{ if } \ell p^{s-1}+1 \le c \le (\ell+1)p^{s-1} \\ \quad \text{with } 0 \le \ell \le p-2; \\ (i+1)p^k \text{ if } p^s - p^{s-k} + (i-1)p^{s-k-1}+1 \\ \quad \le c \le p^s - p^{s-k} + ip^{s-k-1} \text{ with } 1 \le i \le \\ \quad p-1 \text{ and } 1 \le k \le s-1. \end{cases}$$

Proof: By Theorem 20(b), we see that $\text{rank}(\mathcal{C}) = np^s - nc$. Further, by applying Theorems 4 and 6, one can determine the Hamming distance of the code $\mathcal{C}$. □

One can easily observe that the $(\alpha+\gamma u^2)$-constacyclic code $\mathcal{C} = \langle 1\rangle$ of length np^s over $\mathcal{R}$ is MDS with respect to both Hamming and RT metrics. In the following theorem, we list all non-trivial MDS $(\alpha+\gamma u^2)$-constacyclic codes of length np^s over $\mathcal{R}$ with respect to the Hamming metric.

Theorem 27: With respect to the Hamming metric, we have the following:

(a) *When $\gamma \ne 0$, there exists a non-trivial MDS $(\alpha+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$ if and only if $p = 2$ and $n = s = 1$. Furthermore, when $p = 2$ and $n = s = 1$, all the distinct non-trivial MDS $(\alpha+\gamma u^2)$-constacyclic codes of length 2 over $\mathcal{R}$ are given by $\langle x - \alpha_0 + u\gamma^{2^{m-1}} + u^2D_2\rangle$, where $D_2 \in \mathbb{F}_{2^m}$.*

(b) *When $\gamma = 0$, there exists a non-trivial MDS α-constacyclic code of length np^s over $\mathcal{R}$ if and only if $n = 1$. Furthermore, when $n = 1$, all the distinct non-trivial α-constacyclic codes of length p^s over $\mathcal{R}$ are given by*

$$\langle (x-\alpha_0)^a + u(x-\alpha_0)^{t_1}D_1(x) + u^2(x-\alpha_0)^{t_2}D_2(x)\rangle,$$

where $1 \le a \le p-1$ if $s = 1$ while $a \in \{1, p^s-1\}$ if $s \ge 2$, $\max\{0, 2a-p^s\} \le t_1 < a$ if $D_1(x) \ne 0$, $0 \le t_2 < a$ if $D_2(x) \ne 0$, $D_1(x)$ is either 0 or a unit in $\mathcal{R}_\alpha$ of the form $\sum_{k=0}^{a-t_1-1} C_k(x-\alpha_0)^k$ and $D_2(x)$ is either 0 or a unit in $\mathcal{R}_\alpha$ of the form $\sum_{\ell=0}^{a-t_2-1} Q_\ell(x-\alpha_0)^\ell$ with

$C_k, Q_\ell \in \mathbb{F}_{p^m}$ for each relevant k and ℓ, satisfying the following:

$$u^2(x-\alpha_0)^{p^s-a+t_2}D_2(x) - u^2(x-\alpha_0)^{p^s-2a+2t_1} D_1(x)^2 \in \langle u^2(x-\alpha_0)^a\rangle.$$

Proof: Let $\mathcal{C}$ be a non-trivial $(\alpha+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$ with $\mathrm{Tor}_2(\mathcal{C}) = \langle (x^n-\alpha_0)^c\rangle$, where $0 \le c < p^s$ (as determined in Theorems 16 and 18). Here by Theorem 26, we note that $d_H(\mathcal{C}) = d_H(\mathrm{Tor}_2(\mathcal{C}))$. By (1), we have $p^{mn(p^s-c)} = |\mathrm{Tor}_2(\mathcal{C})| \le p^{mn(p^s-d_H(\mathrm{Tor}_2(\mathcal{C}))+1)}$. This gives

$$nc \ge d_H(\mathrm{Tor}_2(\mathcal{C})) - 1 = d_H(\mathcal{C}) - 1. \tag{4}$$

(i) First let $\mathcal{C}$ be of Type I. Here by Theorems 16 and 18, we have $\mathcal{C} = \langle u^2(x^n-\alpha_0)^c\rangle$. By Theorems 16 and 18 again, we see that $|\mathcal{C}| = p^{mn(p^s-c)}$. Now by (1), the code $\mathcal{C}$ is MDS if and only if $p^{mn(p^s-c)} = |\mathcal{C}| = p^{3m(np^s-d_H(\mathcal{C})+1)}$, which holds if and only if

$$2np^s + nc = 3\{d_H(\mathcal{C}) - 1\}. \tag{5}$$

By (4) and using the fact that $p^s > c$, we get $2np^s + nc > 3\{d_H(\mathcal{C}) - 1\}$. This, by (5), implies that the code $\mathcal{C}$ is not MDS in this case.

(ii) Now let $\mathcal{C}$ be of Type II. Here by Theorems 16 and 18, we have $\mathcal{C} = \langle u(x^n-\alpha_0)^b + u^2(x^n-\alpha_0)^t G(x), u^2(x^n-\alpha_0)^c\rangle$, where $0 \le c \le b < p^s$, $\max\{0, c+b-p^s\} \le t < c$ if $G(x) \ne 0$ and $G(x)$ is either 0 or a unit in $\mathcal{R}_{\alpha+\gamma u^2}$ of the form $\sum_{i=0}^{c-t-1} B_i(x)(x^n-\alpha_0)^i$ with $B_i(x) \in \mathcal{P}_n(\mathbb{F}_{p^m})$ for each i. By Theorems 16 and 18 again, we have $|\mathcal{C}| = p^{mn(2p^s-b-c)}$. Now the code $\mathcal{C}$ is MDS if and only if $p^{mn(2p^s-b-c)} = |\mathcal{C}| = p^{3m(np^s-d_H(\mathcal{C})+1)}$, which holds if and only if

$$np^s + nb + nc = 3\{d_H(\mathcal{C}) - 1\}. \tag{6}$$

Now by (4) and using the fact that $p^s > b \ge c$, we get $np^s + nb + nc > 3\{d_H(\mathcal{C}) - 1\}$. This, by (6), shows that the code $\mathcal{C}$ is not MDS in this case.

(iii) Next let $\mathcal{C}$ be of Type III. Here by Theorems 16 and 18, we have $\mathcal{C} = \langle (x^n-\alpha_0)^a + u(x^n-\alpha_0)^{t_1}D_1(x) + u^2(x^n-\alpha_0)^{t_2}D_2(x), u(x^n-\alpha_0)^b + u^2(x^n-\alpha_0)^\theta V(x), u^2(x^n-\alpha_0)^c\rangle$, where $a > 0$, $0 \le c \le b \le a < p^s$, $\max\{0, a+b-p^s\} \le t_1 < b$ if $D_1(x) \ne 0$, $0 \le t_2 < c$ if $D_2(x) \ne 0$, $\max\{0, b+c-p^s\} \le \theta < c$ if $V(x) \ne 0$, $D_1(x)$ is either 0 or a unit in $\mathcal{R}_{\alpha+\gamma u^2}$ of the form $\sum_{k=0}^{b-t_1-1} C_k(x)(x^n-\alpha_0)^k$, $D_2(x)$ is either 0 or a unit in $\mathcal{R}_{\alpha+\gamma u^2}$ of the form $\sum_{\ell=0}^{c-t_2-1} Q_\ell(x)(x^n-\alpha_0)^\ell$ and $V(x)$ is either 0 or a unit in $\mathcal{R}_{\alpha+\gamma u^2}$ of the form $\sum_{i=0}^{c-\theta-1} W_i(x)(x^n-\alpha_0)^i$ with $C_k(x), Q_\ell(x), W_i(x) \in \mathcal{P}_n(\mathbb{F}_{p^m})$ for each relevant k, ℓ and i. Furthermore, by Theorems 16 and 18 again, we see that

$$u^2\{(x^n-\alpha_0)^{p^s-a+t_1-b+\theta}V(x)D_1(x) - (x^n-\alpha_0)^{p^s-a+t_2}D_2(x) - \gamma\} \in \langle u^2(x^n-\alpha_0)^c\rangle, \tag{7}$$

and that $|\mathcal{C}| = p^{mn(3p^s-a-b-c)}$. Now the code $\mathcal{C}$ is MDS if and only if $p^{mn(3p^s-a-b-c)} = |\mathcal{C}| = p^{3m(np^s-d_H(\mathcal{C})+1)}$, which holds if and only if

$$na + nb + nc = 3\{d_H(\mathcal{C}) - 1\}. \tag{8}$$

By (4) and using the fact that $a \ge b \ge c$, we have $na+nb+nc \ge 3\{d_H(\mathcal{C})-1\}$ and equality holds if and only if $na = nb = nc = d_H(\mathcal{C})-1 = d_H(\mathrm{Tor}_2(\mathcal{C}))-1$. Now when $a = b = c$, we see that $u^2\{(x^n-\alpha_0)^{t_1}D_1(x) - (x^n-\alpha_0)^\theta V(x)\} \in \langle u^2(x^n-\alpha_0)^a\rangle$, which implies that $t_1 = \theta$ and $D_1(x) = V(x)$. From this and using (7), we see that

$$u^2\{(x^n-\alpha_0)^{p^s-2a+2t_1}D_1(x)^2 - (x^n-\alpha_0)^{p^s-a+t_2} D_2(x) - \gamma\} \in \langle u^2(x^n-\alpha_0)^a\rangle.$$

This holds if and only if $t_1 = 0$, $p = 2$, $a = 2^{s-1}$ and $D_1(x) \ne 0$ in the case when $\gamma \ne 0$.

Further, we see, by (1) and Theorem 4, that the code $\langle (x^n-\alpha_0)^a\rangle$, $0 \le a < p^s$, of length np^s over $\mathbb{F}_{p^m}$ is MDS with respect to the Hamming metric if and only if

- $0 \le a \le p-1$ when $n = s = 1$;
- $a \in \{0, 1, p^s-1\}$ when $n = 1$ and $s \ge 2$;
- $a = 0$ when $n \ge 2$.

Using this, the desired result follows immediately. □

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 28: Let $\mathcal{C}$ be a non-trivial $(\alpha+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$ with $Tor_2(\mathcal{C}) = \langle (x^n-\alpha_0)^c\rangle$ for some integer c satisfying $0 \le c < p^s$ (as determined in Theorems 16 and 18). Then the code $\mathcal{C}$ is an $[np^s, n(p^s-c), nc+1]$-code with respect to the RT metric.

Proof: To prove the result, we first observe that

$$w_{RT}(Q(x)) \ge w_{RT}(uQ(x)) \text{ for each } Q(x) \in \mathcal{R}_{\alpha+\gamma u^2}. \tag{9}$$

(i) When $\mathcal{C}$ is of Type I, we have $\mathcal{C} = \langle u^2(x^n-\alpha_0)^c\rangle$. Here we note that $\mathcal{C} = \langle u^2(x^n-\alpha_0)^c\rangle = \{u^2(x^n-\alpha_0)^c f(x) : f(x) \in \mathbb{F}_{p^m}[x]\}$. Now for each non-zero $Q(x) \in \mathcal{C}$, by (9), we see that $w_{RT}(Q(x)) \ge w_{RT}(u^2(x^n-\alpha_0)^c) = nc+1$, which implies that $d_{RT}(\mathcal{C}) \ge nc+1$. Since $u^2(x^n-\alpha_0)^c \in \mathcal{C}$, we obtain $d_{RT}(\mathcal{C}) = nc+1$.

(ii) When $\mathcal{C}$ is of Type II, we have $\mathcal{C} = \langle u(x^n-\alpha_0)^b + u^2(x^n-\alpha_0)^t G(x), u^2(x^n-\alpha_0)^c\rangle$, where $c \le b < p^s$, $\max\{0, c+b-p^s\} \le t < c$ if $G(x) \ne 0$ and $G(x)$ is either 0 or a unit in $\mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$. Here by (9), we note that $w_{RT}(Q(x)) \geq w_{RT}(uQ(x))$ for each $Q(x) \in \mathcal{C} \setminus \langle u^2\rangle$, which implies that $w_{RT}(Q(x)) \geq d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle)$ for each $Q(x) \in \mathcal{C} \setminus \langle u^2\rangle$. From this, we get $d_{RT}(\mathcal{C}) \geq d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle)$. Since $\langle u^2(x^n-\alpha_0)^c\rangle \subseteq \mathcal{C}$, we have $d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle) \geq d_{RT}(\mathcal{C})$. This implies that $d_{RT}(\mathcal{C}) = d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle)$. From this and by case (i), we get $d_{RT}(\mathcal{C}) = nc+1$.

(iii) When $\mathcal{C}$ is of Type III, we have $\mathcal{C} = \langle (x^n-\alpha_0)^a + u(x^n-\alpha_0)^{t_1}D_1(x) + u^2(x^n-\alpha_0)^{t_2}D_2(x), u(x^n-\alpha_0)^b + u^2(x^n-\alpha_0)^{\theta}V(x), u^2(x^n-\alpha_0)^c\rangle$, where $c \leq b \leq a < p^s$, $\max\{0, a+b-p^s\} \leq t_1 < b$ if $D_1(x) \neq 0$, $0 \leq t_2 < c$ if $D_2(x) \neq 0$, $\max\{0, b+c-p^s\} \leq \theta < c$ if $V(x) \neq 0$ and $D_1(x), D_2(x), V(x)$ are either 0 or a units in $\mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$. For each $Q(x) \in \mathcal{C} \setminus \langle u\rangle$, by (9), we see that $w_{RT}(Q(x)) \geq w_{RT}(u^2\, Q(x))$. From this, we get $w_{RT}(Q(x)) \geq d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle)$ 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 $Q(x) \in \langle u\rangle$, by (9) again, we see that $w_{RT}(Q(x)) \geq w_{RT}(uQ(x)) \geq d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle)$. This implies that $d_{RT}(\mathcal{C}) \geq d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle)$. On the other hand, as $\langle u^2(x^n-\alpha_0)^c\rangle \subseteq \mathcal{C}$, we have $d_{RT}(u^2(x^n-\alpha_0)^c\rangle) \geq d_{RT}(\mathcal{C})$, which implies that $d_{RT}(\mathcal{C}) = d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle)$. From this and by case (i), we get $d_{RT}(\mathcal{C}) = nc+1$.

From this and by Theorem 20(b), the desired result follows. □

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

Theorem 29: With respect to the RT metric, we have the following:

(a) *When $\gamma \neq 0$, there exists a non-trivial MDS $(\alpha+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$ if and only if $p = 2$. Furthermore, when $p = 2$, all the distinct $(\alpha+\gamma u^2)$-constacyclic codes of length $2^s n$ over $\mathcal{R}$ are given by*

$$\langle (x^n-\alpha_0)^{2^{s-1}} + uD_1(x) + u^2(x^n-\alpha_0)^{t_2}D_2(x)\rangle,$$

where $0 \leq t_2 < 2^{s-1}$ if $D_2(x) \neq 0$, $D_1(x)$ is a unit in $\mathcal{R}_{\alpha+\gamma u^2}$ of the form $\sum_{k=0}^{2^{s-1}-1} B_k(x)(x^n-\alpha_0)^k$ and $D_2(x)$ is either 0 or a unit in $\mathcal{R}_{\alpha+\gamma u^2}$ of the form $\sum_{\ell=0}^{2^{s-1}-t_2-1} C_\ell(x)(x^n-\alpha_0)^\ell$ with $B_k(x), C_\ell(x) \in \mathcal{P}_n(\mathbb{F}_{2^m})$ for each relevant k and ℓ, satisfying the following:

$$u^2\{\gamma - D_1(x)^2\} \in \langle u^2(x^n-\alpha_0)^{2^{s-1}}\rangle.$$

(b) *When $\gamma = 0$, all the distinct non-trivial MDS α-constacyclic codes of length np^s over $\mathcal{R}$ are given by*

$$\langle (x^n-\alpha_0)^a + u(x^n-\alpha_0)^{t_1}D_1(x) + u^2(x^n-\alpha_0)^{t_2}D_2(x)\rangle,$$

where $1 \leq a \leq p^s-1$, $\max\{0, 2a-p^s\} \leq t_1 < a$ if $D_1(x) \neq 0$, $0 \leq t_2 < a$ if $D_2(x) \neq 0$, $D_1(x)$ is either 0 or a unit in $\mathcal{R}_\alpha$ of the form $\sum_{k=0}^{a-t_1-1} Q_k(x)(x^n-\alpha_0)^k$ and $D_2(x)$ is either 0 or a unit in $\mathcal{R}_\alpha$ of the form $\sum_{\ell=0}^{a-t_2-1} W_\ell(x)(x^n-\alpha_0)^\ell$ with $Q_k(x), W_\ell(x) \in \mathcal{P}_n(\mathbb{F}_{p^m})$ for each relevant k and ℓ, satisfying the following:

$$u^2\{(x^n-\alpha_0)^{p^s-a+t_2}D_2(x) - (x^n-\alpha_0)^{p^s-2a+2t_1} D_1(x)^2\} \in \langle u^2(x^n-\alpha_0)^a\rangle.$$

Proof: To prove this, let $\mathcal{C}$ be a non-trivial $(\alpha+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$ with $\mathrm{Tor}_2(\mathcal{C}) = \langle (x^n-\alpha_0)^c\rangle$, where $0 \leq c < p^s$ (as determined in Theorems 16 and 18). Then by Theorem 28, we see that $d_{RT}(\mathcal{C}) = nc+1$.

(i) First let $\mathcal{C}$ be of Type I. Here by Theorems 16 and 18, we have $\mathcal{C} = \langle u^2(x^n-\alpha_0)^c\rangle$. By Theorems 16 and 18 again, we see that $|\mathcal{C}| = p^{mn(p^s-c)}$. Now the code $\mathcal{C}$ is MDS with respect to the RT metric if and only if $p^{mn(p^s-c)} = |\mathcal{C}| = p^{3m(np^s-d_{RT}(\mathcal{C})+1)}$, which holds if and only if

$$2np^s + nc = 3\{d_{RT}(\mathcal{C})-1\} = 3nc. \quad (10)$$

As $p^s > c$, we get $2np^s+nc > 3nc$. From this and by (10), we see that the code $\mathcal{C}$ is not MDS in this case.

(ii) Let $\mathcal{C}$ be of Type II. Here by Theorems 16 and 18, we have $\mathcal{C} = \langle u(x^n-\alpha_0)^b + u^2(x^n-\alpha_0)^t G(x), u^2(x^n-\alpha_0)^c\rangle$, where $0 \leq b < p^s$, $\max\{0, c+b-p^s\} \leq t < c$ if $G(x) \neq 0$ and $G(x)$ is either 0 or a unit in $\mathcal{R}_{\alpha+\gamma u^2}$ of the form $\sum_{i=0}^{c-t-1} B_i(x)(x^n-\alpha_0)^i$ with $B_i(x) \in \mathcal{P}_n(\mathbb{F}_{p^m})$ for each i. By Theorems 16 and 18 again, we have $|\mathcal{C}| = p^{mn(2p^s-b-c)}$. Now the code $\mathcal{C}$ is MDS with respect to the RT metric if and only if $p^{mn(2p^s-b-c)} = |\mathcal{C}| = p^{3m(np^s-d_H(\mathcal{C})+1)}$, which holds if and only if

$$np^s + nb + nc = 3\{d_{RT}(\mathcal{C})-1\} = 3nc. \quad (11)$$

Now as $p^s > b \geq c$, we have $np^s+nb+nc > 3nc$. From this and by (11), we see that the code $\mathcal{C}$ is not MDS in this case.

(iii) Let $\mathcal{C}$ be of Type III. Here by Theorems 16 and 18, we have $\mathcal{C} = \langle (x^n-\alpha_0)^a + u(x^n-\alpha_0)^{t_1}D_1(x) + u^2(x^n-\alpha_0)^{t_2}D_2(x), u(x^n-\alpha_0)^b + u^2(x^n-\alpha_0)^{\theta}V(x), u^2(x^n-\alpha_0)^c\rangle$, where $0 \leq b \leq a < p^s$, $\max\{0, a+b-p^s\} \leq t_1 < b$ if $D_1(x) \neq 0$, $0 \leq t_2 < c$ if $D_2(x) \neq 0$, $\max\{0, b+c-p^s\} \leq \theta < c$ if $V(x) \neq 0$, $D_1(x)$ is either 0 or a unit in $\mathcal{R}_{\alpha+\gamma u^2}$ of the form $\sum_{k=0}^{b-t_1-1} C_k(x)(x^n-\alpha_0)^k$, $D_2(x)$ is either 0 or a unit in $\mathcal{R}_{\alpha+\gamma u^2}$ of the form $\sum_{\ell=0}^{c-t_2-1} Q_\ell(x)(x^n-\alpha_0)^\ell$ and $V(x)$ is either 0 or a unit in $\mathcal{R}_{\alpha+\gamma u^2}$ of the form $\sum_{i=0}^{c-\theta-1} W_i(x)(x^n-\alpha_0)^i$ with $C_k(x), Q_\ell(x), W_i(x) \in \mathcal{P}_n(\mathbb{F}_{p^m})$ for each relevant

k,ℓ and i. By Theorems 16 and 18 again, we see that

$$u^2\{(x^n-\alpha_0)^{p^s-a+t_1-b+\theta}V(x)D_1(x) \\ -(x^n-\alpha_0)^{p^s-a+t_2}D_2(x)-\gamma\}\in\langle u^2(x^n-\alpha_0)^c\rangle, \quad (12)$$

and that $|\mathcal{C}| = p^{mn(3p^s-a-b-c)}$. Now the code $\mathcal{C}$ is MDS with respect to the RT metric if and only if $p^{mn(3p^s-a-b-c)} = |\mathcal{C}| = p^{3m(np^s-d_{RT}(\mathcal{C})+1)}$, which holds if and only if

$$na+nb+nc = 3\{d_{RT}(\mathcal{C})-1\} = 3nc. \quad (13)$$

Using the fact that $a\geq b\geq c$, we obtain $na+nb+nc\geq 3nc$, and the equality holds if and only if $a=b=c$. Now when $a=b=c$, we see that $u^2\{(x^n-\alpha_0)^{t_1}D_1(x) -(x^n-\alpha_0)^{\theta}V(x)\}\in\langle u^2(x^n-\alpha_0)^a\rangle$, which implies that $t_1=\theta$ and $D_1(x)=V(x)$. From this and using (12), we get $u^2\{(x^n-\alpha_0)^{p^s-2a+2t_1}D_1(x)^2-(x^n-\alpha_0)^{p^s-a+t_2}D_2(x)-\gamma\}\in\langle u^2(x^n-\alpha_0)^a\rangle$. This holds if and only if $t_1=0$, $p=2$, $a=2^{s-1}$ and $D_1(x)\neq 0$ in the case when $\gamma\neq 0$.
From this, the desired result follows.

□

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 30: Let $\mathcal{C}$ be an $(\alpha+\gamma u^2)$-constacyclic code of length np^s over $\mathcal{R}$ with $Tor_0(\mathcal{C})=\langle(x^n-\alpha_0)^a\rangle$, $Tor_1(\mathcal{C})=\langle(x^n-\alpha_0)^b\rangle$ and $Tor_2(\mathcal{C})=\langle(x^n-\alpha_0)^c\rangle$ for some integers a,b,c satisfying $0\leq c\leq b\leq a\leq p^s$ (as determined in Theorems 16 and 18). For $0\leq\rho\leq np^s$, let $\mathcal{A}_\rho$ denote the number of codewords in $\mathcal{C}$ having the RT weight as ρ.

(a) *If $\mathcal{C}=\{0\}$, then we have $\mathcal{A}_0=1$ and $\mathcal{A}_\rho=0$ for $1\leq\rho\leq np^s$.*
(b) *If $\mathcal{C}=\langle 1\rangle$, then we have $\mathcal{A}_0=1$ and $\mathcal{A}_\rho=(p^{3m}-1)p^{3m(\rho-1)}$ 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*

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

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

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

(e) *If $\mathcal{C}=\langle(x^n-\alpha_0)^a+u(x^n-\alpha_0)^{t_1}D_1(x)+u^2(x^n-\alpha_0)^{t_2}D_2(x), u(x^n-\alpha_0)^b+u^2(x^n-\alpha_0)^{\theta}V(x), u^2(x^n-\alpha_0)^c\rangle$ is of Type III, then we have*

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

Proof: Proofs of parts (a) and (b) are trivial. To prove parts (c)-(e), by Theorem 28(c), we see that $d_{RT}(\mathcal{C})=nc+1$, which implies that $\mathcal{A}_\rho=0$ for $1\leq\rho\leq nc$. So from now on, we assume that $nc+1\leq\rho\leq np^s$.

(c) Let $\mathcal{C}=\langle u^2(x^n-\alpha_0)^c\rangle$. Here we see that $\mathcal{C}=\langle u^2(x^n-\alpha_0)^c\rangle=\{u^2(x^n-\alpha_0)^cF(x) : F(x)\in\mathbb{F}_{p^m}[x]\}$. This implies that the codeword $u^2(x^n-\alpha_0)^cF(x)\in\mathcal{C}$ has RT weight ρ if and only if $\deg F(x)=\rho-nc-1$. From this, we obtain $\mathcal{A}_\rho=(p^m-1)p^{m(\rho-nc-1)}$.
(d) Let $\mathcal{C}=\langle u(x^n-\alpha_0)^b+u^2(x^n-\alpha_0)^tG(x), u^2(x^n-\alpha_0)^c\rangle$. Here we observe that each codeword $Q(x)\in\mathcal{C}$ can be uniquely expressed as $Q(x)=(u(x^n-\alpha_0)^b+u^2(x^n-\alpha_0)^tG(x))A_Q(x)+u^2(x^n-\alpha_0)^cB_Q(x)$, where $A_Q(x),B_Q(x)\in\mathbb{F}_{p^m}[x]$ 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 ρ if and only if $A_Q(x)=0$ and $\deg B_Q(x)=\rho-nc-1$. This implies that $\mathcal{A}_\rho=(p^m-1)p^{m(\rho-nc-1)}$ 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 ρ 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 $\deg A_Q(x)\leq$
$textrho-nb-2$ and $\deg B_Q(x)=\rho-nc-1$. From this, we get $\mathcal{A}_\rho=(p^{2m}-1)p^{m(2\rho-nb-nc-2)}$ for $nb+1\leq\rho\leq np^s$.
(e) Let $\mathcal{C}=\langle(x^n-\alpha_0)^a+u(x^n-\alpha_0)^{t_1}D_1(x)+u^2(x^n-\alpha_0)^{t_2}D_2(x), u(x^n-\alpha_0)^b+u^2(x^n-\alpha_0)^{\theta}V(x)$, $u^2(x^n-\alpha_0)^c\rangle$. Here we see that each codeword $Q(x)\in\mathcal{C}$ can be uniquely expressed as $Q(x)=((x^n-\alpha_0)^a+u(x^n-\alpha_0)^{t_1}D_1(x)+u^2(x^n-\alpha_0)^{t_2}D_2(x))M_Q(x)+(u(x^n-\alpha_0)^b+u^2(x^n-\alpha_0)^{\theta}V(x))N_Q(x)+u^2(x^n-\alpha_0)^cW_Q(x)$, where $M_Q(x),N_Q(x),W_Q(x)\in\mathbb{F}_{p^m}[x]$ 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 $W_Q(x)\neq 0$.
If $nc+1\leq\rho\leq nb$, then the codeword $Q(x)\in\mathcal{C}$ has RT weight ρ if and only if $M_Q(x)=N_Q(x)=0$ and $\deg W_Q(x)=\rho-nc-1$. This implies that $\mathcal{A}_\rho=(p^m-1)p^{m(\rho-nc-1)}$.
Further, if $nb+1\leq\rho\leq na$, then the RT weight of the codeword $Q(x)\in\mathcal{C}$ is ρ if and only if $M_Q(x)=0$ and one of the following two conditions are satisfied:

(i) $\deg N_Q(x) = \rho - nb - 1$ and $W_Q(x)$ is either 0 or $\deg W_Q(x) \leq \rho - 1 - nc$; and (ii) $N_Q(x)$ is either 0 or $\deg N_Q(x) \leq \rho - nb - 2$ and $\deg W_Q(x) = \rho - nc - 1$. This implies that $\mathcal{A}_\rho = (p^{2m}-1)p^{m(2\rho - n\omega - n\mu - 2)}$.

Next let $na + 1 \leq \rho \leq np^s$. Here the RT weight of the codeword $Q(x) \in \mathcal{C}$ is ρ if and only if exactly one of the following three conditions is satisfied: (i) $\deg M_Q(x) = \rho - na - 1$, $N_Q(x)$ is either 0 or $\deg N_Q(x) \leq \rho - nb - 1$ and $W_Q(x)$ is either 0 or $\deg W_Q(x) \leq \rho - nc - 1$; (ii) $M_Q(x)$ is either 0 or $\deg M_Q(x) \leq \rho - na - 2$, $\deg N_Q(x) = \rho - nb - 1$ and $W_Q(x)$ is either 0 or $\deg W_Q(x) \leq \rho - nc - 1$; and (iii) $M_Q(x)$ is either 0 or $\deg M_Q(x) \leq \rho - na - 2$, $N_Q(x)$ is either 0 or $\deg N_Q(x) \leq \rho - nb - 2$ and $\deg W_Q(x) = \rho - nc - 1$. This implies that $\mathcal{A}_\rho = (p^{3m}-1)p^{m(3\rho - na - nb - nc - 3)}$ for $na + 1 \leq \rho \leq np^s$.

This completes the proof of the theorem. □

V. HAMMING DISTANCES OF CONSTACYCLIC CODES OF LENGTH $2p^s$ OVER $\mathcal{R}$ AND DETERMINATION OF MDS CODES

Throughout this section, let p be an odd prime. Here we will determine Hamming distances of all constacyclic codes of length $2p^s$ over $\mathcal{R}$, and we will also identify all MDS constacyclic codes of length $2p^s$ over $\mathcal{R}$ with respect to the Hamming metric. For this, we recall that $\lambda = \alpha + \beta u + \gamma u^2$, where α, β, γ are elements of $\mathbb{F}_{p^m}$ and α is non-zero. By Lemma 3(b), we see that there exists $\alpha_0 (\neq 0) \in \mathbb{F}_{p^m}$ such that $\alpha = \alpha_0^{p^s}$. Here we have $\mathcal{R}_\lambda = \mathcal{R}[x]/\langle x^{2p^s} - \lambda\rangle$.

When $\alpha_0 \in \mathbb{F}_{p^m}$ is not a square in $\mathbb{F}_{p^m}$, the binomial $x^2 - \alpha_0$ is irreducible over $\mathbb{F}_{p^m}$, and one can determine Hamming distances of all $(\alpha + \beta u + \gamma u^2)$-constacyclic codes of length $2p^s$ over $\mathcal{R}$ and identify all MDS codes within this class of codes on taking $n = 2$ in Theorems 21, 22, 26 and 27.

So from now on, throughout this section, we assume that $\alpha_0 (\neq 0) \in \mathbb{F}_{p^m}$ is a square in $\mathbb{F}_{p^m}$, i.e., there exists $\zeta (\neq 0) \in \mathbb{F}_{p^m}$ such that $\alpha_0 = \zeta^2$. This implies that $x^2 - \alpha_0 = (x+\zeta)(x-\zeta)$. From this and working as in Section III, we get

$$\mathcal{R}_\lambda \simeq \mathcal{K}_1 \oplus \mathcal{K}_2,$$

where $\mathcal{K}_1 = \mathcal{R}[x]/\left\langle (x+\zeta)^{p^s} + ug_1(x) + u^2 h_1(x)\right\rangle$ and $\mathcal{K}_2 = \mathcal{R}[x]/\left\langle (x-\zeta)^{p^s} + ug_2(x) + u^2 h_2(x)\right\rangle$, where for $j \in \{1,2\}$, the polynomials $g_j(x), h_j(x) \in \mathbb{F}_{p^m}[x]$ satisfy $\gcd(x+\zeta, g_1(x)) = \gcd(x-\zeta, g_2(x)) = 1$ when $\beta \neq 0$, $g_j(x) = h_j(x) = 0$ when $\beta = \gamma = 0$, while $g_j(x) = 0$ and $\gcd(x+\zeta, h_1(x)) = \gcd(x-\zeta, h_2(x)) = 1$ when $\beta = 0$ and $\gamma \neq 0$.

Now let $\mathcal{C}$ be an $(\alpha + \beta u + \gamma u^2)$-constacyclic code of length $2p^s$ over $\mathcal{R}$, i.e., an ideal of the ring $\mathcal{R}_\lambda$. Then by Proposition 8, we have

$$\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2, \tag{14}$$

where $\mathcal{C}_j$ is an ideal of $\mathcal{K}_j$ for $j \in \{1,2\}$. Further, we note that an element $a(x) \in \mathcal{R}_\lambda$ can be written as $a(x) = a_0(x) + ua_1(x) + u^2 a_2(x)$, where $a_0(x), a_1(x), a_2(x) \in \mathbb{F}_{p^m}[x]/\langle (x^2-\alpha_0)^{p^s}\rangle$. Let us define $\text{Tor}_0(\mathcal{C}) = \{c_0(x) \in \mathbb{F}_{p^m}[x]/\langle (x^2-\alpha_0)^{p^s}\rangle : c_0(x) + uc_1(x) + u^2 c_2(x) \in \mathcal{C}$ for some $c_1(x), c_2(x) \in \mathbb{F}_{p^m}[x]/\langle (x^2-\alpha_0)^{p^s}\rangle\}$, $\text{Tor}_1(\mathcal{C}) = \{c_1(x) \in \mathbb{F}_{p^m}[x]/\langle (x^2-\alpha_0)^{p^s}\rangle : uc_1(x) + u^2 c_2(x) \in \mathcal{C}$ for some $c_2(x) \in \mathbb{F}_{p^m}[x]/\langle (x^2-\alpha_0)^{p^s}\rangle\}$ and $\text{Tor}_2(\mathcal{C}) = \{c_2(x) \in \mathbb{F}_{p^m}[x]/\langle (x^2-\alpha_0)^{p^s}\rangle : u^2 c_2(x) \in \mathcal{C}\}$. Then we make the following observation.

Proposition 31: Let $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$ be an $(\alpha + \beta u + \gamma u^2)$-constacyclic code of length $2p^s$ over $\mathcal{R}$ (i.e., an ideal of the ring $\mathcal{R}_\lambda$), where $\mathcal{C}_j$ is an ideal of $\mathcal{K}_j$ for $j \in \{1,2\}$. Then $Tor_0(\mathcal{C})$, $Tor_1(\mathcal{C})$ and $Tor_2(\mathcal{C})$ are ideals of $\mathbb{F}_{p^m}[x]/\langle (x^2-\alpha_0)^{p^s}\rangle$. Moreover, we have $Tor_i(\mathcal{C}) = Tor_i(\mathcal{C}_1) \oplus Tor_i(\mathcal{C}_2)$ for $0 \leq i \leq 2$, where for $i \in \{0,1,2\}$, $Tor_i(\mathcal{C}_1)$ and $Tor_i(\mathcal{C}_2)$ are ideals of $\mathbb{F}_{p^m}[x]/\langle (x+\zeta)^{p^s}\rangle$ and $\mathbb{F}_{p^m}[x]/\langle (x-\zeta)^{p^s}\rangle$, respectively.

Proof: Proof is trivial. □

Remark 32: Each $(\alpha + \beta u + \gamma u^2)$-constacyclic code $\mathcal{C}$ of length $2p^s$ over $\mathcal{R}$ can be expressed as $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$, where $\mathcal{C}_j$ is an ideal of $\mathcal{K}_j$ for $j \in \{1,2\}$. By Proposition 31, we see that $Tor_0(\mathcal{C})$, $Tor_1(\mathcal{C})$ and $Tor_2(\mathcal{C})$ are ideals of $\mathbb{F}_{p^m}[x]/\langle (x^2-\alpha_0)^{p^s}\rangle$, and that $Tor_i(\mathcal{C}) = Tor_i(\mathcal{C}_1) \oplus Tor_i(\mathcal{C}_2)$ for $0 \leq i \leq 2$, where for $i \in \{0,1,2\}$, $Tor_i(\mathcal{C}_1)$ and $Tor_i(\mathcal{C}_2)$ are ideals of $\mathbb{F}_{p^m}[x]/\langle (x+\zeta)^{p^s}\rangle$ and $\mathbb{F}_{p^m}[x]/\langle (x-\zeta)^{p^s}\rangle$, respectively. Further, as $\mathbb{F}_{p^m}[x]/\langle (x+\zeta)^{p^s}\rangle$ and $\mathbb{F}_{p^m}[x]/\langle (x-\zeta)^{p^s}\rangle$ are finite commutative chain rings with the respective maximal ideals as $\langle x+\zeta\rangle$ and $\langle x-\zeta\rangle$, we have $Tor_0(\mathcal{C}_1) = \langle (x+\zeta)^{a_1}\rangle$, $Tor_0(\mathcal{C}_2) = \langle (x-\zeta)^{a_2}\rangle$, $Tor_1(\mathcal{C}_1) = \langle (x+\zeta)^{b_1}\rangle$, $Tor_1(\mathcal{C}_2) = \langle (x-\zeta)^{b_2}\rangle$, $Tor_2(\mathcal{C}_1) = \langle (x+\zeta)^{c_1}\rangle$ and $Tor_2(\mathcal{C}_2) = \langle (x-\zeta)^{c_2}\rangle$ for some integers $a_1, b_1, c_1, a_2, b_2, c_2$ satisfying $0 \leq c_1 \leq b_1 \leq a_1 \leq p^s$ and $0 \leq c_2 \leq b_2 \leq a_2 \leq p^s$. Now by applying the Chinese Remainder Theorem, we get $Tor_0(\mathcal{C}) = \langle (x+\zeta)^{a_1}(x-\zeta)^{a_2}\rangle$, $Tor_1(\mathcal{C}) = \langle (x+\zeta)^{b_1}(x-\zeta)^{b_2}\rangle$ and $Tor_2(\mathcal{C}) = \langle (x+\zeta)^{c_1}(x-\zeta)^{c_2}\rangle$.

In the following theorem, Hamming distances of all non-zero $(\alpha + \beta u + \gamma u^2)$-constacyclic codes of length $2p^s$ over $\mathcal{R}$ are determined.

Theorem 33: Let $\mathcal{C}$ be a non-zero $(\alpha + \beta u + \gamma u^2)$-constacyclic code of length $2p^s$ over $\mathcal{R}$ with $Tor_2(\mathcal{C}) = \langle (x+\zeta)^{c_1}(x-\zeta)^{c_2}\rangle$ for some integers c_1, c_2 satisfying $0 \leq c_1, c_2 \leq p^s$.

(a) *When $c_1 \geq c_2$, the Hamming distance $d_H(\mathcal{C})$ of the code $\mathcal{C}$ is given by*

$$d_H(\mathcal{C}) = \begin{cases} 1 & \text{if } c_1 = c_2 = 0; \\ 2 & \text{if } c_2 = 0 \text{ and } 0 < c_1 \leq p^s; \\ \min\{(\ell+2)p^k, 2(\ell_1+2)p^{k'}\} & \text{if } p^s - p^{s-k} + \ell p^{s-k-1} + 1 \leq c_1 \leq p^s - p^{s-k} + (\ell+1)p^{s-k-1} \text{ and } p^s - p^{s-k'} + \ell_1 p^{s-k'-1} + 1 \leq c_2 \leq p^s - p^{s-k'} + (\ell_1+1)p^{s-k'-1} \text{ with } 0 \leq \ell, \ell_1 \leq p-2, \text{ and } 0 \leq k' \leq k \leq s-1; \\ 2(\ell_1+2)p^{k'} & \text{if } c_1 = p^s \text{ and } p^s - p^{s-k'} + \ell_1 p^{s-k'-1} + 1 \leq c_2 \leq p^s - p^{s-k'} + (\ell_1+1)p^{s-k'-1} \text{ with } 0 \leq \ell_1 \leq p-2 \text{ and } 0 \leq k' \leq s-1. \end{cases}$$

(b) *When $c_2 \geq c_1$, the Hamming distance $d_H(\mathcal{C})$ of the code $\mathcal{C}$ is given by*

$$d_H(\mathcal{C}) = \begin{cases} 1 & \text{if } c_1 = c_2 = 0; \\ 2 & \text{if } c_1 = 0 \text{ and } 0 < c_2 \leq p^s; \\ \min\{(\ell+2)p^k, 2(\ell_1+2)p^{k'}\} \text{ if} \\ \quad p^s - p^{s-k} + \ell p^{s-k-1} + 1 \leq c_2 \leq p^s - p^{s-k} \\ \quad + (\ell+1)p^{s-k-1} \text{ and } p^s - p^{s-k'} \\ \quad + \ell_1 p^{s-k'-1} + 1 \leq c_1 \leq p^s - p^{s-k'} \\ \quad + (\ell_1+1)p^{s-k'-1} \text{ with } 0 \leq \ell, \ell_1 \leq p-2, \\ \quad \text{and } 0 \leq k' \leq k \leq s-1; \\ 2(\ell_1+2)p^{k'} \text{ if } c_2 = p^s \text{ and } p^s - p^{s-k'} \\ \quad + \ell_1 p^{s-k'-1} + 1 \leq c_1 \leq p^s - p^{s-k'} \\ \quad + (\ell_1+1)p^{s-k'-1} \text{ with } 0 \leq \ell_1 \leq p-2 \\ \quad \text{and } 0 \leq k' \leq s-1. \end{cases}$$

Proof: It follows immediately by applying Theorems 5 and 6. □

In the following theorem, we derive a necessary and sufficient conditions for an $(\alpha + \beta u + \gamma u^2)$-constacyclic code of length $2p^s$ over $\mathcal{R}$ to be an MDS code with respect to the Hamming metric.

Theorem 34: Let $\mathcal{C}$ be an $(\alpha+\beta u+\gamma u^2)$-constacyclic code of length $2p^s$ over $\mathcal{R}$ with $Tor_0(\mathcal{C}) = \langle (x+\zeta)^{a_1}(x-\zeta)^{a_2}\rangle$, $Tor_1(\mathcal{C}) = \langle (x+\zeta)^{b_1}(x-\zeta)^{b_2}\rangle$ and $Tor_2(\mathcal{C}) = \langle (x+\zeta)^{c_1}(x-\zeta)^{c_2}\rangle$ for some integers $a_1, b_1, c_1, a_2, b_2, c_2$ satisfying $0 \leq c_1 \leq b_1 \leq a_1 \leq p^s$ and $0 \leq c_2 \leq b_2 \leq a_2 \leq p^s$. Then the code $\mathcal{C}$ is an MDS code with respect to the Hamming metric if and only if $a_1 = b_1 = c_1$, $a_2 = b_2 = c_2$ and $Tor_2(\mathcal{C})$ is an MDS α-constacyclic code of length $2p^s$ over $\mathbb{F}_{p^m}$ with respect to the Hamming metric.

Proof: To prove this, we see, by (14), that $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$, where $\mathcal{C}_j$ is an ideal of $\mathcal{K}_j$ for $j \in \{1, 2\}$. Further, by applying Proposition 31 and the Chinese Remainder Theorem, we get $\text{Tor}_0(\mathcal{C}_1) = \langle (x+\zeta)^{a_1}\rangle$, $\text{Tor}_0(\mathcal{C}_2) = \langle (x-\zeta)^{a_2}\rangle$, $\text{Tor}_1(\mathcal{C}_1) = \langle (x+\zeta)^{b_1}\rangle$, $\text{Tor}_1(\mathcal{C}_2) = \langle (x-\zeta)^{b_2}\rangle$, $\text{Tor}_2(\mathcal{C}_1) = \langle (x+\zeta)^{c_1}\rangle$ and $\text{Tor}_2(\mathcal{C}_2) = \langle (x-\zeta)^{c_2}\rangle$.

Now since $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$, by Lemma 11, we have

$$|\mathcal{C}| = |\mathcal{C}_1||\mathcal{C}_2| = |\text{Tor}_0(\mathcal{C}_1)||\text{Tor}_1(\mathcal{C}_1)||\text{Tor}_2(\mathcal{C}_1)||\text{Tor}_0(\mathcal{C}_2)| \times |\text{Tor}_1(\mathcal{C}_2)||\text{Tor}_2(\mathcal{C}_2)| = p^{m(6p^s - a_1 - a_2 - b_1 - b_2 - c_1 - c_2)}$$

From this, we observe that the code $\mathcal{C}$ is MDS with respect to the Hamming metric if and only if

$$p^{m(6p^s - a_1 - a_2 - b_1 - b_2 - c_1 - c_2)} = |\mathcal{C}| = p^{3m(2p^s - d_H(\mathcal{C})+1)},$$

which holds if and only if

$$a_1 + a_2 + b_1 + b_2 + c_1 + c_2 + 3 = 3d_H(\mathcal{C}).$$

Next by Theorem 6, we see that the Hamming distance $d_H(\mathcal{C})$ of the code $\mathcal{C}$ is equal to the Hamming distance $d_H(\text{Tor}_2(\mathcal{C}))$ of the α-constacyclic code $\text{Tor}_2(\mathcal{C}) = \langle (x+\zeta)^{c_1}(x-\zeta)^{c_2}\rangle$ of length $2p^s$ over $\mathbb{F}_{p^m}$. Now by the Singleton bound (1) for $\text{Tor}_2(\mathcal{C})$, we have $p^{m(2p^s - c_1 - c_2)} \leq p^{m(2p^s - d_H(\text{Tor}_2(\mathcal{C}))+1)}$, which implies that $c_1 + c_2 + 1 \geq d_H(\text{Tor}_2(\mathcal{C})) = d_H(\mathcal{C})$. From this and using the fact that $p^s \geq a_1 \geq b_1 \geq c_1 \geq 0$ and $p^s \geq a_2 \geq b_2 \geq c_2 \geq 0$, we obtain $a_1 + a_2 + b_1 + b_2 + c_1 + c_2 + 3 \geq 3d_H(\mathcal{C})$, with the equality holds if and only if $a_1 = b_1 = c_1$, $a_2 = b_2 = c_2$ and $\text{Tor}_2(\mathcal{C})$ is an MDS code of length $2p^s$ over $\mathbb{F}_{p^m}$ with respect to the Hamming metric. This completes the proof of the theorem. □

In the following theorem, we list all non-trivial MDS $(\alpha + \beta u + \gamma u^2)$-constacyclic codes of length $2p^s$ over $\mathcal{R}$ with respect to the Hamming metric.

Theorem 35: With respect to the Hamming metric, we have the following:

(a) *When either β is non-zero or γ is non-zero, there does not exist any non-trivial MDS $(\alpha + \beta u + \gamma u^2)$-constacyclic code of length $2p^s$ over $\mathcal{R}$.*

(b) *When $\beta = \gamma = 0$, all the distinct non-trivial α-constacyclic codes of length $2p^s$ over $\mathcal{R}$ are as listed below:*

- $\langle (x+\zeta)^{a_1} + u(x+\zeta)^{t_1}D_1(x) + u^2(x+\zeta)^{t_2}D_2(x)\rangle \oplus \mathcal{C}_2$, *where either $a_1 = p^s - 1$ and $\mathcal{C}_2 = \{0\}$ or $a_1 = 1$ and $\mathcal{C}_2 = \langle 1\rangle = \mathcal{K}_2$ with $\max\{0, 2a_1 - p^s\} \leq t_1 < a_1$ if $D_1(x) \neq 0$, $0 \leq t_2 < a_1$ if $D_2(x) \neq 0$, $D_1(x)$ is either 0 or a unit in $\mathcal{K}_1$ of the form $\sum_{k=0}^{a_1-t_1-1} C_k(x+\zeta)^k$ and $D_2(x)$ is either 0 or a unit in $\mathcal{K}_1$ of the form $\sum_{\ell=0}^{a_1-t_2-1} Q_\ell(x+\zeta)^\ell$ with $C_k, Q_\ell \in \mathbb{F}_{p^m}$ for each relevant k and ℓ, satisfying the following:*

$$u^2(x+\zeta)^{p^s - a_1 + t_2}D_2(x) - u^2(x+\zeta)^{p^s - 2a_1 + 2t_1} D_1(x)^2 \in \langle u^2(x+\zeta)^{a_1}\rangle.$$

- $\mathcal{C}_1 \oplus \langle (x-\zeta)^{a_2} + u(x-\zeta)^{k_1}V_1(x) + u^2(x-\zeta)^{k_2}V_2(x)\rangle$, *where either $a_2 = p^s - 1$ and $\mathcal{C}_1 = \{0\}$ or $a_2 = 1$ and $\mathcal{C}_1 = \langle 1\rangle = \mathcal{K}_1$ with $\max\{0, 2a_2 - p^s\} \leq k_1 < a_2$ if $V_1(x) \neq 0$, $0 \leq k_2 < a_2$ if $V_2(x) \neq 0$, $V_1(x)$ is either 0 or a unit in $\mathcal{K}_2$ of the form $\sum_{k=0}^{a_1-t_1-1} C_k(x-\zeta)^k$ and $V_2(x)$ is either 0 or a unit in $\mathcal{K}_2$ of the form $\sum_{\ell=0}^{a_2-k_2-1} Q_\ell(x-\zeta)^\ell$ with $C_k, Q_\ell \in \mathbb{F}_{p^m}$ for each relevant k and ℓ, satisfying the following:*

$$u^2(x-\zeta)^{p^s - a_2 + k_2}V_2(x) - u^2(x-\zeta)^{p^s - 2a_2 + 2k_1} V_1(x)^2 \in \langle u^2(x-\zeta)^{a_2}\rangle.$$

Proof: To prove the result, let $\mathcal{C}$ be a non-zero $(\alpha + \beta u + \gamma u^2)$-constacyclic code of length $2p^s$ over $\mathcal{R}$ with $\text{Tor}_0(\mathcal{C}) = \langle (x+\zeta)^{a_1}(x-\zeta)^{a_2}\rangle$, $\text{Tor}_1(\mathcal{C}) = \langle (x+\zeta)^{b_1}(x-\zeta)^{b_2}\rangle$ and $\text{Tor}_2(\mathcal{C}) = \langle (x+\zeta)^{c_1}(x-\zeta)^{c_2}\rangle$ for some integers $a_1, b_1, c_1, a_2, b_2, c_2$ satisfying $0 \leq c_1 \leq b_1 \leq a_1 \leq p^s$ and $0 \leq c_2 \leq b_2 \leq a_2 \leq p^s$. Then by (14), we have $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$, where $\mathcal{C}_j$ is an ideal of $\mathcal{K}_j$ for $j \in \{1, 2\}$. Further, by applying Proposition 31 and the Chinese Remainder Theorem, we have $\text{Tor}_0(\mathcal{C}_1) = \langle (x+\zeta)^{a_1}\rangle$, $\text{Tor}_0(\mathcal{C}_2) = \langle (x-\zeta)^{a_2}\rangle$, $\text{Tor}_1(\mathcal{C}_1) = \langle (x+\zeta)^{b_1}\rangle$, $\text{Tor}_1(\mathcal{C}_2) = \langle (x-\zeta)^{b_2}\rangle$, $\text{Tor}_2(\mathcal{C}_1) = \langle (x+\zeta)^{c_1}\rangle$ and $\text{Tor}_2(\mathcal{C}_2) = \langle (x-\zeta)^{c_2}\rangle$.

By Theorem 34, we see that the code $\mathcal{C}$ is MDS with respect to the Hamming metric if and only if $a_1 = b_1 = c_1$, $a_2 = b_2 = c_2$ and $\text{Tor}_2(\mathcal{C})$ is an MDS α-constacyclic code of length $2p^s$ over $\mathbb{F}_{p^m}$ with respect to the Hamming metric. Now we shall distinguish the following two cases: (i) $\beta \neq 0$ and (ii) $\beta = 0$.

(i) First let $\beta \neq 0$. Here by Lemma 10(b), we note that $\langle (x+\zeta)^{p^s}\rangle = \langle u\rangle$ in $\mathcal{K}_1$ and $\langle (x-\zeta)^{p^s}\rangle = \langle u\rangle$ in $\mathcal{K}_2$. This implies that when $1 \leq a_1, a_2 \leq p^s - 1$, we have $u \in \mathcal{C}_1$ and $u \in \mathcal{C}_2$, which implies that $b_1 = c_1 = 0$ and $b_2 = c_2 = 0$. In view of this and by applying Theorems 34 and 5, we observe that the code $\mathcal{C}$ is MDS if and only if $a_1 = b_1 = c_1 = 0$ and $a_2 = b_2 = c_2 = 0$. So the code $\mathcal{C} = \langle 1\rangle$ is the only MDS $(\alpha + \beta u + \gamma u^2)$-constacyclic code of length $2p^s$ over $\mathcal{R}$ with respect to the Hamming metric.

(ii) Next let $\beta = 0$. Here we see that $(x+\zeta)^{p^s}(2\zeta^{p^s})^{-1} - (x-\zeta)^{p^s}(2\zeta^{p^s})^{-1} = 1$, which gives

$$x^{2p^s} - \alpha - \gamma u^2 = \Big((x+\zeta)^{p^s} + u^2\gamma(2\zeta^{p^s})^{-1}\Big) \times \Big((x-\zeta)^{p^s} - u^2\gamma(2\zeta^{p^s})^{-1}\Big).$$

From this, we have $g_1(x) = g_2(x) = 0$, $h_1(x) = \gamma(2\zeta^{p^s})^{-1}$ and $h_2(x) = -\gamma(2\zeta^{p^s})^{-1}$. Now we proceed to determine all MDS codes in this case.

To do this, by Theorems 34 and 5, we observe that the code $\mathcal{C}$ is an MDS code if and only if exactly one of the following conditions is satisfied:

- $a_1 = b_1 = c_1 = p^s - 1$ and $a_2 = b_2 = c_2 = p^s$.
- $a_1 = b_1 = c_1 = p^s$ and $a_2 = b_2 = c_2 = p^s - 1$;
- $a_1 = b_1 = c_1 = 1$ and $a_2 = b_2 = c_2 = 0$;
- $a_1 = b_1 = c_1 = 0$ and $a_2 = b_2 = c_2 = 1$; and
- $a_1 = b_1 = c_1 = a_2 = b_2 = c_2 = 0$.

Let us first consider the case $a_1 = b_1 = c_1 = p^s - 1$ and $a_2 = b_2 = c_2 = p^s$. In this case, we must have $\mathcal{C}_2 = \{0\}$. As $a_1 = b_1 = c_1$, by Theorems 16 and 18, we observe that the code $\mathcal{C}_1$ must be of Type III. So we have $\mathcal{C} = \langle (x+\zeta)^{a_1} + u(x+\zeta)^{t_1}D_1(x) + u^2(x+\zeta)^{t_2}D_2(x), u(x+\zeta)^{a_1} + u^2(x+\zeta)^{\theta}V(x), u^2(x+\zeta)^{a_1}\rangle$, where $\max\{0, 2a_1 - p^s\} \leq t_1 < a_1$ if $D_1(x) \neq 0$, $0 \leq t_2 < a_1$ if $D_2(x) \neq 0$, $\max\{0, 2a_1 - p^s\} \leq \theta < a_1$ if $V(x) \neq 0$, $D_1(x)$ is either 0 or a unit in $\mathcal{K}_1$ of the form $\sum\limits_{k=0}^{a_1-t_1-1} C_k(x+\zeta)^k$, $D_2(x)$ is either 0 or a unit in $\mathcal{K}_1$ of the form $\sum\limits_{\ell=0}^{a_1-t_2-1} Q_\ell(x+\zeta)^\ell$ and $V(x)$ is either 0 or a unit in $\mathcal{K}_1$ of the form $\sum\limits_{i=0}^{a_1-\theta-1} W_i(x+\zeta)^i$ with $C_k, Q_\ell, W_i \in \mathbb{F}_{p^m}$ for each relevant k, ℓ and i. Furthermore, by Theorems 16 and 18 again, we see that

$$u^2\{\gamma(2\zeta^{p^s})^{-1} + (x+\zeta)^{p^s-2a_1+t_1+\theta}V(x)D_1(x) - (x+\zeta)^{p^s-a_1+t_2}D_2(x)\} \in \langle u^2(x+\zeta)^{a_1}\rangle. \quad (15)$$

We also note that $u^2\{(x+\zeta)^{t_1}D_1(x) - (x+\zeta)^{\theta}V(x)\} \in \langle u^2(x+\zeta)^{a_1}\rangle$, which implies that $t_1 = \theta$ and $D_1(x) = V(x)$. From this and by (15), we get

$$u^2\{\gamma(2\zeta^{p^s})^{-1} + (x+\zeta)^{p^s-2a+2t_1}D_1(x)^2 - (x+\zeta)^{p^s-a+t_2}D_2(x)\} \in \langle u^2(x+\zeta)^{a_1}\rangle.$$

This holds if and only if $t_1 = 0$, $p = 2$, $a = 2^{s-1}$ and $D_1(x) \neq 0$ in the case when $\gamma \neq 0$. Hence we get a contradiction in this case when γ is non-zero.

Working in a similar manner as above in the remaining four cases, the desired result follows immediately. □

VI. CONCLUSION AND FUTURE WORK

Let p be a prime, n, s, m be positive integers with $\gcd(n, p) = 1$, $\mathbb{F}_{p^m}$ 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 $\alpha, \beta, \gamma \in \mathbb{F}_{p^m}$ and $\alpha \neq 0$. When α is an nth power of an element in $\mathbb{F}_{p^m}$ and $\beta \neq 0$, one can determine all $(\alpha + \beta u + \gamma u^2)$-constacyclic codes of length np^s over $\mathcal{R}$ by applying the results derived in Cao [7] and by establishing a ring isomorphism from $\mathcal{R}[x]/\langle x^{np^s} - 1 - \alpha^{-1}\beta u - \alpha^{-1}\gamma u^2\rangle$ onto $\mathcal{R}[x]/\langle x^{np^s} - \alpha - \beta u - \gamma u^2\rangle$. However, when α is not an nth power of an element in $\mathbb{F}_{p^m}$, algebraic structures of all $(\alpha + \beta u + \gamma u^2)$-constacyclic codes of length np^s over $\mathcal{R}$ 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 $\mathcal{R}$ and their dual codes. We also listed some isodual $(\alpha + \beta u + \gamma u^2)$-constacyclic codes of length np^s over $\mathcal{R}$ when the binomial $x^n - \alpha_0$ is irreducible over $\mathbb{F}_{p^m}$. We also obtained Hamming distances, RT distances and RT weight distributions of all $(\alpha + \beta u + \gamma u^2)$-constacyclic codes of length np^s over $\mathcal{R}$ and determined all MDS $(\alpha + \beta u + \gamma u^2)$-constacyclic codes of length np^s over $\mathcal{R}$ with respect to the Hamming and RT metrics when the binomial $x^n - \alpha_0$ is irreducible over $\mathbb{F}_{p^m}$. Besides this, we obtained Hamming distances of all constacyclic codes of length $2p^s$ over $\mathcal{R}$ and identified all MDS codes within this class of constacyclic codes with respect to the Hamming metric.

It would be interesting to determine their Hamming distances, RT distances and RT weight distributions in the case when $n \geq 3$ and the binomial $x^n - \alpha_0$ is reducible over $\mathbb{F}_{p^m}$. 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.*, vol. 30, no. 2, pp. 277–285, Jul. 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.*, vol. 73, no. 1, pp. 13–42, Dec. 2003.

[3] A. Batoul, K. Guenda, and T. Aaron Gulliver, "Some constacyclic codes over finite chain rings," 2012, *arXiv:1212.3704*. [Online]. Available: http://arxiv.org/abs/1212.3704

[4] E. R. Berlekamp, *Algebraic Coding Theory*. New York, NY, USA: McGraw-Hill, 1968.

[5] A. Bonnecaze and P. Udaya, "Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1250–1255, May 1999.

[6] A. R. Calderbank, A. R. Hammons, P. V. Kumar, N. J. A. Sloane, and P. Solé, "A linear construction for certain Kerdock and Preparata codes," *Bull. Amer. Math. Soc.*, vol. 29, no. 2, pp. 218–222, 1993.

[7] Y. Cao, "On constacyclic codes over finite chain rings," *Finite Fields Their Appl.*, vol. 24, pp. 124–135, Nov. 2013.

[8] Y. Cao, Y. Cao, H. Q. Dinh, F.-W. Fu, J. Gao, and S. Sriboonchitta, "Constacyclic codes of length np^s over $\mathbb{F}_p^m + u\mathbb{F}_p^m$," *Adv. Math. Commun.*, vol. 12, no. 2, pp. 231–262, May 2018.

[9] Y. Cao, Y. Cao, H. Q. Dinh, F.-W. Fu, Y. Gao, and S. Sriboonchitta, "Type 2 constacyclic codes over $\mathbb{F}_2^m/\langle u^3\rangle$ of oddly even length," *Discrete Math.*, vol. 342, no. 2, pp. 412–426, Feb. 2019.

[10] Y. Cao, Y. Cao, H. Q. Dinh, F.-W. Fu, J. Gao, and S. Sriboonchitta, "A class of repeated-root constacyclic codes over $\mathbb{F}_p^m/\langle u^e\rangle$ of Type 2," *Finite Fields Appl.*, vol. 55, no. 1, pp. 238–267, Jan. 2019.

[11] Y. Cao, Y. Cao, and L. Dong, "Complete classification of $(\delta + \alpha u^2)$-constacyclic codes over $\mathbb{F}_3^m/\langle u^4\rangle$ of length $3n$," *Appl. Algebra Engrg. Commun. Comput.*, vol. 29, no. 1, pp. 13–39, Jan. 2018.

[12] Y. Cao, Y. Cao, and J. Gao, "On a class of $(\delta + \alpha u^2)$-constacyclic codes over $\mathbb{F}_q/\langle u^4\rangle$," *IEICE Trans. Fundamentals*, vol. 99, no. 7, pp. 1438–1445, Jul. 2016.

[13] Y. Cao, Y. Cao, and F. Ma, "Complete classification of $(\delta + \alpha u^2)$-constacyclic codes over $\mathbb{F}_2^m/\langle u^4\rangle$ of length $2n$," *Discrete Math.*, vol. 340, no. 12, pp. 2840–2852, Dec. 2017.

[14] B. Chen, H. Q. Dinh, H. Liu, and L. Wang, "Constacyclic codes of length p^s over $F^{p^m} + uF^{p^m}$," *Finite Fields Appl.*, vol. 37, pp. 108–130, Jan. 2016.

[15] H. Q. Dinh, "Constacyclic codes of length p^s over $\mathbb{F}_p^m + u\mathbb{F}_p^m$," *J. Algebra*, vol. 324, no. 5, pp. 940–950, 2010.

[16] 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.*, vol. 31, pp. 178–201, Jan. 2015.

[17] H. Q. Dinh and S. R. Lopez-Permouth, "Cyclic and negacyclic codes over finite chain rings," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1728–1744, Aug. 2004.

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

[19] S. T. Dougherty and K. Shiromoto, "Maximum distance codes over rings of order 4," *IEEE Trans. Inf. Theory*, vol. 47, no. 1, pp. 400–404, Jan. 2001.

[20] S. T. Dougherty and M. M. Skriganov, "Maximum distance separable codes in the ρ metric over arbitrary alphabets," *J. Algebr. Combinatorics*, vol. 16, no. 1, pp. 71–81, 2002.

[21] 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. Inf. Theory*, vol. 40, no. 2, pp. 301–319, Mar. 1994.

[22] 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.*, vol. 13, no. 3, pp. 681–712, Jul. 2007.

[23] J. Y. Hyun and H. K. Kim, "Maximum distance separable poset codes," *Designs, Codes Cryptogr.*, vol. 48, no. 3, pp. 247–261, Sep. 2008.

[24] X. Li and Q. Yue, "On the Hamming distances of repeated-root cyclic codes of length $5p^s$," 2019, *arXiv:1911.07542*. [Online]. Available: http://arxiv.org/abs/1911.07542

[25] 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. Scientia*, vol. 34, no. 3, pp. 829–839, May 2014.

[26] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[27] S. R. López-Permouth, H. Özadam, F. Özbudak, and S. Szabo, "Polycyclic codes over galois rings with applications to repeated-root constacyclic codes," *Finite Fields Their Appl.*, vol. 19, no. 1, pp. 16–38, Jan. 2013.

[28] A. A. Nechaev, "Kerdock code in a cyclic form," *Discrete Math. Appl.*, vol. 1, no. 4, pp. 365–384, 1991.

[29] G. H. Norton and A. Salagean, "On the Hamming distance of linear codes over a finite chain ring," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 1060–1067, May 2000.

[30] M. Y. Rosenbloom and M. A. Tsfasman, "Codes for the m-metric," *Problems Inform. Transmiss.*, vol. 33, no. 1, pp. 45–52, 1997.

[31] R. C. Singleton, "Maximum distance q-ary codes," *IEEE Trans. Inf. Theory*, vol. IT-10, no. 8, pp. 116–118, May 1964.

[32] A. Sharma, "Repeated-root constacyclic codes of length $l^t p^s$ and their dual codes," *Cryptogr. Commun.*, vol. 7, no. 2, pp. 229–255, 2015.

[33] A. Sharma and S. Rani, "Repeated-root constacyclic codes of length $4l^m p^n$," *Finite Fields Appl.*, vol. 40, pp. 163–200, Jul. 2016.

[34] A. Sharma and T. Sidana, "Repeated-root constacyclic codes of arbitrary lengths over the galois ring GR(p^2,m)," *Discrete Math., Algorithms Appl.*, vol. 10, no. 3, Jun. 2018, Art. no. 1850036, doi: 10.1142/S1793830918500362.

[35] R. Sobhani, "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 Appl.*, vol. 34, pp. 123–138, Jul. 2015.

[36] P. Udaya and A. Bonnecaze, "Decoding of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 2148–2157, Sep. 1999.

[37] Y. Wu and Q. Yue, "Factorizations of binomial polynomials and enumerations of LCD and self-dual constacyclic codes," *IEEE Trans. Inf. Theory*, vol. 65, no. 3, pp. 1740–1751, Mar. 2019.

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

[39] S. Zhu, X. Kai, and P. Li, "Negacyclic MDS codes over $GR(2^a, m)$," in *Proc. IEEE Int. Symp. Inform. Theory*, Jul. 2009, pp. 1730–1733.

TANIA SIDANA received the M.Sc. degree in mathematics from the Centre for Advanced Study in Mathematics, Panjab University, Chandigarh, India, in 2015. She is currently pursuing the Ph.D. degree with the Department of Mathematics, Indraprastha Institute of Information Technology, Delhi (IIIT-Delhi), New Delhi, India. Her research interests include coding theory, number theory, and group algebras.

ANURADHA SHARMA received the B.Sc. degree (Hons.) in mathematics and the M.Sc. and Ph.D. degrees in mathematics from the Centre for Advanced Study in Mathematics, Panjab University, Chandigarh, India, in 2000, 2002, and 2006, respectively. She is currently an Associate Professor with the Department of Mathematics, Indraprastha Institute of Information Technology, Delhi (IIIT-Delhi), New Delhi, India. Prior to joining IIIT-Delhi, she has worked as an Assistant Professor with the Department of Mathematics, IIT Delhi, for around five and a half years and an Assistant Professor with the Centre for Advanced Study in Mathematics, Panjab University, for around three years. She is also working in algebraic coding theory. Her other research interests include number theory and algebra. At IIT Delhi, she received the Kusuma Outstanding Young Faculty Fellowship. She was awarded the University Gold Medal for standing first in M.Sc.